FireEye, Inc.
Form 424B4
March 07, 2014
Table of Contents

Filed Pursuant to Rule 424(b)(4)
Registration No. 333-193717

PROSPECTUS

14,000,000 Shares

COMMON STOCK

FireEye, Inc. is offering 5,582,215 shares of its common stock. Certain stockholders of FireEye, Inc. identified in this prospectus are offering an additional 8,417,785 shares. We will not receive any of the proceeds from the sale of the shares being sold by the selling stockholders.

Our common stock is listed on The NASDAQ Global Select Market under the symbol FEYE. On March 6, 2014, the last reported sale price of our common stock on The NASDAQ Global Select Market was $89.55 per share.

We are an emerging growth company under the U.S. federal securities laws and are subject to reduced public company reporting requirements. Investing in our common stock involves risks. See Risk Factors beginning on page 15.

PRICE $82.00 A SHARE

	Price to Public	Underwriting Discounts and Commissions[1]	Proceeds to FireEye	Proceeds to Selling Stockholders
Per Share	*$82.00*	*$2.46*	*$79.54*	*$79.54*
Total	*$1,148,000,000*	*$34,440,000*	*$444,009,381*	*$669,550,619*

(1) See Underwriters beginning on page 175 for additional information regarding underwriting compensation.

The underwriters have the option to purchase up to 2,100,000 additional shares from us at the public offering price less the underwriting discount.

The Securities and Exchange Commission and any state securities regulators have not approved or disapproved of these securities, or determined if this prospectus is truthful or complete. Any representation to the contrary is a criminal offense.

The underwriters expect to deliver the shares of common stock to purchasers on March 12, 2014.

MORGAN STANLEY BARCLAYS J.P. MORGAN GOLDMAN, SACHS & CO.
UBS INVESTMENT BANK DEUTSCHE BANK SECURITIES CITIGROUP
PACIFIC CREST SECURITIES NOMURA

March 6, 2014

Table of Contents

Table of Contents

Table of Contents

TABLE OF CONTENTS

You should rely only on the information contained in this prospectus or contained in any free writing prospectus filed with the Securities and Exchange Commission. Neither we, the selling stockholders nor any of the underwriters have authorized anyone to provide any information or make any representations other than those contained in this prospectus or in any free writing prospectus filed with the Securities and Exchange Commission. We take no responsibility for, and can provide no assurance as to the reliability of, any other information that others may give you. We are offering to sell, and seeking offers to buy, shares of common stock only in jurisdictions where offers and sales are permitted. The information contained in this prospectus is accurate only as of the date of this prospectus, regardless of the time of delivery of this prospectus or of any sale of the common stock. Our business, financial condition, results of operations and prospects may have changed since such date.

For investors outside of the United States: Neither we, the selling stockholders nor any of the underwriters have done anything that would permit this offering or possession or distribution of this prospectus in any jurisdiction where action for that purpose is required, other than in the United States. You are required to inform yourselves about, and to observe any restrictions relating to, this offering and the distribution of this prospectus outside of the United States.

Table of Contents

PROSPECTUS SUMMARY

This summary highlights information contained elsewhere in this prospectus. This summary is not complete and does not contain all of the information you should consider in making your investment decision. You should read the following summary together with the more detailed information appearing elsewhere in this prospectus, including Risk Factors, Management s Discussion and Analysis of Financial Condition and Results of Operations and our consolidated financial statements and related notes before deciding whether to purchase shares of our common stock.

FIREEYE, INC.

Overview

We provide a comprehensive solution of products and services for detecting, preventing and resolving advanced cybersecurity threats. We have invented a purpose-built, virtual machine-based security platform that provides real-time protection to enterprises and governments worldwide that are facing the next generation of cyber attacks. Our technology approach represents a paradigm shift from how IT security has been conducted since the earliest days of the information technology industry. The core of our purpose-built, virtual machine-based security platform is our virtual execution, or MVX, engine, which identifies and protects against known and unknown threats that existing signature-based technologies are unable to detect. The new generation of cyber attacks on organizations, including large and small enterprises and governments worldwide, is characterized by an unprecedented escalation in the complexity and scale of advanced malware created by criminal organizations and nation-states. These highly sophisticated cyber attacks routinely circumvent traditional signature-based defenses by launching dynamic, stealthy and targeted malware that penetrates defenses in multiple stages and through multiple entry points of an IT network. Our proprietary virtual machine-based technology represents a new approach to detecting these cyber attacks in real time with high efficacy while also scaling in response to ever-increasing network performance requirements. We believe it is imperative for organizations to invest in this new approach to security to protect their critical assets, such as intellectual property and customer and financial data, from the global pandemic of cybercrime, cyber espionage and cyber warfare.

Our over ten years of research and development in proprietary virtual machine technology, anomaly detection and associated heuristic, or experience-based, algorithms enables us to provide real-time, dynamic threat protection without the use of signatures while delivering high efficacy and network performance. We provide a comprehensive platform that employs a virtualized execution engine and a cloud-based threat intelligence network that uniquely protects organizations from next-generation threats at all stages of the attack lifecycle and across all primary threat vectors, including Web, email, file and mobile. Our MVX engine detonates, or runs, Web objects, suspicious attachments and files within purpose-built virtual machine environments to detect and block the full array of next-generation threats, including attacks that leverage unknown vulnerabilities in widely used software programs, also known as zero-day attacks. Newly identified threats are quarantined to prevent exposure to the organization s actual network environment, and information regarding such threats is sent to our Dynamic Threat Intelligence, or DTI, cloud. Our DTI cloud enables real-time global sharing of threat intelligence uploaded by our customers cloud-connected FireEye appliances. In over 95% of our prospective customer evaluations, we have discovered incidents of next-generation threats that were conducting malicious activities and that successfully evaded the prospective customers existing security infrastructure, including traditional firewalls, next-generation firewalls, intrusion prevention systems, anti-virus software, email security and Web filtering appliances. By deploying our platform, organizations can stop inbound attacks and outbound theft of valuable intellectual property and data with a negligible false-positive rate, enabling them to avoid potentially catastrophic financial and intellectual property losses, reputational harm and damage to critical infrastructures.

1

Table of Contents

In December 2013, we acquired privately held Mandiant Corporation, or Mandiant, the leading provider of advanced endpoint security incident response management solutions. FireEye and Mandiant have been strategic partners with integrated product offerings since April 2012. We believe the combination of the two companies deepens this partnership and creates the industry s leading advanced threat protection vendor with the ability to find and stop attacks at every stage of the attack life cycle. The combination of our industry leading security products and threat intelligence with products and services from Mandiant enables us to provide a complete solution for detecting, preventing and resolving advanced cybersecurity threats.

Our platform is delivered through a family of software-based appliances and includes our cloud subscription services as well as support and maintenance services. Our principal threat prevention appliance families address four critical vectors of attack: Web, email, file and mobile. We also provide a family of threat prevention appliances that enable rapid identification and remediation of attacks that have penetrated and are residing on an organization s endpoints, such as desktop computers, laptops, or mobile devices. Our management appliances serve as a central nervous system unifying reporting and configuration, while monitoring and correlating attacks that simultaneously cross multiple vectors of the network, thereby increasing the efficacy of our security platform. Our management appliances enable us to share intelligence regarding threats at a local implementation level and also across the organization. In addition, we enhance the efficacy of our solution by sharing with customers anonymized global threat data through our DTI cloud. We also offer a forensic analysis appliance that provides IT security analysts with the ability to test, characterize and conduct forensic examinations on next-generation cyber attacks by simulating their execution path with our virtual machine technology. Our cloud-based mobile threat prevention platform identifies and stops mobile threats by analyzing mobile applications within our MVX engine. Finally, we offer incident response and managed services to assist our customers who have been breached as part of our full service solution to combat advanced threats.

Our sales model consists of a direct sales team and channel partners that collaborate to identify new sales prospects, sell products and services, and provide post-sale support. We believe this approach allows us to maintain face-to-face connectivity with our customers, including key enterprise accounts, and helps us support our partners, while leveraging their reach and capabilities. Further, we believe our leading incident response capabilities position us as a trusted advisor to our customers and offer us the opportunity to help customers prevent future breaches through the use of our products and services. As of December 31, 2013, including customers of Mandiant, we had over 1,900 end-customers across more than 60 countries, including over 130 of the Fortune 500. Our customers include leading enterprises in a diverse set of industries, including telecommunications, technology, financial services, public utilities, healthcare and oil and gas, as well as leading U.S. and international governmental agencies.

For 2011, 2012 and 2013, our revenue was $33.7 million, $83.3 million and $161.6 million, respectively, representing year-over-year growth of 186% for 2011, 148% for 2012 and 94% for 2013, and our net losses were $16.8 million, $35.8 million and $120.6 million, respectively. Subscription and services revenue has increased as a percentage of revenue over the last three years, from 26% in 2011 to 37% in 2012 and to 45% in 2013, while our product revenue has decreased as a percentage of revenue, from 74% in 2011 to 63% in 2012 and to 55% in 2013. The increase in subscription and services revenue as a percentage of total revenue is primarily due to the growth of our installed base in conjunction with the increase in product sales and renewals of the related subscription and services from existing customers.

Industry Background

Organizations Are Spending Billions On Legacy Signature-Based Security Technologies

Organizations today are embracing a confluence of technologies to enhance the productivity of their employees, generate new revenue sources and improve their operating efficiency. These technologies include

cloud services, mobile computing and online services and social networking sites, such as LinkedIn, Facebook and Twitter. This greater reliance on information technology has significantly increased the attack surface within these organizations that is vulnerable to potential security attacks and has resulted in significant investments in IT security to help protect against a myriad of potential threats. According to IDC, a global market research firm, 2013 worldwide IT security spending was approximately $16.8 billion, including investments in traditional security technologies such as firewalls, virtual private networking, Web security, unified threat management, intrusion detection and prevention, messaging security and corporate endpoint security.[1]

To date, organizations have deployed IT security products to defend against earlier generations of security threats by utilizing legacy signature-based threat protection technology. The signature model works by forensically examining the code base of known malware and, if no match is found, subsequently developing a signature that network security devices can match against future incoming traffic. These signatures are gathered by IT security companies and distributed periodically to organizations that subscribe to the company s update service. This signature-based approach is the principal foundation of existing IT threat protection technologies.

The Threat Landscape Has Evolved: Organizations Face A New Generation Of Threat Actors

The historical threat landscape was defined by amateur hackers who launched attacks principally for fame or mischief. While these hackers garnered a lot of press, they caused relatively little damage, and signature-based security solutions were effective at detecting and preventing them. Today s organizations face an advanced malware pandemic of unprecedented severity led by advanced persistent threat actors, such as cyber-criminal organizations, nation-states and hacktivists, who are utilizing highly sophisticated next-generation threats to circumvent traditional IT defenses at an alarming rate. Cybercriminals are expending significant resources to exfiltrate sensitive intellectual property and personal data, causing financial and reputational damage; nation-states are pursuing cyber espionage and warfare targeting critical infrastructure, such as power grids and highly sensitive information that can threaten national security; and hacktivists, who are ideologically driven, are defacing Websites, stealing information and launching denial of service attacks.

Next-Generation Threats Exhibit A Unique Set Of Challenges

Next-generation threats, utilized by advanced persistent threat actors, are fundamentally different from earlier generation threats, with a unique set of characteristics that create a new set of detection and prevention challenges. One of the most dangerous characteristics of next-generation threats is their ability to take advantage of a previously unknown vulnerability in widely used software programs, creating what is known as zero day threats. By exploiting this vulnerability, significant damage can be done because it can take days before signature-based software vendors discover the vulnerability and patch it, and an even longer period of time for traditional security products to update their signature databases accordingly. Next-generation threats are stealthy by design and are significantly harder to detect. Further compounding the problem, next-generation threats are dynamic, or polymorphic, meaning they are designed to mutate quickly and retain their function while changing their code, making it almost impossible for traditional signature technologies that rely on pattern matching to detect them. These threats are also targeted, which enables them to present specific individuals within organizations networks with customized messages or content that maximizes the likelihood of the individual becoming an unwitting accomplice to the attack. Next-generation threats are also persistent and can perform malicious activity over a significantly longer period of time by remaining in the network and spreading undetected across devices for a specific period of time before conducting their activity, thereby resulting in higher damage potential. An additional level of complexity created by these threats is that they can target all primary entry points of a network by launching advanced malware attacks at the organization through Web, email, file and mobile vectors. These attacks may also include blended attacks that target multiple vectors simultaneously to gain entry to an organization s IT environment.

1 See note (2) in Market and Industry Data.

Table of Contents

Next-generation threats are significantly more complex in the way they carry out their attacks. The threats formulate over multiple steps, and they are difficult to detect via legacy security technologies at each step. The typical next-generation attack lifecycle contains the following five steps:

1. *Initial Exploit:* An exploit is typically a small amount of seemingly harmless content, often just a few hundred bytes in size, that when inserted into vulnerable software can make the software execute code it was not programmed to run. The initial exploit phase is critical and occurs when cyber attackers take advantage of inherent vulnerabilities in widely used software and applications, such as Adobe Acrobat, Flash and Internet Explorer, to initially penetrate a victim system. The exploit is stealthy and its code can enter an organization even when a user does nothing more than visit a Web page that has been compromised. Importantly, this entire process happens within the compromised system s random access memory and does not involve writing any files to the hard drive, making it almost impossible to detect with legacy security solutions that are focused on examining files and executables once they are written to the hard drive on a host computer.

2. *Malware Download:* Once the initial exploit is successful in penetrating a victim s system, a larger malware program in the form of a file can be downloaded onto the hard drive of the compromised system. Because the download is initiated by seemingly innocuous software from inside the organization and the malware file can be obfuscated to seem harmless, legacy security systems cannot detect the threat. As an example, the file can be presented as a .jpg (a picture) instead of an .exe (executable) file and therefore avoid detection by legacy security technologies designed to look for executables. In addition, the malware program is encrypted and the key to decrypt the file is only available in the exploit code. Therefore, only if a security product detects the initial exploit code, can it collect the key to decrypt, detect and block the larger malware program.

3. *Callback and Establish Control:* After the larger malware download is successful, it will initiate an outbound connection to an external command and control server operated by a threat actor. Once the program has successfully made a connection, the cyber attacker has full control over the compromised host. Many legacy security solutions do not analyze outbound traffic for malicious transmissions and destinations. Other solutions that attempt to detect malicious outbound transmissions can only find transmissions to known destination IP addresses of servers, and are not able to identify malicious transmissions to unknown destinations.

4. *Data Exfiltration:* Having established a secure connection with the command and control server, the malware will proceed to take control of the host computer as well as transfer sensitive data, such as intellectual property, credit card information, user credentials, and sensitive file content. Because legacy security solutions cannot detect any of the previous three steps exploit, malware download and callback they are unable to detect and block the outbound transfer of data.

5. *Lateral Movement:* At any point after the malware is downloaded, the malware may conduct reconnaissance across the network to locate other vulnerable systems, and then spread laterally to file shares located deep within the organization s network to search for additional data that is valuable to exfiltrate. As the lateral movement is conducted within the enterprise, firewalls and other perimeter security solutions focused on blocking malicious traffic from entering an organization are not able to detect the movement of malware within the organization.

Existing Security Solutions Are Not Architected To Protect Against Next-Generation Threats

The evolving threat landscape has rendered traditional defenses incapable of protecting organizations against next-generation threats. This includes traditional and next-generation firewalls, which provide the ability to manage policies for network and application traffic but are not fundamentally designed to detect advanced cyber attacks in a granular and scalable fashion. In addition, although products like intrusion prevention systems,

4

Table of Contents

or IPS, anti-virus, or AV, whitelisting and Web filtering technologies were designed with the intent of detecting the full spectrum of cyber attacks, their signature-based approaches have left them increasingly unsuccessful in detecting and blocking next-generation threats.

Protecting Today s IT Infrastructure Requires A Fundamentally Different Approach To Security

A solution to protect against next-generation threats needs to be built from the ground up and have the following key capabilities:

- detection and protection capability that overcomes the limitations of signature-based approaches;
- the ability to protect the organization s infrastructure across multiple threat vectors;
- visibility into each stage of the attack life cycle and particularly the ability to detect and block attacks at the exploit phase;
- negligible false-positive rate, thereby allowing the organization s IT infrastructure to be secure without hindering business productivity;
- the ability to scan all relevant traffic without noticeable degradation of network performance;
- the ability to dynamically leverage knowledge gained by prior threat analysis;
- rapid deployment and streamlined management capabilities; and
- the ability to rapidly identify, contain and remediate breaches.

Our Solution

Our technology platform, built on our proprietary MVX engine, is able to identify and protect against known and unknown threats without relying on existing signature-based technologies employed by legacy IT security vendors and best-of-breed point solution vendors. To complement our threat prevention platform, our endpoint-based incident response technology platform enables rapid identification, containment and remediation of attacks on the network. We also provide a team of industry-leading experts in the security industry and managed services to help organizations respond faster to breaches and minimize the exposure to their businesses. The key benefits of our platform include:

- ***Proprietary MVX engine to enable dynamic, real-time protection against next-generation threats.*** Our virtual execution technology detonates Web objects and suspicious attachments within purpose-built virtual machine environments in order to detect and block the full array of next-generation threats. Our solution does not require a pre-existing signature of the threat to identify it.

Proactive defense from network to endpoint. Our broad product portfolio includes software-based appliances, cloud services and endpoint solutions to protect against Web and email threat vectors, malware resident on file shares, malicious mobile applications and targeted endpoints. We can also coordinate threat intelligence across all four vectors to further enhance our overall efficacy rates and protect against blended attacks.

Visibility of each stage of the attack life cycle and particularly the ability to detect and block attacks at the exploit phase. Our platform enables a comprehensive, stage-by-stage analysis of next-generation threats, from initial system exploitation to data exfiltration and lateral movement. Furthermore, because we can watch the execution path of the initial exploit with a high degree of granularity, we have high detection accuracy at the exploit level.

High efficacy next-generation threat detection. We can address hundreds of permutations of software versions targeted by advanced malware attacks by concurrently deploying thousands of virtual machines across an organization s network, allowing us to monitor attempted exploits of multiple

Table of Contents

operating system and application versions and hundreds of object types at line speed. This approach allows for high detection efficacy with negligible false-positive rates, resulting in minimal disruption to the business and IT organization.

Real-time detection of all network traffic with negligible performance degradation. Our high-performance virtual machine technology, working in concert with our DTI cloud and advanced heuristic algorithms, enables us to deliver industry-leading protection against next-generation threats. Our appliances are capable of operating in-line, providing comprehensive and highly accurate detection and protection without slowing down the network.

Global cloud-based data sharing within and across organizations. Our Central Management System, or CMS, correlates threat information generated by threat prevention appliances and facilitates rapid sharing of information across multiple appliances within a customer environment as well as across customer networks around the world. In addition, by sharing anonymous real-time global threat data through our DTI cloud, our customers have access to a system that leverages the network effects of a globally distributed, automated threat analysis network.

Rapid deployment and streamlined management capabilities. Our threat prevention appliances are easy to deploy with minimal modification to existing networks and seamlessly integrate with other devices in such networks. These appliances are generally deployed in a few hours and most often find existing next-generation threats immediately after deployment. Our CMS appliances offer rich management capabilities, such as coordinating software upgrades, automating the configuration of multiple appliances and presenting security data in an intuitive interface to facilitate reporting and auditing.

Tightly integrated incident response, managed services and contextual data. Our in-depth understanding of advanced threats and how they manifest themselves in a customer environment allows us to offer various high value-added security services that complement our product portfolio, including managed defense and incident response and remediation services.

Our Market Opportunity

According to IDC, worldwide IT security spending in 2013 was approximately $16.8 billion across firewalls, virtual private networking, Web security, unified threat management, intrusion detection and prevention, messaging security and corporate endpoint security.[2] While this spending is focused principally on traditional IT security products, we believe the rise in next-generation threats is creating significant new demand from organizations for products that offer advanced protection against this new threat paradigm. Gartner, Inc., a global market research firm, estimates that, By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2013.[3] We believe our platform is essential to protect these organizations against next-generation threats. As organizations seek new defenses against next-generation threats, we believe that our virtualization-based approach, which represents a paradigm shift from how IT security has been conducted in the past, will take an increasing share of IT security spending from the traditional enterprise IT security markets. Specifically, we believe this approach can be applied to initially supplement, and ultimately replace, any threat protection technology that utilizes a traditional signature-based approach. These markets consist of Web security ($2.1 billion), messaging security ($2.6 billion), intrusion detection and prevention ($1.9 billion) and corporate endpoint security ($3.7 billion), and aggregate to a total projected spending of $10.3 billion in 2013, in each case according to IDC.[2] We also provide solutions that address the IT security consulting industry, which was $6.2 billion in 2013, according to IDC.[2] With the acquisition of Mandiant, we have added solutions that address portions of the managed security services, or MSS,

2 See note (2) in Market and Industry Data.
3 See note (1) in Market and Industry Data.

market and the security incident and event management, or SIEM, market. In a recent report, Gartner estimated that the MSS Market will grow from US$12 billion in 2013 to more than US$22.5 billion in 2017.[4] Separately, Gartner has also estimated that SIEM spending would total approximately $1.6 billion in 2013.[4]

Our Competitive Strengths

We have developed the following key competitive advantages that we believe will allow us to maintain and extend our leadership position:

Leader in protecting organizations against the new breed of cyber attacks. We invented a purpose-built, virtual machine-based security solution that provides real-time protection against next-generation threats, and we believe we are a leader in the market.

Platform built from the ground up to address next-generation threats. We were founded with the sole purpose of developing a platform to defend and block next-generation threats. Therefore, we developed a proprietary hypervisor (i.e., software that creates and runs virtual machines) and MVX engine to meet the specific challenges associated with high throughput processing of next-generation threats. Our MVX engine is designed to be undetectable by these new threats. We can run hundreds of permutations of files, operating systems, software versions, languages and applications to mimic desktop operating environments and force malicious software to reveal itself. In addition, our platform is scalable and can run over 1,000 concurrent virtual execution tasks on a single appliance to simultaneously detect multiple threats.

Unique capabilities across threat detection, prevention and resolution. We offer a comprehensive solution for detecting, preventing and resolving advanced cybersecurity threats. The integration of detection and response provides a seamless solution that enables more rapid threat identification and resolution and lowers the cost of ownership for customers by reducing the number of products they would otherwise have to separately integrate. We believe we are the only vendor that offers an end-to-end solution for advanced threat protection and that we are uniquely positioned to take advantage of the broad applicability of our platform to meet all of our customers advanced threat protection needs.

Network effects from our customer base and DTI cloud. The combination of our global customer base of over 1,900 end-customers with our over two million virtual machines across customer environments provides us with rich and broad sets of dynamic threat protection data. We believe that by sharing this data with our global customer base, we are able to provide both a higher level of protection and higher performance. This relationship between customers and differentiated threat intelligence drives a network effect around our company, leading additional customers to be increasingly attracted to the depth and breadth of our capabilities and intelligence.

Strong management team with significant IT security expertise. We have a highly knowledgeable management team with extensive IT security expertise. Our team includes experts with a strong track record of developing the fundamental new technologies behind advanced malware detection.

Comprehensive platform that enables modular deployment options. Our customers typically initially deploy our solution to provide either Web, email, file or mobile protection and in conjunction with existing security solutions. Once deployed, our customers can then deploy additional appliances to protect the first threat vector, as well as expand their level of protection to additional vectors to achieve end-to-end protection for the primary vectors for next-generation threats to enter.

Significant technology lead. Our technology is recognized as innovative and is protected by, among other things, a combination of copyright, trademark and trade secret laws; confidentiality procedures and contractual provisions; and a patent portfolio including 16 issued and 78 pending U.S. patents.

4 See note (3) in Market and Industry Data.

Table of Contents

Our Strategy

Our objective is to be the global leader in virtual machine-based security solutions for the entire IT security market. The key elements of our growth strategy include:

Invest in research and development efforts to extend our technology leadership. We plan to build upon our current performance and current technology leadership to enhance our product capabilities, such as protecting new threat vectors and providing focused solutions for certain markets, such as small and medium-sized enterprises and service providers.

Expand our sales organization to acquire new customers. We intend to continue to invest in our sales organization around the globe as we pursue larger enterprise and government opportunities outside of the United States.

Expand our channel relationship and develop our partner ecosystem. We have established a distribution channel program that, as of December 31, 2013, had approximately 625 channel partners worldwide. We intend to continue adding distributors and resellers and incentivizing them to drive greater sales to enable us to further leverage our internal sales organization.

Drive greater penetration into our customer base. Typically, customers initially deploy our platform to protect a portion of their IT infrastructure against one type of security threat, such as Web-based threats. We see a significant opportunity to upsell and cross sell additional products, subscriptions and services as our customers realize the increasing value of our platform.

Leverage our innovative virtual machine technology in additional product markets. We intend to apply our purpose-built virtual machine security engine to any threat protection technology that utilizes a traditional signature-based approach, such as intrusion prevention and related mobile security markets.

Risks Associated With Our Business

Our business is subject to numerous risks and uncertainties, including those highlighted in the section entitled Risk Factors immediately following this prospectus summary. These risks include, among others, the following:

if the IT security market does not continue to adopt our virtual machine-based security platform, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations and financial condition would be harmed;

recent and future acquisitions and investments could disrupt our business and harm our financial condition and operating results;

our limited operating history makes it difficult to evaluate our current business and prospects and may increase the risk that we will not be successful;

if we do not effectively expand and train our direct sales force, we may be unable to add new customers or increase sales to our existing customers, and our business will be adversely affected;

if we fail to effectively manage our growth, our business, financial condition and results of operations would be harmed;

fluctuating economic conditions make it difficult to predict revenue for a particular period, and a shortfall in revenue may harm our operating results;

our results of operations are likely to vary significantly from period to period, which could cause the trading price of our common stock to decline; and

Table of Contents

our directors, executive officers and each of our stockholders who owns greater than 5% of our outstanding common stock, in the aggregate, will beneficially own approximately % of the outstanding shares of our common stock after the completion of this offering, which could limit your ability to influence the outcome of key transactions, including a change of control.

Corporate Information

Our principal executive offices are located at 1440 McCarthy Blvd., Milpitas, California 95035, and our telephone number is (408) 321-6300. Our Website address is www.fireeye.com. Information contained on, or that can be accessed through, our Website is not incorporated by reference into this prospectus, and you should not consider information on our Website to be part of this prospectus. We were incorporated in Delaware in February 2004 under the name NetForts, Inc., and changed our name to FireEye, Inc. in September 2005.

The mark FireEye, the FireEye design logo and other trademarks or service marks of FireEye appearing in this prospectus are the property of FireEye, Inc. This prospectus contains additional trade names, trademarks, and service marks of other companies, and such tradenames, trademarks and service marks are the property of their respective owners. We do not intend our use or display of other companies trade names, trademarks, or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

Emerging Growth Company

The Jumpstart Our Business Startups Act, or the JOBS Act, was enacted in April 2012 with the intention of encouraging capital formation in the United States and reducing the regulatory burden on newly public companies that qualify as emerging growth companies. We are an emerging growth company within the meaning of the JOBS Act. As an emerging growth company, we may take advantage of certain exemptions from various public reporting requirements, including the requirement that our internal control over financial reporting be audited by our independent registered public accounting firm pursuant to Section 404 of the Sarbanes-Oxley Act of 2002, certain requirements related to the disclosure of executive compensation in this prospectus and in our periodic reports and proxy statements, and the requirement that we hold a nonbinding advisory vote on executive compensation and any golden parachute payments. We may take advantage of these exemptions until we are no longer an emerging growth company.

We will remain an emerging growth company until the earliest to occur of (i) the last day of the fiscal year in which we have more than $1.0 billion in annual revenue; (ii) the date we qualify as a large accelerated filer, with at least $700 million of equity securities held by non-affiliates; (iii) the date on which we have issued, in any three-year period, more than $1.0 billion in non-convertible debt securities; and (iv) the last day of the fiscal year ending after the fifth anniversary of the completion of our initial public offering on September 25, 2013.

For certain risks related to our status as an emerging growth company, see *Risk Factors Risks Related to this Offering and Ownership of Our Common Stock We are an emerging growth company, and we cannot be certain if the reduced disclosure requirements applicable to emerging growth companies will make our common stock less attractive to investors*.

Table of Contents

THE OFFERING

Common stock offered by us	5,582,215 shares
Common stock offered by the selling stockholders	8,417,785 shares
Option to purchase additional shares being offered by us	2,100,000 shares
Common stock to be outstanding after this offering	144,136,573 shares (146,236,573 shares, if the underwriters exercise their option to purchase additional shares from us in full)
Use of proceeds	We estimate that the net proceeds from this offering will be approximately $442.1 million ($609.1 million, if the underwriters exercise their option to purchase additional shares from us in full), based on the public offering price of $82.00 per share, after deducting the underwriting discounts and commissions and estimated offering expenses payable by us. The principal purposes of this offering are to increase our capitalization and financial flexibility, obtain additional capital, facilitate an orderly distribution of shares for the selling stockholders in this offering and increase our public float. We intend to use the net proceeds we receive from this offering for general corporate purposes, including headcount expansion, working capital, sales and marketing activities, product development, general and administrative matters and capital expenditures. We also may use a portion of the net proceeds from this offering to acquire or invest in technologies, solutions or businesses that complement our business, although we have no present commitments to complete any such transactions at this time. We will not receive any proceeds from the sale of shares offered by the selling stockholders. See Use of Proceeds and Principal and Selling Stockholders.
NASDAQ symbol	FEYE

The number of shares of our common stock to be outstanding after this offering is based on 138,554,358 shares of our common stock outstanding as of December 31, 2013, after giving effect to the assumed issuance of 796,846 shares of common stock to be acquired by certain selling stockholders upon the exercise of outstanding stock options and the vesting of outstanding restricted stock units in order to sell such shares in this offering, and excludes:

- 26,657,087 shares of common stock issuable upon the exercise of stock options outstanding as of December 31, 2013, with a weighted-average exercise price of $5.49 per share;
- 605,100 shares of common stock issuable upon the exercise of stock options granted after December 31, 2013, with a weighted-average exercise price of $73.94 per share;
- 1,757,031 shares of common stock issuable upon the vesting of restricted stock units outstanding as of December 31, 2013;

Table of Contents

835,011 shares of common stock issuable upon the vesting of restricted stock units granted after December 31, 2013;

311,747 shares of common stock issuable upon the exercise of warrants outstanding as of December 31, 2013, with a weighted-average exercise price of $0.72 per share;

11,015,257 shares of common stock reserved for future grants as of December 31, 2013 under our 2013 Equity Incentive Plan (which reserve includes 1,440,111 shares of common stock issuable upon the exercise of stock options and the vesting of restricted stock units granted after December 31, 2013, as described in the bullets above), plus an additional 6,887,875 shares of common stock that became available for future grants under our 2013 Equity Incentive Plan as of January 1, 2014 pursuant to provisions thereof that automatically increase the share reserve under such plan each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans ;

2,500,000 shares of common stock reserved for future issuance as of December 31, 2013 under our 2013 Employee Stock Purchase Plan, plus an additional 1,377,575 shares of common stock that became available for future grants under our 2013 Employee Stock Purchase Plan as of January 1, 2014 pursuant to provisions thereof that automatically increase the share reserve under such plan each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans ; and

any shares of common stock that become available subsequent to this offering under our 2013 Equity Incentive Plan and 2013 Employee Stock Purchase Plan pursuant to provisions thereof that automatically increase the share reserves under such plans each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans.

Except for historical financial statements and as otherwise indicated, all information in this prospectus assumes:

the issuance of 764,089 shares of common stock to be sold by certain selling stockholders upon the exercise of vested stock options immediately prior to the closing of this offering, as if such issuance had occurred as of December 31, 2013;

the issuance of 32,757 shares of common stock to be sold by a certain selling stockholder upon the vesting of restricted stock units on the date of this prospectus, as if such issuance had occurred as of December 31, 2013;

no exercise of outstanding stock options or warrants subsequent to December 31, 2013, except for the stock option exercises described in the first bullet above;

no vesting of outstanding restricted stock units subsequent to December 31, 2013, except for the vesting of restricted stock units described in the second bullet above; and

no exercise of the underwriters option to purchase additional shares of common stock from us in this offering.

Table of Contents

SUMMARY CONSOLIDATED FINANCIAL DATA

The summary consolidated statements of operations data presented below for the years ended December 31, 2011, 2012 and 2013 are derived from audited consolidated financial statements included elsewhere in this prospectus. The following summary consolidated financial data should be read with Management s Discussion and Analysis of Financial Condition and Results of Operations and our consolidated financial statements and related notes included elsewhere in this prospectus. Our historical results are not necessarily indicative of the results that may be expected for the full fiscal year or any period in the future.

	Year Ended December 31,		
	2011	2012	2013
	(In thousands, except per share data)		
Consolidated Statements of Operations Data:			
Revenue:			
Product	$ 24,888	$ 52,265	$ 88,253
Subscription and services	8,770	31,051	73,299
Total revenue	33,658	83,316	161,552
Cost of revenue:			
Product[(1)]	5,690	14,467	28,912
Subscription and services	1,590	3,163	18,853
Total cost of revenue	7,280	17,630	47,765
Total gross profit	26,378	65,686	113,787
Operating expenses:			
Research and development[(1)]	7,275	16,522	66,036
Sales and marketing[(1)]	30,389	67,562	167,466
General and administrative[(1)]	4,428	15,221	52,503
Total operating expenses	42,092	99,305	286,005
Operating loss	(15,714)	(33,619)	(172,218)
Interest income	3	7	68
Interest expense	(194)	(537)	(525)
Other expense, net	(806)	(2,572)	(7,257)
Loss before income taxes	(16,711)	(36,721)	(179,932)
Provision for (benefit from) income taxes	71	(965)	(59,297)
Net loss attributable to common stockholders	$ (16,782)	$ (35,756)	$ (120,635)
Net loss per share attributable to common stockholders, basic and diluted	$ (1.99)	$ (3.28)	$ (2.66)
Weighted-average shares used to compute net loss per share attributable to common stockholders, basic and diluted	8,447	10,917	45,271

Table of Contents

(1) Includes stock-based compensation expense as follows:

	Year Ended December 31,		
	2011	2012	2013
	(In thousands)		
Stock-Based Compensation Expense:			
Cost of revenue	$ 39	$ 170	$ 2,810
Research and development	148	1,465	6,958
Sales and marketing	360	1,672	10,748
General and administrative	168	3,536	8,342
Total stock-based compensation expense	$ 715	$ 6,843	$ 28,858

Our consolidated balance sheet as of December 31, 2013 is presented on:

an actual basis;

a pro forma basis, giving effect to (i) the issuance and sale of 5,582,215 shares of common stock by us in this offering, based on the public offering price of $82.00 per share, after deducting underwriting discounts and commissions and estimated offering expenses payable by us, and (ii) the issuance of 796,846 shares of common stock to be acquired by certain selling stockholders upon the exercise of stock options or the vesting of restricted stock units in order to sell such shares in this offering.

	As of December 31, 2013	
	Actual	Pro Forma
	(in thousands)	
Consolidated Balance Sheet Data:		
Cash and cash equivalents	$ 173,918	$ 617,671
Working capital, excluding deferred revenue and costs	219,707	663,460
Total assets	1,376,313	1,820,066
Total deferred revenue	187,514	187,514
Total stockholders equity	1,048,102	1,491,855

Table of Contents

	Year Ended or as of December 31,		
	2011	2012	2013
	(Dollars in thousands)		
Key Business Metrics:			
Product revenue	$ 24,888	$ 52,265	$ 88,253
Subscription and services revenue	8,770	31,051	73,299
Total revenue	$ 33,658	$ 83,316	$ 161,552
Year-over-year percentage increase	186%	148%	94%
Gross margin percentage	78%	79%	70%
Deferred revenue, current portion at period end[(1)]	$ 16,215	$ 43,750	$ 110,535
Deferred revenue, non-current portion at period end	$ 13,887	$ 32,656	$ 76,979
Billings (non-GAAP)[(2)]	$ 57,494	$ 129,620	$ 256,561
Net cash provided by (used in) operating activities[(3)]	$ 5,111	$ 21,500	$ (69,762)
Free cash flow (non-GAAP)[(4)]	$ (106)	$ 2,652	$ (127,322)

(1) Our deferred revenue consists of amounts that have been invoiced but have not yet been recognized as revenue as of the period end. For the year ended December 31, 2013, deferred revenue includes the addition of $16.1 million of deferred revenue assumed in connection with the Mandiant acquisition. The majority of our deferred revenue balance consists of the unamortized portion of revenue from sales of our Email Threat Prevention product, subscriptions to our DTI cloud and Email Threat Prevention Attachment/URL Engine, and support and maintenance contracts. Because invoiced amounts for subscriptions and services can be for multiple years, we classify our deferred revenue as current or non-current depending on when we expect to recognize the related revenue. If the deferred revenue is expected to be recognized within 12 months, it is classified as current. Otherwise, the deferred revenue is classified as non-current. We monitor our deferred revenue balance because it represents a significant portion of revenue to be recognized in future periods.

(2) We define billings as revenue recognized plus the change in deferred revenue from the beginning to the end of the period. For the year ended December 31, 2013, billings exclude the addition of $16.1 million of deferred revenue assumed in connection with the Mandiant acquisition. We consider billings to be a useful metric for management and investors because billings drives deferred revenue, which is an important indicator of the health and visibility of our business and represents a significant percentage of our revenue. See Management s Discussion and Analysis of Financial Condition and Results of Operations Key Business Metrics for more information and a reconciliation of billings to revenue, the most directly comparable financial measure calculated and presented in accordance with U.S. generally accepted accounting principles, or GAAP.

(3) We monitor cash flow provided by (used in) operating activities as a measure of our overall business performance. Our cash flow provided by (used in) operating activities is driven in large part by sales of our products and from up-front payments for both new and renewal contracts for subscription and support and maintenance. Monitoring cash flow provided by (used in) operating activities enables us to analyze our financial performance without the non-cash effects of certain items such as depreciation, amortization, and stock-based compensation costs, thereby allowing us to better understand and manage the cash needs of our business.

(4) We define free cash flow as net cash provided by operating activities less purchases of property and equipment and demonstration units. We consider free cash flow to be a liquidity measure that provides useful information to management and investors about the amount of cash generated by the business that, after the purchases of property and equipment and demonstration units, can be used for strategic opportunities, including investing in our business, making strategic acquisitions, and strengthening the balance sheet. See Management s Discussion and Analysis of Financial Condition and Results of Operations Key Business Metrics for more information and a reconciliation of free cash flow to cash flow provided by (used in) operating activities, the most directly comparable financial measure calculated and presented in accordance with GAAP.

Table of Contents

RISK FACTORS

Investing in our common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, together with all of the other information in this prospectus, including our consolidated financial statements and related notes, before investing in our common stock. If any of the following risks are realized, in whole or in part, our business, financial condition, results of operations and prospects could be materially and adversely affected. In that event, the price of our common stock could decline, and you could lose part or all of your investment.

Risks Related to Our Business and Our Industry

If the IT security market does not continue to adopt our virtual machine-based security platform, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations and financial condition would be harmed.

We are seeking to disrupt the IT security market with our virtual machine-based security platform. Our platform interoperates with but does not replace most signature-based IT security products. Enterprises and governments that use signature-based security products, such as firewalls, intrusion prevention systems, or IPS, anti-virus, or AV, and Web and messaging gateways, for their IT security may be hesitant to purchase our virtual machine-based security platform if they believe that signature-based products are more cost effective, provide substantially the same functionality as our platform or provide a level of IT security that is sufficient to meet their needs. Currently, most enterprises and governments have not allocated a fixed portion of their budgets to protect against next-generation advanced cyber attacks. As a result, to expand our customer base, we need to convince potential customers to allocate a portion of their discretionary budgets to purchase our platform. However, even if we are successful in doing so, any future deterioration in general economic conditions may cause our customers to cut their overall IT spending, and such cuts may fall disproportionately on products and services like ours, for which no fixed budgetary allocation has been made. If we do not succeed in convincing customers that our platform should be an integral part of their overall approach to IT security and that a fixed portion of their annual IT budgets should be allocated to our platform, our sales will not grow as quickly as anticipated, or at all, which would have an adverse impact on our business, results of operations and financial condition.

Even if there is significant demand for virtual machine-based security solutions like ours, if our competitors include functionality that is, or is perceived to be, better than or equivalent to that of our platform in signature-based or other products that are already generally accepted as necessary components of an organization s IT security architecture, we may have difficulty increasing the market penetration of our platform. Furthermore, even if the functionality offered by other IT security providers is different and more limited than the functionality of our platform, organizations may elect to accept such limited functionality in lieu of adding products from additional vendors like us.

If enterprises and governments do not continue to adopt our virtual machine-based security platform for any of the reasons discussed above, our sales would not grow as quickly as anticipated, or at all, and our business, results of operations and financial condition would be harmed.

Recent and future acquisitions and investments could disrupt our business and harm our financial condition and operating results.

Our success will depend, in part, on our ability to expand our platform and grow our business in response to changing technologies, customer demands and competitive pressures. In some circumstances, we may decide to do so through the acquisition of complementary businesses and technologies rather than through internal development, including, for example, our recent acquisition of Mandiant Corporation, or Mandiant, a

provider of advanced endpoint security products and security incident response management solutions. The identification of

Table of Contents

suitable acquisition candidates can be difficult, time-consuming and costly, and we may not be able to successfully complete acquisitions that we target in the future. The risks we face in connection with acquisitions, including our recent acquisition of Mandiant, include:

- diversion of management time and focus from operating our business to addressing acquisition integration challenges;
- coordination of research and development and sales and marketing functions;
- integration of product and service offerings;
- retention of key employees from the acquired company;
- changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisition;
- cultural challenges associated with integrating employees from the acquired company into our organization;
- integration of the acquired company s accounting, management information, human resources and other administrative systems;
- the need to implement or improve controls, procedures, and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;
- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we don t adequately address and that cause our reported results to be incorrect;
- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities;
- unanticipated write-offs or charges; and
- litigation or other claims in connection with the acquired company, including claims from terminated employees, customers, former stockholders or other third parties.

Our failure to address these risks or other problems encountered in connection with our past or future acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally. For example, we only recently completed our acquisition of Mandiant, and substantially all of the acquisition integration risks remain. Future acquisitions could also result in dilutive issuances of equity securities. For example, we recently issued approximately 16.9 million shares of common stock and assumed options to purchase approximately 4.6 million shares of our common stock in connection with our acquisition of Mandiant. There is also a risk that future acquisitions will result in the incurrence of debt, contingent liabilities, amortization expenses, incremental operating expenses or the write-off of goodwill, any of which could harm our financial condition or operating results.

Our limited operating history makes it difficult to evaluate our current business and prospects and may increase the risk that we will not be successful.

We were founded in 2004, and our first commercially successful product was our Web Threat Prevention appliance, which we first shipped in 2008. We expanded our platform in 2011, 2012 and 2013 to include our Email Threat Prevention appliance, File Threat Prevention appliance and our latest Web Threat Prevention appliance, the NX 10000, respectively. In December 2013, we expanded our platform through the addition of Mandiant s endpoint threat detection, response and remediation products; advanced threat intelligence capabilities; and incident response and security consulting services. The majority of our revenue growth began in 2010. Our limited operating history and our recent acquisition of Mandiant make it difficult to evaluate our current business and prospects and plan for and model our future growth. We have encountered and will continue to encounter risks and uncertainties frequently encountered by rapidly growing companies in developing markets.

Table of Contents

If our assumptions regarding these risks and uncertainties are incorrect or change in response to changes in the IT security market, our results of operations and financial results could differ materially from our plans and forecasts. Although we have experienced rapid growth for the past several years, there is no assurance that such growth will continue. Any success we may experience in the future will depend in large part on our ability to, among other things:

- maintain and expand our customer base and the ways in which customers use our products and services;
- expand revenue from existing customers through increased or broader use of our products and services within their organizations;
- convince customers to allocate a fixed portion of their annual IT budgets to our products and services;
- improve the performance and capabilities of our platform through research and development;
- effectively expand our business domestically and internationally, which will require that we rapidly expand our sales force and service professionals and fill key management positions, particularly internationally; and
- successfully compete with other companies that currently provide, or may in the future provide, solutions like ours that protect against next-generation advanced cyber attacks.

If we are unable to achieve our key objectives, including the objectives listed above, our business and results of operations will be adversely affected and the fair market value of our common stock could decline.

If we do not effectively expand and train our direct sales force, we may be unable to add new customers or increase sales to our existing customers, and our business will be adversely affected.

We continue to be substantially dependent on our direct sales force to obtain new customers and increase sales with existing customers. There is significant competition for sales personnel with the skills and technical knowledge that we require. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel to support our growth, particularly in international markets. New hires require significant training and may take significant time before they achieve full productivity. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. In addition, because we continue to grow rapidly, a large percentage of our sales force is new to our company. If we are unable to hire and train a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business will be adversely affected.

If we fail to effectively manage our growth, our business, financial condition and results of operations would be harmed.

Our headcount increased from more than 175 employees as of December 31, 2011 to over 1,600 employees as of December 31, 2013. We expect our headcount to continue to grow rapidly. In addition, our number of end-customers increased from more than 425 to more than 1,900 over the

same period. This rapid growth has placed significant demands on our management and our operational and financial infrastructure. To improve our infrastructure, we have recently implemented a new enterprise resource planning system, including revenue recognition and management software, and we plan to implement additional systems. There is no assurance that we will be able to successfully scale improvements to our enterprise resource planning system or other systems and processes in a manner that keeps pace with our growth or that such systems will be effective in preventing or detecting errors, omissions or fraud.

As part of our efforts to improve our internal systems, processes and controls, we have licensed technology from third parties. The support services available for such third-party technology is outside of our control and may be negatively affected by consolidation in the software industry. In addition, if we do not receive adequate

support for the software underlying our systems, processes and controls, our ability to provide products and services to our customers in a timely manner may be impaired, which may cause us to lose customers, limit us to smaller deployments of our platform or increase our technical support costs.

To manage this growth effectively, we must continue to improve our operational, financial and management systems and controls by, among other things:

- effectively attracting, training and integrating a large number of new employees, particularly members of our sales and management teams;
- further improving our key business applications, processes and IT infrastructure, including our data centers, to support our business needs;
- enhancing our information and communication systems to ensure that our employees and offices around the world are well coordinated and can effectively communicate with each other and our growing base of channel partners and customers;
- improving our internal control over financial reporting and disclosure controls and procedures to ensure timely and accurate reporting of our operational and financial results; and
- appropriately documenting our IT systems and business processes.

These and other improvements in our systems and controls will require significant capital expenditures and the allocation of valuable management and employee resources. If we fail to implement these improvements effectively, our ability to manage our expected growth, ensure uninterrupted operation of key business systems and comply with the rules and regulations applicable to public reporting companies would be impaired, and our business, financial condition and results of operations would be harmed.

Fluctuating economic conditions make it difficult to predict revenue for a particular period, and a shortfall in revenue may harm our operating results.

Our revenue depends significantly on general economic conditions and the demand for products in the IT security market. Economic weakness, customer financial difficulties, and constrained spending on IT security may result in decreased revenue and earnings. Such factors could make it difficult to accurately forecast our sales and operating results and could negatively affect our ability to provide accurate forecasts to our contract manufacturers and manage our contract manufacturer relationships and other expenses. In addition, concerns regarding the impact of the U.S. federal sequestration on the IT budgets of various agencies of the U.S. government, as well as continued budgetary challenges in the United States and Europe and geopolitical turmoil in many parts of the world have and may continue to put pressure on global economic conditions and overall spending on IT security. Currently, most enterprises and governments have not allocated a fixed portion of their budgets to protect against next-generation advanced cyber attacks. If we do not succeed in convincing customers that our platform should be an integral part of their overall approach to IT security and that a fixed portion of their annual IT budgets should be allocated to our platform, general reductions in IT spending by our customers are likely to have a disproportionate impact on our business, results of operations and financial condition. General economic weakness may also lead to longer collection cycles for payments due from our customers, an increase in customer bad debt, restructuring initiatives and associated expenses, and impairment of investments. Furthermore, the continued weakness and uncertainty in worldwide credit markets, including the sovereign debt situation in certain countries in the European Union, may adversely impact the ability of our customers to adequately fund their expected capital expenditures, which could lead to delays or cancellations of planned purchases of our

platform.

Uncertainty about future economic conditions also makes it difficult to forecast operating results and to make decisions about future investments. Future or continued economic weakness for us or our customers, failure of our customers and markets to recover from such weakness, customer financial difficulties, and reductions in spending on IT security could have a material adverse effect on demand for our platform and consequently on our business, financial condition and results of operations.

Table of Contents

Our results of operations are likely to vary significantly from period to period, which could cause the trading price of our common stock to decline.

Our results of operations have varied significantly from period to period, and we expect that our results of operations will continue to vary as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including:

- our ability to attract and retain new customers;
- the budgeting cycles, seasonal buying patterns and purchasing practices of customers;
- the timing of shipments of our products and length of our sales cycles;
- changes in customer or reseller requirements or market needs;
- changes in the growth rate of the IT security market, particularly the market for threat protection solutions like ours that target next-generation advanced cyber attacks;
- the timing and success of new product and service introductions by us or our competitors or any other change in the competitive landscape of the IT security market, including consolidation among our customers or competitors;
- the level of awareness of IT security threats, particularly advanced cyber attacks, and the market adoption of our platform;
- deferral of orders from customers in anticipation of new products or product enhancements announced by us or our competitors;
- our ability to successfully expand our business domestically and internationally;
- reductions in customer renewal rates for our subscriptions;
- decisions by organizations to purchase IT security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
- any disruption in, or termination of, our relationship with channel partners;
- decreases in our customers subscription renewal rates;

our inability to fulfill our customers orders due to supply chain delays or events that impact our manufacturers or their suppliers;

insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our products, subscriptions and services, or confronting our key suppliers, particularly our sole source suppliers, which could disrupt our supply chain;

the cost and potential outcomes of existing and future litigation;

seasonality in our business;

general economic conditions, both domestic and in our foreign markets;

future accounting pronouncements or changes in our accounting policies or practices;

the amount and timing of operating costs and capital expenditures related to the expansion of our business;

a change in our mix of products, subscriptions and services; and

increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates.

Table of Contents

Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other operating results from period to period. As a result of this variability, our historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for these or other reasons, the market price of our common stock could fall substantially, and we could face costly lawsuits, including securities class action suits.

We have had operating losses each year since our inception, and may not achieve or maintain profitability in the future.

We have incurred operating losses each year since 2004, including net losses of $16.8 million, $35.8 million and $120.6 million in 2011, 2012 and 2013, respectively. We expect our operating expenses to increase in the future as we expand our sales and marketing efforts and continue to invest in research and development of our technologies. These efforts may be more costly than we expect, and we may not be able to increase our revenue to offset our increased operating expenses. Our revenue growth may slow or our revenue may decline for a number of other reasons, including reduced demand for our platform, increased competition, a decrease in the growth or size of the IT security market, particularly the market for solutions that target the next generation of advanced cyber attacks, or any failure to capitalize on growth opportunities. Any failure to increase our revenue as we grow our business could prevent us from achieving or maintaining profitability. If we are unable to meet these risks and challenges as we encounter them, our business, financial condition and results of operations may suffer.

We expect our revenue growth rate to decline, and as our costs increase, we may not be able to generate sufficient revenue to achieve and maintain profitability over the long term.

From the year ended December 31, 2010 to the year ended December 31, 2013, our revenue grew from $11.8 million to $161.6 million, which represents a compounded annual growth rate of approximately 139%. We expect that, to the extent our revenue increases to higher levels, our revenue growth rate will decline, and we may not be able to generate sufficient revenue to achieve or maintain profitability. We also expect our costs to increase in future periods, which could negatively affect our future operating results if our revenue does not increase. In particular, we expect to continue to expend substantial financial and other resources on:

- research and development related to our platform, including investments in our research and development team;
- sales and marketing, including a significant expansion of our sales organization, particularly in international markets;
- international expansion of our business;
- expansion of our professional services organization; and
- general administration expenses, including legal and accounting expenses related to being a public company.

These investments may not result in increased revenue or growth in our business. If we are unable to increase our revenue at a rate sufficient to offset the expected increase in our costs, our business, financial position and results of operations will be harmed, and we may not be able to achieve or maintain profitability over the long term.

Seasonality may cause fluctuations in our revenue.

We believe there are significant seasonal factors that may cause us to record higher revenue in some quarters compared with others. We believe this variability is largely due to our customers budgetary and spending patterns, as many customers spend the unused portions of their discretionary budgets prior to the end of

Table of Contents

their fiscal years. For example, we have historically recorded our highest level of revenue in our fourth quarter, which we believe corresponds to the fourth quarter of a majority of our customers. Similarly, we have historically recorded our second-highest level of revenue in our third quarter, which corresponds to the fourth quarter of U.S. federal agencies and other customers in the U.S. federal government. In addition, our rapid growth rate over the last couple years may have made seasonal fluctuations more difficult to detect. If our rate of growth slows over time, seasonal or cyclical variations in our operations may become more pronounced, and our business, results of operations and financial position may be adversely affected.

We face intense competition and could lose market share to our competitors, which could adversely affect our business, financial condition and results of operations.

The market for security products and services is intensely competitive and characterized by rapid changes in technology, customer requirements, industry standards and frequent new product introductions and improvements. We anticipate continued challenges from current competitors, which in many cases are more established and enjoy greater resources than us, as well as by new entrants into the industry. If we are unable to anticipate or effectively react to these competitive challenges, our competitive position could weaken, and we could experience a decline in our growth rate or revenue that could adversely affect our business and results of operations.

Our competitors and potential competitors include large networking vendors such as Cisco Systems, Inc. and Juniper Networks, Inc. that may emulate or integrate virtual-machine features similar to ours into their own products; large companies such as Intel, IBM, and HP that have acquired large IT security specialist vendors in recent years and have the technical and financial resources and broad customer bases needed to bring competitive solutions to the market; independent IT security vendors such as Sourcefire (which was recently acquired by Cisco Systems, Inc.) and Palo Alto Networks that offer products that claim to perform similar functions to our platform; small and large companies that offer point solutions that compete with some of the features present in our platform; and other providers of incident response services. Other IT providers offer, and may continue to introduce, security features that compete with our platform, either in stand-alone security products or as additional features in their network infrastructure products. Many of our existing competitors have, and some of our potential competitors could have, substantial competitive advantages such as:

- greater name recognition, longer operating histories and larger customer bases;
- larger sales and marketing budgets and resources;
- broader distribution and established relationships with channel and distribution partners and customers;
- greater customer support resources;
- greater resources to make acquisitions;
- lower labor and research and development costs;
- larger and more mature intellectual property portfolios; and

substantially greater financial, technical and other resources.

In addition, some of our larger competitors have substantially broader product offerings and may be able to leverage their relationships with distribution partners and customers based on other products or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing our products, subscriptions and services, including by selling at zero or negative margins, product bundling or offering closed technology platforms. Potential customers may also prefer to purchase from their existing suppliers rather than a new supplier regardless of product performance or features. As a result, even if the features of our platform are superior, customers may not purchase our products. In addition, new innovative start-up companies, and larger companies that are making significant investments in research and development, may invent similar or superior products and technologies that compete with our platform. Our current and potential

competitors may also establish cooperative relationships among themselves or with third parties that may further enhance their resources. If we are unable to compete successfully, or if competing successfully requires us to take costly actions in response to the actions of our competitors, our business, financial condition and results of operations could be adversely affected.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. As a result, our sales and revenue are difficult to predict and may vary substantially from period to period, which may cause our results of operations to fluctuate significantly.

Our results of operations may fluctuate, in part, because of the resource intensive nature of our sales efforts, the length and variability of our sales cycle and the short-term difficulty in adjusting our operating expenses. Our results of operations depend in part on sales to large organizations. The length of our sales cycle, from proof of concept to delivery of and payment for our platform, is typically three to nine months but can be more than a year. To the extent our competitors develop products that our prospective customers view as equivalent to ours, our average sales cycle may increase. Because the length of time required to close a sale varies substantially from customer to customer, it is difficult to predict exactly when, or even if, we will make a sale with a potential customer. As a result, large individual sales have, in some cases, occurred in quarters subsequent to those we anticipated, or have not occurred at all. The loss or delay of one or more large transactions in a quarter could impact our results of operations for that quarter and any future quarters for which revenue from that transaction is delayed. As a result of these factors, it is difficult for us to forecast our revenue accurately in any quarter. Because a substantial portion of our expenses are relatively fixed in the short term, our results of operations will suffer if our revenue falls below our or analysts expectations in a particular quarter, which could cause the price of our common stock to decline.

Reliance on shipments at the end of each quarter could cause our revenue for the applicable period to fall below expected levels.

As a result of customer buying patterns and the efforts of our sales force and channel partners to meet or exceed their sales objectives, we have historically received a substantial portion of sales orders and generated a substantial portion of revenue during the last few weeks of each quarter. A significant interruption in our IT systems, which manage critical functions such as order processing, revenue recognition, financial forecasts, inventory and supply chain management, and trade compliance reviews, could result in delayed order fulfillment and decreased revenue for that quarter. If expected revenue at the end of any quarter is delayed for any reason, including the failure of anticipated purchase orders to materialize, our logistics or channel partners inability to ship products prior to quarter-end to fulfill purchase orders received near the end of the quarter, our failure to manage inventory to meet demand, our inability to release new products on schedule, any failure of our systems related to order review and processing, or any delays in shipments based on trade compliance requirements, our revenue for that quarter could fall below our expectations and the estimates of market analysts, which could adversely impact our business and results of operations and cause a decline in the trading price of our common stock.

If we do not accurately anticipate and respond promptly to changes in our customers technologies, business plans or security needs, our competitive position and prospects could be harmed.

Many of our customers operate in markets characterized by rapidly changing technologies and business plans, which require them to add numerous network access points and adapt to increasingly complex IT networks, incorporating a variety of hardware, software applications, operating systems and networking protocols. As their technologies and business plans grow more complex, we expect these customers to face new and increasingly sophisticated methods of attack. We face significant challenges in ensuring that our platform effectively identifies and responds to these advanced and evolving attacks without disrupting our customers network performance. As a result of the continued rapid innovations in the technology industry, including the rapid growth of smart phones, tablets and other devices and the trend of bring your own device in enterprises, we expect the networks of our customers to continue to change rapidly and become more complex.

Table of Contents

We have identified a number of new products and enhancements to our platform that we believe are important to our continued success in the IT security market. For example, in September 2013, we announced the introduction of our latest Web Threat Prevention appliance, the NX 10000, and in December 2013, we released our new SaaS-based Mobile Threat Prevention solution and our solution for small and midsize businesses. There can be no assurance that we will be successful in developing and marketing, on a timely basis, such new products or enhancements or that our new products or enhancements will adequately address the changing needs of the marketplace. In addition, some of our new products and enhancements may require us to develop new hardware architectures that involve complex, expensive and time-consuming research and development processes. Although the market expects rapid introduction of new products and enhancements to respond to new threats, the development of these products and enhancements is difficult and the timetable for commercial release and availability is uncertain, as there can be significant time lags between initial beta releases and the commercial availability of new products and enhancements. We may experience unanticipated delays in the availability of new products and enhancements to our platform and fail to meet customer expectations with respect to the timing of such availability. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing, releasing and making available on a timely basis new products and enhancements to our platform that can adequately respond to advanced threats and our customers needs, our competitive position and business prospects will be harmed. Furthermore, from time to time, we or our competitors may announce new products with capabilities or technologies that could have the potential to replace or shorten the life cycles of our existing products. There can be no assurance that announcements of new products will not cause customers to defer purchasing our existing products.

Additionally, the process of developing new technology is expensive, complex and uncertain. The success of new products and enhancements depends on several factors, including appropriate component costs, timely completion and introduction, differentiation of new products and enhancements from those of our competitors, and market acceptance. To maintain our competitive position, we must continue to commit significant resources to developing new products or enhancements to our platform before knowing whether these investments will be cost-effective or achieve the intended results. There can be no assurance that we will successfully identify new product opportunities, develop and bring new products or enhancements to market in a timely manner, or achieve market acceptance of our platform, or that products and technologies developed by others will not render our platform obsolete or noncompetitive. If we expend significant resources on researching and developing products or enhancements to our platform and such products or enhancements are not successful, our business, financial position and results of operations may be adversely affected.

Disruptions or other business interruptions that affect the availability of our Dynamic Threat Intelligence, or DTI, cloud could adversely impact our customer relationships as well as our overall business.

When a customer purchases one or more of our threat prevention appliances, it must also purchase a subscription to our DTI cloud for a term of either one or three years. Our DTI cloud enables global sharing of threat intelligence uploaded by any of our customers cloud-connected FireEye appliances. Our data center and networks may experience technical failures and downtime, may fail to distribute appropriate updates, or may fail to meet the increased requirements of a growing customer base, any of which could temporarily or permanently expose our customers networks, leaving their networks unprotected against the latest security threats. Our customers depend on the continuous availability of our DTI cloud. Our DTI cloud is vulnerable to damage or interruption from a variety of sources, including damage or interruption caused by fire, earthquake, power loss, telecommunications or computer systems failure, cyber attack, human error, terrorist acts and war. There may also be system or network interruptions if new or upgraded systems are defective or not installed properly. Moreover, interruptions in our subscription updates could result in a failure of our DTI cloud to effectively update customers hardware products and thereby leave our customers more vulnerable to attacks. Interruptions or failures in our service delivery could cause customers to terminate their subscriptions with us, could adversely affect our renewal rates, and could harm our ability to attract new customers. Our business would also be harmed if our customers believe that our DTI cloud is unreliable.

Table of Contents

If we are unable to sell additional products, subscriptions and services, as well as renewals of our subscriptions and services, to our customers, our future revenue and operating results will be harmed.

Our future success depends, in part, on our ability to expand the deployment of our platform with existing customers by selling them additional products, subscriptions and services. This may require increasingly sophisticated and costly sales efforts and may not result in additional sales. In addition, the rate at which our customers purchase additional products, subscriptions and services depends on a number of factors, including the perceived need for additional IT security as well as general economic conditions. If our efforts to sell additional products, subscriptions and services to our customers are not successful, our business may suffer.

Further, existing customers that purchase our platform have no contractual obligation to renew their subscriptions and support and maintenance services after the initial contract period, and given our limited operating history, we may not be able to accurately predict our renewal rates. Our customers renewal rates may decline or fluctuate as a result of a number of factors, including the level of their satisfaction with our platform, our customer support, customer budgets and the pricing of our platform compared with the products and services offered by our competitors. If our customers renew their subscriptions, they may renew for shorter contract lengths or on other terms that are less economically beneficial to us. We cannot assure you that our customers will renew their subscriptions, and if our customers do not renew their subscriptions or renew on less favorable terms, our revenue may grow more slowly than expected, if at all.

We also depend on our installed customer base for future support and maintenance revenue. We offer our support and maintenance agreements for terms that generally range between one and five years. If customers choose not to renew their support and maintenance agreements or seek to renegotiate the terms of their support and maintenance agreements prior to renewing such agreements, our revenue may decline.

If we are unable to increase sales of our platform to large organizations while mitigating the risks associated with serving such customers, our business, financial position and results of operations may suffer.

Our growth strategy is dependent, in part, upon increasing sales of our platform to large enterprises and governments. Sales to large customers involve risks that may not be present (or that are present to a lesser extent) with sales to smaller entities. These risks include:

- increased purchasing power and leverage held by large customers in negotiating contractual arrangements with us;
- more stringent or costly requirements imposed upon us in our support service contracts with such customers, including stricter support response times and penalties for any failure to meet support requirements;
- more complicated implementation processes;
- longer sales cycles and the associated risk that substantial time and resources may be spent on a potential customer that ultimately elects not to purchase our platform or purchases less than we hoped;
- closer relationships with, and dependence upon, large technology companies who offer competitive products; and

more pressure for discounts and write-offs.

In addition, because security breaches with respect to larger, high-profile enterprises are likely to be heavily publicized, there is increased reputational risk associated with serving such customers. If we are unable to increase sales of our platform to large enterprise and government customers while mitigating the risks associated with serving such customers, our business, financial position and results of operations may suffer.

Table of Contents

Our current research and development efforts may not produce successful products or enhancements to our platform that result in significant revenue, cost savings or other benefits in the near future, if at all.

We must continue to dedicate significant financial and other resources to our research and development efforts if we are to maintain our competitive position. However, developing products and enhancements to our platform is expensive and time consuming, and there is no assurance that such activities will result in significant new marketable products or enhancements to our platform, design improvements, cost savings, revenue or other expected benefits. If we spend significant resources on research and development and are unable to generate an adequate return on our investment, our business and results of operations may be materially and adversely affected.

Real or perceived defects, errors or vulnerabilities in our platform or the failure of our platform to block malware or prevent a security breach could harm our reputation and adversely impact our business, financial position and results of operations.

Because our platform is complex, it has contained and may contain design or manufacturing defects or errors that are not detected until after its deployment by our customers. For example, in the past, we expended time and resources addressing certain manufacturing defects that negatively impacted the ability of certain appliances used in our platform to withstand normal transit. Defects in the functionality of our platform may result in vulnerability to security attacks, cause it to fail to secure networks or temporarily interrupt the networking traffic of our customers. In addition, because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our platform is unable to detect or prevent. Moreover, as our platform is adopted by an increasing number of enterprises and governments, it is possible that the individuals and organizations behind advanced malware attacks will begin to focus on finding ways to defeat our platform. If this happens, our networks, products, subscriptions and services could be targeted by attacks specifically designed to disrupt our business and undermine the perception that our platform is capable of providing superior IT security, which, in turn, could have a serious impact on our reputation as a provider of virtual machine-based security solutions.

If any of our customers becomes infected with malware after adopting our platform, even if our platform has blocked the theft of any of such customer s data, such customer could nevertheless be disappointed with our platform. Furthermore, if any enterprises or governments that are publicly known to use our platform are the subject of an advanced cyber attack that becomes publicized, our other current or potential customers may look to our competitors for alternatives to our platform. Real or perceived security breaches of our customers networks could cause disruption or damage to their networks or other negative consequences and could result in negative publicity to us, damage to our reputation, declining sales, increased expenses and customer relations issues. Furthermore, our platform may fail to detect or prevent malware, viruses, worms or similar threats for any number of reasons, including our failure to enhance and expand our platform to reflect industry trends, new technologies and new operating environments, the complexity of the environment of our clients and the sophistication of malware, viruses and other threats. To the extent potential customers or industry analysts believe that the occurrence of such a failure is a flaw or indicates that our products do not provide significant value, our reputation and business could be harmed. Failure to keep pace with technological changes in the IT security industry and changes in the threat landscape could adversely affect our ability to protect against security breaches and could cause us to lose customers.

Any real or perceived defects, errors or vulnerabilities in our platform, or any other failure of our platform to detect an advanced threat, could result in:

- a loss of existing or potential customers or channel partners;
- delayed or lost revenue;

a delay in attaining, or the failure to attain, market acceptance;

Table of Contents

- the expenditure of significant financial and product development resources in efforts to analyze, correct, eliminate, or work around errors or defects, to address and eliminate vulnerabilities, or to identify and ramp up production with alternative third-party manufacturers;

- an increase in warranty claims, or an increase in the cost of servicing warranty claims, either of which would adversely affect our gross margins;

- harm to our reputation or brand; and

- litigation, regulatory inquiries, or investigations that may be costly and further harm our reputation.

We may be unable to protect our intellectual property adequately, which could harm our business, financial condition and results of operations.

We believe that our intellectual property is an essential asset of our business. We rely on a combination of patent, copyright, trademark and trade secret laws, as well as confidentiality procedures and contractual provisions, to establish and protect our intellectual property rights in the United States and abroad. The efforts we have taken to protect our intellectual property may not be sufficient or effective, and our trademarks, copyrights and patents may be held invalid or unenforceable. Any U.S. or other patents issued to us may not be sufficiently broad to protect our proprietary technologies, and given the costs of obtaining patent protection, we may choose not to seek patent protection for certain of our proprietary technologies. We may not be effective in policing unauthorized use of our intellectual property, and even if we do detect violations, litigation may be necessary to enforce our intellectual property rights. Any enforcement efforts we undertake, including litigation, could be time-consuming and expensive, could divert management s attention and may result in a court determining that our intellectual property rights are unenforceable. If we are not successful in cost-effectively protecting our intellectual property rights, our business, financial condition and results of operations could be harmed.

Claims by others that we infringe their proprietary technology or other rights could harm our business.

Technology companies frequently enter into litigation based on allegations of patent infringement or other violations of intellectual property rights. In addition, patent holding companies seek to monetize patents they have purchased or otherwise obtained. As we face increasing competition and gain an increasingly higher profile, the possibility of intellectual property rights claims against us grows. From time to time, third parties have asserted, and we expect that third parties will continue to assert, claims of infringement of intellectual property rights against us. For example, we are currently a party to suits by both a practicing and non-practicing entity alleging, among other things, patent infringement, each of which are in the early stages of litigation. Third parties may in the future also assert claims against our customers or channel partners, whom our standard license and other agreements obligate us to indemnify against claims that our products infringe the intellectual property rights of third parties. While we intend to increase the size of our patent portfolio, many of our competitors and others may now and in the future have significantly larger and more mature patent portfolios than we have. In addition, future litigation may involve patent holding companies or other patent owners who have no relevant product offerings or revenue and against whom our own patents may therefore provide little or no deterrence or protection. Any claim of intellectual property infringement by a third party, even a claim without merit, could cause us to incur substantial costs defending against such claim, could distract our management from our business and could require us to cease use of such intellectual property. Furthermore, because of the substantial amount of discovery required in connection with intellectual property litigation, there is a risk that some of our confidential information could be compromised by the discovery process.

Although third parties may offer a license to their technology or other intellectual property, the terms of any offered license may not be acceptable, and the failure to obtain a license or the costs associated with any license could cause our business, financial condition and results of

operations to be materially and adversely affected. In addition, some licenses may be non-exclusive, and therefore our competitors may have access to the same technology licensed to us. If a third party does not offer us a license to its technology or other intellectual property on reasonable terms, or at all, we could be enjoined from continued use of such intellectual property. As

a result, we may be required to develop alternative, non-infringing technology, which could require significant time (during which we could be unable to continue to offer our affected products, subscriptions or services), effort, and expense and may ultimately not be successful. Furthermore, a successful claimant could secure a judgment or we may agree to a settlement that prevents us from distributing certain products, providing certain subscriptions or performing certain services or that requires us to pay substantial damages, royalties or other fees. Any of these events could harm our business, financial condition and results of operations.

We incorporate technology from third parties into our products, and our inability to obtain or maintain rights to the technology could harm our business.

We incorporate technology from third parties into our products. We cannot be certain that our suppliers and licensors are not infringing the intellectual property rights of third parties or that the suppliers and licensors have sufficient rights to the technology in all jurisdictions in which we may sell our products. Some of our agreements with our suppliers and licensors may be terminated for convenience by them. If we are unable to obtain or maintain rights to any of this technology because of intellectual property infringement claims brought by third parties against our suppliers and licensors or against us, or if we are unable to continue to obtain such technology or enter into new agreements on commercially reasonable terms, our ability to develop and sell products, subscriptions and services containing such technology could be severely limited, and our business could be harmed. Additionally, if we are unable to obtain necessary technology from third parties, including certain sole suppliers, we may be forced to acquire or develop alternative technology, which may require significant time, cost and effort and may be of lower quality or performance standards. This would limit and delay our ability to offer new or competitive products and increase our costs of production. If alternative technology cannot be obtained or developed, we may not be able to offer certain functionality as part of our products, subscriptions and services. As a result, our margins, market share and results of operations could be significantly harmed.

Our products and subscriptions contain third-party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions.

Our products and subscriptions contain software modules licensed to us by third-party authors under open source licenses. The use and distribution of open source software may entail greater risks than the use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code. Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon the type of open source software we use. If we combine our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release the source code of our proprietary software to the public. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us.

Although we monitor our use of open source software to avoid subjecting our products and subscriptions to conditions, the terms of many open source licenses have not been interpreted by U.S. courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions will be effective. From time to time, we may face claims from third parties asserting ownership of, or demanding release of, the open source software or derivative works that we developed using such software (which could include our proprietary source code), or otherwise seeking to enforce the terms of the applicable open source license. These claims could result in litigation. If we are held to have breached the terms of an open source software license, we could be required to seek licenses from third parties to continue offering our products on terms that are not economically feasible, to re-engineer our products, to discontinue the sale of our products if re-engineering could not be accomplished on a timely or cost-effective basis, or to make generally available, in source code form, our proprietary code, any of which could adversely affect our business, results of operations and financial condition.

27

Table of Contents

We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to attract and retain qualified personnel could harm our business.

Our future success is substantially dependent on our ability to attract, retain and motivate the members of our management team and other key employees throughout our organization, including key employees obtained through our recent acquisition of Mandiant. Competition for highly skilled personnel is intense, especially in the San Francisco Bay Area and the Washington D.C. Area, where we have a substantial presence and need for highly skilled personnel. We may not be successful in attracting qualified personnel to fulfill our current or future needs. Our competitors may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. Also, to the extent we hire employees from mature public companies with significant financial resources, we may be subject to allegations that such employees have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees inventions or other work product.

In addition, we believe that it is important to establish and maintain a corporate culture that facilitates the maintenance and transfer of institutional knowledge within our organization and also fosters innovation, teamwork, a passion for customers and a focus on execution. Our Chief Executive Officer, our Chief Operating Officer and certain other key members of our management and finance teams have only been working together for a relatively short period of time. If we are not successful in integrating these key employees into our organization, such failure could delay or hinder our product development efforts and the achievement of our strategic objectives, which could adversely affect our business, financial condition and results of operations.

Our employees, including our executive officers, work for us on an at-will basis, which means they may terminate their employment with us at any time. We do not maintain key person life insurance policies on any of our key employees. If one or more of our key employees resigns or otherwise ceases to provide us with their service, our business could be harmed.

If we are unable to maintain successful relationships with our channel partners and technology alliance partners, or if our channel partners or technology alliance partners fail to perform, our ability to market, sell and distribute our platform will be limited, and our business, financial position and results of operations will be harmed.

In addition to our direct sales force, we rely on our indirect channel partners to sell and support our platform. We derive a substantial portion of our revenue from sales of our products through our indirect channel, and we expect that sales through channel partners will continue to be a significant percentage of our revenue. We also partner with our technology alliance partners to design go-to-market strategies that combine our platform with products or services provided by our technology alliance partners.

Our agreements with our channel partners and our technology alliance partners are generally non-exclusive, meaning our partners may offer customers products from several different companies, including products that compete with ours. If our channel partners do not effectively market and sell our platform, choose to use greater efforts to market and sell their own products or those of our competitors, or fail to meet the needs of our customers, our ability to grow our business and sell our platform may be adversely affected. Our channel partners and technology alliance partners may cease marketing our platform with limited or no notice and with little or no penalty, and new channel partners require extensive training and may take several months or more to achieve productivity. The loss of a substantial number of our channel partners, our possible inability to replace them, or the failure to recruit additional channel partners could materially and adversely affect our results of operations. In addition, sales by channel partners are more likely than direct sales to involve collectability concerns, particularly in developing markets. Our channel partner structure could also subject us to lawsuits or reputational harm if, for example, a channel partner misrepresents the functionality of our platform to customers or violates applicable laws or our corporate policies.

28

Our ability to achieve revenue growth in the future will depend in part on our success in maintaining successful relationships with our channel partners, and to train our channel partners to independently sell and deploy our platform. If we are unable to maintain our relationships with these channel partners or otherwise develop and expand our indirect sales channel, or if our channel partners fail to perform, our business, financial position and results of operations could be adversely affected.

Because we depend on a limited number of manufacturers to build the appliances used in our platform, we are susceptible to manufacturing delays and pricing fluctuations that could prevent us from shipping customer orders on time, or on a cost-effective basis, which may result in the loss of sales and customers.

We depend on a limited number of third-party manufacturers, primarily Flextronics Telecom Systems, Ltd., as sole source manufacturers for our appliances used in our platform. Our reliance on a limited number of third-party manufacturers reduces our control over the manufacturing process and exposes us to risks, including reduced control over quality assurance, product costs, and product supply and timing. Any manufacturing disruption by these third-party manufacturers could severely impair our ability to fulfill orders on time. If we are unable to manage our relationships with these third-party manufacturers effectively, or if these manufacturers suffer delays or disruptions for any reason, experience increased manufacturing lead-times, capacity constraints or quality control problems in their manufacturing operations, or fail to meet our future requirements for timely delivery, our ability to ship products to our customers would be severely impaired, and our business and results of operations would be harmed.

In addition, we may be deemed to manufacture or contract to manufacture products that contain certain minerals that have been designated as conflict minerals under the Dodd-Frank Wall Street Reform and Consumer Protection Act. As a result, in future periods, we may be required to diligence the origin of such minerals and disclose and report whether or not such minerals originated in the Democratic Republic of the Congo or adjoining countries. The implementation of these new requirements could adversely affect the sourcing, availability, and pricing of minerals used in the manufacture of our products. In addition, we may incur additional costs to comply with the disclosure requirements, including costs related to determining the source of any of the relevant minerals and metals used in our products.

Our third-party manufacturers typically fulfill our supply requirements on the basis of individual orders. We are subject to a risk of supply shortages and changes in pricing terms because we do not have long-term contracts with our third-party manufacturers that guarantee capacity, the continuation of particular pricing terms or the extension of credit limits. Our contract with our primary manufacturer permits it to terminate such contract at its convenience, subject to prior notice requirements. Any production interruptions for any reason, such as a natural disaster, epidemic, capacity shortages, or quality problems at one of our manufacturing partners would negatively affect sales of our products and adversely impact our business and results of operations.

We rely on revenue from subscriptions and service contracts, and because we recognize revenue from subscriptions and service contracts over the term of the relevant subscription or service period, downturns or upturns in sales are not immediately reflected in full in our results of operations.

Subscription and services revenue accounts for a significant portion of our total revenue, comprising 26%, 37% and 45% of total revenue for 2011, 2012 and 2013, respectively. Sales of new or renewal subscription and service contracts may decline or fluctuate as a result of a number of factors, including customers level of satisfaction with our products and subscriptions, the prices of our products and subscriptions, the prices of products and subscriptions offered by our competitors or reductions in our customers spending levels. If our sales of new or renewal subscription and service contracts decline, our revenue and revenue growth may decline and adversely affect our business. In addition, we recognize subscription and service revenue ratably over the term of the relevant service period, which is generally between one to five years. As a result, much of the subscription and service revenue we report each quarter is derived from subscription and service contracts that we sold in prior quarters. Consequently, a decline in new or renewed subscription or service contracts in any one

29

quarter will not be fully reflected in revenue in that quarter but will negatively affect our revenue in future quarters. Accordingly, the effect of significant downturns in new or renewed sales of our subscriptions or services is not reflected in full in our results of operations until future periods. Also, it is difficult for us to rapidly increase our subscription revenue through additional sales in any period, as revenue from new and renewal subscription contracts must be recognized ratably over the applicable service period. Furthermore, any increases in the average term of subscriptions contracts would result in revenue for those subscription contracts being recognized over longer periods of time.

U.S. federal, state and local government sales are subject to a number of challenges and risks that may adversely impact our business.

Sales to U.S. federal, state, and local governmental agencies have in the past accounted for, and may in the future account for, a significant portion of our revenue. Sales to such government entities are subject to the following risks:

- selling to governmental agencies can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;
- government certification requirements applicable to our products may change and in doing so restrict our ability to sell into the U.S. federal government sector until we have attained the revised certification;
- government demand and payment for our products and services may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our products and services;
- we sell our platform to governmental agencies through our indirect channel partners, and these agencies may have statutory, contractual or other legal rights to terminate contracts with our distributors and resellers for convenience or due to a default, and any such termination may adversely impact our future results of operations;
- governments routinely investigate and audit government contractors administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and results of operations, or institute fines or civil or criminal liability if the audit uncovers improper or illegal activities; and
- governments may require certain products to be manufactured in the United States and other relatively high-cost manufacturing locations, and we may not manufacture all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies.

Our ability to maintain customer satisfaction depends in part on the quality of our professional service organization and technical and other support services, including the quality of the support provided on our behalf by certain channel partners. Failure to maintain high-quality customer support could have a material adverse effect on our business, financial condition and results of operations.

Once our platform is deployed within our customers networks, our customers depend on our technical and other support services, as well as the support of our channel partners, to resolve any issues relating to the implementation and maintenance of our platform. If we or our channel partners do not effectively assist our customers in deploying our platform, succeed in helping our customers quickly resolve post-deployment issues, or provide effective ongoing support, our ability to sell additional products, subscriptions or services as part of our platform to existing customers would be adversely affected and our reputation with potential customers could be damaged. Many larger organizations have more complex networks and require higher levels of support than smaller customers. If we fail to meet the requirements of our larger customers, it

may be more difficult to execute on our strategy of upselling and cross selling with these customers. Additionally, if our channel partners do not

effectively provide support to the satisfaction of our customers, we may be required to provide this level of support to those customers, which would require us to hire additional personnel and to invest in additional resources. We are also in the process of expanding our professional services organization. It can take significant time and resources to recruit, hire, and train qualified technical support and professional services employees. We may not be able to hire such resources fast enough to keep up with demand, particularly when the sales of our platform exceed our internal forecasts. To the extent that we or our channel partners are unsuccessful in hiring, training, and retaining adequate support resources, our ability and the ability of our channel partners to provide adequate and timely support to our customers will be negatively impacted, and our customers satisfaction with our platform will be adversely affected. Additionally, to the extent that we need to rely on our sales engineers to provide post-sales support while we are ramping our professional services organization, our sales productivity will be negatively impacted, which would harm our results of operations.

The sales prices of our products, subscriptions and services may decrease, which may reduce our gross profits and adversely impact our financial results.

The sales prices for our products, subscriptions and services may decline for a variety of reasons, including competitive pricing pressures, discounts, a change in our mix of products and subscriptions, anticipation of the introduction of new products or subscriptions, or promotional programs. Competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the price of products or subscriptions that compete with ours or may bundle them with other products and subscriptions. Additionally, although we price our products and subscriptions worldwide in U.S. dollars, currency fluctuations in certain countries and regions may negatively impact actual prices that partners and customers are willing to pay in those countries and regions. Furthermore, we anticipate that the sales prices and gross profits for our products will decrease over product life cycles. We cannot assure you that we will be successful in developing and introducing new offerings with enhanced functionality on a timely basis, or that our new product and subscription offerings, if introduced, will enable us to maintain our prices and gross profits at levels that will allow us to maintain positive gross margins and achieve profitability.

Managing the supply of our products and their components is complex. Insufficient supply and inventory may result in lost sales opportunities or delayed revenue, while excess inventory may harm our gross margins.

Our third-party manufacturers procure components and build our products based on our forecasts, and we generally do not hold inventory for a prolonged period of time. These forecasts are based on estimates of future demand for our products, which are in turn based on historical trends and analyses from our sales and marketing organizations, adjusted for overall market conditions. In order to reduce manufacturing lead times and plan for adequate component supply, from time to time we may issue forecasts for components and products that are non-cancelable and non-returnable.

Our inventory management systems and related supply chain visibility tools may be inadequate to enable us to make accurate forecasts and effectively manage the supply of our products and product components. Supply management remains an area of increasing focus as we balance the need to maintain supply levels that are sufficient to ensure competitive lead times against the risk of obsolescence because of rapidly changing technology and customer requirements. If we ultimately determine that we have excess supply, we may have to reduce our prices and write-down inventory, which in turn could result in lower gross margins. Alternatively, insufficient supply levels may lead to shortages that result in delayed revenue or loss of sales opportunities altogether as potential customers turn to competitors products that may be readily available. Additionally, any increases in the time required to manufacture or ship our products could result in supply shortfalls. If we are unable to effectively manage our supply and inventory, our results of operations could be adversely affected.

Table of Contents

Because some of the key components in our products come from limited sources of supply, we are susceptible to supply shortages or supply changes, which could disrupt or delay our scheduled product deliveries to our customers and may result in the loss of sales and customers.

Our platform relies on key components, including a motherboard and chassis, which our third-party manufacturers purchase on our behalf from a sole source provider. The manufacturing operations of some of our component suppliers are geographically concentrated in Asia, which makes our supply chain vulnerable to regional disruptions. A localized health risk affecting employees at these facilities, such as the spread of a pandemic influenza, could impair the total volume of components that we are able to obtain, which could result in substantial harm to our results of operations. Similarly, a fire, flood, earthquake, tsunami or other disaster, condition or event such as political instability, civil unrest or a power outage that adversely affects any of these component suppliers facilities could significantly affect our ability to obtain the components needed for our products, which could result in a substantial loss of sales and revenue and a substantial harm to our results of operations.

We do not have volume purchase contracts with any of our component suppliers, and they could cease selling to us at any time. In addition, our component suppliers change their selling prices frequently in response to market trends, including industry-wide increases in demand, and because we do not have contracts with these suppliers, we are susceptible to price fluctuations related to raw materials and components. If we are unable to pass component price increases along to our customers or maintain stable pricing, our gross margins and results of operations could be negatively impacted. If we are unable to obtain a sufficient quantity of these components in a timely manner for any reason, sales of our products could be delayed or halted or we could be forced to expedite shipment of such components or our products at dramatically increased costs, which would negatively impact our revenue and gross margins. Additionally, poor quality in any of the sole-sourced components in our products could result in lost sales or lost sales opportunities. If the quality of the components does not meet our or our customers requirements, if we are unable to obtain components from our existing suppliers on commercially reasonable terms, or if any of our sole source providers cease to remain in business or continue to manufacture such components, we could be forced to redesign our products and qualify new components from alternate suppliers. The resulting stoppage or delay in selling our products and the expense of redesigning our products could result in lost sales opportunities and damage to customer relationships, which would adversely affect our business and results of operations.

Our failure to adequately protect personal information could have a material adverse effect on our business.

A wide variety of provincial, state, national, and international laws and regulations apply to the collection, use, retention, protection, disclosure, transfer and other processing of personal data. These data protection and privacy-related laws and regulations are evolving and may result in ever-increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. Our failure to comply with applicable laws and regulations, or to protect such data, could result in enforcement action against us, including fines, imprisonment of company officials and public censure, claims for damages by customers and other affected individuals, damage to our reputation and loss of goodwill (both in relation to existing customers and prospective customers), any of which could have a material adverse effect on our operations, financial performance and business. Evolving and changing definitions of personal data and personal information within the European Union, the United States, and elsewhere, especially relating to classification of IP addresses, machine identification, location data and other information, may limit or inhibit our ability to operate or expand our business, including limiting technology alliance partners that may involve the sharing of data. Even the perception of privacy concerns, whether or not valid, may harm our reputation and inhibit adoption of our products by current and future customers.

If the general level of advanced cyber attacks declines, or is perceived by our current or potential customers to have declined, our business could be harmed.

Our business is substantially dependent on enterprises and governments recognizing that advanced cyber attacks are pervasive and are not effectively prevented by legacy security solutions. High visibility attacks on prominent enterprises and governments have increased market awareness of the problem of advanced cyber

32

attacks and help to provide an impetus for enterprises and governments to devote resources to protecting against advanced cyber attacks, such as testing our platform, purchasing it, and broadly deploying it within their organizations. If advanced cyber attacks were to decline, or enterprises or governments perceived that the general level of advanced cyber attacks have declined, our ability to attract new customers and expand our offerings within existing customers could be materially and adversely affected. A reduction in the threat landscape could increase our sales cycles and harm our business, results of operations and financial condition.

Our technology alliance partnerships expose us to a range of business risks and uncertainties that could have a material adverse impact on our business and financial results.

We have entered, and intend to continue to enter, into technology alliance partnerships with third parties to support our future growth plans. Such relationships include technology licensing, joint technology development and integration, research cooperation, co-marketing activities and sell-through arrangements. We face a number of risks relating to our technology alliance partnerships that could prevent us from realizing the desired benefits from such partnerships on a timely basis or at all, which, in turn, could have a negative impact on our business and financial results.

Technology alliance partnerships require significant coordination between the parties involved, particularly if a partner requires that we integrate its products with our products. This could involve a significant commitment of time and resources by our technical staff and their counterparts within our technology alliance partner. The integration of products from different companies may be more difficult than we anticipate, and the risk of integration difficulties, incompatible products and undetected programming errors or defects may be higher than the risks normally associated with the introduction of new products. It may also be more difficult to market and sell products developed through technology alliance partnerships than it would be to market and sell products that we develop on our own. Sales and marketing personnel may require special training, as the new products may be more complex than our other products.

We invest significant time, money and resources to establish and maintain relationships with our technology alliance partners, but we have no assurance that any particular relationship will continue for any specific period of time. Generally, our agreements with these technology alliance partners are terminable without cause with no or minimal notice or penalties. If we lose a significant technology alliance partner, we could lose the benefit of our investment of time, money and resources in the relationship. In addition, we could be required to incur significant expenses to develop a new strategic alliance or to determine and implement an alternative plan to pursue the opportunity that we targeted with the former partner.

If our estimates or judgments relating to our critical accounting policies are based on assumptions that change or prove to be incorrect, our results of operations could fall below the expectations of securities analysts and investors, resulting in a decline in our stock price.

The preparation of financial statements in conformity with generally accepted accounting principles, or GAAP, requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as provided in the section entitled Management s Discussion and Analysis of Financial Condition and Results of Operations, the results of which form the basis for making judgments about the carrying values of assets, liabilities, equity, revenue and expenses that are not readily apparent from other sources. Our results of operations may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our results of operations to fall below the expectations of securities analysts and investors, resulting in a decline in our stock price. Significant assumptions and estimates used in preparing our consolidated financial statements include those related to assets, liabilities, revenue, expenses and related disclosures.

33

Table of Contents

We are exposed to the credit risk of some of our distributors and resellers and to credit exposure in weakened markets, which could result in material losses.

Most of our sales are on an open credit basis. Although we have programs in place that are designed to monitor and mitigate these risks, we cannot assure you these programs will be effective in reducing our credit risks, especially as we expand our business internationally. If we are unable to adequately control these risks, our business, results of operations and financial condition could be harmed.

Our failure to raise additional capital or generate the significant capital necessary to expand our operations and invest in new products could reduce our ability to compete and could harm our business.

We intend to continue to make investments to support our business growth and may require additional funds to respond to business challenges, including the need to develop new products and enhancements to our platform, improve our operating infrastructure or acquire complementary businesses and technologies. Accordingly, we may need to engage in equity or debt financings to secure additional funds. If we raise additional equity financing, our stockholders may experience significant dilution of their ownership interests and the per share value of our common stock could decline. Furthermore, if we engage in debt financing, the holders of debt would have priority over the holders of common stock, and we may be required to accept terms that restrict our ability to incur additional indebtedness. We may also be required to take other actions that would otherwise be in the interests of the debt holders and force us to maintain specified liquidity or other ratios, any of which could harm our business, results of operations, and financial condition. If we need additional capital and cannot raise it on acceptable terms, we may not be able to, among other things:

- develop or enhance our products and subscriptions;
- continue to expand our sales and marketing and research and development organizations;
- acquire complementary technologies, products or businesses;
- expand operations, in the United States or internationally;
- hire, train and retain employees; or
- respond to competitive pressures or unanticipated working capital requirements.

Our failure to do any of these things could harm our business, financial condition and results of operations.

If our products do not effectively interoperate with our customers IT infrastructure, installations could be delayed or cancelled, which would harm our business.

Our products must effectively interoperate with our customers existing or future IT infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products from multiple vendors, and contains multiple generations of products that have been added over time. As a result, when problems occur in a network, it may be difficult to identify the sources of these problems. If we find errors in the existing software or defects in the hardware used in our customers infrastructure or problematic network configurations or settings, we may have to modify our software or hardware so that our products will interoperate with our customers infrastructure. In such cases, our products may be unable to provide significant performance improvements for applications deployed in our customers infrastructure. These issues could cause longer installation times for our products and could cause order cancellations, either of which would adversely affect our business, results of operations and financial condition. In addition, government and other customers may require our products to comply with certain security or other certifications and standards. If our products are late in achieving or fail to achieve compliance with these certifications and standards, or our competitors achieve compliance with these certifications and standards, we may be disqualified from selling our products to such customers, or may otherwise be at a competitive disadvantage, either of which would harm our business, results of operations, and financial condition.

Table of Contents

Failure to comply with governmental laws and regulations could harm our business.

Our business is subject to regulation by various U.S. federal, state, local and foreign governments. In certain jurisdictions, these regulatory requirements may be more stringent than those in the United States. Noncompliance with applicable regulations or requirements could subject us to investigations, sanctions, mandatory product recalls, enforcement actions, disgorgement of profits, fines, damages, civil and criminal penalties, injunctions or other collateral consequences. If any governmental sanctions are imposed, or if we do not prevail in any possible civil or criminal litigation, our business, results of operations, and financial condition could be materially adversely affected. In addition, responding to any action will likely result in a significant diversion of management s attention and resources and an increase in professional fees. Enforcement actions and sanctions could harm our business, results of operations and financial condition.

We generate a significant amount of revenue from sales to resellers, distributors and customers outside of the United States, and we are therefore subject to a number of risks associated with international sales and operations.

We have a limited history of marketing, selling, and supporting our platform internationally. As a result, we must hire and train experienced personnel to staff and manage our foreign operations. To the extent that we experience difficulties in recruiting, training, managing, and retaining international employees, particularly managers and other members of our international sales team, we may experience difficulties in sales productivity in foreign markets. We also enter into strategic distributor and reseller relationships with companies in certain international markets where we do not have a local presence. If we are not able to maintain successful strategic distributor relationships with our international channel partners or recruit additional channel partners, our future success in these international markets could be limited. Business practices in the international markets that we serve may differ from those in the United States and may require us to include non-standard terms in customer contracts, such as extended payment or warranty terms. To the extent that we enter into customer contracts in the future that include non-standard terms related to payment, warranties, or performance obligations, our results of operations may be adversely impacted.

Additionally, our international sales and operations are subject to a number of risks, including the following:

- greater difficulty in enforcing contracts and managing collections, as well as longer collection periods;
- higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for our international operations;
- fluctuations in exchange rates between the U.S. dollar and foreign currencies in markets where we do business;
- management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of our platform that may be required in foreign countries;
- greater risk of unexpected changes in regulatory practices, tariffs, and tax laws and treaties;

compliance with anti-bribery laws, including, without limitation, compliance with the U.S. Foreign Corrupt Practices Act of 1977, as amended, the U.S. Travel Act and the UK Bribery Act 2010, violations of which could lead to significant fines, penalties and collateral consequences for our company;

heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;

the uncertainty of protection for intellectual property rights in some countries;

- general economic and political conditions in these foreign markets;
- foreign exchange controls that might prevent us from repatriating cash earned outside the United States;
- political and economic instability in some countries; and
- double taxation of our international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which we operate.

These and other factors could harm our ability to generate future international revenue and, consequently, materially impact our business, results of operations and financial condition.

We are exposed to fluctuations in currency exchange rates, which could negatively affect our financial condition and results of operations.

Our sales contracts are denominated in U.S. dollars, and therefore our revenue is not subject to foreign currency risk. However, a strengthening of the U.S. dollar could increase the real cost of our products, subscriptions and services to our customers outside of the United States, which could adversely affect our financial condition and results of operations. In addition, we are incurring an increasing portion of our operating expenses outside the United States. These expenses are denominated in foreign currencies and are subject to fluctuations due to changes in foreign currency exchange rates. We do not currently hedge against the risks associated with currency fluctuations but may do so in the future.

We are subject to governmental export and import controls that could subject us to liability or impair our ability to compete in international markets.

Our products are subject to U.S. export controls, specifically the Export Administration Regulations and economic sanctions enforced by the Office of Foreign Assets Control. We incorporate standard encryption algorithms into our products, which, along with the underlying technology, may be exported outside of the U.S. only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of an encryption registration and classification request. Furthermore, U.S. export control laws and economic sanctions prohibit the shipment of certain products and services to countries, governments, and persons targeted by U.S. sanctions. While we have taken precautions to prevent our products and services from being exported in violation of these laws, in certain instances in the past we shipped our encryption products prior to obtaining the required export authorizations and/or submitting the required requests, including a classification request and request for an encryption registration number, resulting in an inadvertent violation of U.S. export control laws. As a result, in February 2013, we filed a Voluntary Self Disclosure with the U.S. Department of Commerce s Bureau of Industry and Security, or BIS, concerning these potential violations. In June 2013, BIS notified us that it had completed its review of this matter and closed its review with the issuance of a warning letter. No monetary penalties were assessed. Even though we take precautions to ensure that our channel partners comply with all relevant regulations, any failure by our channel partners to comply with such regulations could have negative consequences, including reputational harm, government investigations and penalties.

In addition, various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our products or could limit our customers ability to implement our products in those countries. Changes in our products or changes in export and import regulations may create delays in the introduction of our products into international markets, prevent our customers with international operations from deploying our products globally or, in some cases, prevent the export or import of our products to certain countries, governments or persons altogether. Any change in export or import regulations, economic

sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such

regulations, could result in decreased use of our products by, or in our decreased ability to export or sell our products to, existing or potential customers with international operations. Any decreased use of our products or limitation on our ability to export or sell our products would likely adversely affect our business, financial condition and results of operations.

Our business is subject to the risks of earthquakes, fire, power outages, floods and other catastrophic events, and to interruption by man-made problems such as terrorism.

A significant natural disaster, such as an earthquake, a fire, a flood, or significant power outage could have a material adverse impact on our business, results of operations, and financial condition. Our corporate headquarters and servers hosting our cloud services are located in California, a region known for seismic activity. In addition, natural disasters could affect our supply chain, manufacturing vendors, or logistics providers ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. In the event that our or our service providers information technology systems or manufacturing or logistics abilities are hindered by any of the events discussed above, shipments could be delayed, resulting in missed financial targets, such as revenue and shipment targets, for a particular quarter. In addition, acts of terrorism and other geo-political unrest could cause disruptions in our business or the business of our supply chain, manufacturers, logistics providers, partners, or customers or the economy as a whole. Any disruption in the business of our supply chain, manufacturers, logistics providers, partners or end-customers that impacts sales at the end of a fiscal quarter could have a significant adverse impact on our financial results. All of the aforementioned risks may be further increased if the disaster recovery plans for us and our suppliers prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, or the delay in the manufacture, deployment or shipment of our products, our business, financial condition and results of operations would be adversely affected.

If we fail to comply with environmental requirements, our business, financial condition, results of operations and reputation could be adversely affected.

We are subject to various environmental laws and regulations including laws governing the hazardous material content of our products and laws relating to the collection and recycling of electrical and electronic equipment. Examples of these laws and regulations include the European Union, or EU, Restrictions on the Use of certain Hazardous Substances in Electronic Equipment Directive and the EU Waste Electrical and Electronic Equipment Directive as well as the implementing legislation of the EU member states. Similar laws and regulations have been passed or are pending in China, South Korea and Japan and may be enacted in other regions, including in the United States, and we are, or may in the future be, subject to these laws and regulations.

Our failure to comply with past, present, and future laws could result in reduced sales of our products, substantial product inventory write-offs, reputational damage, penalties, and other sanctions, any of which could harm our business and financial condition. We also expect that our products will be affected by new environmental laws and regulations on an ongoing basis. To date, our expenditures for environmental compliance have not had a material impact on our results of operations or cash flows, and although we cannot predict the future impact of such laws or regulations, they will likely result in additional costs and may increase penalties associated with violations or require us to change the content of our products or how they are manufactured, which could have a material adverse effect on our business, results of operations and financial condition.

The enactment of legislation implementing changes in the U.S. taxation of international business activities or the adoption of other tax reform policies could materially impact our financial position and results of operations.

Recent changes to U.S. tax laws, including limitations on the ability of taxpayers to claim and utilize foreign tax credits and the deferral of certain tax deductions until earnings outside of the United States are repatriated to the United States, as well as changes to U.S. tax laws that may be enacted in the future, could impact the tax

treatment of our foreign earnings. Due to expansion of our international business activities, any changes in the U.S. taxation of such activities may increase our worldwide effective tax rate and adversely affect our financial condition and operating results.

If we do not achieve increased tax benefits as a result of our new corporate structure, our operating results and financial condition may be negatively impacted.

We generally conduct our international operations through wholly-owned subsidiaries and report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. We recently completed the reorganization of our corporate structure and intercompany relationships to more closely align our corporate organization with the expansion of our international business activities. Although we anticipate achieving a reduction in our overall effective tax rate in the future as a result of this new corporate structure, we may not realize any benefits. Our intercompany relationships are subject to complex transfer pricing regulations administered by taxing authorities in various jurisdictions. The relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur, and our position were not sustained, we could be required to pay additional taxes, interest and penalties, which could result in one-time tax charges, higher effective tax rates, reduced cash flows and lower overall profitability of our operations. In addition, if the intended tax treatment of our new corporate structure is not accepted by the applicable taxing authorities, changes in tax law negatively impact the structure or we do not operate our business consistent with the structure and applicable tax laws and regulations, we may fail to achieve any tax advantages as a result of the new corporate structure, and our future operating results and financial condition may be negatively impacted.

We could be subject to additional tax liabilities.

We are subject to U.S. federal, state, local and sales taxes in the United States and foreign income taxes, withholding taxes and transaction taxes in numerous foreign jurisdictions. Significant judgment is required in evaluating our tax positions and our worldwide provision for taxes. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination is uncertain. In addition, our tax obligations and effective tax rates could be adversely affected by changes in the relevant tax, accounting and other laws, regulations, principles and interpretations, including those relating to income tax nexus, by recognizing tax losses or lower than anticipated earnings in jurisdictions where we have lower statutory rates and higher than anticipated earnings in jurisdictions where we have higher statutory rates, by changes in foreign currency exchange rates, or by changes in the valuation of our deferred tax assets and liabilities. We may be audited in various jurisdictions, and such jurisdictions may assess additional taxes, sales taxes and value-added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have a material adverse effect on our operating results or cash flows in the period or periods for which a determination is made.

Our ability to use our net operating losses to offset future taxable income may be subject to certain limitations.

In general, under Section 382 of the Internal Revenue Code of 1986, as amended, or the Code, a corporation that undergoes an ownership change is subject to limitations on its ability to utilize its pre-change net operating losses, or NOLs, to offset future taxable income. Our existing NOLs may be subject to limitations arising from previous ownership changes. Future changes in our stock ownership, some of which are outside of our control, could result in an ownership change under Section 382 of the Code and adversely affect our ability to utilize our NOLs in the future. Furthermore, our ability to utilize NOLs of companies that we may acquire in the future may be subject to limitations. There is also a risk that due to regulatory changes, such as suspensions on the use of NOLs, or other unforeseen reasons, our existing NOLs could expire or otherwise be unavailable to offset future income tax liabilities. For these reasons, we may not be able to utilize a material portion of the NOLs reflected on our balance sheet, even if we attain profitability.

38

Table of Contents

Risks Related to this Offering and Ownership of Our Common Stock

We may fail to meet our publicly announced guidance or other expectations about our business and future operating results, which would cause our stock price to decline.

We have provided and may continue to provide guidance about our business and future operating results. In developing this guidance, our management must make certain assumptions and judgments about our future performance. Our business results may vary significantly from such guidance due to a number of factors, many of which are outside of our control and which could adversely affect our operations and operating results. Furthermore, if our publicly announced guidance of future operating results fails to meet expectations of securities analysts, investors or other interested parties, the price of our common stock would decline.

The price of our common stock has been and may continue to be volatile, and the value of your investment could decline.

The trading price of our common stock has been volatile since our initial public offering and is likely to continue to be volatile. Since the date of our initial public offering, the closing price of our common stock has ranged from $33.36 to $43.69 through December 31, 2013, and the last reported sale price on March 6, 2014 was $89.55. The trading price of our common stock may fluctuate widely in response to various factors, some of which are beyond our control. These factors include:

- announcements of new products, services or technologies, commercial relationships, acquisitions or other events by us or our competitors;
- changes in how customers perceive the effectiveness of our platform in protecting against advanced cyber attacks or other reputational harm;
- publicity concerning cyber attacks in general or high profile cyber attacks against specific organizations;
- price and volume fluctuations in the overall stock market from time to time;
- significant volatility in the market price and trading volume of technology companies in general and of companies in the IT security industry in particular;
- fluctuations in the trading volume of our shares or the size of our public float;
- actual or anticipated changes or fluctuations in our results of operations;
- whether our results of operations and, in particular, our revenue growth rates meet the expectations of securities analysts or investors;

actual or anticipated changes in the expectations of investors or securities analysts, whether as a result of our forward-looking statements, our failure to meet such expectations or otherwise;

litigation involving us, our industry, or both;

regulatory developments in the United States, foreign countries or both;

general economic conditions and trends;

major catastrophic events;

sales of large blocks of our common stock; or

departures of key personnel.

In addition, if the market for technology stocks or the stock market in general experiences a loss of investor confidence, the trading price of our common stock could decline for reasons unrelated to our business, results of operations or financial condition. The trading price of our common stock might also decline in reaction to events

that affect other companies in our industry even if these events do not directly affect us. In the past, following periods of volatility in the market price of a company s securities, securities class action litigation has often been brought against that company. If our stock price is volatile, we may become the target of securities litigation. Securities litigation could result in substantial costs and divert our management s attention and resources from our business. This could have a material adverse effect on our business, results of operations and financial condition.

Sales of substantial amounts of our common stock in the public markets, or the perception that such sales might occur, could reduce the price that our common stock might otherwise attain and may dilute your voting power and your ownership interest in us.

Sales of a substantial number of shares of our common stock in the public market after this offering, or the perception that such sales could occur, could adversely affect the market price of our common stock and may make it more difficult for you to sell your common stock at a time and price that you deem appropriate. Based on the total number of outstanding shares of our common stock as of December 31, 2013, upon completion of this offering, we will have 144,136,573 shares of common stock outstanding, assuming no exercise of our outstanding options or vesting of our outstanding restricted stock units after December 31, 2013, other than 796,846 shares to be sold in this offering by certain selling stockholders upon the exercise of vested stock options and the vesting of restricted stock units.

Upon completion of this offering, all 17,450,000 shares of common stock sold in our initial public offering and all 5,582,215 shares of common stock sold in this offering by us and any shares sold upon the exercise of the underwriters option to purchase additional shares from us will be freely tradable in the public market without restriction or further registration under the Securities Act, unless these shares are held by affiliates, as that term is defined in Rule 144 under the Securities Act. In addition, Morgan Stanley & Co. LLC and Goldman, Sachs & Co., representatives of the underwriters for our initial public offering, have consented to the release of the lock-up restrictions with respect to 8,417,785 shares of common stock to be sold in this offering by the selling stockholders, including certain of our directors, executive officers and employees, who executed lock-up agreements with the underwriters that are scheduled to expire on March 19, 2014. The release took effect upon the pricing of this offering.

As a result of the lock-up agreements described in Shares Eligible for Future Sale and Underwriters, the remaining shares of our common stock will be available for sale in the public market at various times as follows, subject to the provisions of Rules 144 and 701 under the Securities Act and, where applicable, compliance with our insider trading policy:

- 14,664,639 shares will be eligible for sale in the public market on March 19, 2014 upon the expiration of lock-up agreements entered into in connection with our initial public offering;
- 95,610,568 shares will be eligible for sale in the public market upon the expiration of the lock-up agreements entered into in connection with this offering, assuming the prior effectiveness of the resale registration statement for former stockholders of Mandiant (as described under Shares Eligible for Future Sale Resale Rights for Former Stockholders of Mandiant); and
- 1,927 shares will be eligible for sale in the public market on June 30, 2014.

The remaining restricted securities will continue to be held in escrow subject to the terms and conditions of the merger agreement governing our acquisition of Mandiant.

In addition, holders of up to approximately 84,310,480 shares of our common stock, or 58.5% of our total outstanding common stock, based on shares outstanding as of December 31, 2013, will be entitled to rights with respect to registration of these shares under the Securities Act pursuant to an investors rights agreement. If these holders of our common stock, by exercising their registration rights, sell a large number of shares, they could

adversely affect the market price for our common stock. If we file a registration statement for the purpose of selling additional shares of common stock to raise capital and are required to include shares held by these holders pursuant to the exercise of their registration rights, our ability to raise capital may be impaired. Furthermore, all of our executive officers and certain of our directors have adopted, and other directors may in the future adopt, written plans, known as Rule 10b5-1 Plans, under which they have contracted, or may in the future contract, with a broker to sell shares of our common stock on a periodic basis to diversify their assets and investments. Sales of substantial amounts of our common stock in the public markets following the release of the lock-ups or otherwise, including, but not limited to, sales made by our executive officers and directors pursuant to Rule 10b5-1 Plans, or the perception that these sales could occur, could cause the market price of our common stock to decline.

The issuance of additional stock in connection with financings, acquisitions, investments, our stock incentive plans or otherwise will dilute all other stockholders.

Our amended and restated certificate of incorporation authorizes us to issue up to 1,000,000,000 shares of common stock and up to 100,000,000 shares of preferred stock with such rights and preferences as may be determined by our board of directors. Subject to compliance with applicable rules and regulations, we may issue shares of common stock or securities convertible into our common stock from time to time in connection with a financing, acquisition, investment, our stock incentive plans or otherwise. For example, we recently issued approximately 16.9 million shares of common stock and assumed options to purchase approximately 4.6 million shares of our common stock in connection with our acquisition of Mandiant. Any future issuances could result in substantial dilution to our existing stockholders and cause the trading price of our common stock to decline.

Insiders have substantial control over us, which could limit your ability to influence the outcome of key transactions, including a change of control.

Our directors, executive officers and each of our stockholders who, as of January 31, 2014, owned greater than 5% of our outstanding common stock will beneficially own approximately 64.5% of the total outstanding shares of our common stock after the completion of this offering. As a result, these stockholders, if acting together, will be able to influence or control matters requiring approval by our stockholders, including the election of directors and the approval of mergers, acquisitions or other extraordinary transactions. They may also have interests that differ from yours and may vote in a way with which you disagree and which may be adverse to your interests. This concentration of ownership may have the effect of delaying, preventing or deterring a change of control of our company, could deprive our stockholders of an opportunity to receive a premium for their common stock as part of a sale of our company and might ultimately affect the market price of our common stock.

We have broad discretion in the use of the net proceeds that we receive in this offering.

Our management will have broad discretion over the specific use of the net proceeds that we receive in this offering and might not be able to obtain a significant return, if any, on investment of these net proceeds. Investors in this offering will need to rely upon the judgment of our management with respect to the use of proceeds. If we do not use the net proceeds that we receive in this offering effectively, our business, results of operations and financial condition could be harmed.

We do not intend to pay dividends for the foreseeable future.

We have never declared or paid any dividends on our common stock. We intend to retain any earnings to finance the operation and expansion of our business, and we do not anticipate paying any cash dividends in the future. As a result, you may only receive a return on your investment in our common stock if the market price of our common stock increases.

Table of Contents

The requirements of being a public company may strain our resources, divert management s attention and affect our ability to attract and retain qualified board members.

As a public company, we are subject to the reporting requirements of the Securities Exchange Act of 1934, as amended, or the Exchange Act, the listing requirements of the NASDAQ Stock Market and other applicable securities rules and regulations. Compliance with these rules and regulations has increased and will continue to increase our legal and financial compliance costs, has made and will continue to make some activities more difficult, time-consuming or costly, and has increased and will continue to increase demand on our systems and resources. Among other things, the Exchange Act requires that we file annual, quarterly and current reports with respect to our business and results of operations and maintain effective disclosure controls and procedures and internal control over financial reporting. In order to maintain and, if required, improve our disclosure controls and procedures and internal control over financial reporting to meet this standard, significant resources and management oversight may be required. As a result, management s attention may be diverted from other business concerns, which could harm our business and results of operations. Although we have already hired additional employees to comply with these requirements, we may need to hire even more employees in the future, which will increase our costs and expenses.

In addition, changing laws, regulations and standards relating to corporate governance and public disclosure are creating uncertainty for public companies, increasing legal and financial compliance costs, and making some activities more time consuming. These laws, regulations and standards are subject to varying interpretations, in many cases due to their lack of specificity, and as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. We intend to invest resources to comply with evolving laws, regulations, and standards, and this investment will increase our general and administrative expense and a diversion of management s time and attention from revenue-generating activities to compliance activities. If our efforts to comply with new laws, regulations, and standards are unsuccessful, regulatory authorities may initiate legal proceedings against us and our business may be harmed.

We also expect that being a public company and these new rules and regulations will make it more expensive for us to obtain and maintain director and officer liability insurance, and in the future, we may be required to accept reduced coverage or incur substantially higher costs to obtain coverage. These factors could also make it more difficult for us to attract and retain qualified executive officers and members of our board of directors, particularly to serve on our audit committee and compensation committee.

In addition, as a result of our disclosure obligations as a public company, we have reduced strategic flexibility and are under pressure to focus on short-term results, which may adversely impact our ability to achieve long-term profitability.

We are an emerging growth company, and we cannot be certain if the reduced disclosure requirements applicable to emerging growth companies will make our common stock less attractive to investors.

For so long as we remain an emerging growth company, as defined in the Jumpstart Our Business Startups Act, or the JOBS Act, we may take advantage of certain exemptions from various requirements that are applicable to public companies that are not emerging growth companies, including not being required to comply with the independent auditor attestation requirements of Section 404 of the Sarbanes-Oxley Act, reduced disclosure obligations regarding executive compensation in our periodic reports and proxy statements, and exemptions from the requirements of holding a nonbinding advisory vote on executive compensation and stockholder approval of any golden parachute payments not previously approved. We will remain an emerging growth company until the earliest of (i) the last day of the fiscal year following the fifth anniversary of the completion of our IPO, (ii) the last day of the first fiscal year in which our annual gross revenue is $1 billion or more, (iii) the date on which we have, during the previous rolling three-year period, issued more than $1 billion in non-convertible debt securities or (iv) the date on which we are deemed to be a large accelerated filer as

42

defined in the Exchange Act. We cannot predict if investors will find our common stock less attractive because we may rely on these exemptions. If some investors find our common stock less attractive as a result, there may be a less active trading market for our common stock, and our stock price may be more volatile and may decline.

As a public company, we are obligated to implement and maintain proper and effective internal control over financial reporting. We may not complete our analysis of our internal control over financial reporting in a timely manner, or these internal controls may not be determined to be effective, which may adversely affect investor confidence in our company and, as a result, the value of our common stock.

As a public company, we are required, pursuant to the Exchange Act, to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting for the fiscal year ending December 31, 2014. This assessment will need to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting.

We are currently evaluating our internal controls, identifying and remediating deficiencies in those internal controls and documenting the results of our evaluation, testing and remediation. We may not be able to complete our evaluation, testing and any required remediation in a timely fashion. During the evaluation and testing process, if we identify one or more material weaknesses in our internal control over financial reporting that we are unable to remediate before the end of the same fiscal year in which the material weakness is identified, we will be unable to assert that our internal controls are effective. If we are unable to assert that our internal control over financial reporting is effective, or if our auditors, when required, are unable to attest to management s report on the effectiveness of our internal controls, we could lose investor confidence in the accuracy and completeness of our financial reports, which would cause the price of our common stock to decline.

As a public company, we are required to disclose material changes made in our internal control and procedures on a quarterly basis. Once we are no longer an emerging growth company, as defined in the JOBS Act, our independent registered public accounting firm will be required to formally attest to the effectiveness of our internal control over financial reporting pursuant to Section 404 of the Sarbanes-Oxley Act. To comply with the requirements of being a public company, we may need to undertake various actions, such as implementing new internal controls and procedures and hiring accounting or internal audit staff.

If securities or industry analysts do not publish research or reports about our business, or publish inaccurate or unfavorable research reports about our business, our share price and trading volume could decline.

The trading market for our common stock, to some extent, depends on the research and reports that securities or industry analysts publish about us or our business. We do not have any control over these analysts. If one or more of the analysts who cover us should downgrade our shares or change their opinion of our shares, industry sector or products, our share price would likely decline. If one or more of these analysts ceases coverage of our company or fails to regularly publish reports on us, we could lose visibility in the financial markets, which could cause our share price or trading volume to decline.

Our charter documents and Delaware law could discourage takeover attempts and lead to management entrenchment.

Our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that could delay or prevent a change in control of our company. These provisions could also make it difficult for stockholders to elect directors who are not nominated by the current members of our board of directors or take other corporate actions, including effecting changes in our management. These provisions include:

a classified board of directors with three-year staggered terms, which could delay the ability of stockholders to change the membership of a majority of our board of directors;

Table of Contents

the ability of our board of directors to issue shares of preferred stock and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquiror;

the exclusive right of our board of directors to elect a director to fill a vacancy created by the expansion of our board of directors or the resignation, death or removal of a director, which prevents stockholders from being able to fill vacancies on our board of directors;

a prohibition on stockholder action by written consent, which forces stockholder action to be taken at an annual or special meeting of our stockholders;

the requirement that a special meeting of stockholders may be called only by our board of directors, the chairperson of our board of directors, our chief executive officer or our president (in the absence of a chief executive officer), which could delay the ability of our stockholders to force consideration of a proposal or to take action, including the removal of directors;

the requirement for the affirmative vote of holders of at least 66 2/3% of the voting power of all of the then outstanding shares of the voting stock, voting together as a single class, to amend the provisions of our amended and restated certificate of incorporation relating to the management of our business (including our classified board structure) or certain provisions of our amended and restated bylaws, which may inhibit the ability of an acquiror to effect such amendments to facilitate an unsolicited takeover attempt;

the ability of our board of directors to amend the bylaws, which may allow our board of directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquiror to amend the bylaws to facilitate an unsolicited takeover attempt; and

advance notice procedures with which stockholders must comply to nominate candidates to our board of directors or to propose matters to be acted upon at a stockholders meeting, which may discourage or deter a potential acquiror from conducting a solicitation of proxies to elect the acquiror s own slate of directors or otherwise attempting to obtain control of us.

In addition, as a Delaware corporation, we are subject to Section 203 of the Delaware General Corporation Law, which may prohibit large stockholders, in particular those owning 15% or more of our outstanding voting stock, from merging or combining with us for a specified period of time.

Table of Contents

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This prospectus, including the sections entitled Prospectus Summary, Risk Factors, Use of Proceeds, Management s Discussion and Analysis of Financial Condition and Results of Operations, and Business contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. The words believe, may, will, potentially, estimate, continue, anticipate, intend, could, would, project, plan, expect, the negative and plural forms of these w expressions that convey uncertainty of future events or outcomes are intended to identify forward-looking statements. These forward-looking statements include, but are not limited to, statements concerning the following:

- the evolution of the threat landscape facing our customers and prospects;
- our ability to educate the market regarding the advantages of our virtual machine-based security solution;
- our ability to maintain an adequate rate of revenue growth;
- our future financial and operating results;
- our business plan and our ability to effectively manage our growth and associated investments;
- beliefs and objectives for future operations;
- our ability to expand our leadership position in advanced network security;
- our ability to attract and retain customers;
- our ability to further penetrate our existing customer base;
- our expectations concerning renewal rates for subscriptions and services by existing customers;
- our ability to maintain our competitive technological advantages against new entrants in our industry;
- our ability to timely and effectively scale and adapt our existing technology;
- our ability to innovate new products and bring them to market in a timely manner;
- our ability to maintain, protect, and enhance our brand and intellectual property;

our ability to expand internationally;

the reorganization of our corporate structure and intercompany relationships and our ability to improve our overall effective tax rate;

the effects of increased competition in our market and our ability to compete effectively;

cost of revenue, including changes in costs associated with production, manufacturing and customer support;

operating expenses, including changes in research and development, sales and marketing, and general and administrative expenses;

anticipated income tax rates;

sufficiency of cash to meet cash needs for at least the next 12 months;

our ability to maintain our good standing with the United States and international governments and capture new contracts;

costs associated with defending intellectual property infringement and other claims, such as those claims discussed in Business Legal Proceedings ;

our expectations concerning relationships with third parties, including channel partners and logistics providers;

Table of Contents

- the release of new products, including FireEye Mobile Threat Prevention, our recently released SaaS-based mobile platform;
- economic and industry trends or trend analysis;
- the attraction and retention of qualified employees and key personnel;
- future acquisitions of or investments in complementary companies, products, subscriptions or technologies; and
- the effects of seasonal trends on our results of operations.

These forward-looking statements are subject to a number of risks, uncertainties, and assumptions, including those described in Risk Factors and elsewhere in this prospectus. Moreover, we operate in a very competitive and rapidly changing environment, and new risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties, and assumptions, the forward-looking events and circumstances discussed in this prospectus may not occur, or unanticipated events or circumstances that we did not foresee may materialize, either of which could cause actual results to differ materially and adversely from those anticipated or implied in our forward-looking statements.

You should not rely upon forward-looking statements as predictions of future events. Although we believe that the expectations reflected in our forward-looking statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Moreover, neither we nor any other person assumes responsibility for the accuracy and completeness of the forward-looking statements. We undertake no obligation to update publicly any forward-looking statements for any reason after the date of this prospectus to conform these statements to actual results or to changes in our expectations, except as required by law.

You should read this prospectus and the documents that we reference in this prospectus and have filed with the SEC as exhibits to the registration statement of which this prospectus is a part with the understanding that our actual future results, levels of activity, performance and events and circumstances may be materially different from what we expect.

Table of Contents

MARKET AND INDUSTRY DATA

Unless otherwise indicated, information contained in this prospectus concerning our industry and the markets in which we operate, including our general expectations and market position, market opportunity, and market size, is based on information from various sources, including Gartner, Inc., or Gartner, and International Data Corporation, or IDC, on assumptions we have made based on such data and other similar sources and on our knowledge of the markets for our products, subscriptions and services. This information involves a number of assumptions and limitations, and you are cautioned not to give undue weight to such estimates. In addition, projections, assumptions and estimates of our future performance and the future performance of the industry in which we operate is necessarily subject to a high degree of uncertainty and risk due to a variety of factors, including those described in Risk Factors and elsewhere in this prospectus. These and other factors could cause actual results to differ materially from the estimates made by the independent parties and by us.

The Gartner Reports described herein represents data, research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, and are not representations of fact. The Gartner Reports speak as of their original publication date (and not as of the date of this prospectus), and the opinions expressed in the Gartner Reports are subject to change without notice.

In certain instances, the sources of the market and industry data contained in this prospectus are identified by superscript notations. The sources of these data are provided below:

(1) Gartner, *Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence*, Gartner Published: May 30, 2013.

(2) IDC, *Worldwide Network Security 2013 2017 Forecast and 2012 Vendor Shares*, #241926, June 2012, IDC, *Worldwide Web Security 2013 2017 Forecast and 2012 Vendor Shares*, #242033, July 2012, IDC, *Worldwide Messaging Security 2013 2017 Forecast and 2012 Vendor Shares*, #24225, June 2012 and IDC, *Worldwide Endpoint Security 2013 2017 Forecast and 2012 Vendor Shares*, #242618, July 2012.

(3) Gartner, *Market Trends: Managed Security Services, Worldwide, 2013* dated 30 August 2013 *and Forecast: Information Security, Worldwide, 2011-2017, 4Q13 Update* dated 29 January 2014.

Table of Contents

USE OF PROCEEDS

We estimate that the net proceeds from our sale of 5,582,215 shares of common stock in this offering at the public offering price of $82.00 per share, after deducting underwriting discounts and commissions and estimated offering expenses payable by us, will be approximately $442.1 million, or $609.1 million if the underwriters exercise their option to purchase additional shares in full. We will not receive any proceeds from the sale of shares of common stock by the selling stockholders.

The principal purposes of this offering are to increase our capitalization and financial flexibility, obtain additional capital, facilitate an orderly distribution of shares for the selling stockholders in this offering and increase our public float. We intend to use the net proceeds received from this offering primarily for general corporate purposes, including headcount expansion, working capital, sales and marketing activities, product development, general and administrative matters, and capital expenditures. We may also use a portion of the net proceeds for the acquisition of, or investment in, technologies, solutions or businesses that complement our business, although we have no present commitments to complete any such transactions at this time. We will have broad discretion over the uses of the net proceeds of this offering. Pending these uses, we intend to invest the net proceeds from this offering in short-term, investment-grade interest-bearing securities such as money market accounts, certificates of deposit, commercial paper, and guaranteed obligations of the U.S. government.

MARKET PRICE OF COMMON STOCK

Our common stock has been listed on The NASDAQ Global Select Market under the symbol FEYE since September 20, 2013. Prior to that date, there was no public trading market for our common stock. The following table sets forth for the periods indicated the high and low sales prices per share of our common stock as reported on The NASDAQ Global Select Market:

	High	Low
Year Ended December 31, 2013		
Third Quarter (from September 20, 2013)	$ 44.89	$ 35.25
Fourth Quarter	$ 44.55	$ 33.30
Year Ending December 31, 2014		
First Quarter (through March 6, 2014)	$ 97.35	$ 40.41

On March 6, 2014, the closing price of our common stock on The NASDAQ Global Select Market was $89.55 per share. As of December 31, 2013, we had 352 holders of record of our common stock. The actual number of stockholders is greater than this number of record holders and includes stockholders who are beneficial owners but whose shares are held in street name by brokers and other nominees. This number of holders of record also does not include stockholders whose shares may be held in trust by other entities.

DIVIDEND POLICY

We have never declared or paid cash dividends on our common stock. We currently intend to retain all available funds and any future earnings for use in the operation of our business and do not anticipate paying any dividends on our common stock in the foreseeable future, if at all. Any future determination to declare dividends will be made at the discretion of our board of directors and will depend on our financial condition, operating results, capital requirements, general business conditions and other factors that our board of directors may deem relevant.

48

Table of Contents

CAPITALIZATION

The following table sets forth our cash and cash equivalents and capitalization as of December 31, 2013 on:

- an actual basis; and
- a pro forma basis, giving effect to (i) the issuance and sale by us of 5,582,215 shares of common stock in this offering, at the public offering price of $82.00 per share, after deducting underwriting discounts and commissions and estimated offering expenses payable by us, and (ii) the issuance of 796,846 shares of common stock to be acquired by certain selling stockholders upon the exercise of stock options or the vesting of restricted stock units in order to sell such shares in this offering.

You should read this table together with Management s Discussion and Analysis of Financial Condition and Results of Operations and our audited consolidated financial statements and related notes included elsewhere in this prospectus.

	December 31, 2013	
	Actual	Pro Forma
Cash and cash equivalents	$ 173,918	$ 617,671
Total debt, current and non-current portion		
Stockholders equity:		
Preferred stock, par value of $0.0001 per share; 100,000,000 shares authorized, no shares issued and outstanding, actual; 100,000,000 shares authorized, no shares issued and outstanding, pro forma		
Common stock, par value of $0.0001 per share; 1,000,000,000 shares authorized, 137,757,512 issued and outstanding, actual; 1,000,000,000 shares authorized, 144,136,573 issued and outstanding, pro forma	14	14
Additional paid-in capital	1,271,590	1,715,343
Accumulated deficit	(223,502)	(223,502)
Total stockholders equity	1,048,102	1,491,855
Total capitalization	$ 1,048,102	$ 1,491,855

The number of shares of our common stock to be outstanding after this offering is based on 138,554,358 shares of our common stock outstanding as of December 31, 2013, after giving effect to the assumed issuance of 796,846 shares of common stock to be acquired by certain selling stockholders upon the exercise of outstanding stock options and the vesting of outstanding restricted stock units in order to sell such shares in this offering, and excludes:

- 26,657,087 shares of common stock issuable upon the exercise of stock options outstanding as of December 31, 2013, with a weighted-average exercise price of $5.49 per share;
- 605,100 shares of common stock issuable upon the exercise of stock options granted after December 31, 2013, with a weighted-average exercise price of $73.94 per share;

1,757,031 shares of common stock issuable upon the vesting of restricted stock units outstanding as of December 31, 2013;

835,011 shares of common stock issuable upon the vesting of restricted stock units granted after December 31, 2013;

311,747 shares of common stock issuable upon the exercise of warrants outstanding as of December 31, 2013, with a weighted-average exercise price of $0.72 per share;

11,015,257 shares of common stock reserved for future grants as of December 31, 2013 under our 2013 Equity Incentive Plan (which reserve includes 1,440,111 shares of common stock issuable upon the

Table of Contents

exercise of stock options and the vesting of restricted stock units granted after December 31, 2013, as described in the bullets above), plus an additional 6,887,875 shares of common stock that became available for future grants under our 2013 Equity Incentive Plan as of January 1, 2014 pursuant to provisions thereof that automatically increase the share reserve under such plan each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans ;

2,500,000 shares of common stock reserved for future issuance as of December 31, 2013 under our 2013 Employee Stock Purchase Plan, plus an additional 1,377,575 shares of common stock that became available for future grants under our 2013 Employee Stock Purchase Plan as of January 1, 2014 pursuant to provisions thereof that automatically increase the share reserve under such plan each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans ; and

any shares of common stock that become available subsequent to this offering under our 2013 Equity Incentive Plan and 2013 Employee Stock Purchase Plan pursuant to provisions thereof that automatically increase the share reserves under such plans each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans.

Table of Contents

DILUTION

If you invest in our common stock, your interest will be diluted to the extent of the difference between the amount per share paid by purchasers of shares of common stock in this offering and the pro forma net tangible book value per share of common stock immediately after the completion of this offering.

As of December 31, 2013, our historical net tangible book value was approximately $60.4 million, or $0.44 per share of common stock. Our net tangible book value per share represents the amount of our total tangible assets reduced by the amount of our total liabilities and divided by the total number of shares of our common stock outstanding as of December 31, 2013.

After giving effect to (i) the issuance and sale in this offering of 5,582,215 shares of our common stock, at the public offering price of $82.00 per share, after deducting underwriting discounts and commissions and estimated offering expenses payable by us, and (ii) the issuance of 796,846 shares of common stock to be acquired by certain selling stockholders upon the exercise of stock options or the vesting of restricted stock units in order to sell such shares in this offering, our pro forma net tangible book value as of December 31, 2013 would have been approximately $504.2 million, or $3.50 per share of our common stock. This represents an immediate increase in pro forma net tangible book value of $3.06 per share to our existing stockholders and an immediate dilution of $78.50 per share to investors purchasing shares in this offering.

The following table illustrates this dilution:

Public offering price per share		$ 82.00
Net tangible book value per share as of December 31, 2013, before giving effect to this offering	$ 0.44	
Increase per share attributable to this offering	3.06	
Pro forma net tangible book value, as adjusted to give effect to this offering		3.50
Dilution in pro forma net tangible book value per share to new investors purchasing shares in this offering		$ 78.50

If the underwriters exercise their option to purchase additional shares in full, the pro forma net tangible book value per share of our common stock after giving effect to this offering would be $4.59, and the dilution in net tangible book value per share to investors in this offering would be $77.41 per share.

The following table summarizes, on a pro forma basis as of December 31, 2013 after giving effect to the completion of this offering at the public offering price of $82.00 per share, the difference between existing stockholders and new investors with respect to the number of shares of common stock purchased from us, the total consideration paid to us, and the average price per share paid, before deducting underwriting discounts and commissions and estimated offering expenses:

	Shares Purchased		Total Consideration		Average Price
	Number	Percent	Amount	Percent	Per Share

Existing stockholders	138,554,358	96.1%	$ 1,273,263,868	73.6%	$ 9.19
New public investors	5,582,215	3.9	457,741,630	26.4	82.00
Total	144,136,573	100.0%	$ 1,731,005,498	100.0%	

To the extent that any of our outstanding warrants or outstanding stock options are exercised, outstanding restricted stock units vest or additional warrants, stock options, restricted stock units or shares of common stock are issued in the future, investors will experience further dilution.

Except as otherwise indicated, the above discussion and tables assume no exercise of the underwriters option to purchase additional shares. If the underwriters exercise their option to purchase additional shares in full,

Table of Contents

our existing stockholders would own 94.7% and our new investors would own 5.3% of the total number of shares of our common stock outstanding upon the completion of this offering.

The number of shares of our common stock to be outstanding after this offering is based on 138,554,358 shares of our common stock outstanding as of December 31, 2013, after giving effect to the assumed issuance of 796,846 shares of common stock to be acquired by certain selling stockholders upon the exercise of outstanding stock options and the vesting of outstanding restricted stock units in order to sell such shares in this offering, and excludes:

- 26,657,087 shares of common stock issuable upon the exercise of stock options outstanding as of December 31, 2013, with a weighted-average exercise price of $5.49 per share;
- 605,100 shares of common stock issuable upon the exercise of stock options granted after December 31, 2013, with a weighted-average exercise price of $73.94 per share;
- 1,757,031 shares of common stock issuable upon the vesting of restricted stock units outstanding as of December 31, 2013;
- 835,011 shares of common stock issuable upon the vesting of restricted stock units granted after December 31, 2013;
- 311,747 shares of common stock issuable upon the exercise of warrants outstanding as of December 31, 2013, with a weighted-average exercise price of $0.72 per share;
- 11,015,257 shares of common stock reserved for future grants as of December 31, 2013 under our 2013 Equity Incentive Plan (which reserve includes 1,440,111 shares of common stock issuable upon the exercise of stock options and the vesting of restricted stock units granted after December 31, 2013, as described in the bullets above), plus an additional 6,887,875 shares of common stock that became available for future grants under our 2013 Equity Incentive Plan as of January 1, 2014 pursuant to provisions thereof that automatically increase the share reserve under such plan each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans ;
- 2,500,000 shares of common stock reserved for future issuance as of December 31, 2013 under our 2013 Employee Stock Purchase Plan, plus an additional 1,377,575 shares of common stock that became available for future grants under our 2013 Employee Stock Purchase Plan as of January 1, 2014 pursuant to provisions thereof that automatically increase the share reserve under such plan each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans ; and
- any shares of common stock that become available subsequent to this offering under our 2013 Equity Incentive Plan and 2013 Employee Stock Purchase Plan pursuant to provisions thereof that automatically increase the share reserves under such plans each year, as more fully described in Executive Compensation Employee Benefit and Stock Plans.

Table of Contents

SELECTED CONSOLIDATED FINANCIAL DATA

The selected consolidated statements of operations data for the years ended December 31, 2011, 2012 and 2013 and the consolidated balance sheet data as of December 31, 2012 and 2013 are derived from our audited consolidated financial statements included elsewhere in this prospectus. The selected consolidated statements of operations for the year ended December 31, 2009 and 2010 and the selected consolidated balance sheet data as of December 31, 2009, 2010 and 2011 are derived from our audited consolidated financial statements that are not included in this prospectus. The selected consolidated financial data below should be read in conjunction with the section entitled Management s Discussion and Analysis of Financial Condition and Results of Operations and our consolidated financial statements and related notes included elsewhere in this prospectus. The selected consolidated financial data in this section are not intended to replace our consolidated financial statements and the related notes, and are qualified in their entirety by the consolidated financial statements and related notes included elsewhere in this prospectus. Our historical results are not necessarily indicative of the results that may be expected for any period in the future.

	Year Ended December 31,				
	2009	2010	2011	2012	2013
	(In thousands, except per share data)				
Consolidated Statements of Operations Data:					
Revenue:					
Product	$ 1,353	$ 9,270	$ 24,888	$ 52,265	$ 88,253
Subscription and services	288	2,495	8,770	31,051	73,299
Total revenue	1,641	11,765	33,658	83,316	161,552
Cost of revenue:					
Product[(1)]	1,171	2,054	5,690	14,467	28,912
Subscription and services	135	277	1,590	3,163	18,853
Total cost of revenue	1,306	2,331	7,280	17,630	47,765
Total gross profit	335	9,434	26,378	65,686	113,787
Operating expenses:					
Research and development[(1)]	3,910	5,291	7,275	16,522	66,036
Sales and marketing[(1)]	3,063	11,357	30,389	67,562	167,466
General and administrative[(1)]	2,208	1,943	4,428	15,221	52,503
Total operating expenses	9,181	18,591	42,092	99,305	286,005
Operating loss	(8,846)	(9,157)	(15,714)	(33,619)	(172,218)
Interest income	1	3	3	7	68
Interest expense	(5)	(158)	(194)	(537)	(525)
Other income (expense), net	43	(156)	(806)	(2,572)	(7,257)
Loss before income taxes	(8,807)	(9,468)	(16,711)	(36,721)	(179,932)
Provision for (benefit from) income taxes	(7)	13	71	(965)	(59,297)
Net loss attributable to common stockholders	$ (8,800)	$ (9,481)	$ (16,782)	$ (35,756)	$ (120,635)
Net loss per share attributable to common stockholders, basic and diluted	$ (1.42)	$ (1.30)	$ (1.99)	$ (3.28)	$ (2.66)
Weighted-average shares used to compute net loss per share attributable to common stockholders	6,211	7,271	8,447	10,917	45,271

53

Table of Contents

(1) Includes stock-based compensation expense as follows:

	Year Ended December 31,				
	2009	2010	2011	2012	2013
	(In thousands)				
Stock-Based Compensation Expense:					
Cost of product revenue	$ 7	$ 4	$ 39	$ 170	$ 2,810
Research and development	43	60	148	1,465	6,958
Sales and marketing	5	63	360	1,672	10,748
General and administrative	9	10	168	3,536	8,342
Total stock-based compensation expense	$ 64	$ 137	$ 715	$ 6,843	$ 28,858

	As of December 31,				
	2009	2010	2011	2012	2013
	(In thousands)				
Consolidated Balance Sheet Data:					
Cash and cash equivalents	$ 1,265	$ 7,665	$ 10,676	$ 60,200	$ 173,918
Working capital, excluding deferred revenue and costs	1,501	10,302	18,319	75,074	219,707
Total assets	3,210	15,676	35,646	125,273	1,376,313
Total deferred revenue	2,502	6,266	30,102	76,406	187,514
Total long-term debt, current portion	83	497	1,400	1,231	
Total long-term debt, non-current portion	25	3,174	4,528	10,916	
Preferred stock warrant liability	8	189	994	3,529	
Total stockholders equity (deficit)	(409)	1,348	(14,651)	5,390	1,048,102

	Year Ended or as of December 31,		
	2011	2012	2013
	(Dollars in thousands)		
Key Business Metrics:			
Product revenue	$ 24,888	$ 52,265	$ 88,253
Subscription and services revenue	8,770	31,051	73,299
Total revenue	$ 33,658	$ 83,316	$ 161,552
Year-over-year percentage increase	186%	148%	94%
Gross margin percentage	78%	79%	70%
Deferred revenue, current portion at period end[1]	$ 16,215	$ 43,750	$ 110,535
Deferred revenue, non-current portion at period end	$ 13,887	$ 32,656	$ 76,979
Billings (non-GAAP)[2]	$ 57,494	$ 129,620	$ 256,561
Net cash provided by (used in) operating activities[3]	$ 5,111	$ 21,500	$ (69,762)
Free cash flow (non-GAAP)[4]	$ (106)	$ 2,652	$ (127,322)

(1) Our deferred revenue consists of amounts that have been invoiced but have not yet been recognized as revenue as of the period end. For the year ended December 31, 2013, deferred revenue includes the addition of $16.1 million of deferred revenue assumed in connection with the Mandiant acquisition. The majority of our deferred revenue balance consists of the unamortized portion of revenue from sales of our Email Threat Prevention product, subscriptions to our DTI cloud and Email Threat Prevention Attachment/URL Engine, and support and maintenance contracts. Because invoiced amounts for subscriptions and services can be for multiple years, we classify our deferred revenue as current or non-current depending on when we expect to recognize the related revenue. If the deferred revenue is expected to be recognized within 12 months, it is

classified as

current. Otherwise, the deferred revenue is classified as non-current. We monitor our deferred revenue balance because it represents a significant portion of revenue to be recognized in future periods.

(2) We define billings as revenue recognized plus the change in deferred revenue from the beginning to the end of the period. For fiscal year 2013, billings exclude the addition of $16.1 million of deferred revenue assumed as part of the Mandiant acquisition. We consider billings to be a useful metric for management and investors because billings drives deferred revenue, which is an important indicator of the health and visibility of our business and represents a significant percentage of our revenue. See Management s Discussion and Analysis of Financial Condition and Results of Operations Key Business Metrics for more information and a reconciliation of billings to revenue, the most directly comparable financial measure calculated and presented in accordance with U.S. generally accepted accounting principles, or GAAP.

(3) We monitor cash flow provided by (used in) operating activities as a measure of our overall business performance. Our cash flow provided by (used in) operating activities is driven in large part by sales of our products and from up-front payments for both new and renewal contracts for subscription and support and maintenance. Monitoring cash flow provided by (used in) operating activities enables us to analyze our financial performance without the non-cash effects of certain items such as depreciation, amortization, and stock-based compensation costs, thereby allowing us to better understand and manage the cash needs of our business.

(4) We define free cash flow as net cash provided by operating activities less purchases of property and equipment and demonstration units. We consider free cash flow to be a liquidity measure that provides useful information to management and investors about the amount of cash generated by the business that, after the purchases of property and equipment and demonstration units, can be used for strategic opportunities, including investing in our business, making strategic acquisitions, and strengthening the balance sheet. See Management s Discussion and Analysis of Financial Condition and Results of Operations Key Business Metrics for more information and a reconciliation of free cash flow to cash flow provided by (used in) operating activities, the most directly comparable financial measure calculated and presented in accordance with GAAP.

Table of Contents

MANAGEMENT S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

You should read the following discussion and analysis of our financial condition and results of operations together with the consolidated financial statements and related notes that are included elsewhere in this prospectus. This discussion contains forward-looking statements based upon current plans, expectations and beliefs that involve risks and uncertainties. Our actual results may differ materially from those anticipated in these forward-looking statements as a result of various factors, including those set forth under Risk Factors and in other parts of this prospectus.

Overview

We provide a comprehensive solution of products and services for detecting, preventing and resolving advanced cybersecurity threats. We have invented a purpose-built, virtual machine-based security platform that provides real-time protection to enterprises and governments worldwide against the next generation of cyber attacks. Our technology approach represents a paradigm shift from how IT security has been conducted since the earliest days of the information technology industry. The core of our purpose-built, virtual machine-based security platform is our virtual execution engine, to which we refer as our MVX engine, which identifies and protects against known and unknown threats that existing signature-based technologies are unable to detect. We believe it is imperative for organizations to invest in this new approach to security to protect their critical assets, such as intellectual property and customer and financial data, from the global pandemic of cybercrime, cyber espionage and cyber warfare.

We were founded in 2004 to address the fundamental limitations of legacy signature-based technologies in detecting and blocking sophisticated cyber attacks. From 2004 to 2008, we focused our efforts on research and development to build our virtual machine technology. We released our first product, the Web Threat Prevention appliance, in 2008. Our Web Threat Prevention appliance is designed to analyze and block advanced attacks via the Web. Since that time, we have continued to enhance our product portfolio, releasing our Email Threat Prevention appliance in 2011 and our File Threat Prevention appliance in 2012. Our Email and File Threat Prevention products address advanced threats that are introduced through email attachments and file shares. Due to the scale of our customer deployments and our customers desire for deeper analysis of potential malicious software, we also provide management and analysis appliances, specifically our Central Management System and our Forensic Analysis System. We support and enhance the functionality of our products through our Dynamic Threat Intelligence, or DTI, cloud, a subscription service that offers global threat intelligence sharing and provides a closed-loop system that leverages the network effects of a globally distributed, automated threat analysis network. Our over ten years of research and development in virtual machine technology, anomaly detection and associated heuristic algorithms has enabled us to provide signature-less threat protection against next-generation cyber attacks.

We primarily market and sell our virtual machine-based security platform to Global 2000 companies in a broad range of industries and governments worldwide. As of December 31, 2013, we had over 1,900 end-customers across more than 60 countries, including over 130 of the Fortune 500.

We have experienced rapid growth over the last several years, increasing our revenue at a compound annual growth rate of 139% from 2010 to 2013. We have also increased our number of employees from 35 as of December 31, 2008 to 416 and 1,679 as of December 31, 2012 and December 31, 2013, respectively. We expect to continue rapidly scaling our organization to meet the needs of our customers and to pursue opportunities in new and existing markets. We intend to continue to invest in the development of our sales and marketing teams, with a particular focus on expanding our network of international channel partners, opening sales offices, hiring key sales and marketing personnel and carrying out associated marketing activities in key geographies. As of December 31, 2013, we were selling our solution to end-customers in over 60 countries, and we expect revenue from international sales to grow as a percentage of our overall revenue. In 2013, we completed the

reorganization

of our corporate structure and intercompany relationships to more closely align our corporate organization with the expansion of our international business activities and improve our overall effective tax rate. We intend to continue to invest in our product development organization to enhance the functionality of our existing platform, introduce new products and subscriptions, and build upon our technology leadership. Due to our continuing investments to scale our business, particularly internationally, reorganize our corporate structure for improved tax efficiency, pursue new opportunities, enhance our product functionality, introduce new products and build upon our technology leadership in advance of, and in preparation for, our expected increase in sales and expansion of our customer base, we are continuing to incur expenses in the near term for which we may not realize any long-term benefit. As a result, we do not expect to be profitable for the foreseeable future.

During the years ended December 31, 2011, 2012 and 2013, our revenue was $33.7 million, $83.3 million and $161.6 million, representing year-over-year growth of 186%, 148% and 94%, respectively. Our net losses were $16.8 million, $35.8 million and $120.6 million during the years ended December 31, 2011, 2012 and 2013, respectively. During the year ended December 31, 2012, approximately 80%, 8% and 8% of our revenue came from the United States, Asia Pacific and Japan (APAC), and Europe, the Middle East and Africa (EMEA), respectively. During the year ended December 31, 2013, approximately 72%, 10% and 14% of our revenue came from the United States, APAC and EMEA, respectively.

In September 2013, we closed our initial public offering, or IPO, in which we sold 17,450,000 shares of common stock (inclusive of 2,275,000 shares of common stock from the exercise of the over-allotment option granted to the underwriters). The public offering price of the shares sold in the IPO was $20.00 per share. The total gross proceeds from the offering were $349.0 million. After deducting underwriting discounts and commissions and offering expenses, the aggregate net proceeds received by us totaled approximately $321.0 million.

On December 30, 2013, we acquired privately held Mandiant Corporation, or Mandiant, the leading provider of advanced endpoint security products and security incident response management solutions. We believe this combination creates the industry s leading advanced threat protection vendor with the ability to detect, prevent and resolve cyber attacks at every stage of the attack life cycle. Under the terms of the merger agreement governing the transaction, we delivered to the former security holders of Mandiant merger consideration with an aggregate value equal to approximately $1,020.3 million, consisting of approximately $106.5 million in net cash and an aggregate of 21.5 million shares and options to purchase shares of our common stock.

This acquisition creates risks for us. These risks are set forth more fully in the section of this prospectus titled Risk Factors. Audited Mandiant financial statements and unaudited pro forma condensed combined financial statements are included in this prospectus following our financial statements and should be read by investors in conjunction with the respective accompanying notes. The results of operations of Mandiant have been included in our consolidated statements of operations since December 30, 2013, the acquisition date. Our balance sheet as of December 31, 2013 reflects items assumed from the Mandiant acquisition.

We believe that the growth of our business and our short and long term success are dependent upon many factors, including our ability to extend our technology leadership, grow our base of end-customers, expand deployment of our platform within existing end-customers, and focus on end-customer satisfaction. While these areas present significant opportunities for us, they also pose challenges and risks that we must successfully address in order to sustain the growth of our business and improve our operating results.

We have experienced rapid growth and increased demand for our products over the last few years. To manage any future growth effectively, we must continue to improve and expand our information technology and financial infrastructure, our operating and administrative systems and controls, and our ability to manage headcount, capital, and processes in an efficient manner. Additionally, we face intense competition in our market, and to succeed, we need to innovate and offer products that are differentiated from existing infrastructure

57

Table of Contents

products, as well as effectively hire, retain, train, and motivate qualified personnel and senior management. If we are unable to successfully address these challenges, our business, operating results, and prospects could be adversely affected.

For a description of factors that may impact our future performance, see the disclosure below under Factors Affecting our Performance.

Our Business Model

We generate revenue from sales of our products, subscriptions and services. Our product revenue consists primarily of revenue from the sale of our threat prevention portfolio of software-based appliances, consisting of our Web Threat Prevention, Email Threat Prevention and File Threat Prevention, as well as sales of our Forensic Analysis System and Central Management System appliances. We offer this portfolio as a complete solution to protect the various entry points of a customer s network from the next generation of cyber attacks. Because the typical customer s network has more Web entry points to protect than email and file entry points, customers that purchase our threat prevention portfolio generally purchase more Web Threat Prevention appliances than Email or File Threat Prevention appliances. As a result, Web Threat Prevention accounts for the largest portion of our threat prevention product revenue. In addition, because most malicious attacks occur through the Web threat vector, smaller customers and customers who do not have the budget to purchase the full threat prevention portfolio often only purchase Web Threat Prevention. While we have experienced steady growth in sales of our Email Threat Prevention appliance since its introduction in 2011, these sales have not contributed as quickly to the growth in our overall product revenue because revenue associated with Email Threat Prevention is recognized ratably over the longer of the contractual term or the estimated period the customer is expected to benefit from the product. By contrast, revenue associated with our Web Threat Prevention, File Threat Prevention, Central Management System and Forensic Analysis System products is recognized upon shipment. Finally, we introduced our File Threat Prevention appliance in the second quarter of 2012, and as a result, revenue from our File Threat Prevention product represents a small percentage of our product revenue.

We require customers to purchase a subscription to our DTI cloud and support and maintenance services when they purchase any part of our product portfolio. In addition, we require customers that purchase our Email Threat Prevention product to also purchase a subscription to our Email Threat Prevention Attachment/URL Engine. Our customers generally purchase these subscriptions and services for a one or three year term, and revenue from such subscriptions is recognized ratably over the subscription period. Sales of these subscriptions and services, along with sales of Email Threat Prevention for multi-year terms, have increased our deferred revenue. As of December 31, 2011, 2012 and 2013, our total deferred revenue was $30.1 million, $76.4 million and $187.5 million, respectively. Amortization of this growing deferred revenue has increased our subscription and services revenue as a percentage of total revenue. For the years ended December 31, 2011, 2012 and 2013, subscription and services revenue as a percentage of total revenue was 26%, 37% and 45%, respectively. While most of the growth in our subscription and services revenue during such years relates to the amortization of the initial subscription and services agreements, renewals of such agreements have also contributed to this growth. Our renewal rate for subscriptions expiring in 2012 and 2013 was in excess of 90%, and we expect to maintain high renewal rates in the future due to the significant value we believe these subscriptions and services add to the efficacy of our product portfolio.

Table of Contents

Key Business Metrics

We monitor the key business metrics set forth below to help us evaluate growth trends, establish budgets, measure the effectiveness of our sales and marketing efforts, and assess operational efficiencies. We discuss revenue and gross margin below under Components of Operating Results. Deferred revenue, billings, net cash flow provided by (used in) operating activities, and free cash flow are discussed immediately below the following table.

	Year Ended or as of December 31,		
	2011	2012	2013
	(Dollars in thousands)		
Product revenue	$ 24,888	$ 52,265	$ 88,253
Subscription and services revenue	8,770	31,051	73,299
Total revenue	$ 33,658	$ 83,316	$ 161,552
Year-over-year percentage increase	186%	148%	94%
Gross margin percentage	78%	79%	70%
Deferred revenue, current portion	$ 16,215	$ 43,750	$ 110,535
Deferred revenue, non-current portion	$ 13,887	$ 32,656	$ 76,979
Billings (non-GAAP)	$ 57,494	$ 129,620	$ 256,561
Net cash provided by (used in) operating activities	$ 5,111	$ 21,500	$ (69,762)
Free cash flow (non-GAAP)	$ (106)	$ 2,652	$ (127,322)

Deferred revenue. Our deferred revenue consists of amounts that have been invoiced but have not yet been recognized as revenue as of the period end. For the year ended December 31, 2013, deferred revenue includes the addition of $16.1 million of deferred revenue assumed in connection with the Mandiant acquisition. The majority of our deferred revenue consists of the unamortized balance of revenue from sales of our Email Threat Prevention products, subscriptions to our DTI cloud and Email Threat Prevention Attachment/URL Engine, and support and maintenance contracts. Because invoiced amounts for subscriptions and services can be for multiple years, we classify our deferred revenue as current or non-current depending on when we expect to recognize the related revenue. If the deferred revenue is expected to be recognized within 12 months, it is classified as current. Otherwise, the deferred revenue is classified as non-current. We monitor our deferred revenue balance because it represents a significant portion of revenue to be recognized in future periods.

Billings. Billings is a non-GAAP financial metric that we define as revenue recognized in accordance with generally accepted accounting principles, or GAAP, plus the change in deferred revenue from the beginning to the end of the period. For the year ended December 31, 2013, billings exclude the addition of $16.1 million of deferred revenue assumed in connection with the Mandiant acquisition. We consider billings to be a useful metric for management and investors, as a supplement to the corresponding GAAP measure, because billings drive deferred revenue, which is an important indicator of the health and visibility of trends in our business, and represents a significant percentage of revenue. However, it is important to note that other companies, including companies in our industry, may not use billings, may calculate billings differently, may have different billing frequencies, or may use other financial measures to evaluate their performance, all of which could reduce the usefulness of billings as a comparative measure. A reconciliation of billings to revenue, the most directly comparable financial measure calculated and presented in accordance with GAAP, is provided below:

	Year Ended or as of December 31,		
	2011	2012	2013
	(In thousands)		
Revenue	$ 33,658	$ 83,316	$ 161,552
Deferred revenue, end of period	30,102	76,406	187,514
Less: deferred revenue, beginning of period	6,266	30,102	76,406

Less: Mandiant deferred revenue assumed			16,099
Billings (non-GAAP)	$ 57,494	$ 129,620	$ 256,561

Table of Contents

Net cash provided by (used in) operating activities. We monitor net cash provided by (used in) operating activities as a measure of our overall business performance. Our net cash provided by (used in) operating activities is driven in large part by sales of our products and from up-front payments for both subscriptions and support and maintenance services. Monitoring net cash provided by (used in) operating activities enables us to analyze our financial performance without the non-cash effects of certain items such as depreciation, amortization, and stock-based compensation costs, thereby allowing us to better understand and manage the cash needs of our business.

Free cash flow. Free cash flow is a non-GAAP financial measure we define as net cash provided by (used in) operating activities less purchases of property and equipment and demonstration units. We consider free cash flow to be a liquidity measure that provides useful information to management and investors about the amount of cash generated by our business that, after the purchases of property and equipment and demonstration units, can be used by us for strategic opportunities, including investing in our business, making strategic acquisitions and strengthening our balance sheet. However, it is important to note that other companies, including companies in our industry, may not use free cash flow, may calculate free cash flow differently, or may use other financial measures to evaluate their performance, all of which could reduce the usefulness of free cash flow as a comparative measure. A reconciliation of free cash flow to cash flow provided by (used in) operating activities, the most directly comparable financial measure calculated and presented in accordance with GAAP, is provided below:

	Year Ended or as of December 31,		
	2011	2012	2013
	(In thousands)		
Cash flow provided by (used in) operating activities	$ 5,111	$ 21,500	$ (69,762)
Less: purchase of property and equipment and demonstration units	(5,217)	(18,848)	(57,560)
Free cash flow (non-GAAP)	$ (106)	$ 2,652	$ (127,322)
Net cash used in investing activities	$ (5,224)	$ (20,215)	$ (148,469)
Net cash provided by financing activities	$ 3,124	$ 48,239	$ 331,949

Factors Affecting our Performance

Market Adoption. We rely on market education to raise awareness of today s next-generation cyber attacks, articulate the need for our virtual machine-based security solution and, in particular, the reasons to purchase our products. Our prospective customers often do not have a specific portion of their IT budgets allocated for products that address the next generation of advanced cyber attacks. We invest heavily in sales and marketing efforts to increase market awareness, educate prospective customers and drive adoption of our solution. This market education is critical to creating new IT budget dollars or allocating IT budget dollars across enterprises and governments for next-generation threat protection solutions, and in particular, our platform. Our investment in market education has also increased awareness of us and our solution in international markets. However, we believe that we will need to invest additional resources in targeted international markets to drive awareness and market adoption. The degree to which prospective customers recognize the mission critical need for next-generation threat protection solutions, and subsequently allocate budget dollars for our platform, will drive our ability to acquire new customers and increase renewals and follow-on sales opportunities, which, in turn, will affect our future financial performance.

Sales Productivity. Our sales organization consists of a direct sales team, made up of field and inside sales personnel, and indirect channel sales teams to support our channel partner sales. We utilize a direct-touch sales model whereby we work with our channel partners to secure prospects, convert prospects to customers, and pursue follow-on sales opportunities. To date, we have primarily targeted large enterprise and government customers, who typically have sales cycles from three to six months. We have also recently expanded our inside sales teams to pursue customers in the small and medium enterprise, or SME, market.

Our growth strategy contemplates increased sales and marketing investments internationally. Newly hired sales and marketing resources will require several months to establish prospect relationships and drive overall

sales productivity. In addition, sales teams in international regions will face local markets that have not had significant market education about advanced security threats that our platform addresses. All of these factors will influence timing and overall levels of sales productivity, impacting the rate at which we will be able to convert prospects to sales and drive revenue growth.

Renewal Rates. New or existing customers that purchase one of our appliances are required to purchase a one or three year subscription to our DTI cloud and, in the case of our Email Threat Prevention products, to our Email Threat Prevention Attachment/URL Engine, as well as support and maintenance services. New or existing customers that purchase one of our Forensic Analysis System or Central Management System appliances are required to purchase support and maintenance services for a term of one or three years.

We believe our renewal rate is an important metric to measure the long-term value of customer agreements and our ability to retain our customers. We calculate our renewal rate by dividing the number of renewing customers that were due for renewal in any rolling 12 month period by the number of customers that were due for renewal in that rolling 12 month period. Our renewal rate at December 31, 2011, 2012 and 2013 was over 90%. These high renewal rates are primarily attributable to the incremental value added to our appliances by our DTI cloud and support and maintenance services. As DTI cloud subscriptions and support and maintenance services represented 26%, 37% and 45% of our total revenue during the years ended December 31, 2011, 2012 and 2013, respectively, we expect our ability to maintain high renewal rates for these subscriptions and services to have a material impact on our future financial performance.

Follow-On Sales. After the initial sale to a new customer, we focus on expanding our relationship with such customer to sell additional products, subscriptions and services. To grow our revenue, it is important that our customers make additional purchases of our platform. Sales to our existing customer base can take the form of incremental sales of appliances, subscriptions and services, either to deploy our platform into additional parts of their network or to protect additional threat vectors. Our opportunity to expand our customer relationships through follow-on sales will increase as we add new customers, broaden our product portfolio to support more threat vectors, increase network performance and enhance functionality. Follow-on sales lead to increased revenue over the lifecycle of a customer relationship and can significantly increase the return on our sales and marketing investments. With some of our most significant customers, we have realized follow-on sales that were multiples of the value of their initial purchases.

Components of Operating Results

Revenue

We generate revenue from the sales of our products, subscriptions and services. As discussed further in Critical Accounting Policies and Estimates Revenue Recognition below, revenue is recognized when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed or determinable and collectability is reasonably assured.

Our total revenue consists of the following:

Product revenue. Our product revenue is generated from sales of our appliances. For our Web Threat Prevention, File Threat Prevention, Forensic Analysis System and Central Management System appliances, we recognize product revenue at the time of shipment, provided that all other revenue recognition criteria have been met. For our Email Threat Prevention appliance, we recognize product revenue ratably over the longer of the contractual term of the subscription service or the estimated period the

customer is expected to benefit from the product. Because we have only been selling our Email Threat Prevention since April 2011, we have a limited history with respect to subscription renewals for such product. As a result, revenue from all Email Threat Prevention products sold by us through December 31, 2013 has been recognized ratably over the contractual term of the subscription services.

Table of Contents

Subscription and services revenue. Subscription and services revenue is generated primarily from our DTI cloud, our Email Threat Prevention Attachment/URL Engine, and support and maintenance services. Our DTI cloud subscription is determined as a percentage of the price of the related appliance. The Email Threat Prevention Attachment/URL Engine is priced on a per-user basis. We recognize revenue from subscriptions and support and maintenance services over the one or three year contract term, as applicable.

Cost of Revenue

Our total cost of revenue consists of cost of product revenue and cost of subscription and services revenue. Personnel costs associated with our operations and global customer support organizations consist of salaries, benefits, bonuses and stock-based compensation. Overhead costs consist of certain facilities, depreciation, benefits, and information technology costs.

Cost of product revenue. Cost of product revenue primarily consists of costs paid to our third-party contract manufacturers and personnel and other costs in our manufacturing operations department. Our cost of product revenue also includes product testing costs, allocated costs and shipping costs. We expect our cost of product revenue to increase as our product revenue increases.

Cost of subscription and services revenue. Cost of subscription and services revenue consists of personnel costs for our global customer support organization and allocated costs. We expect our cost of subscription and services revenue to increase as our customer base grows and as we hire additional professional services personnel.

Gross Margin

Gross margin, or gross profit as a percentage of revenue, has been and will continue to be affected by a variety of factors, including the average sales price of our products, subscriptions and services, manufacturing costs, the mix of products sold, and the mix of revenue among products, subscriptions and services. We expect our gross margins to fluctuate over time depending on the factors described above.

Operating Expenses

Our operating expenses consist of research and development, sales and marketing, and general and administrative expense. Personnel costs are the most significant component of operating expenses and consist of salaries, benefits, bonuses, stock-based compensation and, with regard to sales and marketing expense, sales commissions. Operating expenses also include overhead costs for facilities, IT and depreciation.

Research and development. Research and development expense consists primarily of personnel costs and allocated overhead. Research and development expense also includes prototype-related expenses. We expect research and development expense to continue to increase in absolute dollars as we continue to invest in our research and product development efforts to enhance our product capabilities, address new threat vectors and access new customer markets, although such expense may fluctuate as a percentage of total revenue.

Sales and marketing. Sales and marketing expense consists primarily of personnel costs, incentive commission costs and allocated overhead. We expense commission costs as incurred. Sales and marketing expense also includes costs for market development

programs, promotional and other marketing activities, travel, office equipment, depreciation of proof-of-concept evaluation units and outside consulting costs. We expect sales and marketing expense to continue to increase in absolute dollars as we increase the size of our sales and marketing organizations and expand our international operations, although such expense may fluctuate as a percentage of total revenue.

General and administrative. General and administrative expense consists of personnel costs, professional services and allocated overhead. General and administrative personnel include our executive, finance, human resources, facilities and legal organizations. Professional services consist

primarily of legal, auditing, accounting and other consulting costs. We expect general and administrative expense to continue to increase in absolute dollars as we have recently incurred, and expect to continue to incur, additional general and administrative expenses as we grow our operations and comply with public company regulations, including higher legal, corporate insurance, and accounting expenses.

Interest Income

Interest income consists of interest earned on our cash and cash equivalent balances. We have historically invested our cash in money-market funds and other short-term, investment-grade investments. We expect interest income to vary each reporting period depending on our average investment balances during the period, types and mix of investments and market interest rates.

Interest Expense

Interest expense consists of interest on our outstanding debt. See Note 6 to our consolidated financial statements included elsewhere in this prospectus for more information about our debt.

Other Expense, Net

Other expense, net consists primarily of the change in fair value of our preferred stock warrant liability and gains or losses on disposal of fixed assets. Convertible preferred stock warrants are classified as a liability on our consolidated balance sheets and remeasured to fair value at each balance sheet date with the corresponding change recorded as other expense. Upon the completion of our initial public offering, the liability was reclassified to stockholders equity, at which time it was no longer subject to fair value accounting.

Provision for (Benefit from) Income Taxes

Provision for (benefit from) income taxes consists primarily of U.S. federal and state income taxes in the United States and income taxes in certain foreign jurisdictions in which we conduct business. Our effective tax rate for the year ended December 31, 2013 was different from the U.S. statutory tax rate applied to our pretax loss primarily due to tax benefits from the valuation allowance release on U.S. deferred tax assets offset by different tax rates in foreign jurisdictions which are indefinitely reinvested. Our effective tax rate for the years ended December 31, 2011 and 2012 was different than the U.S. statutory tax rate primarily due to the valuation allowance on our U.S. deferred tax assets.

Table of Contents

Results of Operations

The following tables summarize our results of operations for the periods presented and as a percentage of our total revenue for those periods. The period-to-period comparison of results is not necessarily indicative of results for future periods.

	Year Ended December 31,		
	2011	2012	2013
	(In thousands)		
Revenue:			
Product	$ 24,888	$ 52,265	$ 88,253
Subscription and services	8,770	31,051	73,299
Total revenue	33,658	83,316	161,552
Cost of revenue:			
Product	5,690	14,467	28,912
Subscription and services	1,590	3,163	18,853
Total cost of revenue	7,280	17,630	47,765
Total gross profit	26,378	65,686	113,787
Operating expenses:			
Research and development	7,275	16,522	66,036
Sales and marketing	30,389	67,562	167,466
General and administrative	4,428	15,221	52,503
Total operating expenses	42,092	99,305	286,005
Operating loss	(15,714)	(33,619)	(172,218)
Interest income	3	7	68
Interest expense	(194)	(537)	(525)
Other expense, net	(806)	(2,572)	(7,257)
Loss before income taxes	(16,711)	(36,721)	(179,932)
Provision for (benefit from) income taxes	71	(965)	(59,297)
Net loss attributable to common stockholders	$ (16,782)	$ (35,756)	$ (120,635)

Table of Contents

	Year Ended December 31,		
	2011	2012	2013
	(As a percentage of total revenue)		
Revenue:			
Product	74%	63%	55%
Subscription and services	26	37	45
Total revenue	100	100	100
Cost of revenue:			
Product	17	17	18
Subscription and services	5	4	12
Total cost of revenue	22	21	30
Total gross profit	78	79	70
Operating expenses:			
Research and development	22	20	41
Sales and marketing	90	81	104
General and administrative	13	18	32
Total operating expenses	125	119	177
Operating loss	(47)	(40)	(107)
Interest income			
Interest expense	(1)	(1)	
Other expense, net	(2)	(3)	(4)
Loss before income taxes	(50)	(44)	(111)
Provision for (benefit from) income taxes		(1)	(36)
Net loss attributable to common stockholders	(50)%	(43)%	(75)%

Comparison of the Years Ended December 31, 2012 and 2013

Revenue

	Year Ended December 31,					
	2012		2013		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Revenue:						
Product	$ 52,265	63%	$ 88,253	55%	$ 35,988	69%
Subscription and services	31,051	37%	73,299	45%	42,248	136%
Total revenue	$ 83,316	100%	$ 161,552	100%	$ 78,236	94%
Revenue by geographic region:						
United States	$ 66,556	80%	$ 116,730	72%	$ 50,174	75%
EMEA	6,628	8%	22,845	14%	16,217	245%

APAC	6,488	8%	16,004	10%	9,516	147%
Other	3,644	4%	5,973	4%	2,329	64%
Total revenue	$ 83,316	100%	$ 161,552	100%	$ 78,236	94%

Table of Contents

Total revenue increased by $78.2 million, or 94%, during the year ended December 31, 2013 compared to the year ended December 31, 2012. The increase in product revenue was primarily driven by growth in our installed base of customers, which grew from 927 as of December 31, 2012 to 1,964 as of December 31, 2013, as well as follow-on purchases from customers expanding their initial deployments of our product portfolio. Our Web Threat Prevention product continued to account for the largest portion of our product revenue as customers that purchase our product portfolio generally purchase more Web Threat Prevention appliances than Email Threat Prevention or File Threat Prevention appliances, reflecting the fact that their networks typically have more Web entry points than email or file entry points to protect. In addition, revenue associated with our Web Threat Prevention product is recognized upon shipment whereas revenue associated with our Email Threat Prevention product is recognized ratably over the longer of the contractual term or the estimated period the customer is expected to benefit from the product.

Revenue from the amortization of deferred subscription and services revenue related to initial customer purchases was $25.1 million and $55.3 million for the years ended December 31, 2012 and 2013, respectively. Revenue from the amortization of deferred subscription and services revenue related to renewals was $6.0 million and $18.0 million for the years ended December 31, 2012 and 2013, respectively. Given our high renewal rate and increasing base of customers, we expect revenue from the amortization of deferred subscription and services revenue related to renewals to increase as a percentage of our total revenue from deferred subscription and services revenue. Our renewal rate for subscription and services agreements expiring in the 12 months ended December 31, 2013 was in excess of 90%.

International revenue increased $28.1 million, or 167%, during the year ended December 31, 2013 compared to the year ended December 31, 2012, which reflects our increasing presence in international markets.

Cost of Revenue and Gross Margin

	Year Ended December 31,				
	2012		2013		Change
	Amount	Gross Margin	Amount	Gross Margin	Amount
	(Dollars in thousands)				
Cost of revenue:					
Product	$ 14,467		$ 28,912		$ 14,445
Subscription and services	3,163		18,853		15,690
Total cost of revenue	$ 17,630		$ 47,765		$ 30,135
Gross margin:					
Product		72%		67%	
Subscription and services		90%		74%	
Total gross margin		79%		70%	

Total cost of revenue increased $30.1 million, or 171%, during the year ended December 31, 2013 compared to the year ended December 31, 2012. The increase in cost of product revenue was driven primarily by an increase in product revenue and an increase in personnel costs in our manufacturing operations department as we continue to add capacity and build out our global supply chain. The increase in cost of subscription and services revenue was driven primarily by increased personnel costs in customer support.

Gross margin decreased for the year ended December 31, 2013 compared to the year ended December 31, 2012. The decrease in product gross margin was driven primarily by our increased investment in our manufacturing operations to increase capacity. The decrease in subscription and services gross margin was due primarily to an increase in our investment in customer support personnel and infrastructure.

66

Table of Contents

Operating Expenses

	Year Ended December 31,					
	2012		2013		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Operating expenses:						
Research and development	$ 16,522	20%	$ 66,036	41%	$ 49,514	300%
Sales and marketing	67,562	81	167,466	104	99,904	148
General and administrative	15,221	18	52,503	32	37,282	245
Total operating expenses	$ 99,305	119%	$ 286,005	177%	$ 186,700	188%
Includes stock-based compensation expense of:						
Research and development	$ 1,465		$ 6,958			
Sales and marketing	1,672		10,748			
General and administrative	3,536		8,342			
Total	$ 6,673		$ 26,048			

Research and Development

Research and development expense increased $49.5 million, or 300%, during the year ended December 31, 2013 compared to the year ended December 31, 2012, primarily due to a $24.3 million increase in personnel costs and a $1.3 million increase in related consulting costs as we increased our headcount and consultants to support continued investment in our future product and service offerings, and a $2.9 million increase in nonrecurring engineering activities. Additionally, overhead allocations and depreciation related to capital expenditures for departmental expansion increased by $18.6 million during the year ended December 31, 2013.

Sales and Marketing

Sales and marketing expense increased $99.9 million, or 148%, during the year ended December 31, 2013 compared to the year ended December 31, 2012, primarily due to a $56.9 million increase in personnel costs of which $13.2 million related to increased commissions for higher headcount and billings, a $4.7 million increase in depreciation expense, a $1.1 million increase in recruiting expenses related to new hires, a $6.8 million increase in travel-related costs and a $2.6 million increase in marketing activity, primarily related to an increase in lead generation services and costs associated with trade shows and conventions, Website development and partner programs. The change was also attributable to a $2.0 million increase in consulting costs and a $23.8 million increase in overhead allocations driven by the increase in sales and marketing personnel.

General and Administrative

General and administrative expense increased $37.3 million, or 245%, during the year ended December 31, 2013 compared to the year ended December 31, 2012, primarily due to a $14.3 million increase in personnel costs, a $13.1 million increase in professional services, including legal, accounting and recruiting services, and a $0.8 million increase in consulting costs. The change was also attributable to a $5.6 million increase in overhead allocations associated with departmental expansion. The increase in personnel costs, professional services and consulting costs was primarily a result of growth in our operations and our preparations to operate as a public company.

Table of Contents

Interest Income

	Year Ended December 31,		Change	
	2012	2013	Amount	%
	(Dollars in thousands)			
Interest income	$ 7	$ 68	$ 61	871%

The change in interest income resulted from the significant increase in the average balances in cash and cash equivalents during the year ended December 31, 2013 compared to the year ended December 31, 2012.

Interest Expense

	Year Ended December 31,		Change	
	2012	2013	Amount	%
	(Dollars in thousands)			
Interest expense	$ (537)	$ (525)	$ 12	(2)%

The decrease in interest expense resulted from decreased bank borrowings during the year ended December 31, 2013 compared to the year ended December 31, 2012.

Other Expense, Net

	Year Ended December 31,		Change	
	2012	2013	Amount	%
	(Dollars in thousands)			
Other expense, net	$ (2,572)	$ (7,257)	$ (4,685)	182%

The change in other expense, net was primarily due to an increase in the estimated fair value of preferred stock warrant liability during the year ended December 31, 2013 compared to the year ended December 31, 2012. At the time of our IPO, our preferred stock warrants were converted into common stock warrants, and the warrant liability was reclassified to stockholders equity. We will not incur expenses related to these warrants in future periods.

Provision for (Benefit from) Income Taxes

	Year Ended December 31,	
	2012	2013

		(Dollars in thousands)
Provision for (benefit from) income taxes	$ (965)	$ (59,297)
Effective tax rate	3%	33%

The increase in our tax benefit from income taxes during the year ended December 31, 2013 is primarily due to the release of the valuation allowance on the majority of U.S. deferred tax assets resulting from recording a deferred tax liability on acquisition related intangibles for which no tax benefit will be derived, partially offset by different tax rates in foreign jurisdictions. The tax benefit for the year ended December 31, 2012 is primarily due to a reduction of the valuation allowance for U.S. deferred tax assets resulting from recording a deferred tax liability on acquisition related intangibles for which no tax benefit will be derived, partially offset by an increase in pre-tax income related to international operations.

Table of Contents

Comparison of the Years Ended December 31, 2011 and 2012

Revenue

	Year Ended December 31,					
	2011		2012		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Revenue:						
Product	$ 24,888	74%	$ 52,265	63%	$ 27,377	110%
Subscription and services	8,770	26	31,051	37	22,281	254%
Total revenue	$ 33,658	100%	$ 83,316	100%	$ 49,658	148%
Revenue by geographic region:						
United States	$ 30,050	89%	$ 66,556	80%	$ 36,506	121%
EMEA	1,129	3	6,628	8	5,499	487%
APAC	1,142	4	6,488	8	5,346	468%
Other	1,337	4	3,644	4	2,307	173%
Total revenue	$ 33,658	100%	$ 83,316	100%	$ 49,658	148%

Total revenue increased by $49.7 million, or 148%, during the year ended December 31, 2012 compared to the year ended December 31, 2011. The increase in product revenue was primarily driven by growth in our installed base of customers, which grew from 485 as of December 31, 2011 to 927 as of December 31, 2012, as well as follow-on purchases from customers expanding their initial deployments of our product portfolio. Revenue from our Web Threat Prevention product accounted for the largest portion of our product revenue.

Revenue from the amortization of deferred subscription and services revenue related to initial customer purchases was $7.6 million and $25.1 million for the years ended December 31, 2011 and 2012, respectively. Revenue from the amortization of deferred subscription and services revenue related to renewals was $1.2 million and $6.0 million for the years ended December 31, 2011 and 2012, respectively. Our renewal rate for subscription and services agreements that expired in 2011 and 2012 was in excess of 90%. Finally, international revenue increased $13.2 million, or 365%, from 2011 to 2012 as we began to see a return on our investment in increasing our international market presence.

Cost of Revenue and Gross Margin

	Year Ended December 31,				
	2011		2012		Change
	Amount	Gross Margin	Amount	Gross Margin	Amount
	(Dollars in thousands)				
Cost of revenue:					
Product	$ 5,690		$ 14,467		$ 8,777
Subscription and services	1,590		3,163		1,573

Total cost of revenue	$ 7,280	$ 17,630	$ 10,350
Gross margin:			
Product	77%	72%	
Subscription and services	82%	90%	
Total gross margin	78%	79%	

Table of Contents

Total cost of revenue increased $10.4 million, or 142%, during the year ended December 31, 2012 compared to the year ended December 31, 2011. The increase in cost of product revenue was driven primarily by an increase in product revenue and an increase in personnel costs in our manufacturing operations department. The increase in cost of subscription and services revenue was driven primarily by increased personnel costs in customer support. The decrease in product gross margin was driven by our increased investment in our manufacturing operations department. The increase in subscription and services gross margin was due to the growth of our product, subscription and services revenue, partially offset by an increase in our investment in customer support personnel and infrastructure.

Operating Expenses

	Year Ended December 31,					
	2011		2012		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Operating expenses:						
Research and development	$ 7,275	22%	$ 16,522	20%	$ 9,247	127%
Sales and marketing	30,389	90	67,562	81	37,173	122%
General and administrative	4,428	13	15,221	18	10,793	244%
Total operating expenses	$ 42,092	125%	$ 99,305	119%	$ 57,213	136%
Includes stock-based compensation expense of:						
Research and development	$ 148		$ 1,465		$ 1,317	
Sales and marketing	360		1,672		1,312	
General and administrative	168		3,536		3,368	
Total	$ 676		$ 6,673		$ 5,997	

Research and Development

Research and development expense increased $9.2 million, or 127%, during the year ended December 31, 2012 compared to the year ended December 31, 2011, primarily due to a $6.1 million increase in personnel costs and a $0.6 million increase in consulting costs as we increased our headcount and consultants to support continued investment in our future product and service offerings. Additionally, overhead allocations and depreciation related to capital expenditures for departmental expansion increased by $1.7 million during the year ended December 31, 2012.

Sales and Marketing

Sales and marketing expense increased $37.2 million, or 122%, during the year ended December 31, 2012 compared to the year ended December 31, 2011, primarily due to a $20.7 million increase in personnel costs attributable to increased headcount and higher commissions, a $2.0 million increase in depreciation expense and costs associated with shipping evaluation units, a $0.8 million increase in consulting costs and a $3.5 million increase in marketing activity, primarily related to an increase in lead generation services and costs associated with trade shows and conventions, Website development and partner programs. The change was also attributable to a $2.8 million increase in travel-related costs and a $5.0 million increase in overhead allocations associated with additional sales and marketing personnel.

70

Table of Contents

General and Administrative

General and administrative expense increased $10.8 million, or 244%, during the year ended December 31, 2012 compared to the year ended December 31, 2011, primarily due to a $5.5 million increase in personnel costs, a $1.4 million increase in consulting costs and a $2.6 million increase in professional services, including legal, accounting and recruiting services. The change was also attributable to a $1.1 million increase in overhead allocations associated with departmental expansion.

Interest Income

	Year Ended December 31,		Change	
	2011	2012	Amount	%
	(Dollars in thousands)			
Interest income	$ 3	$ 7	$ 4	133%

The increase in interest income resulted from higher average balances in cash and cash equivalents during the year ended December 31, 2012 compared to the year ended December 31, 2011.

Interest Expense

	Year Ended December 31,		Change	
	2011	2012	Amount	%
	(Dollars in thousands)			
Interest expense	$ (194)	$ (537)	$ 343	177%

The increase in interest expense resulted from increased bank borrowings during the year ended December 31, 2012 compared to the year ended December 31, 2011.

Other Expense, Net

	Year Ended December 31,		Change	
	2011	2012	Amount	%
	(Dollars in thousands)			
Other expense, net	$ (806)	$ (2,572)	$ 1,766	219%

The change in other expense, net was due to an increase in fair value of preferred stock warrant liability during the year ended December 31, 2012 compared to the year ended December 31, 2011. Upon the completion of our initial public offering, the liability was reclassified to stockholders equity, at which time it was no longer subject to fair value accounting.

Provision for (Benefit from) Income Taxes

	Year Ended December 31,	
	2011	2012
	(Dollars in thousands)	
Provision for (benefit from) income taxes	$ 71	$ (965)
Effective tax rate	0%	3%

The increase in provision for (benefit from) income taxes during the year ended December 31, 2012 compared to the year ended December 31, 2011 was primarily due to a reduction in the valuation allowance resulting from recording a deferred tax liability on acquisition related intangibles for which no tax benefit will be derived partially offset by an increase in pre-tax income related to international operations.

Table of Contents

Quarterly Results of Operations

The following tables set forth selected unaudited quarterly consolidated statements of operations data for each of the eight quarters in the period ended December 31, 2013, as well as the percentage that each line item represents of total revenue for each quarter. The information for each of these quarters has been prepared on the same basis as the audited annual consolidated financial statements included elsewhere in this prospectus and, in the opinion of management, includes all adjustments of a normal, recurring nature that are necessary for the fair presentation of the results of operations for these periods in accordance with generally accepted accounting principles in the United States. This data should be read in conjunction with our audited consolidated financial statements and related notes included elsewhere in this prospectus. These quarterly operating results are not necessarily indicative of our operating results for any future period.

	Three Months Ended							
	Mar. 31, 2012	Jun. 30, 2012	Sept. 30, 2012	Dec. 31, 2012	Mar. 31, 2013	Jun. 30, 2013	Sep. 30, 2013	Dec. 31, 2013
	(In thousands)							
Revenue:								
Product	$ 8,550	$ 9,651	$ 13,754	$ 20,310	$ 14,988	$ 17,240	$ 23,729	$ 32,296
Subscription and services	5,256	6,284	8,142	11,369	13,428	15,982	18,923	24,966
Total revenue	13,806	15,935	21,896	31,679	28,416	33,222	42,652	57,262
Cost of revenue:								
Product	2,319	3,268	3,813	5,067	4,962	5,804	7,358	10,788
Subscription and services	599	680	904	980	1,920	4,482	6,079	6,372
Total cost of revenue	2,918	3,948	4,717	6,047	6,882	10,286	13,437	17,160
Total gross profit	10,888	11,987	17,179	25,632	21,534	22,936	29,215	40,102
Operating expenses:								
Research and development	2,489	3,134	4,191	6,708	10,062	14,016	20,492	21,466
Sales and marketing	11,824	14,230	16,734	24,774	28,569	37,594	44,414	56,889
General and administrative	1,884	2,826	4,188	6,323	7,311	10,370	11,704	23,118
Total operating expenses	16,197	20,190	25,113	37,805	45,942	61,980	76,610	101,473
Operating loss	(5,309)	(8,203)	(7,934)	(12,173)	(24,408)	(39,044)	(47,395)	(61,371)
Interest income	2	1	2	2	4	48	1	15
Interest expense	(82)	(128)	(167)	(160)	(144)	(132)	(243)	(6)
Other expense, net	(210)	(339)	(699)	(1,324)	(2,200)	(723)	(4,206)	(128)
Loss before income taxes	(5,599)	(8,669)	(8,798)	(13,655)	(26,748)	(39,851)	(51,843)	(61,490)
Provision for (benefit from) income taxes	26	34	54	(1,079)	213	384	(917)	(58,977)
Net loss attributable to common stockholders	$ (5,625)	$ (8,703)	$ (8,852)	$ (12,576)	$ (26,961)	$ (40,235)	$ (50,926)	$ (2,513)

Table of Contents

	Three Months Ended							
	Mar. 31, 2012	Jun. 30, 2012	Sept. 30, 2012	Dec. 31, 2012	Mar. 31, 2013	Jun. 30, 2013	Sep. 30, 2013	Dec. 31, 2013
	(as a percentage of revenue)							
Revenue:								
Product	62%	61%	63%	64%	53%	52%	56%	56%
Subscription and services	38%	39%	37%	36%	47%	48%	44%	44%
Total revenue	100%	100%	100%	100%	100%	100%	100%	100%
Cost of revenue:								
Product	17%	21%	18%	16%	17%	17%	17%	19%
Subscription and services	4%	4%	4%	3%	7%	14%	14%	11%
Total cost of revenue	21%	25%	22%	19%	24%	31%	31%	30%
Total gross profit	79%	75%	78%	81%	76%	69%	69%	70%
Operating expenses:								
Research and development	18%	20%	19%	21%	35%	42%	48%	38%
Sales and marketing	85%	89%	76%	78%	101%	113%	104%	99%
General and administrative	14%	18%	20%	20%	26%	32%	27%	40%
Total operating expenses	117%	127%	115%	119%	162%	187%	179%	177%
Operating loss	(38)%	(51)%	(36)%	(38)%	(86)%	(118)%	(110)%	(107)%
Interest income	%	%	%	%	%	%	%	%
Interest expense	(1)%	(1)%	(1)%	(1)%	%	%	(1)%	%
Other expense, net	(2)%	(2)%	(3)%	(4)%	(8)%	(2)%	(10)%	%
Loss before income taxes	(41)%	(54)%	(40)%	(43)%	(94)%	(120)%	(121)%	(107)%
Provision for (benefit from) income taxes	%	1%	%	(4)%	1%	1%	(2)%	(103)%
Net loss attributable to common stockholders	(41)%	(55)%	(40)%	(39)%	(95)%	(121)%	(119)%	(4)%

Quarterly Revenue Trends

Our quarterly revenue increased year-over-year for all periods presented due to increased sales to new customers, as well as upsells to existing customers. Comparisons of our year-over-year total quarterly revenue are more meaningful than comparisons of our sequential results due to seasonality in the sale of our products and subscriptions and services. Our fourth quarter has historically been our strongest quarter for sales as a result of large enterprise buying patterns. While we believe that these seasonal trends have affected and will continue to affect our quarterly results, our rapid growth has largely masked seasonal trends to date. We believe that our business may become more seasonal in the future. Historical patterns in our business may not be a reliable indicator of our future sales activity or performance.

Quarterly Gross Margin Trends

Total gross profit increased year-over-year for all periods presented. Total gross margin has remained relatively consistent over all periods presented, and any fluctuation is primarily due to shifts in the mix of sales between products and subscriptions and services, as well as the types and volumes of products sold. For the three months ended June 30, 2013, September 30, 2013 and December 31, 2013, gross margin declined year-over-year primarily due to an increase in cost of subscription and services revenue relating to increased personnel costs in customer support.

Quarterly Expense Trends

Total operating expenses increased year-over-year for all periods presented primarily due to the addition of personnel in connection with the expansion of our business. Research and development expense increased sequentially over the periods as we increased our headcount to support continued investment in our future product and subscription and services offerings. Sales and marketing expense increased significantly in the three months ended December 31, 2012 compared to the three months ended September 30, 2012, primarily due to an

Table of Contents

increase in personnel costs related to increases in headcount, higher commission expense related to higher sales, and higher stock-based compensation expense. Sales and marketing expense increased significantly in both the three months ended June 30, 2013 and September 30, 2013 compared to the three months ended March 31, 2013, primarily due to an increase in personnel costs related to increases in headcount, higher commission expense related to higher sales, higher stock-based compensation expense and an increase in overhead allocations associated with additional sales and marketing personnel. General and administrative expense increased significantly in the three months ended December 31, 2012 compared to the three months ended September 30, 2012, in both the three months ended June 30, 2013 and September 30, 2013 compared to the three months ended March 31, 2013, primarily due to an increase in personnel, legal expense and higher professional services fees for preparing to be a public company. In the three months ended December 31, 2013 compared to the three months ended September 30, 2013, general and administrative expenses increased primarily due to approximately $8.5 million of expenses incurred in connection with the acquisition of Mandiant and increases in stock compensation expense. For the three months ended December 31, 2012, we recorded a benefit for income taxes due to a reduction in the valuation allowance resulting from recording a deferred tax liability on acquisition-related intangibles for which no tax benefit will be derived, partially offset by an increase in pre-tax income related to international operations.

Liquidity and Capital Resources

	As of December 31,		
	2011	2012	2013
		(In thousands)	
Cash and cash equivalents	$ 10,676	$ 60,200	$ 173,918

	Year Ended December 31,		
	2011	2012	2013
		(In thousands)	
Cash provided by (used in) operating activities	$ 5,111	$ 21,500	$ (69,762)
Cash used in investing activities	(5,224)	(20,215)	(148,469)
Cash provided by financing activities	3,124	48,239	331,949
Net increase in cash and cash equivalents	$ 3,011	$ 49,524	$ 113,718

As of December 31, 2013, our cash and cash equivalents of $173.9 million were held for working capital, capital expenditures, investment in technology and business acquisition purposes, of which approximately $16.0 million was held outside of the United States and is not presently available to fund domestic operations and obligations. If we were to repatriate cash held outside of the United States, it could be subject to U.S. income taxes, less any previously paid foreign income taxes. We have no current plans to repatriate this cash.

In June 2010, we entered into a loan agreement that provides for: (i) a revolving line of credit facility, (ii) an equipment facility and (iii) a term loan. In addition, this loan agreement was amended and restated in August 2011 to provide for additional borrowings under a growth facility. As of December 31, 2013, we had no outstanding borrowings under the revolving line of credit. The line of credit carries a floating interest rate equal to prime plus 1.5%, and borrowings under the line of credit are collateralized by all of our assets, excluding intellectual property. The availability of borrowings under the line of credit are subject to certain borrowing base limitations on our outstanding accounts receivable. As of December 31, 2013, amounts available under the line of credit amounted to $25.0 million. These amounts have a maturity date of December 31, 2014. In October 2013, we repaid the outstanding balance of $20.0 million.

Prior to our initial public offering, or IPO, in September 2013, we financed our operations primarily through private sales of equity securities and, to a lesser extent, proceeds from our bank facility and cash generated from

operations. In September 2013, we completed our IPO pursuant to which we sold 17,450,000 shares of our common stock (inclusive of 2,275,000 shares of common stock from the exercise of the over-allotment option granted to the underwriters) at a public offering price of $20.00 per share, resulting in net proceeds of $321.0 million, after underwriting discounts and commissions and offering expenses.

On December 30, 2013, we acquired privately held Mandiant, a leading provider of advanced endpoint security products and security incident response management solutions. We believe this combination creates the industry s leading advanced threat protection vendor with the ability to find and stop attacks at every stage of the attack life cycle. Under the terms of the merger agreement governing the transaction, we delivered to the former security holders of Mandiant merger consideration with an aggregate value equal to approximately $1,020.3 million, consisting of approximately $106.5 million in net cash and an aggregate of 21.5 million shares and options to purchase shares of our common stock.

We believe that our existing cash and cash equivalents will be sufficient to meet our anticipated cash needs for at least the next 12 months. Our future capital requirements will depend on many factors, including our growth rate, the timing and extent of spending to support development efforts, the expansion of sales and marketing activities, the introduction of new and enhanced product and service offerings, and the continuing market acceptance of our products. In the event that additional financing is required from outside sources, we may not be able to raise such financing on terms acceptable to us or at all. If we are unable to raise additional capital when desired, our business, operating results, and financial condition would be adversely affected.

Operating Activities

During the year ended December 31, 2013, operating activities used $69.8 million in cash as a result of a net loss of $120.6 million, adjusted by non-cash charges of $4.8 million and a net increase of $55.6 million in our net operating assets and liabilities. The net increase in our net operating assets and liabilities was primarily the result of a $95.0 million increase in deferred revenue as a result of increases in sales of subscriptions and support and maintenance services, a $11.5 million increase in accounts payable due to growth in our business and a $19.4 million increase in accrued compensation as a result of the growth in our headcount. This increase was partially offset by increases of $35.1 million in accounts receivable and $15.6 million in prepaid expenses, a $18.5 million decrease in accrued liabilities due to payment of Mandiant transaction costs, and a $3.1 million increase in inventory primarily driven by a large purchase of appliances from our legacy contract manufacturer to build our service inventory as we transitioned to a new contract manufacturer.

During the year ended December 31, 2012, operating activities provided $21.5 million in cash as a result of a net loss of $35.8 million, adjusted by non-cash charges of $15.3 million and a net increase of $42.0 million in our net operating assets and liabilities. The net increase in our net operating assets and liabilities was primarily the result of a $46.3 million increase in deferred revenue as a result of increases in sales of subscriptions and support and maintenance services and a $6.2 million increase in accounts payable due to the growth in our business and a $3.2 million increase in accrued compensation as a result of the growth in our headcount. This increase was partially offset by a $10.1 million increase in accounts receivable due to an increase in sales and a $3.1 million increase in prepaid expenses and other assets.

During the year ended December 31, 2011, operating activities provided $5.1 million in cash, primarily as a result of a net loss of $16.8 million, adjusted by non-cash charges of $5.0 million and a net increase of $16.9 million in our net operating assets and liabilities. The net change in our operating assets and liabilities was primarily the result of a $23.8 million increase in deferred revenue as a result of increases in sales of subscriptions and support and maintenance services and, to a lesser extent, increases in accounts payable and accrued compensation. This increase was partially offset by a $13.5 million increase in accounts receivable due to an increase in sales.

Table of Contents

Investing Activities

Cash used in investing activities during the year ended December 31, 2013 was $148.5 million, primarily resulting from the acquisition of Mandiant and from capital expenditures to purchase property and equipment and demonstration units. Cash used in investing activities during the years ended December 31, 2012 and 2011 was $20.2 million and $5.2 million, respectively, primarily resulting from capital expenditures to purchase property and equipment and demonstration units.

Financing Activities

During the year ended December 31, 2013, financing activities provided $331.9 million in cash, primarily from net proceeds of $321.0 million from our IPO, $10.0 million from the issuance of convertible preferred stock, additional borrowings of $10.0 million under our line of credit, proceeds of $7.3 million from the collection of notes receivable from stockholders as of December 31, 2012 and proceeds of $5.4 million from exercises of stock options, partially offset by payments of $22.2 million on bank borrowings.

During the year ended December 31, 2012, financing activities provided $48.2 million in cash, primarily from issuance of convertible preferred stock and proceeds from bank borrowings.

During the year ended December 31, 2011, financing activities provided $3.1 million in cash, primarily from proceeds from bank borrowings, partially offset by payments on bank borrowings.

Contractual Obligations and Commitments

The following summarizes our contractual obligations and commitments as of December 31, 2013:

	Payments Due by Period				
	Total	Less Than 1 Year	1 - 3 Years	3 - 5 Years	More Than 5 Years
			(In thousands)		
Operating leases	$ 40,436	$ 8,283	$ 14,210	$ 8,184	$ 9,759
Purchase obligations	5,957	2,289	3,668		
Contract manufacturer commitments	16,650	16,650			
Total	$ 63,043	$ 27,222	$ 17,878	$ 8,184	$ 9,759

Due to the uncertainty with respect to the timing of future cash flows associated with our unrecognized tax benefits as of December 31, 2013, we are unable to make reasonably reliable estimates of the period of cash settlement with the respective taxing authorities. Therefore, approximately $0.8 million of unrecognized tax benefits classified as Other long-term liabilities in the accompanying consolidated balance sheet as of December 31, 2013, have been excluded from the contractual obligations table above. In addition, we are unable to make reasonably reliable

estimates with respect to approximately $45 million in noncurrent deferred tax liabilities and have therefore excluded such liabilities from the table above. See Note 12 of our consolidated financial statements for a discussion of our income tax liabilities.

Off-Balance Sheet Arrangements

As of December 31, 2012 and December 31, 2013, we did not have any relationships with unconsolidated entities or financial partnerships, such as structured finance or special purpose entities, that were established for the purpose of facilitating off-balance sheet arrangements or other purposes.

Segment Information

We have one primary business activity and operate in one reportable segment.

Table of Contents

Quantitative and Qualitative Disclosures about Market Risk

Foreign Currency Exchange Risk

Our sales contracts are primarily denominated in U.S. dollars. A portion of our operating expenses are incurred outside the United States and are denominated in foreign currencies and are subject to fluctuations due to changes in foreign currency exchange rates, particularly changes in the Indian Rupee, British Pound Sterling, Japanese Yen and Euro. Additionally, fluctuations in foreign currency exchange rates may cause us to recognize transaction gains and losses in our statement of operations. The effect of a hypothetical 10% adverse change in foreign exchange rates on monetary assets and liabilities at December 31, 2013 would not be material to our financial condition or results of operations. To date, foreign currency transaction gains and losses and exchange rate fluctuations have not been material to our financial statements, and we have not engaged in any foreign currency hedging transactions.

As our international operations grow, our risks associated with fluctuation in currency rates will become greater, and we will continue to reassess our approach to managing this risk. In addition, currency fluctuations or a weakening U.S. dollar can increase the costs of our international expansion.

Interest Rate Risk

We had cash and cash equivalents of $60.2 million and $173.9 million as of December 31, 2012 and 2013, respectively, consisting of bank deposits and money market funds. Such interest-earning instruments carry a degree of interest rate risk. To date, fluctuations in interest income have not been significant. We also had total outstanding debt of $12.1 million as of December 31, 2012, of which $1.2 million was due within 12 months. As of December 31, 2013, we had no outstanding debt. The debt outstanding prior to the fourth quarter of 2013 related to an outstanding line of credit in the amount of $20.0 million, which was repaid in October 2013. The line of credit remains available to draw upon and carries a variable interest rate equal to the prime rate plus 1.5% and is available through December 31, 2014.

We do not enter into investments for trading or speculative purposes and have not used any derivative financial instruments to manage our interest rate risk exposure. We have not been exposed to, nor do we anticipate being exposed to, material risks due to changes in interest rates. The interest rate on a significant majority of our outstanding debt is variable, which also reduces our exposure to these interest rate risks. A hypothetical 10% change in interest rates during any of the periods presented would not have had a material impact on our financial statements.

Concentration

Accuvant, one of our resellers, accounted for approximately 10% of our revenue for the year ended December 31, 2012. For the year ended December 31, 2013, Accuvant and Carahsoft, two of our resellers, accounted for approximately 11% and 11% of our revenue, respectively. Our agreements with these resellers were made in the ordinary course of our business and may be terminated with or without cause by either party with advance notice. Although we believe we would experience some short-term disruption in the distribution of our products, subscriptions and services if these agreements were terminated, we believe such termination would not have a material adverse effect on our financial results and that alternative resellers and other channel partners exist to deliver our products to our end-customers.

Critical Accounting Policies and Estimates

Our consolidated financial statements have been prepared in accordance with U.S. generally accepted accounting principles. The preparation of these consolidated financial statements requires us to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenue, expenses, and related disclosures.

Table of Contents

We base our estimates on historical experience and on various other assumptions that we believe are reasonable under the circumstances. We evaluate our estimates and assumptions on an ongoing basis. Actual results may differ from these estimates. To the extent that there are material differences between these estimates and our actual results, our future financial statements will be affected.

The critical accounting policies requiring estimates, assumptions, and judgments that we believe have the most significant impact on our consolidated financial statements are described below.

Revenue Recognition

We generate revenue from the sales of products, subscriptions, support and maintenance and other services, primarily through our indirect relationships with our partners as well as end customers through a direct sales force. Our products include operating system software that is integrated into the appliance hardware and is deemed essential to its functionality. As a result, we account for revenue in accordance with ASC 605 and all related interpretations as all our security appliance deliverables include proprietary operating system software, which together deliver the essential functionality of our products.

Revenue is recognized when all of the following criteria are met:

Persuasive Evidence of an Arrangement Exists. We rely upon non-cancelable sales agreements and purchase orders to determine the existence of an arrangement.

Delivery has Occurred. We use shipping documents or receipt of transmissions of service contract registration codes to verify delivery.

The Fee is Fixed or Determinable. We assess whether the fee is fixed or determinable based on the payment terms associated with the transaction.

Collectability is Reasonably Assured. We assess collectability based on credit analysis and payment history.

Our products include three principal security product families that address critical vectors of attack, including Web, email and file shares. Our Web Threat Prevention, File Threat Prevention, Forensic Analysis System and Central Management System appliances and subscription services qualify as separate units of accounting. Therefore, Web Threat Prevention, File Threat Prevention, Forensic Analysis System and Central Management System appliance product revenue is recognized at the time of shipment. However, unlike our Web Threat Prevention and File Threat Prevention appliances, our Email Threat Prevention appliance cannot function without the use of our Email Threat Prevention Attachment/URL Engine, which analyzes email attachments and URLs embedded in emails for next-generation threats. As such, our Email Threat Prevention and related services do not have stand-alone value and do not qualify as separate units of accounting. Therefore, Email Threat Prevention product revenue is recognized ratably over the longer of the contractual term of the subscription services or the estimated period the customer is expected to benefit from the product, provided that all other revenue recognition criteria have been met. Because we have only been selling our Email Threat Prevention since April 2011, we have a limited history with respect to subscription renewals for such product. As a result, revenue from all Email Threat Prevention products sold by us through December 31, 2013 has been recognized ratably over the contractual term of the subscription services. At the time of shipment, product revenue generally meets the criteria for fixed or determinable fees as our partners receive an order from an end-customer prior to placing an order with us. In addition, payment from our partners is not contingent on the partners collection from their end-customers. Our partners do not stock products and do not have any stock rotation rights. We recognize

subscription and support and maintenance services revenue ratably over the contractual service period, which is typically one or three years. Other services revenue is recognized as the services are rendered and has not been significant to date.

Most of our arrangements, other than renewals of subscriptions and support and maintenance services, are multiple-element arrangements with a combination of product, subscriptions, support and maintenance, and other services. For multiple-element arrangements, we allocate revenue to each unit of accounting based on an

estimated selling price at the arrangement inception. The estimated selling price for each element is based upon the following hierarchy: vendor-specific objective evidence, or VSOE, of selling price, if available, third-party evidence, or TPE, of selling price, if VSOE of selling price is not available, or best estimate of selling price, or BESP, if neither VSOE of selling price nor TPE of selling price are available. The total arrangement consideration is allocated to each separate unit of accounting using the relative estimated selling prices of each unit based on the aforementioned selling price hierarchy. We limit the amount of revenue recognized for delivered elements to an amount that is not contingent upon future delivery of additional products or services or meeting of any specified performance conditions.

To determine the estimated selling price in multiple-element arrangements, we establish VSOE of selling price using the prices charged for a deliverable when sold separately and, for subscriptions and support and maintenance, based on the renewal rates and discounts offered to partners. If VSOE of selling price cannot be established for a deliverable, we establish TPE of selling price by evaluating similar and interchangeable competitor products or services in standalone arrangements with similarly situated partners. However, as our products contain a significant element of proprietary technology and offer substantially different features and functionality from our competitors, we are unable to obtain comparable pricing of our competitors products with similar functionality on a stand-alone basis. Therefore, we have not been able to obtain reliable evidence of TPE of selling price. If neither VSOE nor TPE of selling price can be established for a deliverable, we establish BESP primarily based on historical transaction pricing. Historical transactions are segregated based on our pricing model and our go-to-market strategy, which include factors such as type of sales channel (reseller, distributor, or end-customer), the geographies in which our products and services were sold (domestic or international), offering type (products or services), and whether or not the opportunity was identified by our sales force or by our partners. In analyzing historical transaction pricing, we evaluate whether a majority of the prices charged for a product, as represented by a percentage of list price, fall within a reasonable range. To further support the BESP of selling price as determined by the historical transaction pricing or when such information is unavailable, such as when there are limited sales of a new product, we consider the same factors we have established through our pricing model and go-to-market strategy. The determination of BESP is made through consultation with and approval by our management.

Shipping charges billed to partners are included in revenue and related costs are included in cost of revenue. Sales commissions and other incremental costs to acquire contracts are also expensed as incurred. After receipt of a partner order, any amounts billed in excess of revenue recognized are recorded as deferred revenue.

Stock-Based Compensation

Compensation expense related to stock-based transactions, including employee and non-employee director stock options, is measured and recognized in the financial statements based on the fair value of the awards granted. The fair value of each option award is estimated on the grant date using the Black-Scholes option-pricing model and a single option award approach. Stock-based compensation expense is recognized, net of forfeitures, over the requisite service periods of the awards, which is generally four years.

Our use of the Black-Scholes option-pricing model requires the input of highly subjective assumptions, including the fair value of the underlying common stock, the expected term of the option, the expected volatility of the price of our common stock, risk-free interest rates, and the expected dividend yield of our common stock. The assumptions used in our option-pricing model represent management s best estimates. These estimates involve inherent uncertainties and the application of management s judgment. If factors change and different assumptions are used, our stock-based compensation expense could be materially different in the future.

These assumptions and estimates are as follows:

Fair Value of Common Stock. Because our common stock was not publicly traded until September 20, 2013, we were required to estimate the fair value of common stock for grants made prior to that date, as discussed in Common Stock Valuations below.

Table of Contents

Risk-Free Interest Rate. We base the risk-free interest rate used in the Black-Scholes option-pricing model on the implied yield available on U.S. Treasury zero-coupon issues with a remaining term equivalent to that of the options for each option group.

Expected Term. The expected term represents the period that our stock-based awards are expected to be outstanding. We base the expected term assumption on our historical exercise behavior combined with estimates of the post-vesting holding period.

Volatility. We determine the price volatility factor based on the historical volatilities of our publicly traded peer group as we do not have a trading history for our common stock. Industry peers consist of several public companies in the technology industry that are similar to us in size, stage of life cycle, and financial leverage. We used the same set of peer group companies in all the relevant valuation estimates. We did not rely on implied volatilities of traded options in our industry peers common stock because the volume of activity was relatively low. We intend to continue to consistently apply this process using the same or similar public companies until a sufficient amount of historical information regarding the volatility of our own common stock share price becomes available, or unless circumstances change such that the identified companies are no longer similar to us, in which case, more suitable companies whose share prices are publicly available would be utilized in the calculation.

Dividend Yield. The expected dividend assumption is based on our current expectations about our anticipated dividend policy. Consequently, we used an expected dividend yield of zero.

The following table summarizes the assumptions used in the Black-Scholes option-pricing model to determine the fair value of our stock options as follows:

	Year Ended December 31,					
	2011		2012		2013	
Fair value of common stock	$0.57	$1.65	$1.65	$5.44	$6.05	$42.37
Risk-free interest rate	1.0%	2.8%	0.2%	3.4%	0.6%	2.1%
Expected term (in years)	5	7	1	6	4	6
Volatility	51%	52%	49%	53%	46%	54%
Dividend yield	%		%		%	

In addition to the assumptions used in the Black-Scholes option-pricing model, we must also estimate a forfeiture rate to calculate the stock-based compensation expense for our awards. Our forfeiture rate is based on an analysis of our actual forfeitures. We will continue to evaluate the appropriateness of the forfeiture rate based on actual forfeiture experience, analysis of employee turnover, and other factors. Quarterly changes in the estimated forfeiture rate can have a significant impact on our stock-based compensation expense as the cumulative effect of adjusting the rate is recognized in the period the forfeiture estimate is changed. If a revised forfeiture rate is higher than the previously estimated forfeiture rate, an adjustment is made that will result in a decrease to the stock-based compensation expense recognized in the financial statements. If a revised forfeiture rate is lower than the previously estimated forfeiture rate, an adjustment is made that will result in an increase to the stock-based compensation expense recognized in the financial statements.

We estimate the fair value of the rights to acquire stock under our 2013 Employee Stock Purchase Plan (the ESPP) using the Black-Scholes option pricing formula. Our ESPP typically provides for consecutive twelve month offering periods and we use our peer group volatility data in the valuation of ESPP shares. We recognize such compensation expense on a straight-line basis over the employee s requisite service period

We account for the fair value of restricted stock units (RSUs) using the closing market price of our common stock on the date of grant. For new-hire grants, RSUs typically vest ratably on an annual basis over four years. For annual refresh grants, RSUs typically vest ratably on an annual basis over two to four years.

80

Table of Contents

We account for the fair value of performance stock units (PSUs) using the closing market price of our common stock on the date of grant. We recognize compensation expense when we concluded that it is probable that the performance conditions will be achieved. We will reassess the probability of vesting at each reporting period and adjust our compensation cost based on the probability assessment.

We will continue to use judgment in evaluating the assumptions related to our stock-based compensation on a prospective basis. As we continue to accumulate additional data related to our common stock, we may have refinements to our estimates, which could materially impact our future stock-based compensation expense.

Common Stock Valuations

We are required to estimate the fair value of the common stock underlying our stock-based awards when performing the fair value calculations with the Black-Scholes option-pricing model. Since the completion of our IPO in September 2013, we have determined the fair value our stock price based on the closing price at the date of grant. Prior to the IPO, the fair values of the common stock underlying our stock-based awards were determined by our board of directors, with input from management and third-party valuations. We believe that our board of directors has the relevant experience and expertise to determine the fair value of our common stock. As described below, the exercise price of our stock-based awards was determined by our board of directors based on the most recent contemporaneous third-party valuation as of the grant date. If awards were granted a short period of time preceding the date of a valuation report, we assessed the fair value used for financial reporting purposes after considering the fair value reflected in the subsequent valuation report and other facts and circumstances on the date of grant as discussed below. In such instances, the fair value that we used for financial reporting purposes generally exceeded the exercise price for those awards, although we believe that relying on the preceding valuation report was appropriate for tax purposes.

Prior to our IPO, given the absence of a public trading market for our common stock, and in accordance with the American Institute of Certified Public Accountants Practice Guide, Valuation of Privately-Held-Company Equity Securities Issued as Compensation, our board of directors exercised reasonable judgment and considered numerous objective and subjective factors to determine the best estimate of the fair value of our common stock, including:

- contemporaneous valuations performed by unrelated third-party specialists;
- the prices, rights, preferences, and privileges of our convertible preferred stock relative to those of our common stock;
- the lack of marketability of our common stock;
- our actual operating and financial performance;
- current business conditions and projections;
- our hiring of key personnel and the experience of our management;
- our history and the timing of the introduction of new products and services;

our stage of development;

the likelihood of achieving a liquidity event, such as an initial public offering or a merger or acquisition of our company given prevailing market conditions;

the illiquidity of stock-based awards involving securities in a private company;

the market performance of comparable publicly traded companies; and

the U.S. and global capital market conditions.

In valuing the common stock, the board of directors determined the fair value of our business, or Enterprise Value or EV, by taking a weighted combination of the value indications under an income approach, market approach and Probability Weighted Expected Return Method, or PWERM, approach.

Table of Contents

The income approach estimates the Enterprise Value based on the present value of future estimated cash flows. These future cash flows are discounted to their present values using a discount rate, which is derived from an analysis of the cost of capital of comparable publicly traded companies in the same industry or similar lines of business, or Guideline Companies, as of each valuation date. This weighted-average cost of capital discount rate, or WACC, is adjusted to reflect the risks inherent in the business. The WACC used for these valuations was determined to be reasonable and appropriate given our stage of development at the time of each respective valuation. The valuations performed during this period evaluated our business under the basis that it was initially in either the second or third stage of development as of the December 2011 valuation but moving forward toward the fourth or fifth stage of development in the March, April, May and June 2013 valuations. The income approach also assesses the residual value beyond the forecast period, or the Terminal Value, utilizing multiples from the Guideline Companies to our future revenue projections.

The market approaches were not always relied upon for these valuations. Specifically, the comparable companies market multiple approach and the comparable transactions market approach were not used in these valuations to determine an EV, but methods similar to these were used in the PWERM approach discussed further below. When applicable due to a recent preferred stock offering or a significant common stock repurchase, the prior sale of stock market approach was either assessed as a point of reference or actually utilized in the valuation. This approach involves examining any transactions involving the stock of the business being valued considering the following: the number of shares involved and the timing of the transaction with regard to the valuation date, the class of stock in the transaction, whether other considerations were involved and the participants in the transaction (i.e., related party or new investor), amongst others. Often this involves backing into an Enterprise Value based on the terms of the new financing or stock sale if performed at an arm s length and with new investors.

The PWERM approach estimates the Enterprise Value by evaluating the following multiples as a guide for determining an EV: (1) multiples of the Guideline Companies Enterprise Values compared to either last 12 months revenue or EBITDA, (2) multiples of the Enterprise Values of similar companies that had recently been acquired compared to either last 12 months revenue or EBITDA, or (3) multiples of the Enterprise Values of similar companies that had recently completed an IPO compared to either last 12 months revenue or net income.

The equity values determined by the various valuation approaches, if more than one was used, were then weighted to determine the aggregate equity value of our business. As we moved closer to our proposed initial public offering, the weighting towards the PWERM approach increased, generally resulting in an increase in the fair value of our common stock.

When considering which companies to include as our Guideline Companies, we focused on U.S. based companies in the information technology industry in which we operate. More specifically, we focused on companies that address components of the network security market and networking companies with similar business models of generating revenue from the sale of both products and services, companies with a market capitalization greater than $1 billion, companies with revenue growth rates generally greater than 10%, and companies with net income and positive cash flow from operating activities. In considering companies that had recently completed an initial public offering, we selected those companies with business models similar to ours. The Guideline Companies remained mostly unchanged for the valuations during 2012 and 2013.

In some cases, we considered the amount of time between the valuation date and the grant date to determine whether to use the latest common stock valuation determined pursuant to one of the methods described above or to use another value based on a straight-line calculation between two valuation dates. This determination included an evaluation of whether the subsequent valuation increase was the result of specific events recognized by the board that resulted in the increase during the interim period or whether the increase was due to less visible reasons such as general improvements in the business or changes in the valuation methodologies or components.

The Enterprise Value determined by the income and market approaches, excluding any PWERM valuations, were then allocated to the common stock using the option pricing method, or OPM. The OPM treats common

82

Table of Contents

stock and convertible preferred stock as call options on a business, with exercise prices based on the liquidation preference of the convertible preferred stock. Therefore, the common stock has value only if the funds available for distribution to the stockholders exceed the value of the liquidation preference at the time of a liquidity event such as a merger, sale or initial public offering, assuming the business has funds available to make a liquidation preference meaningful and collectible by the stockholders. The common stock is modeled to be a call option with a claim on the business at an exercise price equal to the remaining value immediately after the convertible preferred stock is liquidated. The OPM uses the Black-Scholes option-pricing model to price the call option. The OPM is appropriate to use when the range of possible future outcomes is so difficult to predict that forecasts would be highly speculative. The PWERM was considered but not used due to the uncertainty of the board s estimates of the probabilities for future potential liquidity events for the valuations as of December 31, 2011, June 30, 2012 and September 30, 2012. However, the PWERM was utilized for the December 31, 2012 and the March 31, April 30, May 31 and June 30, 2013 valuations.

In addition, we also considered an appropriate discount adjustment to recognize the lack of marketability within each valuation due to being a closely held entity.

Between April 1, 2012 and the date of this prospectus, we granted the following stock options:

Grant Date	Number of Awards Granted	Exercise Price	Fair Value Per Share of Common Stock
May 2012	3,726,611	$ 1.65	$ 2.21
June 2012	41,000	1.65	2.48
September 2012	1,307,850	2.48	3.66
November 2012	968,000	3.66	4.47
January 2013	3,570,844	5.44	6.05
February 2013	642,900	5.44	6.46
May 2013	3,058,900	7.93	8.73
May 2013	798,700	7.93	9.17
June 2013	1,295,450	9.68	10.21
July 2013	1,243,000	10.25	12.90
August 2013	952,500	13.00	14.67
September 2013	824,900	13.00	16.00
September 2013	367,000	20.00	20.00
October 2013	99,000	42.37	42.37
November 2013	121,100	38.86	38.86
December 2013	207,500	38.33	38.33
January 2014	314,900	73.57	73.57
February 2014	290,200	74.35	74.35

In addition to the stock options granted, we also granted 2,265,360, 69,632, 26,111, 23,711, 26,670, 240,000 and 5,000 shares of restricted common stock in May 2012, December 2012, May 2013, July 2013, August 2013, September 2013 and November 2013, respectively. In addition, we granted restricted stock units in January 2013, February 2013, August 2013, December 2013, February 2014 and March 2014, which are performance based and the underlying shares of common stock are subject to adjustment. In December 2013, February 2014 and March 2014, we also granted 9,350, 287,194 and 75,000 restricted stock units which are not performance based, respectively. Each of the restricted stock unit grants prior to our IPO is discussed in greater detail in the individual valuation discussions below.

Based upon the initial public offering price of $20.00 per share, the aggregate intrinsic value of options outstanding as of June 30, 2013 was approximately $332.1 million, of which $100.0 million related to vested options and approximately $232.1 million related to unvested options.

83

Table of Contents

We obtained independent third-party valuations, the results and timing of which were as follows:

Valuation Date (As of)	Fair Value Per Share of Common Stock
December 31, 2011	$ 1.65
June 30, 2012	2.48
September 30, 2012	3.66
December 31, 2012	5.44
March 31, 2013	7.93
April 30, 2013	8.63
May 31, 2013	9.68
June 30, 2013	10.25

The following discussion relates primarily to our determination of the fair value per share of our common stock for purposes of calculating stock-based compensation expenses since April 2012. No single event caused the valuation of our common stock to increase during this period. Instead, a combination of the factors described below in each period led to the changes in the fair value of our common stock. Notwithstanding the fair value reassessments described below, we believe we applied a reasonable valuation method to determine the stock option exercise prices on the respective stock option grant dates.

May and June 2012

We granted 3,726,611 stock options in May 2012. Our board of directors set an exercise price of $1.65 per share for these options based in part on a third-party valuation prepared as of December 31, 2011. In addition, we granted 2,265,360 shares of restricted common stock in May 2012 which, by definition, do not have an exercise price. When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we evaluated the two surrounding valuations prepared as of December 31, 2011 and June 30, 2012.

The December 31, 2011 contemporaneous valuation was prepared on a minority, non-marketable basis assuming our business was in the second or third stage of development. We considered our business to be in the second or third stage of development because our product development was generally complete, we were receiving feedback from our customers and sales growth was very strong. However, there was still significant risk associated with our business plan. This valuation was developed using the income approach, specifically a discounted cash flow analysis, to determine our EV. The discounted cash flow analysis was developed based on our forecast through 2014 and utilized a WACC of 35%, which was deemed appropriate considering our stage of development. For purposes of determining a Terminal Value, the valuation applied a multiple consistent with observed revenue multiples from our Guideline Companies. This calculated value was then discounted to present value using the same WACC to determine the final Terminal Value. The resulting equity value was then allocated to the common stock utilizing an OPM with the following assumptions: a time to a liquidity event of 2.25 years, risk-free rate of 0.3%, dividend yield of 0% and volatility of 50% over the time to a liquidity event. The fair value of our common stock, as determined by an OPM and after applying a marketability discount of 30%, was $1.65 per share as of December 31, 2011.

The June 30, 2012 contemporaneous valuation was prepared on a minority, non-marketable basis assuming our business was in the third stage of development. We considered our business to be in the third stage of development because our sales growth remained very strong and profitability was becoming seemingly more achievable, but there was still risk around operating in a competitive market that is subject to technological change with larger established competitors. This valuation was developed using a combination of the income approach, specifically a discounted cash flow analysis, and the prior sales of stock market approach to determine our EV. The discounted cash flow analysis was developed based on our forecast through 2014 and utilized a WACC of 31% which was deemed appropriate considering our stage of development. For purposes of determining a Terminal Value, the valuation applied a multiple consistent with observed revenue multiples from our Guideline Companies. This calculated value was then discounted to present value using the same WACC to

84

determine the final Terminal Value. The resulting equity value was then allocated to the common stock utilizing an OPM with the following assumptions: a time to a liquidity event of 2.0 years, risk-free rate of 0.3%, dividend yield of 0% and volatility of 57% over the time to a liquidity event. The fair value of our common stock under the income approach, as determined by an OPM and after applying a marketability discount of 25%, was $2.35 per share as of June 30, 2012. When combined with the results from the prior sale of stock under the market approach, the fair value of our common stock as of June 30, 2012 was determined to be $2.48 per share.

The primary reasons for the increase in fair value from the December 31, 2011 valuation to the June 30, 2012 valuation was the decrease in the WACC due to the evolution of our business s stage of development and the use of a higher multiple in the Terminal Value calculation as we were recognizing record growth in revenue. These changes directly resulted in an increase in EV from December 2011 to June 2012. In addition, the OPM in the June 2012 valuation utilized a slightly shorter time to a liquidity event due to the passage of time, and the valuation utilized a lower marketability discount as we neared this assumed liquidity event.

For financial reporting purposes for the awards granted in May 2012, we applied a straight-line calculation between the $1.65 per share determined in the contemporaneous third-party valuation as of December 31, 2011 and the $2.48 per share determined in the contemporaneous third-party valuation as of June 30, 2012 to determine the fair value of our common stock on the grant date. Using the benefit of hindsight, we determined that the straight-line calculation would provide the most appropriate conclusion for the valuation of our common stock on the interim dates between valuations because we did not identify any single event or series of events that occurred during this interim period that would have caused a material change in fair value. Based on this calculation, we assessed the fair value of our common stock for awards granted in May 2012 to be $2.21 per share.

In addition, we granted 41,000 stock options in June 2012. Our board of directors set an exercise price of $1.65 per share for these options based in part on a third-party valuation prepared as of December 31, 2011 because the June 30, 2012 valuation was not completed until August 2012.

For financial reporting purposes for the awards granted in June 2012, we utilized the fair value of $2.48 per share determined in the contemporaneous third-party valuation as of June 30, 2012 for the grant date fair value of these awards.

September 2012

We granted 1,307,850 stock options in September 2012. Our board of directors set an exercise price of $2.48 per share for these options based in part on a third-party valuation prepared as of June 30, 2012.

Following the grant of these options, a contemporaneous valuation was prepared as of September 30, 2012 on a minority, non-marketable basis assuming our business was in the third stage of development. We considered our business to still be in the third stage of development because our sales growth remained very strong and it appeared that profitability was becoming more achievable, but there also remained risk around operating in a competitive market that is subject to technological change with larger established competitors. This valuation was developed using the income approach, specifically a discounted cash flow analysis, to determine our EV. The discounted cash flow analysis was developed based on our forecast through 2014 and utilized a WACC of 28% which was deemed appropriate considering our stage of development. For purposes of determining a Terminal Value, the valuation applied a multiple which was unchanged from the June 30, 2012 valuation. This multiple was determined to still be appropriate as it was still consistent with observed revenue multiples from our Guideline Companies. This calculated value was then discounted to present value using the same WACC to determine the final Terminal Value. The resulting equity value was then allocated to the common stock utilizing an OPM with the following assumptions: a time to a liquidity event of 1.75 years, risk-free rate of 0.2%, dividend yield of 0% and volatility of 55% over the time to a liquidity event. The fair value of our common stock, as determined by an OPM and

after applying a marketability discount of 25%, was $3.66 per share as of September 30, 2012.

Table of Contents

The primary reasons for the increase in fair value from the June 30, 2012 valuation to the September 30, 2012 valuation was the decrease in the WACC as we continued to recognize record growth in revenue and improvements in our forecasting ability. In addition, the forecasts for 2013 and 2014 were revised for this valuation to show increases in revenue over the forecast used in the prior valuations. These changes directly resulted in an increase in EV from June to September 2012. In addition, the OPM in the September 2012 valuation utilized a slightly shorter time to a liquidity event due to the passage of time.

For financial reporting purposes for the awards granted in September 2012, we utilized the fair value of $3.66 per share determined in this contemporaneous third-party valuation as of September 30, 2012 to determine the grant date fair value of these awards.

November and December 2012

We granted 968,000 stock options in November 2012 and 69,632 shares of restricted common stock in December 2012. Our board of directors set an exercise price of $3.66 per share for the November 2012 options based in part on a third-party valuation prepared as of September 30, 2012. When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we evaluated the two surrounding valuations prepared as of September 30, 2012 and December 31, 2012.

As discussed in the preceding section, the September 30, 2012 valuation determined a fair value of $3.66 per share as of that date. The December 31, 2012 contemporaneous valuation was prepared on a minority, non-marketable basis. This valuation was developed using a combination of the prior sales of stock market approach and the PWERM approach to determine our EV. The prior sales of stock market approach incorporated our recent convertible preferred stock financing in which we sold shares of Series F convertible preferred stock at approximately $10.53 per share. Using the information from the Series F convertible preferred stock financing, the valuation determined an equity value for our business. The equity value was then allocated to the common stock utilizing an OPM with the following assumptions: a time to liquidity event of 1.5 years, risk-free rate of 0.2%, dividend yield of 0% and volatility of 55% over the time to liquidity event. The fair value of our common stock per the prior sales of stock market approach, as determined by an OPM and after applying a marketability discount of 15%, was $3.15 per share as of December 31, 2012. The ultimate fair value determined in the PWERM approach was developed by combining the results of two similar valuations, one estimating an IPO in September 2013 and the other estimating an IPO in June 2014. However, both of these valuations were derived by developing hypothetical enterprise values for three different scenarios for the selected IPO timing, a low estimate, medium estimate and high estimate, which were all iterated such that the value attributable to the Series F convertible preferred stock was equal to the purchase price of the Series F convertible preferred stock of approximately $10.53 per share in the recent financing. The results from the three scenarios were then weighted as follows: 20% for the scenario that provided the lowest fair value while the other two scenarios were each weighted by 40%. The results from the two IPO PWERM valuations were then combined with the fair value determined in the IPO by September 2013 valuation weighted by 30% and the fair value determined in the IPO by June 2014 valuation by 70%. The resulting equity value was then reduced by a marketability discount of 15% to determine a fair value under the PWERM approach of $7.73 per share. Finally, the fair value determined under the prior sales of stock market approach was weighted by 50% while the fair value determined under the PWERM approach was also weighted by 50% to determine a final fair value of $5.44 per share as of December 31, 2012.

The primary reasons for the increase in fair value from the September 30, 2012 valuation to the December 31, 2012 valuation was inclusion of the information from the Series F convertible preferred stock financing and the increase in multiples assessed in the PWERM approach.

For financial reporting purposes for the awards granted in November 2012, we applied a straight-line calculation between the $3.66 per share determined in the contemporaneous third-party valuation as of September 30, 2012 and the $5.44 per share determined in the contemporaneous third-party valuation as of December 31, 2012 to determine the fair value of our common stock on the grant date. Using the benefit of

hindsight, we determined that the straight-line calculation would provide the most appropriate conclusion for the valuation of our common stock on the interim date between valuations because we did not identify any single event or series of events that occurred during this interim period that would have caused a material change in fair value. Based on this calculation, we determined the fair value of our common stock for awards granted in November 2012 to be $4.47 per share. In addition, we used the fair value of $5.44 per share for financial reporting purposes for the restricted common stock granted in December 2012.

January and February 2013

We granted 3,570,844 stock options in January 2013 and 642,900 stock options in February 2013. Our board of directors set an exercise price of $5.44 per share for these options based in part on a third-party valuation prepared as of December 31, 2012. In addition, we granted restricted stock units in January 2013 and February 2013, which, by definition, do not have an exercise price. The restricted stock units are performance-based awards and do not vest unless we complete our IPO by December 31, 2014. The target shares of common stock to be issued if we meet certain performance conditions would be 327,000 shares of common stock for the January 2013 restricted stock unit grant and 10,000 shares of common stock for the February 2013 restricted stock unit grant. These grants allow for a maximum issuance of 490,500 shares for the January 2013 restricted stock unit grant and 15,000 shares for the February 2013 restricted stock unit grant if we outperform with regard to these conditions. In addition, it was noted that 15,000 target shares from the January 2013 restricted stock unit grant, which allowed for a maximum issuance of 22,500 shares, were cancelled soon after the date of grant in February 2013. Because part of the performance element with respect to the restricted stock unit grants are related to our completion of an IPO, we will not recognize any expense related to these awards until the applicable performance conditions have been met. We determined the fair value of the awards on the respective grant dates based on the valuation discussion immediately following. When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we evaluated the two surrounding valuations prepared as of December 31, 2012 and March 31, 2013.

As discussed in the preceding section, the December 31, 2012 valuation determined a fair value of $5.44 per share as of that date. The March 31, 2013 valuation was prepared on a minority, non-marketable basis assuming our business was in the fourth or fifth stage of development. We considered our business to be in the fourth or fifth stage of development because our forecasting process showed reduced risks and a liquidity event was nearing. This valuation was developed using a combination of the income approach, specifically a discounted cash flow analysis, and the PWERM approach to determine our EV. The discounted cash flow analysis was developed based on our forecast through 2015 and utilized a WACC of 24%, which was deemed appropriate considering our stage of development. For purposes of determining a Terminal Value, the valuation applied a multiple consistent with observed revenue multiples from our Guideline Companies. This calculated value was then discounted to present value using the same WACC to determine the final Terminal Value. The resulting equity value was then allocated to the common stock utilizing an OPM with the following assumptions: a time to liquidity event of 1.0 year, risk-free rate of 0.2%, dividend yield of 0% and volatility of 48% over the time to a liquidity event. The fair value of our common stock from the income approach, as determined by an OPM and after applying a marketability discount of 18%, was $7.50 per share as of March 31, 2013. Similar to the December 2012 valuation, the ultimate fair value determined in the PWERM approach was developed by combining the results of two similar valuations, one estimating an IPO in September 2013 and the other estimating an IPO in June 2014. Both of these valuations, however, were derived by developing hypothetical enterprise values for three different scenarios for the selected IPO timing: a low estimate, medium estimate and high estimate. The hypothetical Enterprise Values were estimated using multiples consistent with an analysis of our Guideline Companies and an analysis of IPOs in the IT space during recent years. The results from the three scenarios were then weighted as follows: 20% for the scenario with the lowest estimated enterprise value and 40% for the other two scenarios. The results from the two IPO valuations were then combined, with the fair value determined in the IPO by September 2013 valuation weighted by 50% and the fair value determined in the IPO by June 2014 valuation weighted by 50%. This derived equity value was then reduced by a marketability discount of 18% to determine a fair value under the PWERM approach of $8.36 per share. Finally, the fair value

determined under the income approach was weighted by 50% while the fair value determined under the PWERM approach was also weighted by 50% to determine a final fair value of $7.93 per share as of March 31, 2013.

The increase in fair value from the December 31, 2012 valuation to the March 31, 2013 valuation was primarily due to our success in continuing to drive revenue growth and the related increase in our forecast, as well as a higher likelihood of an IPO.

For financial reporting purposes for the awards granted in January and February 2013, we applied a straight-line calculation between the $5.44 per share determined in the contemporaneous third-party valuation as of December 31, 2012 and the $7.93 per share determined in the contemporaneous third-party valuation as of March 31, 2013 to determine the fair value of our common stock on the grant date. Using the benefit of hindsight, we determined that the straight-line calculation would provide the most appropriate conclusion for the valuation of our common stock on the interim date between valuations because we did not identify any single event or series of events that occurred during this interim period that would have caused a material change in fair value. Based on this calculation, we assessed the fair value of our common stock to be $6.05 per share for awards granted in January 2013 and $6.46 per share for awards granted in February 2013.

May 2013

We granted 3,857,600 stock options in May 2013. Our board of directors set an exercise price of $7.93 per share for these options based in part on a third-party valuation prepared as of March 31, 2013. In addition, we granted 26,111 shares of restricted common stock in May 2013, which, by definition, do not have an exercise price. When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we evaluated two surrounding valuations prepared as of April 30 and May 31, 2013.

The April 30, 2013 valuation was prepared on a minority, non-marketable basis assuming our business was in the fourth or fifth stage of development. We considered our business to be in the fourth or fifth stage of development because our forecasting process showed reduced risks and an approaching liquidity event. This valuation was also developed using a combination of the income approach, specifically a discounted cash flow analysis, and the PWERM approach to determine our EV. The discounted cash flow analysis was developed based on our forecast through 2015 and utilized a WACC of 24%, which was consistent with the March 31, 2013 valuation and still deemed appropriate considering our stage of development. For purposes of determining a Terminal Value, the valuation applied a multiple consistent with observed revenue multiples from our Guideline Companies. This calculated value was then discounted to present value using the same WACC to determine the final Terminal Value. The resulting equity value was then allocated to our common stock utilizing an OPM with the following assumptions: a time to liquidity event of 1.0 year, risk-free rate of 0.1%, dividend yield of 0% and volatility of 50% over the time to a liquidity event. The fair value of our common stock from the income approach, as determined by an OPM and after applying a marketability discount of 15%, was $8.04 per share as of April 30, 2013. Similar to the December 2012 and March 2013 valuations, the ultimate fair value determined in the PWERM approach was developed by combining the results of two similar valuations, one estimating an IPO in September 2013 and the other estimating an IPO in June 2014. Both of these valuations, however, were derived by developing hypothetical Enterprise Values for three different scenarios for the selected IPO timing: a low estimate, medium estimate and high estimate. The hypothetical Enterprise Values were estimated using multiples consistent with an analysis of our Guideline Companies and an analysis of IPOs in the IT space during recent years. The results from the three scenarios were then weighted as follows: 30% for the scenario with the lowest estimated Enterprise Value and 35% for the other two scenarios. The results from the two IPO valuations were then combined, with the fair value determined in the IPO by September 2013 valuation weighted by 60%, and the fair value determined in the IPO by June 2014 valuation weighted by 40%. This derived equity value was then reduced by a marketability discount of 15% to determine a fair value under the PWERM approach of $9.02 per share. Finally, the fair value determined under the income approach was weighted by 40%, while the fair value determined under the PWERM approach was weighted by 60% to determine a final fair value of $8.63 per share as of April 30, 2013.

Table of Contents

The May 31, 2013 valuation was prepared on a minority, non-marketable basis assuming our business was in the fourth or fifth stage of development. We considered our business to be in the fourth or fifth stage of development because our forecasting process showed reduced risks and an approaching liquidity event. This valuation was also developed using a combination of the income approach, specifically a discounted cash flow analysis, and the PWERM approach to determine our EV. The discounted cash flow analysis was developed based on our forecast through 2015 and utilized a WACC of 23%, which was a small decrease from the April 30, 2013 valuation but still deemed appropriate considering our stage of development. For purposes of determining a Terminal Value, the valuation applied a multiple consistent with observed revenue multiples from our Guideline Companies. This calculated value was then discounted to present value using the same WACC to determine the final Terminal Value. The resulting equity value was then allocated to our common stock utilizing an OPM with the following assumptions: a time to liquidity event of 1.0 year, risk-free rate of 0.1%, dividend yield of 0% and volatility of 50% over the time to a liquidity event. The fair value of our common stock from the income approach, as determined by an OPM and after applying a marketability discount of 13%, was $9.01 per share as of May 31, 2013. Similar to the December 2012 and March and April 2013 valuations, the ultimate fair value determined in the PWERM approach was developed by combining the results of two similar valuations, one estimating an IPO in September 2013 and the other estimating an IPO in June 2014. Both of these valuations, however, were derived by developing hypothetical Enterprise Values for three different scenarios for the selected IPO timing: a low estimate, medium estimate and high estimate. The hypothetical Enterprise Values were estimated using multiples consistent with an analysis of our Guideline Companies and an analysis of IPOs in the IT space during recent years. The results from the three scenarios were then weighted as follows: 30% for the scenario with the lowest estimated Enterprise Value and 35% for the other two scenarios. The results from the two IPO valuations were then combined, with the fair value determined in the IPO by September 2013 valuation weighted by 70%, and the fair value determined in the IPO by June 2014 valuation weighted by 30%. This derived equity value was then reduced by a marketability discount of 13% to determine a fair value under the PWERM approach of $9.97 per share. Finally, the fair value determined under the income approach was weighted by 30%, while the fair value determined under the PWERM approach was weighted by 70% to determine a final fair value of $9.68 per share as of May 31, 2013.

The increase in fair value from the March 31, 2013 valuation to the April 30 and May 31, 2013 valuations was primarily due to a higher likelihood of an IPO and our continued performance to forecast.

For financial reporting purposes for the awards granted in May 2013, we applied a straight-line calculation between the fair value of $8.63 per share determined in the contemporaneous third-party valuation as of April 30, 2013 and the fair value of $9.68 per share determined in the contemporaneous third-party valuation as of May 31, 2013 to determine the fair value of our common stock on the grant dates. More specifically, of the options granted in May 2013, 3,058,900 were granted on May 3, 2013 and 798,700 were granted on May 16, 2013. In addition, the 26,111 shares of restricted common stock were granted on May 3, 2013 as well. Using the benefit of hindsight, we determined that the straight-line calculation would provide the most appropriate conclusion for the valuation of our common stock on the interim date between valuations because we did not identify any single event or series of events that occurred during the month of May 2013 that would have caused a material change in fair value. Based on this calculation, we assessed the fair value of our common stock to be $8.73 per share for awards granted on May 3, 2013 and $9.17 per share for awards granted on May 16, 2013.

June 2013

We granted 1,295,450 stock options in June 2013. Our compensation committee set an exercise price of $9.68 per share for these options based in part on a third-party valuation prepared as of May 31, 2013. When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we evaluated two surrounding valuations prepared as of May 31, 2013 and June 30, 2013.

As discussed in the preceding section, the May 31, 2013 valuation determined a fair value of $9.68 per share as of that date. The June 30, 2013 valuation was prepared on a minority, non-marketable basis assuming our

89

Table of Contents

business was in the fourth or fifth stage of development. We considered our business to be in the fourth or fifth stage of development because our forecasting process showed reduced risks and an approaching liquidity event. This valuation was also developed using a combination of the income approach, specifically a discounted cash flow analysis, and the PWERM approach to determine our EV. The discounted cash flow analysis was developed based on our forecast through 2015 and utilized a WACC of 22%, which was a small decrease from the May 31, 2013 valuation but still deemed appropriate considering our stage of development. For purposes of determining a Terminal Value, the valuation applied a multiple consistent with observed revenue multiples from our Guideline Companies. This calculated value was then discounted to present value using the same WACC to determine the final Terminal Value. The resulting equity value was then allocated to our common stock utilizing an OPM with the following assumptions: a time to liquidity event of 0.75 years, risk-free rate of 0.1%, dividend yield of 0% and volatility of 46% over the time to a liquidity event. The fair value of our common stock from the income approach, as determined by an OPM and after applying a marketability discount of 10%, was $9.67 per share as of June 30, 2013. Similar to the December 2012 and the March, April and May 2013 valuations, the ultimate fair value determined in the PWERM approach was developed by combining the results of two similar valuations, one estimating an IPO in September 2013 and the other estimating an IPO in June 2014. Both of these valuations, however, were derived by developing hypothetical Enterprise Values for three different scenarios for the selected IPO timing: a low estimate, medium estimate and high estimate. The hypothetical Enterprise Values were estimated using multiples consistent with an analysis of our Guideline Companies and an analysis of IPOs in the IT space during recent years. The results from the three scenarios were then weighted as follows: 30% for the scenario with the lowest estimated Enterprise Value and 35% for the other two scenarios. The results from the two IPO valuations were then combined, with the fair value determined in the IPO by September 2013 valuation weighted by 70%, and the fair value determined in the IPO by June 2014 valuation weighted by 30%. This derived equity value was then reduced by a marketability discount of 10% to determine a fair value under the PWERM approach of $10.50 per share. Finally, the fair value determined under the income approach was weighted by 30%, while the fair value determined under the PWERM approach was weighted by 70% to determine a final fair value of $10.25 per share as of June 30, 2013.

The increase in fair value from the May 31, 2013 valuation to the June 30, 2013 valuation was primarily due to our continued performance against forecast.

For financial reporting purposes for the awards granted in June 2013, we applied a straight-line calculation between the fair value of $9.68 per share determined in the contemporaneous third-party valuation as of May 31, 2013 and the fair value of $10.25 per share determined in the contemporaneous third-party valuation as of June 30, 2013 to determine the fair value of our common stock on the grant date. Using the benefit of hindsight, we determined that the straight-line calculation would provide the most appropriate conclusion for the valuation of our common stock on the interim date between valuations because we did not identify any single event or series of events that occurred during the month of June 2013 that would have caused a material change in fair value. Based on this calculation, we assessed the fair value of our common stock to be $10.21 per share for awards granted in June 2013.

July 2013

We granted 1,243,000 stock options in July 2013. Our compensation committee set an exercise price of $10.25 per share for these options based in part on a third-party valuation prepared as of June 30, 2013. In addition, we granted 23,711 shares of restricted common stock in July 2013, which, by definition, do not have an exercise price.

When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we initially evaluated the valuation prepared as of June 30, 2013 and our original anticipated initial offering price range of $11.00 to $15.00 per share.

Table of Contents

We believe the difference between the third-party valuation we obtained as of June 30, 2013, and our original anticipated initial offering price range is a result of the following factors:

First, the initial offering price range necessarily assumed that our initial public offering had occurred and a public market for our common stock had been created and, therefore, excluded the discounts associated with the timing or likelihood of an initial public offering, which were appropriately included in the valuation prepared as of June 30, 2013. The assumptions in the June 2013 valuation that changed in the determination of the initial offering price range include (i) a decrease in the non-marketability discount from 10% to 0%, (ii) a change in the probability of a September 2013 initial public offering from 70% to 100% and (iii) the elimination of using the income approach to inform the initial offering price range.

Second, after discussions among the underwriters, management, and our board of directors, the original anticipated initial offering price range was informed by the performance of a broader group of comparable companies that have recently completed their initial public offerings, including SaaS software companies that were considered as comparable companies for purposes of our initial public offering. The Guideline Companies that informed our June 2013 valuation typically have product offerings that include an equipment component. The additional comparable companies that informed the initial offering price range typically have higher revenue multiples than the Guideline Companies. As a result, the June 2013 valuation assigned a lower hypothetical Enterprise Value than the estimated value that informed the determination of the initial offering price range.

For financial reporting purposes for the awards granted in July 2013, we initially applied a straight-line calculation between the fair value of $10.25 per share determined in the contemporaneous third-party valuation as of June 30, 2013 and the midpoint of the original anticipated initial offering price range of $11.00 to $15.00 per share to determine the fair value of our common stock on the grant date. Using the benefit of hindsight, we determined that the straight-line calculation would provide the most appropriate conclusion for the valuation of our common stock on the interim date between valuations because we did not identify any single event or series of events that occurred during the month of July 2013 that would have caused a material change in fair value. Based on this calculation, we initially assessed the fair value of our common stock to be $11.90 per share for awards granted in July 2013.

As more fully described under Offering Price Range and Fair Value Reassessment below, on September 18, 2013, we retrospectively reassessed the fair value of our common stock for the July 2013 grants for financial reporting purposes to be $12.90 per share.

August 2013

We granted 952,500 stock options in August 2013. In addition, we granted 26,670 shares of restricted common stock in August 2013, which, by definition, do not have an exercise price.

In addition, we granted restricted stock units in August 2013, which, by definition, do not have an exercise price. The restricted stock units are performance-based awards and were not scheduled to vest unless we completed our IPO by December 31, 2014. The target shares of common stock to be issued if we meet certain performance conditions would be 40,000 shares of common stock. This grant allows for a maximum issuance of 60,000 shares if we outperform with regard to these conditions. Because part of the performance element with respect to the restricted stock unit grants are related to our completion of an IPO, we will not recognize any expense related to these awards until the applicable performance conditions have been met.

When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we initially used the midpoint of our original anticipated initial public offering price range of $11.00 to $15.00 per share.

As more fully described under Offering Price Range and Fair Value Reassessment below, on September 18, 2013, we retrospectively reassessed the fair value of our common stock for the August 2013 grants for financial reporting purposes to be $14.67 per share.

Table of Contents

September 2013

We granted 824,900 stock options on September 4, 2013. In addition, we granted 240,000 shares of restricted common stock on September 3, 2013, which, by definition, do not have an exercise price.

When assessing the appropriate fair value for purposes of calculating the related stock-based compensation expense for these awards, we initially used $13.00, the midpoint of the price range reflected on the cover page of our preliminary prospectus dated September 9, 2013.

As more fully described under Offering Price Range and Fair Value Reassessment below, on September 18, 2013, we retrospectively reassessed the fair value of our common stock for the September 4, 2013 grants for financial reporting purposes to be $16.00 per share.

We granted 367,000 stock options on September 19, 2013 with an exercise price of $20.00 per share, which was equal to the initial public offering price.

Offering Price Range and Fair Value Reassessment

On September 9, 2013, we, along with our managing underwriters, began the marketing phase of our proposed initial public offering. At that time, our preliminary prospectus continued to reflect a preliminary price range of $12.00 to $14.00 per share. After a series of meetings with potential investors that took place during the week of September 9, 2013, our board of directors met with our managing underwriters and members of our senior management team on September 16, 2013 and determined that, as a result of the level of interest in our proposed initial public offering from potential investors, we should increase our preliminary price range to $15.00 to $17.00 per share. On September 17, 2013, we filed an updated preliminary prospectus with the SEC reflecting the increase in our preliminary price range.

As a result of the increase in our preliminary price range, we revised our estimate of the fair value of our common stock for the July 2013, August 2013 and September 2013 grants described above. We applied a straight-line calculation between the fair value of $10.25 per share determined in the contemporaneous third-party valuation as of June 30, 2013 and the midpoint of the increased anticipated initial offering price range of $16.00 per share to determine the fair value of our common stock for the July 2013 and August 2013 grants. We used the midpoint of the increased price range of $16.00 per share as our estimated fair value for the September 2013 grants. Using the benefit of hindsight, we determined that the straight-line calculation would provide the most appropriate conclusion for the valuation of our common stock during this period because we did not identify any single event or series of events that occurred during this period that would have caused a material change in fair value.

As a result of reassessing the fair value of our common stock, we recorded additional stock-based compensation expense over the vesting period of the awards granted in July 2013, August 2013 and September 2013.

Stock-Based Awards Granted Subsequent to our Initial Public Offering.

For stock-based awards granted subsequent to our IPO, our board of directors determined the fair market value based on the closing price of our common stock as reported on The NASDAQ Global Select Market on the date of grant.

Warrants

Warrants to purchase shares of our convertible preferred stock are classified as a liability on the consolidated balance sheet at fair value because the warrants contain down-round protection and therefore, do not meet the scope exception for treatment as a derivative. The fair value of the warrants is estimated using the

Table of Contents

Monte Carlo model at each reporting date. The change in fair value of the warrants is then recorded on the consolidated statements of operations as other expense. We use management judgment to estimate the fair value of these warrants, and these estimates could differ significantly in the future. We determined the fair value of the outstanding convertible preferred stock warrants utilizing a Monte Carlo model with the following assumptions as of December 31, 2012:

	As of December 31, 2012	
Remaining contractual term (in years)	2.6	8.7
Risk-free interest rate	0.3%	1.5%
Volatility	55%	64%
Change of control probability	25%	50%
Control premium	40%	
IPO threshold (in billions)	$0.6	$1.8

The above assumptions were determined as follows:

Remaining contractual term The remaining contractual term represents the time from the date of the valuation to the expiration of the warrant;

Risk-free interest rate The risk-free interest rate is based on the U.S. Treasury yield in effect as of December 31, 2011 and 2012 for zero coupon U.S. Treasury notes with maturities approximately equal to the term of the warrant;

Volatility The volatility is derived from historical volatilities of several unrelated publicly listed peer companies over a period approximately equal to the term of the warrant because we have limited information on the volatility of the convertible preferred stock because there is currently no trading history. When making the selections of industry peer companies to be used in the volatility calculation, we considered the size, operational and economic similarities to our principle business operations;

Change of control probability The change of control probability is the board of directors estimate of the probability that we are involved with a change of control transaction; and

Control premium The control premium represents an additional amount above the value of an entity s common stock that an investor would be willing to pay to obtain control over that entity.

Prior to our IPO, the fair value of the warrants was recorded as a warrant liability upon issuance. The warrant was recorded at its estimated fair value utilizing the Monte Carlo model with changes in the fair value of the warrant liability reflected in other expense, net. Upon the completion of our IPO, the shares underlying the warrants were converted from preferred stock into approximately 616,000 shares of common stock, and the related balance of the preferred stock warrant liability was reclassified to additional paid-in capital and was no longer subject to fair value accounting.

As of December 31, 2012, all of the convertible preferred stock warrants remained outstanding as follows (in thousands, except share and per share amounts):

Class of Shares	Issuance Dates	Expiration Dates	No. of Shares	Exercise Price per Share	Fair Value as of December 31, 2012
Series A-2	2005 and 2006	2015 and 2016	245,899	$ 0.61	$ 1,632
Series B	2006 through 2008	2016 through 2018	118,942	$ 1.32	925
Series D	June 2010	June 2020	100,000	$ 0.39	634
Series E	August 2011	August 2021	60,661	$ 1.36	338
Total					$ 3,529

During the years ended December 31, 2011, 2012 and 2013, we recognized charges in the amount of $0.8 million, $2.5 million and $6.5 million, respectively, from the remeasurement of the fair value of the warrants, which was recorded through other expense, net in our consolidated statements of operations.

Income Taxes

We account for income taxes using the asset and liability method, which requires the recognition of deferred tax assets and liabilities for the expected future tax consequences of events that have been recognized in our financial statements or tax returns. In addition, deferred tax assets are recorded for the future benefit of utilizing net operating losses and research and development credit carryforwards. Valuation allowances are provided when necessary to reduce deferred tax assets to the amount expected to be realized.

We apply the authoritative accounting guidance prescribing a threshold and measurement attribute for the financial recognition and measurement of a tax position taken or expected to be taken in a tax return. We recognize liabilities for uncertain tax positions based on a two-step process. The first step is to evaluate the tax position for recognition by determining if the weight of available evidence indicates that it is more likely than not that the position will be sustained on audit, including resolution of related appeals or litigation processes, if any. The second step requires us to estimate and measure the tax benefit as the largest amount that is more than 50% likely to be realized upon ultimate settlement.

Significant judgment is required in evaluating our uncertain tax positions and determining our provision for income taxes. Although we believe our reserves are reasonable, no assurance can be given that the final tax outcome of these matters will not be different from that which is reflected in our historical income tax provisions and accruals. We adjust these reserves in light of changing facts and circumstances, such as the closing of a tax audit or the refinement of an estimate. To the extent that the final tax outcome of these matters is different than the amounts recorded, such differences may impact the provision for income taxes in the period in which such determination is made.

Significant judgment is also required in determining any valuation allowance recorded against deferred tax assets. In assessing the need for a valuation allowance, we consider all available evidence, including scheduled reversal of deferred tax liabilities, past operating results, estimates of future taxable income, and the feasibility of tax planning strategies. We reversed our valuation allowance on U.S. federal and certain state deferred tax assets during the year ended December 31, 2013 as a result of the scheduled reversal of deferred tax liabilities established in purchase accounting. We have maintained a valuation allowance on California net deferred tax assets as it is not more likely than not that these net deferred tax assets will be realized. As we reverse deferred tax liabilities in subsequent periods, we will likely re-establish a valuation allowance in these jurisdictions as it is not more likely than not that these deferred tax assets can be realized outside of the scheduled reversal of deferred tax liabilities.

Estimates of future taxable income are based on assumptions that are consistent with our plans. Assumptions represent management s best estimates and involve inherent uncertainties and the application of management s judgment. Should actual amounts differ from our estimates, the amount of our tax expense and liabilities could be materially impacted.

We do not provide for a U.S. income tax liability on undistributed foreign earnings of our foreign subsidiaries. The earnings of non-U.S. subsidiaries are indefinitely reinvested in non-U.S. operations.

Contract Manufacturer Liabilities

We outsource most of our manufacturing, repair, and supply chain management operations to our independent contract manufacturers and payments to them are a significant portion of our product cost of revenue. Although we could be contractually obligated to purchase manufactured products, we generally do not own the manufactured products. Product title transfers from our independent contract manufacturers to us and immediately to our partners upon shipment. Our independent contract manufacturers assemble our products using

design specifications, quality assurance programs, and standards that we establish, and they procure components and assemble our products based on our demand forecasts. These forecasts represent our estimates of future demand for our products based upon historical trends and analysis from our sales and product management functions as adjusted for overall market conditions. If the actual component usage and product demand are significantly lower than forecast, we accrue for costs for contractual manufacturing commitments in excess of our forecasted demand, including costs for excess components or for carrying costs incurred by our contract manufacturers. To date, we have not accrued any significant costs associated with this exposure.

As of December 31, 2012 and 2013, we had approximately $3.3 million and $16.7 million, respectively, of open orders with our contract manufacturers that may not be cancelable.

Loss Contingencies

We are subject to the possibility of various loss contingencies arising in the ordinary course of business. We consider the likelihood of loss or impairment of an asset, or the incurrence of a liability, as well as our ability to reasonably estimate the amount of loss, in determining loss contingencies. An estimated loss contingency is accrued when it is probable that an asset has been impaired or a liability has been incurred and the amount of loss can be reasonably estimated. If we determine that a loss is possible and the range of the loss can be reasonably determined, then we disclose the range of the possible loss. We regularly evaluate current information available to us to determine whether an accrual is required, an accrual should be adjusted or a range of possible loss should be disclosed.

Warranties

We generally provide a one-year warranty on our hardware and a three-month warranty on our software products. We do not accrue for potential warranty claims as a component of cost of product revenue as all product warranty claims are satisfied under our support and maintenance contracts.

Goodwill

Goodwill is the excess of the aggregate purchase price paid over the fair value of the net tangible assets acquired. Goodwill is not amortized and is tested for impairment at least annually or whenever events or changes in circumstances indicate that the carrying value may not be recoverable. We have determined that we operate as one reporting unit and have selected December 1 as the date to perform our annual impairment test. In the valuation of our goodwill, we must make assumptions regarding estimated future cash flows to be derived from our business. If these estimates or their related assumptions change in the future, we may be required to record impairment for these assets. The first step of the impairment test involves comparing the fair value of the reporting unit to its net book value, including goodwill. If the net book value exceeds its fair value, then we would perform the second step of the goodwill impairment test to determine the amount of the impairment loss. The impairment loss would be calculated by comparing our implied fair value to our net book value. In calculating the implied fair value of our goodwill, our fair value would be allocated to all of the other assets and liabilities based on their fair values. The excess of our fair value over the amount assigned to our other assets and liabilities is the implied fair value of goodwill. An impairment loss would be recognized when the carrying amount of goodwill exceeds its implied fair value. There was no impairment of goodwill recorded for the years ended December 31, 2013, 2012 or 2011.

Recent Accounting Pronouncements

In February 2013, the FASB issued guidance which addresses the presentation of amounts reclassified from accumulated other comprehensive income. This guidance does not change current financial reporting requirements, instead an entity is required to cross-reference to other required disclosures that provide additional detail about amounts reclassified out of accumulated other comprehensive income. In addition, the guidance

Table of Contents

requires an entity to present significant amounts reclassified out of accumulated other comprehensive income by line item of net income if the amount reclassified is required to be reclassified to net income in its entirety in the same reporting period. Adoption of this standard is required for periods beginning after December 15, 2012 for public companies. This new guidance impacts how we report comprehensive income and will have no effect on our results of operations, financial position or liquidity upon its required adoption on January 1, 2013.

Table of Contents

BUSINESS

Overview

We provide a comprehensive solution of products and services for detecting, preventing and resolving advanced cybersecurity threats. We have invented a purpose-built, virtual machine-based security platform that provides real-time protection to enterprises and governments worldwide that are facing the next generation of cyber attacks. Our technology approach represents a paradigm shift in how IT security has been conducted since the earliest days of the information technology industry. The core of our purpose-built, virtual machine-based security platform is our virtual execution, or MVX, engine, which identifies and protects against known and unknown threats that existing signature-based technologies are unable to detect. The new generation of cyber attacks on organizations, including large and small enterprises and governments worldwide, is characterized by an unprecedented escalation in the complexity and scale of advanced malware created by criminal organizations and nation-states. These highly sophisticated cyber attacks routinely circumvent traditional signature-based defenses by launching dynamic, stealthy and targeted malware that penetrates defenses in multiple stages and through multiple entry points of an IT network. Our proprietary virtual machine-based technology represents a new approach to detecting these cyber attacks in real time with high efficacy while also scaling in response to ever-increasing network performance requirements. We believe it is imperative for organizations to invest in this new approach to security to protect their critical assets, such as intellectual property and customer and financial data, from the global pandemic of cybercrime, cyber espionage and cyber warfare.

Our over ten years of research and development in proprietary virtual machine technology, anomaly detection and associated heuristic, or experience-based, algorithms enables us to provide real-time, dynamic threat protection without the use of signatures while delivering high efficacy and network performance. We provide a comprehensive platform that employs a virtualized execution engine and a cloud-based threat intelligence network that uniquely protects organizations from next-generation threats at all stages of the attack lifecycle and across all primary threat vectors, including Web, email, file and mobile. Our MVX engine detonates, or runs, Web objects, suspicious attachments and files within purpose-built virtual machine environments to detect and block the full array of next-generation threats, including attacks that leverage unknown vulnerabilities in widely used software programs, also known as zero-day attacks. Newly identified threats are quarantined to prevent exposure to the organization s actual network environment, and information regarding such threats is sent to our Dynamic Threat Intelligence, or DTI, cloud. Our DTI cloud enables real-time global sharing of threat intelligence uploaded by our customers cloud-connected FireEye appliances.

In December 2013, we acquired privately held Mandiant, the leading provider of advanced endpoint security products and security incident response management solutions. FireEye and Mandiant have been strategic partners with integrated product offerings since April 2012. We believe the combination of the two companies deepens this partnership and creates the industry s leading advanced threat protection vendor with the ability to find and stop attacks at every stage of the attack life cycle. The combination of our industry leading security products and threat intelligence with products and services from Mandiant enables us to provide a complete solution for detecting, preventing and resolving advanced cybersecurity threats across three distinct disciplines:

First, Mandiant provides endpoint-based advanced threat detection and response. Mandiant s endpoint products enable security teams to enhance their visibility and make faster, more accurate decisions about potential security incidents occurring across an organization s network and endpoints.

Second, Mandiant brings significant depth in intelligence on next-generation attacks, which is continually gathered from ongoing monitoring of more than two million endpoints and by incident response and remediation teams that serve on the front lines combating the most advanced attacks. When this depth of threat intelligence is paired with the breadth of the FireEye real-time threat intelligence gathered from more than two million virtual machines, organizations will have robust detection and contextual information about attempted attacks, including the level of risk, the identity of the attackers, and the intended target of the attacks.

97

Table of Contents

Third, Mandiant s team of highly skilled incident response experts has performed hundreds of incident response investigations across numerous industries at some of the largest organizations in the world. In addition, Mandiant brings its Managed Defense monitoring service to FireEye. The addition of these skills and expertise significantly expands our ability to offer value-added services to our customers.

Our platform is delivered through a family of software-based appliances and includes our cloud subscription services as well as support and maintenance services. Our principal threat prevention appliance families address four critical vectors of attack: Web, email, file and mobile. We also provide a family of threat prevention appliances that enable rapid identification and remediation of attacks that have penetrated and are residing on an organization s endpoints, such as desktop computers, laptops, or mobile devices. Our management appliances serve as a central nervous system unifying reporting and configuration, while monitoring and correlating attacks that simultaneously cross multiple vectors of the network, thereby increasing the efficacy of our security platform. Our management appliances enable us to share intelligence regarding threats at a local implementation level and also across the organization. In addition, we enhance the efficacy of our solution by sharing with customers anonymized global threat data through our DTI cloud. We also offer a forensic analysis appliance that provides IT security analysts with the ability to test, characterize and conduct forensic examinations on next-generation cyber attacks by simulating their execution path with our virtual machine technology. Our cloud-based mobile threat prevention platform identifies and stops mobile threats by analyzing mobile applications within our MVX engine. Finally, we offer incident response and managed services to assist our customers who have been breached as part of our full service solution to combat advanced threats.

As part of our sales strategy, we often provide prospective customers with our products for a short-term evaluation period. As of December 31, 2013, we had conducted over 4,400 of these evaluations across many countries and with companies of all sizes. In each case, our products are deployed within the prospective customer s network, typically for a period ranging from one week to several months. During this period, the prospective customer conducts evaluations with the assistance of our system engineers and members of our security research team. These evaluations have been part of our ordinary course business practices for the past two years. In over 95% of these prospective customer evaluations, we have discovered incidents of next-generation threats that were conducting malicious activities and that successfully evaded the prospective customers existing security infrastructure, including traditional firewalls, next-generation firewalls, intrusion prevention systems, anti-virus software, email security and Web filtering appliances. By deploying our platform, organizations can stop inbound attacks and outbound theft of valuable intellectual property and data with a negligible false-positive rate, enabling them to avoid potentially catastrophic financial and intellectual property losses, reputational harm and damage to critical infrastructures.

Our sales model consists of a direct sales team and channel partners that collaborate to identify new sales prospects, sell products and services, and provide post-sale support. We believe this approach allows us to maintain face-to-face connectivity with our customers, including key enterprise accounts, and helps us support our partners, while leveraging their reach and capabilities. Further, we believe our leading incident response capabilities position us as a trusted advisor to our customers and offer us the opportunity to help customers prevent future breaches through the use of our products and services. As of December 31, 2013, we had over 1,900 end-customers across more than 60 countries, including over 130 of the Fortune 500. Our customers include leading enterprises in a diverse set of industries, including telecommunications, technology, financial services, public utilities, healthcare and oil and gas, as well as leading U.S. and international governmental agencies.

For 2011, 2012 and 2013, our revenue was $33.7 million, $83.3 million and $161.6 million, respectively, representing year-over-year growth of 148% for 2012 and 94% for 2013, and our net losses were $16.8 million, $35.8 million and $120.6 million, respectively. Subscription and services revenue, which represents a recurring portion of our revenue, has increased as a percentage of revenue over the last three years, from 37% in 2012 to 45% for 2013.

Table of Contents

Industry Background

Organizations Are Spending Billions On Signature-Based Security Technologies

Organizations today are embracing a confluence of technologies to enhance the productivity of their employees, generate new revenue sources and improve their operating efficiency. These technologies include cloud services, mobile computing and online services and social networking sites, such as LinkedIn, Facebook and Twitter. This emergence of an increasingly distributed IT infrastructure, along with the explosion in the diversity, scale and importance of this infrastructure has greatly increased the vulnerability of these organizations to potential security attacks. This greater reliance on information technology has resulted in significant investments in IT security products and personnel to help protect against a myriad of potential threats. According to IDC, a global market research firm, 2013 worldwide IT security spending was approximately $16.8 billion, including investments in traditional security technologies such as firewalls, virtual private networking, Web security, unified threat management, intrusion detection and prevention, messaging security and corporate endpoint security.[5] In order to deploy and manage these products, organizations are relying upon an increasingly large staff of highly specialized IT security personnel.

To date, organizations have deployed security products to protect their IT infrastructure against earlier generations of security threats. These security products typically fell into two main categories. First, technologies like firewalls were developed in order to enforce a set of policies that governed which types of traffic would be allowed onto an organization s network. Second, technologies like intrusion detection and anti-virus software were developed to protect against potential security threats embedded within an organization s traffic. These technologies defended against earlier generations of security threats by utilizing signature-based threat protection technology. The signature model works by forensically examining the code base of known malware and, if no match is found, subsequently developing a signature that network security devices can match against future incoming traffic. These signatures are gathered by IT security companies and distributed periodically to organizations that subscribe to the security company s update service. This signature-based approach is the principal foundation of existing threat protection technologies.

Next-Generation Threats Present New Challenges For Organizations

In general, cyber attacks from the late 1990s and early 2000s were intentionally designed to be visible and to be distributed as separate stand-alone software components, making them relatively easy and straightforward for security devices to identify, analyze and prevent. These early generation attacks were deployed less frequently than advanced threats. As a result, IT departments were generally able to respond more effectively to patch system vulnerabilities. These attacks generally consisted of malicious software, or malware, that would be performed only the first time it was encountered by the organization. Because this type of malware was not designed to be persistent, it had significantly less potential to cause incremental damage beyond its initial attack. Moreover, the historical threat landscape was defined by amateur hackers who launched attacks principally for fame or mischief. While these hackers garnered media attention, they caused relatively little damage, and signature-based security solutions were effective at detecting and preventing them. These threats were not targeted at specific individuals or specific IT security vulnerabilities within an organization. Rather, the attacks were broad based in nature and therefore less damaging. Attacks such as these represent the majority of attacks faced by organizations during the last 20 years.

Today s security attacks are being conducted by increasingly sophisticated threat actors

Today s organizations face an advanced malware pandemic of unprecedented severity led by advanced persistent threat actors, such as cybercriminals, nation-states and hacktivists. Cybercriminals are expending significant resources to exfiltrate sensitive intellectual property and personal data from organizations, causing financial and reputational damage; nation-states are pursuing cyber espionage and warfare targeting

critical infrastructure, such as power grids, and highly sensitive information that can threaten national security; and

5 See note (2) in Market and Industry Data.

Table of Contents

hacktivists, who are driven by political ideologies, are defacing Websites, stealing information and launching denial of service attacks. These threat actors are utilizing highly sophisticated next-generation threats to circumvent traditional IT defenses at an alarming rate. Given their significant resources, nation-states and organized cyber criminals are now employing automated, constantly changing threats known as polymorphic attacks to penetrate mission critical systems. These sophisticated groups are constantly evolving their capabilities to penetrate IT infrastructure, steal sensitive information, and conduct espionage and cyber warfare. They have the human and financial resources to continuously modify and improve attacks to identify and exploit network vulnerabilities that will allow them to breach a target s network. A 2011 Ponemon Institute study estimated a 44% increase in successful cyber attacks from the prior year. Contributing to this trend is a rise in state sponsored cyber-espionage with many countries armed for cyber warfare. The problem has become so severe that the United States Department of Defense recently elevated cyberspace in the 2010 Quadrennial Defense Report to be a domain on the same level of importance as land, sea, air and space. In addition, cyber attacks are listed as a top national security threat in the 2013 Worldwide Threat Assessment of the US Intelligence Community.

These threat actors are utilizing highly sophisticated techniques that differ dramatically from earlier generation threats

Next-generation threats, utilized by advanced persistent threat actors, are fundamentally different from earlier generation threats, with a unique set of characteristics that create a new set of detection and prevention challenges. One of the most dangerous characteristics of next-generation threats is their ability to take advantage of a previously unknown vulnerability in widely used software programs, creating what is known as zero day threats. By exploiting this vulnerability, significant damage can be done because it can take days before signature-based software vendors discover the vulnerability and patch it, and an even longer period of time for traditional security products to update their signature databases accordingly. Next-generation threats are stealthy by design and are significantly harder to detect. Further compounding the problem, next-generation threats are dynamic, or polymorphic, meaning they are designed to mutate quickly and retain their function while changing their code, making it almost impossible for traditional signature technologies to detect them. These threats are also targeted, which enables them to present specific individuals within organizations networks with customized messages or content that maximizes the likelihood of the individual becoming an unwitting accomplice to the attack. Finally, these attacks are persistent and can perform malicious activity over a significantly longer period of time by remaining resident in the network and spreading undetected across devices for a specific period of time before conducting their activity, thereby resulting in higher damage potential.

Next-generation threats are attacking all primary entry points and manifesting themselves over a complex series of stages

Next-generation threats target all possible entry points of a network by launching advanced malware attacks at the organization through Web, email, file and mobile vectors. Web-based attacks happen when users unknowingly navigate to malicious Websites and click on links or buttons that then execute code on the user s browser or activate applications on the user s computer that serve as the initial insertion point for the threat. Worse still, some Web-based attacks, called drive-by downloads, require no user interaction beyond simply visiting the Web page to infect user devices. Email attacks typically happen when users are presented with a customized message to lure them into clicking on a link in the email, which then directs the unwitting user to a malicious Website or executes a local application, creating an initial insertion point for malware. File-based attacks happen when a malicious program has already entered the network and is free to propagate malware to network file shares, such as Microsoft network file sharing service, from which it is able to exfiltrate high-value data. Mobile-based attacks typically happen when a malicious application is downloaded on the Android platform. These applications can be downloaded from widely available commercial application stores as well as custom enterprise applications. Once a mobile device is infected, the malicious application can steal any and all information from the device. An additional level of complexity in advanced malware is that the same threat can simultaneously target multiple vectors of a network to gain entry, such as through a Web page, email, file or mobile applications. These advanced blended attacks have become increasingly commonplace and significantly increase the difficulty of detection by legacy security products.

Table of Contents

Next-generation threats are difficult to detect and block at each step of their attack lifecycle

Next-generation threats are significantly more complex in the way they carry out their attacks. The threats formulate over multiple steps, and they are difficult to detect via legacy security technologies at each step. The typical next-generation attack lifecycle contains the following five steps:

1. *Initial Exploit:* An exploit is typically a small amount of seemingly harmless content, often just a few hundred bytes in size, that when inserted into vulnerable software can make the software execute code it was not programmed to run. The initial exploit phase is critical and occurs when cyber attackers take advantage of inherent vulnerabilities in widely used software and applications, such as Adobe Acrobat, Flash, and Internet Explorer, to initially penetrate a victim system. The exploit is stealthy and its code can enter an organization even when a user does nothing more than visit a Web page that has been compromised. Importantly, this entire process happens within the compromised system s random access memory and does not involve writing any files to the hard drive, making it almost impossible to detect with legacy security solutions that are focused on examining files and executables once they are written to the hard drive on a host computer.

2. *Malware Download:* Once the initial exploit is successful in penetrating a victim s system, a larger malware program in the form of a file can be downloaded onto the hard drive of the compromised system. Because the download is initiated by seemingly innocuous software from inside the organization and the malware file can be obfuscated to seem harmless, legacy security systems cannot detect the threat. As an example, the file can be presented as a .jpg (a picture) instead of an .exe (executable) file and therefore avoid detection by legacy security technologies designed to look for executables. In addition, the malware program is encrypted and the key to decrypt the file is only available in the exploit code. Therefore, only if a security product detects the initial exploit code, can it collect the key to decrypt, detect and block the larger malware program.

3. *Callback and Establish Control*: After the larger malware download is successful, it will initiate an outbound connection to an external command and control server operated by a threat actor. Once the program has successfully made a connection, the cyber attacker has full control over the compromised host. Many legacy security solutions do not analyze outbound traffic for malicious transmissions and destinations. Other solutions that attempt to detect malicious outbound transmissions can only find transmissions to known destination IP addresses of servers, and are not able to identify malicious transmissions to unknown destinations.

4. *Data Exfiltration:* Having established a secure connection with the command and control server, the malware will proceed to take control of the host computer as well as transfer sensitive data, such as intellectual property, credit card information, user credentials, and sensitive file content. Because legacy security solutions cannot detect any of the previous three steps exploit, malware download and callback they are unable to detect and block the outbound transfer of data.

5. *Lateral Movement:* At any point after the malware is downloaded, the malware may conduct reconnaissance across the network to locate other vulnerable systems, and then spread laterally to file shares located deep within the organization s network to search for additional data that is valuable to exfiltrate. As the lateral movement is conducted within the enterprise, firewalls and other perimeter security solutions focused on blocking malicious traffic from entering an organization are not able to detect the movement of malware within the organization.

Next-generation threats have already caused significant damage to organizations

Next-generation threats are pervasive and cause substantial damage to organizations around the world. Below are examples of well-known next-generation attacks that breached the legacy network security technologies deployed by large organizations:

Flame: The Flame cyber attacks were discovered in 2012. These attacks targeted private individuals, governments, enterprises and educational organizations in the Middle East, predominantly in Iran. The

Table of Contents

malware associated with Flame was built specifically for information gathering and ongoing monitoring of victims. It could activate microphones and Web cameras to record audio and video and use blue tooth connections to download data from devices connected to infected computers. Flame has been called the most sophisticated malware ever found. The malware had several unique characteristics that made it extremely hard to detect. One feature allowed the malware to identify security programs on the host and transform its code base to ensure that it evaded the specific security program identified. Flame is an example of modern day espionage, in the form of a cyber attack that targets a broad base of victims. This type of espionage is becoming the strategy of choice for intelligence agencies to execute their missions.

RSA Attack: The infiltration of RSA, discovered in 2011, is an example that is commonly referred to as an advanced persistent threat. This cyber attack started out as a spear phishing email titled 2011 Recruitment Plan with an excel attachment. Once opened, the excel sheet would infect the host computers. The code would then slowly harvest user credentials and look for ways to get onto additional computers of users with higher level credentials. The attackers slowly gained the credentials they needed to infiltrate the core RSA SecureID token master key database, thereby compromising the security of thousands of other companies. This attack took substantial time and effort to access the SecureID token database, which was only one step of a larger plan to attack the organizations using these stolen credentials.

Operation Aurora: Discovered in 2010, Operation Aurora compromised the systems of several Fortune 500 companies by relying on a zero-day threat to gain access to well protected IT infrastructure. Specifically, there was a vulnerability within Internet Explorer that allowed malicious code to infect a user s computer when the user took no action other than visiting a Website. This is an example of how a small zero-day exploit on one type of software can allow cyber attackers to compromise even the most sophisticated organizations.

Shady RAT: Operation Shady RAT, or Shady RAT, is an ongoing series of cyber attacks that started in 2006. The attacks hit and penetrated over 70 organizations, including major defense contractors, the United Nations and the International Olympic Committee. The campaign used spear phishing emails targeted at users with administrative privileges and took advantage of known exploits. The attack is notable for the range of victims and length of the infections. The United Nations was breached for nearly two years and the International Olympic Committee for 28 months before the infection was identified. This is one of the most successful coordinated breaches publicly disclosed and shows the breadth of victims and serious deficiencies in IT security.

A widespread underground community has formed to significantly increase the accessibility of attack tools

To further compound the problem, attacks like those described above are now being created with automated processes and software easily accessible on the Internet. The software development tool kits necessary to create new unique malware can be purchased for a few hundred U.S. dollars. These tools have shortened the time to threat creation and deployment, resulting in a significant increase in the volume and diversity of unknown threats attacking an organization. A cybercrime ecosystem of developers, consultants, technology providers and funding sources has emerged to support the large and growing market for next-generation threats. Advanced persistent threat actors can purchase the latest technology from this ecosystem or even contract with developers to launch attacks. This ecosystem provides a critical source of funding and resources for the development of the latest advanced malware technology, which has led to a pronounced increase in the proliferation of highly sophisticated cyber attacks.

Existing Security Solutions Are Not Architected For Next-Generation Threats

The evolving threat landscape has rendered traditional defenses incapable of protecting organizations against next-generation threats. The list below identifies the major security product categories available in the market today and their respective shortcomings in defending against next-generation threats.

Traditional firewall. Firewalls regulate incoming and outgoing network traffic by limiting which internal and external systems can communicate with each other, and which ports and protocols can be used for

Table of Contents

those communications. Most attacks and subsequent malware communications tunnel over widely used port and protocol configurations, such as port 80 and HTTP, which organizations must allow through the firewall. Traditional firewalls were not designed to inspect the communications of the traffic itself, making them blind to the potentially malicious content being carried through network traffic that they are allowing into the organization. Also, since firewalls operate at the network perimeter, they are unable to block threats that have bypassed the perimeter and spread onto internal file shares or that have attempted to enter through a different vector of attack, such as through the email gateway.

Next-generation firewall. Next-generation firewalls, or NGFWs, have recently been adopted by organizations to improve upon the capabilities of traditional firewalls. NGFWs add layers of policy rules based on users and applications. This allows administrators to selectively enable the use of certain applications and represents a major improvement in policy-oriented challenges faced by organizations. However, this approach does not address the inability of the firewall itself to intelligently process and inspect traffic to detect potentially malicious content.

Intrusion prevention system. Intrusion prevention systems, or IPS, were developed to address the firewall s visibility and granularity limitations. IPS products utilize a signature database of known threats and network vulnerabilities to scan for potentially malicious traffic, making them reactive and unable to look for exploits targeting unknown vulnerabilities. Furthermore, IPS offerings were originally built to detect and analyze network services-based attacks, rather than the client-side application attacks that have become the more popular target for cyber attackers. Everyday client applications being used by individuals, such as browsers, PDF readers and Flash plug-ins, rather than server applications, are the primary targets for advanced malware attacks. Because cyber attackers can disguise these client-side application attacks within multiple layers of application and network protocols, it is nearly impossible for IPS products, to examine the contents of the applications with any granularity.

Endpoint security. Endpoint security products, like anti-virus, are commonplace in IT environments. As endpoint products rely purely on signatures, on their own they are incapable of detecting next-generation threats that exploit new vulnerabilities in commercial software. The endpoint approach forces organizations to wait as long as a few months before known attacks are forensically examined and the appropriate signatures are propagated through the distribution network. In addition, even if endpoint providers are technically able to prepare signatures quickly, they will often delay the dissemination of signature updates to avoid creating liability for themselves if their signature is faulty and inadvertently causes damage to an organization. Furthermore, whitelisting approaches, which are used to tag trusted applications, are vulnerable because approved applications or servers running on whitelisted IP addresses can be infiltrated by threat actors and become conduits for next-generation threats.

Web filters. These appliances provide Web filtering and Web browsing security, but rely on a constantly updated database of bad Website addresses when filtering traffic. Given the pace of change of domains and URLs and the transient nature of the Web, these signatures have become outdated and less relevant for organizations.

Protecting Today s IT Infrastructure Requires a Fundamentally Different Approach to Security

The rapid and unprecedented escalation in the complexity and scale of next-generation threats has made traditional IT security products almost powerless in their ability to defend the world s organizations from the advanced persistent threat actors that are developing them. Any solution that could effectively address these threats would have to be built from the ground up and include the following key capabilities:

Detection and protection capability that overcomes limitations of signature-based approaches. Being able to defend against next-generation threats is now the most critical aspect of any IT security strategy. Central to defending against these threats is a solution that is capable of identifying unknown threats without relying on a signature database and dynamically blocking any exfiltration of sensitive data outside the organization.

Table of Contents

The ability to protect the infrastructure across multiple threat vectors. Today s most sophisticated attacks target all parts of the IT infrastructure across threat vectors what may appear benign in one threat vector may be nefarious when combined with threat data from other threat vectors. To achieve adequate levels of security, IT security administrators must put solutions in place that cover Web, email, file and mobile, which are the four primary ways in which organizations exchange and store information.

Visibility into each stage of the attack life cycle and particularly the ability to detect and block attacks at the exploit phase. Given the complexity of next-generation threats today, it is critical to have visibility into any and all phases of an attack lifecycle for any given threat. The initial exploit is extremely difficult to detect because it is stealthy, can be delivered through tiny bits of code and resides within memory as opposed to within a file on the hard drive. It is paramount that any solution be able to detect and block this initial exploit, because once the exploit has penetrated a system, a beachhead has been established allowing for the payload to be delivered and the attack to be carried out. To effectively detect the exploit phase, it is important to have visibility from the network layer to the operating system to applications, browsers, files and plug-ins. Also, subsequent stages of the attack can then be obfuscated, such as through the encryption of a piece of malware that is downloaded onto a host site. It is also important for this platform to be aware of any process that may represent one of the other stages of an attack lifecycle, as advanced malware can lie dormant but then over time attempt to call back to criminal servers, or be introduced to the network from portable devices like USB drives.

Negligible false-positive rates, thereby allowing the organization s IT infrastructure to be secure without hindering business productivity. An effective solution must deliver a high degree of detection accuracy and minimize the amount of manual intervention required to tune the system.

The ability to scan all relevant traffic without degrading network performance. An effective solution must be able to block threats as effectively as it detects them. As a result, such a solution must have the ability to operate in the line of network traffic without introducing additional latency in the network. In order to do so, a platform must be capable of accurately detecting malicious threats while exhibiting performance capabilities that scale with today s ever-increasing network throughput requirements.

The ability to dynamically leverage knowledge gained by prior threat analysis. An effective solution needs to learn rapidly from previously identified threats, as they occur in real time, and automatically assemble and distribute this intelligence to other devices locally and across a global threat intelligence network.

Rapid deployment and streamlined management capabilities. The majority of existing enterprise-grade security solutions require extensive resources to deploy and operate, often taking weeks to properly install. They also require significant time from IT teams for ongoing configuration and maintenance of the overall solution offering. Security solutions need to deliver faster time to value through rapid deployment with minimal human intervention, as well as simplified and intuitive management capabilities.

Ability to rapidly identify, contain and remediate breaches. In situations where an enterprise is breached, it is critical for the organization to rapidly identify which machines have been compromised across potentially hundreds of thousands of endpoints and contain the breach. Existing endpoint security products lack the ability to rapidly identify the presence of a wide array of potential indicators of compromise, or IOCs, as well as understand the pattern of behavior of the attacker s movements and the nature of the attacking organization itself. Furthermore, most IT security professionals within enterprises are busy with focusing on their everyday business tasks and are not exclusively focused on tracking the latest cybersecurity threats, techniques and threat actors. Organizations need a combination of a software-based product platform and a team of security experts with significant domain expertise to enable them to effectively triage and contain attacks and minimize their exposure after a breach.

Table of Contents

Our Solution

We provide a comprehensive solution for detecting, preventing and resolving advanced cybersecurity threats. We invented a purpose-built, virtual machine-based security platform that provides real-time protection to enterprises and governments against the next generation of cyber attacks. Our technology platform, built on our proprietary MVX engine, is able to identify and protect against known and unknown threats without relying on existing signature-based technologies employed by legacy IT security vendors and best-of-breed point solution vendors. To complement our threat prevention platform, our endpoint-based incident response technology platform enables rapid identification, containment and remediation of attacks on the network. Finally, we offer a team of industry-leading experts in the security industry and managed services to help organizations respond faster to breaches and minimize the exposure to their business.

The key benefits of our solution include:

Proprietary MVX engine to enable dynamic, real-time protection against next-generation threats. Our appliance combines dynamic threat intelligence with our proprietary virtual execution engine to analyze network traffic in real time. Our proprietary virtual execution engine is able to capture, analyze, execute, identify and report on next-generation threats. Because our hypervisor, or software that creates and runs virtual machines, resides below the operating system, we are able to detect attacks throughout the protocol stack from the network layer to the operating system, to files, applications, browsers and plug-ins. By executing the potential threat in a virtual environment created by our MVX engine, our appliance can accurately determine if the behavior exhibited by the software is malicious before it enters the network. Each virtual machine has the unique ability to test hundreds of different applications and a complete set of all versions of those applications, Web objects and attachment types. It also has the ability to mimic hundreds of different potential customer operating system environments and versions. Our MVX engine has the ability to run numerous virtual machines per appliance, which can run hundreds of permutations of attacks across four primary vectors (i.e., Web, email, file and mobile) and all stages of the attack life cycle. Our platform can support thousands of virtual machines across multiple appliances within an organization. Finally, our global intelligence network, in concert with our CMS appliance, coordinates and correlates all of this Dynamic Threat Intelligence, or DTI, information at both an enterprise and global level. We believe this ability to process millions of data points and find the needle in the haystack, or the set of potentially malicious threats, is a significant achievement in the field of computer science and represents a foundational competitive advantage.

Proactive defense from network to endpoint. Our broad product portfolio includes software-based appliances, cloud services and endpoint solutions to protect against Web and email threat vectors, malware resident on file shares, malicious mobile applications and targeted endpoints. Each of these elements of our product portfolio interoperates seamlessly with the others, enabling the real-time sharing and correlation of information across all of the appliances within a customer s infrastructure. By deploying our products across all vectors of attack, we provide not only the broadest level of protection for our customers, from network to endpoint, but also utilize in-depth contextual analysis and coordinated threat intelligence to further enhance our overall efficacy rates because many advanced cyber attacks, such as blended attacks, infiltrate the organization through more than one vector.

Visibility of each stage of the attack life cycle and particularly the ability to detect and block attacks at the exploit phase. Our platform enables a comprehensive, stage-by-stage analysis of next-generation threats, from initial system exploitation to data exfiltration. Because our virtual execution engine can detonate all suspicious traffic flowing through the network, we virtually execute all of the flows of an attack, enabling us to play out the execution path of a piece of malware over a prolonged period of time and uncover, for example, any attempts to call back to a command and control server. Furthermore, because we can watch the execution path of the initial exploit with a high degree of granularity, we have high detection accuracy at the exploit level. Next-generation threats often encrypt the malware they download, making virtual execution impossible unless it has been monitored at the exploit phase. In the exploit phase, our appliance collects the encryption key necessary to properly execute the

program in a virtual environment. We are also able to detect threats by running the exploit, not just the malware, through our virtual execution engine, which provides greater defense efficacy since we have an additional point at which we can detect suspicious behavior.

High efficacy next-generation threat detection. When evaluating a potential threat, our proprietary virtual execution engine mimics multiple production environments simultaneously, causing the potential malicious software to reveal itself by executing in what appears to be a real machine. We can address the hundreds of permutations of software environment targeted by advanced malware attacks by concurrently deploying thousands of virtual machines across an organization s network, allowing us to monitor attempted exploits of multiple operating system and application versions and hundreds of object types at line speed. This approach allows for high detection efficacy with negligible false-positive rates, resulting in minimal disruption to the business and IT organization.

Real-time detection across all network traffic with negligible performance degradation. All of our software-based appliances are capable of operating in-line, providing comprehensive and highly accurate detection and protection without slowing down the network. We accomplish this by deploying a scalable technology architecture that processes traffic through our proprietary anomaly detection and associated heuristic algorithms that complement the virtual machine analysis. As a result, we limit the network traffic to be processed by our virtual machine technology. Furthermore, our DTI cloud provides significant intelligence on next-generation threats that are already known, enabling us to confidently block certain traffic that we have already previously identified. Our proprietary technology enables us to process the remaining traffic in a scalable fashion, running hundreds of potential virtual machines at any given time for each appliance. Our high-performance virtual machine technology, working in concert with our cloud services and advanced heuristic algorithms, enables us to deliver industry-leading protection against next-generation threats while scaling with our customers network throughput requirements.

Global cloud-based data sharing within and across organizations. Our CMS correlates threat information generated by our Threat Prevention appliances and facilitates rapid sharing of information across multiple appliances within a customer environment as well as across thousands of customer networks. In addition, by sharing anonymous real-time global threat data through our DTI cloud, our customers have access to a system that leverages the network effects of a globally distributed, automated threat analysis network. By combining our MVX engine with our DTI cloud, our platform is able to increase performance while providing robust and comprehensive threat protection.

Rapid deployment and rich centralized management capabilities. Our Threat Prevention appliances are easy to deploy with minimal modification to existing networks and seamlessly integrate with other devices in such networks. These appliances are generally deployed in a few hours and most often find existing next-generation threats immediately after deployment. Our CMS appliances offer rich management capabilities, such as coordinating software upgrades, automating the configuration of multiple appliances and presenting security data in an intuitive interface to facilitate reporting and auditing. By designing our solutions to be easy to deploy and manage, we enable our customers to shorten the time to value for our products.

Tightly integrated incident response, managed services and contextual data. Our in-depth understanding of advanced threats and how they manifest themselves in a customer environment allows us to offer various high value-added security services that complement our product portfolio. We offer managed defense services through which we proactively notify customers in the event of advanced threats, thereby allowing customers to focus on their business yet minimizing the time to respond to such threats. We can deploy and manage additional endpoint and network technologies that, when combined with other elements of our solution, allow us to provide customers with precise and actionable intelligence regarding the threat, the likely actors behind the threat, the assets these actors are after, and next steps to contain the threat and remediate any damage done. Furthermore, in the event of a breach, we can leverage our industry-leading team of consultants to respond quickly to threats to a customer s environment, scope and minimize damage, and quickly restore the environment to an operational state.

Table of Contents

Our Market Opportunity

According to IDC, worldwide IT security spending in 2013 was approximately $16.8 billion across firewalls, virtual private networking, Web security, unified threat management, intrusion detection and prevention, messaging security and corporate endpoint security.[6] While this spending is focused principally on traditional IT security products, we believe the rise in next-generation threats is creating significant new demand from organizations for products that offer advanced protection against this new threat paradigm. Gartner, Inc., a global market research firm, estimates that, By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2013.[7]

Our technology approach represents a paradigm shift from how IT security has been conducted since the earliest days of the information technology industry. We believe it will be a critical imperative for organizations worldwide to invest in new solutions that protect their IT infrastructure from next-generation threats. We believe our platform is essential to protect these organizations against next-generation threats. As such, we believe that this approach will take an increasing share of IT security spending from traditional enterprise IT security markets. Specifically, we believe this approach can be applied to initially supplement, and ultimately replace, any threat protection technology that utilizes a traditional signature-based approach. These markets consist of Web security ($2.1 billion), messaging security ($2.6 billion), intrusion detection and prevention ($1.9 billion) and corporate endpoint security ($3.7 billion), and aggregate to a total projected spending of $10.3 billion in 2013, in each case according to IDC.[6] We also provide solutions that address the IT security consulting industry, which was $6.2 billion in 2013, according to IDC.[6] With the acquisition of Mandiant, we have added solutions that address portions of the managed security services, or MSS, market and the security incident and event management, or SIEM, market. In a recent report, Gartner estimated that the MSS Market will grow from US$12 billion in 2013 to more than US$22.5 billion in 2017.[8] Separately, Gartner has also estimated that SIEM spending would total approximately $1.6 billion in 2013.[8]

Our Competitive Strengths

We believe we are the leader in protecting enterprises and governments against advanced cyber attacks. We have developed the following key competitive advantages that we believe will allow us to maintain and extend our leadership position:

Leader in protecting organizations against the new breed of cyber attacks. We are the inventor of and a leader in providing a virtual machine security approach to protect enterprises and governments against the next generation of cyber attacks. Given the significant potential cost and reputational damage to organizations that can arise from being vulnerable to next-generation threats, we believe that we have become a mission critical vendor to the most discerning customers in the world. This provides us with a strong leadership position, which allows us to attract top technical talent and brands us as the de-facto standard in a rapidly growing and increasingly important market.

Platform built from the ground up to address next-generation threats. We were founded with the sole purpose of developing a platform to detect and block next-generation threats. To achieve this goal, we developed a proprietary hypervisor (i.e., software that creates and runs virtual machines) and MVX engine to meet the specific challenges associated with high throughput processing of next-generation threats. Our proprietary hypervisor, which is purpose built for security, allows us to achieve a significant level of accuracy and processing efficiency. Unlike recent attempts by others to process next-generation threats with sandbox approaches that use third-party hypervisors, our proprietary hypervisor technology allows us to make fundamental improvements and scale our technology to run several virtual machines on each appliance to simultaneously detect multiple threats. We have over one million virtual machines running across our customer environments. We can also embed strict,

6 See note (2) in Market and Industry Data.

7 See note (1) in Market and Industry Data.
8 See note (3) in Market and Industry Data.

government-grade security defenses in our hypervisor to prevent the virtual machine itself from being compromised and also make the virtual environment indistinguishable from a real host environment. In addition, we can run hundreds of permutations of files, operating systems, software versions, languages and applications to mimic desktop operating environments and force malicious software to reveal itself. We have custom built our anomaly detector, which is now in its third generation, with a focus on helping to filter potentially suspicious data from benign traffic. This filtering allows most normal traffic to pass through and any other traffic to be executed in our virtual machine. While our virtual machine can ultimately process all traffic, using an anomaly detector helps to increase network throughput and limit the amount of traffic that requires virtual execution.

Unique capabilities across threat detection, prevention and resolution. We offer a comprehensive solution for detecting, preventing and resolving advanced cybersecurity threats. The integration of detection and response provides a seamless solution that enables more rapid threat identification and resolution and lowers the cost of ownership for customers by reducing the number of products they would otherwise have to separately integrate. We believe we are the only vendor that offers an end-to-end solution for advanced threat protection and that we are uniquely positioned to capture market share based on the broad applicability of our platform and ability to meet all of our customers advanced threat protection needs.

Network effects from our customer base and DTI cloud. The combination of our global installed base of over 1,900 end-customers with over two million virtual machines across customer environments provides us with a rich and broad set of dynamic threat protection data. By sharing this data with our global customer base, we are able to provide both a higher level of protection and higher performance. Because we are protecting many high-profile enterprise and government targets, we are the first to see the most advanced threats and attack techniques, often months or years before our competitors, and are therefore able to develop superior defensive countermeasures that continue to perpetuate our ability to provide the highest level of protection. Our close relationship with customers also allows us to develop insights and knowledge into how they use our products, which we are able to translate into platform enhancements. This relationship between customers and differentiated threat intelligence drives a network effect around our company, leading additional customers to be increasingly attracted to the depth and breadth of our capabilities and intelligence.

Strong management team with significant IT security expertise. We have a highly experienced management team with extensive IT security expertise gained from past service in leading IT security and networking companies. Our Chief Executive Officer, David G. DeWalt, previously served as the Chief Executive Officer of McAfee and is also a member of the President s National Security Telecommunications Advisory Committee. Our Founder, Chief Technology Officer and Chief Strategy Officer, Ashar Aziz, is an inventor on multiple patents in the areas of cryptography, network security and networking and is widely regarded as an IT security visionary. Our Senior Vice President and Chief Operating Officer, Kevin Mandia, is the founder and former Chief Executive Officer of Mandiant and previously served as the director of computer forensics at Foundstone, as the director of information security for Sytex and as an officer in the United States Air Force. We believe that our management team and unique engineering talent places us at the leading edge of the IT security industry and positions us well to continue to lead the broader IT security industry to adopt our proprietary virtual machine-based approach.

Comprehensive platform that enables modular deployment options. Our customers typically initially deploy our solution at one of the threat vectors that we protect, such as Web, email, file or mobile. Once deployed for an initial threat vector, our customers can then deploy additional appliances to protect the same threat vector, as well as expand their level of protection to additional vectors to achieve end-to-end protection for the primary vectors through which next-generation threats enter IT environments. Customers can also purchase our CMS appliances, which enhance the management of multiple appliances and the overall level of threat intelligence across appliances protecting different vectors. Our comprehensive multi-vector platform enables us to enter a customer network for a single

Table of Contents

use case and expand over time, allowing us to become a critical part of our customers security infrastructure and offering us significant revenue opportunities. In addition, customers can expand protection from the network to the endpoint by deploying our endpoint threat prevention solutions.

Significant technology lead. Our technology is recognized as innovative and is protected by, among other things, a combination of copyright, trademark and trade secret laws; confidentiality procedures and contractual provisions; and a patent portfolio including 16 issued and 78 pending U.S. patents.

Our Strategy

We are the global leader in virtual machine-based security solutions that protect against next-generation threats. Our objective is to extend our global leadership by making virtual machine-based security the standard for how IT security is conducted across all categories of threat protection. The key elements of our strategy include:

Invest in research and development efforts to extend our technology leadership. We plan to build upon our current performance and current technology leadership to enhance our product capabilities, such as protecting new threat vectors and providing focused solutions for certain markets, such as small and medium-sized enterprises and service providers. Moreover, we intend to deliver additional physical and virtual appliances to address the changing security needs of our customers as well as access new product markets and threat vectors.

Expand our sales organization to acquire new customers. We intend to continue to invest in our sales organization to drive the efficient acquisition of new customers. In particular, we intend to significantly increase our investments in our international sales organizations as we pursue larger enterprise and government opportunities outside of the United States. As of December 31, 2013, we had grown our sales organization to 495 employees, including direct field and inside sales employees and sales support engineers.

Expand our channel relationships and develop our partner ecosystem. We believe our channel serves a critical role in our direct-touch sales process, and we intend to continue to invest in our channel and partner ecosystem. In particular, we believe the role our channel partners play in international markets is vital to the sale of our products in those regions. We have established a channel program that, as of December 31, 2013, had approximately 625 channel partners worldwide. We work with many of the world s leading IT security channel partners. We intend to continue adding and incentivizing our distributors and resellers to drive greater sales and enable further leverage for our internal sales organization. We may also develop OEM relationships as other providers of security, networking and application infrastructure products seek to enhance the security of their products by embedding our proprietary virtual machine-based technology.

Drive greater penetration into our customer base. We believe our over 1,900 end-customers provide us a large market opportunity to drive incremental sales. Typically, customers initially deploy our platform to protect a portion of their IT infrastructure against one type of security threat, such as Web-based threats. We see a significant opportunity to upsell and cross sell additional products, subscriptions and services as our customers realize the increasing value of our platform. We often expand our presence within our customers IT infrastructures to cover a broader portion of their network, address additional threat vectors, such as email and file-based threats, and manage multiple appliances. With the addition of Mandiant, we believe there is significant opportunity to leverage the inherent synergies between products and services. For customers that are initially interested in purchasing our products, we are able to offer them the additional protection and expertise that our services provide. Similarly, when our team of cyber security experts are assisting customers that have experienced a breach, we can help prevent future breaches by introducing them to the value and protection provided by our products.

Leverage our innovative virtual machine technology in additional product markets. We believe our patented virtual machine technology can serve as a foundational element for the next generation of IT security products. We intend to apply our purpose-built

virtual machine security engine to additional

Table of Contents

security markets that can benefit from the real-time virtual execution of potentially malicious software. In particular, we believe our technology can apply to any threat-protection technology that utilizes a traditional signature-based approach, such as IPS and Web filters. We believe these additional solutions will be critical for organizations to adapt to the rapidly evolving threat landscape.

Our Products and Services

Products

Threat Prevention System. Our Threat Prevention System consists of vector-specific security appliances that provide comprehensive next-generation threat protection, from network to endpoint, for both inbound and outbound network traffic that may contain sensitive information. Our portfolio of Threat Prevention appliances include the following appliances covering the Web, email and file threat vectors:

Web Threat Prevention. Our Web Threat Prevention appliances are deployed in-line at enterprise Internet access points to analyze all Web traffic. Utilizing our MVX engine, these appliances identify and block next-generation threats deeply embedded inside Web traffic, create real-time protection descriptors from the identified threats, and capture potential multi-protocol outbound communication data from threats that may already be inside the network. Our MVX engine detects advanced attacks exploiting unknown vulnerabilities as well as malicious code embedded in common Web and multimedia content. Our MVX engine executes suspicious software against a range of browsers, plug-ins, applications, and operating environments that are instrumental in tracking malicious actions. As potential threats can sometimes enter the network via user devices and may have been resident in the network previously, our MVX engine also analyzes outbound traffic for threats that may attempt to extract sensitive information or enable control of devices within the network by communicating with servers. In September 2013, we introduced the NX 10000, a multi-gigabit throughput appliance that can be deployed in-line at Internet egress points to block Web exploits and outbound multi-protocol callbacks. Using our MVX engine, the NX 10000 confirms zero-day attacks, generates real-time security intelligence and captures dynamic callback destinations to defend against attacks. In December 2013, we introduced our NX 900 to enable threat protection at various remote and branch offices as well as at the homes of an organization s executive officers and key personnel.

Email Threat Prevention. Our Email Threat Protection appliances detect and stop advanced attacks that exploit unknown OS, browser, and application vulnerabilities as well as malicious code embedded in email content. Using our MVX engine, these appliances analyze all email attachments, including all common file and archive formats. In particular, these appliances secure networks against spear phishing emails, which bypass traditional anti-spam and reputation-based technologies. Spear phishing is a common next-generation threat that is effectively a method used by cybercriminals for financial gain or to extract sensitive information by sending professionally disguised email to users hoping the users respond to what they believe are benign email communications. Our MVX engine actively executes, and is able to quickly identify, this malicious content.

File Threat Prevention. Our File Threat Prevention appliances analyze network file servers to detect and quarantine malicious software brought into the network by users within the organization through technologies, such as online file sharing and associated collaboration tools, which bypass traditional network solutions. These appliances analyze files using our MVX engine and detect malicious code embedded in common file types, including PDF, Microsoft Office documents, archived files, and multimedia content such as QuickTime and other video, audio and image files. Our File Threat Prevention appliances perform recursive, scheduled, and on-demand scanning of accessible network file servers to continuously identify and quarantine resident threats.

Central Management System. Our Central Management System, or CMS, unifies reporting, configuration, and threat data sharing and manages the overall deployment of our Threat Prevention

110

Table of Contents

System. CMS appliances are used to distribute the dynamic descriptor content locally to the appliances in our Threat Prevention System to provide real-time protection throughout our entire deployment. The CMS also provides cross-enterprise threat data correlation to identify and block blended attacks wherever they may occur in a large global enterprise. It also consolidates the management, reporting, and data sharing of threat data in an easy-to-deploy, network-based appliance. The CMS consolidates activities and improves organization-wide situational awareness with a unified security dashboard, which provides a real-time view of the number of infected systems and enables users to drill down directly to infection details.

Forensic Analysis System. Our Forensic Analysis System provides powerful auto-configured test environments to allow forensics teams to manually execute and inspect advanced malware, zero-day, and other advanced cyber attacks embedded in files, email attachments, and Web objects. The Forensic Analysis System inspects single files or batches of files for malware and tracks outbound connection attempts across multiple protocols. In virtual execution mode, the Forensic Analysis System analyzes the execution path of a particular malware sample to generate a dynamic and anonymized profile that can be distributed to other FireEye appliances on the network. Malware attack profiles include identifiers of malware code, exploit URLs, and other sources of infections and attacks. To fully analyze the behavior of every unknown file, the Forensic Analysis System provides full malware life cycle analysis. While the Forensic Analysis System is not required for deployments, our larger customers typically purchase the product to enable advanced and deeper analysis of potential malicious software outside of the real-time traffic scanning done by our Threat Prevention appliances.

Endpoint Threat Prevention System. Our Endpoint Threat Prevention System is an appliance and endpoint agent-based system that equips security organizations to confidently detect, analyze and resolve security incidents in a fraction of the time it takes using conventional approaches. The Endpoint Threat Prevention System enables security operations teams to connect the dots between security incidents in their networks and endpoints to provide the holistic picture required to find and scope security breaches as they are unfolding. In addition to applying proprietary intelligence to sweep for indicators of compromise, or IOCs, our Endpoint Prevention System automatically investigates alerts generated by FireEye products, SIEM, log management and other network security solutions, to identify the specific devices that have been impacted and assess the potential risk. Security operations teams receive the information they need, when they need it, to make rapid, accurate decisions about potential incidents. When a suspected incident is confirmed, the endpoints involved can be contained with a single click to deny the attacker access while still allowing forensic investigations to continue.

Subscription and Services

Product Subscriptions. The following product subscriptions are attached to our product sales:

Dynamic Threat Intelligence Cloud (DTI). Our Dynamic Threat Intelligence, or DTI, cloud interconnects the FireEye appliances deployed within customer networks, technology partner networks, and service providers around the world. Our global FireEye Labs team identifies emerging threats, collects threat samples, and replicates, reviews and characterizes attacks. Threat intelligence is also dynamically generated by each MVX engine to provide real-time forensics used to protect the local network and can be shared globally through our DTI cloud. We leverage the threat intelligence we conduct as well as the real-time analysis from our appliances to update our malware descriptors, attack definitions, scanning engines, and other security solution components. We can easily distribute these updates to customers through our DTI cloud. Our DTI cloud provides a closed-loop system that leverages the network effects of a globally distributed, automated threat analysis network enabled by our Threat Prevention appliances. Customers are required to purchase either a one or three year DTI cloud subscription as part of their initial appliance purchase.

Email Threat Prevention Attachment/URL Engine. Our Email Threat Prevention Attachment/URL engine analyzes email attachments and URLs embedded in emails for next-generation

Table of Contents

threats. Customers who purchase the Email Threat Prevention appliance are also required to purchase a one or three year subscription to our Email Threat Prevention Attachment/URL engine.

Security-as-a-Service Offerings.

Managed Defense. Managed Defense is a hosted service whereby we monitor a customer s network and provide a full-service offering that brings together all of the experts, experience and technology required to find attackers at any stage of the attack and respond aggressively before they complete their mission. Managed Defense delivers timely, actionable reports of compromise with negligible false positive rates. We do this through real-time network monitoring and traffic analysis, layered with advanced sweeps of enterprise endpoints and active hunting for adversaries, maintaining vigilance 24x7. Analysis is delivered to provide organizations with the context they need to fully understand the threat, assess risk and prioritize action. We can also provide precise, actionable intelligence to customers regarding how to contain the threat and remediate the environment. In cases where a breach has occurred, the Managed Defense team can bring our incident response consultants onsite as an additional value-added service.

Cloud-Based Email Threat Prevention. Our cloud-based Email Threat Prevention service protects against today s advanced email attacks. With no hardware or software to install, the cloud-based Email Threat Prevention service is a particularly good fit for organizations already moving their email infrastructure into the cloud. To start protecting against malicious emails, organizations simply route messages to the Email Threat Prevention service. The cloud then uses the signature-less MVX engine to detect threats and stop APT attacks in real time.

Mobile Threat Prevention. Our Mobile Threat Prevention service identifies malicious applications downloaded onto the Android platform and works with the organization s infrastructure to prevent these applications from causing damage to the organization. These mobile applications can be downloaded from widely available commercial application stores as well as custom enterprise applications. Rather than relying on malware signatures, which are powerless against today s fast-moving, constantly changing threats, our Mobile Threat Prevention service executes applications within our MVX engine and provides an automated mobile threat assessment that enables organizations to enforce security policies in the mobile environment.

Customer Support and Consulting Services. We provide the following customer support and consulting services that are marketed under the Mandiant brand.

Incident response and related consulting services. We have a team of cyber security experts that can quickly respond to customers that have experienced a breach and help them understand the scope of the incident and quickly remediate the attack. Our cyber security experts will inform customers who is behind the attack (i.e., organized crime, nation state or malicious insider) and how much damage was done, and will work with them to recover from the incident while minimizing the impact of the event on the organization. We have performed hundreds of successful computer security investigations across all industries, organization sizes and technical environments. As part of our services, we can help customers organize their own security programs, help with litigation support and forensics, and assist with threat and vulnerability assessments.

Training and professional services. We offer training services to our customers and channel partners through our training department and authorized training partners. For both our customers and our channel partners, these services are designed to provide education regarding implementation, use and functionality, and maintenance and support of our products. Specifically for our channel partners, we also provide training regarding how to manage all stages of our sales cycle. We also offer professional services to customers for large implementations where expert technical resources are required. Our professional services consultants help in the design of deployments of our products and work closely with customer engineers, managers and other project team members to implement our products according to design, utilizing network analysis

Table of Contents

tools, attack simulation software and scripts. We provide professional services directly to our customers, but also deliver these resources by enabling our authorized partners, who provide similar services to our customers.

Customer Support and Maintenance Services. We offer technical support on our products and subscriptions. We provide multiple levels of support and have regional support centers located across the globe. Our service representatives work with customers to qualify and solve technical challenges that they may encounter. In addition to post sales support activities, our support organization places emphasis on service readiness by coordinating with our product management team to ensure the attainment of defined pre-requisite quality levels for our products and services prior to release. Like our subscription services, our support and maintenance contracts have terms of either one or three years.

Our products are designed to address security requirements for small-to-mid sized businesses, remote offices, large enterprises, governments and service providers. The table below presents an overview of the various FireEye appliance models and capabilities:

Product Category	Models / Types	Key Features	Subscriptions
Web Threat Prevention	NX 900	1U to 2U Rack-mount	DTI
	NX 1400	10Mbps to 4 Gbps throughput	
	NX 2400	50 40,000 users	
	NX 4400	Broad Web object support	
	NX 4420		
	NX 7400		
	NX 7420		
	NX 1000		
Email Threat Prevention	EX 3400	1U to 2U Rack-mount	DTI
	EX 5400	Email quarantine	Email Threat Prevention Attachment/URL Engine
	EX 8400	Spear phishing security	
	EX8420	Anti-Virus integration	
File Threat Prevention	FX 5400	1U to 2U Rack-mount	DTI
	FX 8400	File quarantine	
		Deep file analysis	
		Anti-virus integration	
		Broad file type support	
Central Management	CM 4400	1U to 2U Rack-mount	
	CM 7400	Threat Prevention Appliance management	

	CM 9400	Blended attack correlation	
		SIEM Integration	
		Detailed reporting	
Forensic Analysis	AX 5400	1U to 2U Rack-mount	DTI
	AX 8400	Full threat lifecycle analysis	
		Sandbox and honeypot modes	
		Broad file type support	
Endpoint Threat Prevention	HX Series	Endpoint validation for advanced threats	DTI
		One-click containment across all endpoints	
		Agent Anywhere technology to monitor within and outside corporate network	

Table of Contents

The list price of our products range from approximately $8,000 to $350,000 based on throughput and other performance requirements.

Our Technology

The key technologies underlying our platform have been built from the ground up to address next-generation threats. Our foundational technologies are: (i) line rate anomaly detection, (ii) proprietary MVX, (iii) exploit stage monitoring, (iv) cross correlation, and (v) evolved network security architecture. We have built our technology over ten years of research and development, and we believe it represents a significant competitive advantage for us.

Custom Anomaly Detector. Commercial anomaly detectors are common place in IT security. While such anomaly detectors are the foundation for IPS solutions, they generate a significant number of false positives, making their efficacy in detecting IT security threats challenging. We have custom built our anomaly detector with a focus on helping to filter potentially suspicious data from benign traffic. This filtering allows for most normal traffic to pass through and any other traffic to be executed in our virtual machine. While our virtual machine can ultimately process all traffic, using an anomaly detector helps to increase network throughput and limit the amount of traffic that requires virtual execution. We are constantly improving the efficacy of our anomaly detector as we discover new threats in our virtual machine. Our anomaly detector also receives updates from our DTI cloud in the attributes, or markers, it looks for when inspecting potentially suspicious data. Uniquely, because the line rate anomaly detector is designed to feed suspicious flows to our MVX engine, it can focus on minimizing missed attacks by aggressively categorizing traffic as suspicious. Any potential false alerts in the output of this system are automatically weeded out by our MVX engine, which confirms whether a suspicious flow or object is malicious. Because we first identify suspicious flows with our line rate anomaly detector and then, through a separate process, use our MVX engine to determine whether such suspicious flows are malicious, our solution is able to achieve negligible false-positive rates and missed attacks, which are the desired results of the ideal detection engine.

Proprietary MVX Engine**.** Our appliances utilize a proprietary virtual execution engine to execute potentially suspicious software code. We have built our virtual execution engine to take advantage of advances in multi-core processing and run on many-core network processors. As we do not use a commercially available virtual machine, we are not encumbered by any incremental overhead beyond the execution of our environments and the detection of threats. We are also free to make modifications to the code base of our virtual execution engine, which our competitors are not able to do. Our virtual execution engine mimics operating systems and configurations of several user devices, including several popular operating systems, applications and Web browsers. Once the unknown software code is loaded into this environment, our engine monitors the software s behavior. Using a proprietary behavior analysis technology, our appliances determine if the actions the code is taking in the virtual environment are malicious or benign. We have developed our MVX engine over the past nine years to provide high performance next-generation threat protection while maintaining high threat detection efficacy, negligible false-positive rates, and minimal impact on network performance.

Exploit Stage Monitoring**.** Our appliances are able to monitor the full spectrum of data that enters the network. This allows visibility into all stages of an attack, including the exploit phase, where an attacker first compromises a program. The exploit object can be embedded in any piece of content, such as an ordinary Web page. This stage is invisible to legacy network security technologies that are focused on examining files and executables once they are written to the hard drive on a host computer. Next-generation threats often encrypt the malware file they download, making virtual execution impossible unless it has been monitored at the exploit phase. In the exploit phase, our appliance collects the encryption key necessary to properly execute the program in a virtual environment. We are also able to detect threats by running the exploit, not just the malware, through our virtual execution engine, which provides greater defense efficacy since we have an additional point at which we can detect suspicious behavior.

Table of Contents

Multi-Vector Cross Correlation. Our Threat Prevention appliances, when deployed with the CMS appliance, communicate in real time on threat information as well as receive updates from our DTI cloud. This awareness allows our appliances, which are specific to threat vectors, to communicate threat data to each other in real time to prevent sophisticated multi-vector threats, particularly blended attacks. This cross-fertilization of traffic information enables our appliances to piece together seemingly benign components of a broader blended or multi-vector attack. Cross correlation requires Threat Prevention appliances that target different vectors and our CMS appliance work in concert.

Evolved Network Security Architecture. Our appliances are designed to operate as part of a comprehensive architecture to defend networks against next-generation threats. This allows appliances to be deployed at the right vectors and have visibility into the traffic streams necessary to detect and block next-generation threats. The ability to monitor all traffic and file stores is critical to detecting next-generation threats that will enter through multiple vectors and move laterally across the network. This is impossible for legacy network security providers to achieve with architectures that were built around traditional threats and file scanning and don t have visibility into the traffic sources next-generation threats utilize during attacks.

Advanced Endpoint Validation and Containment. Our Endpoint Threat Prevention System is an appliance and endpoint agent-based solution that enables real-time automated validation of security incidents across thousands of endpoints to contain the impact of an incident. The Endpoint Threat Prevention System allows customers to uncover attacks in their environment by identifying indicators of compromise, or IOCs, on endpoints left behind by attacker activity. Suspicious hosts are flagged using non-signature based intelligence so customers can confirm the scope of the attack, identify and contain all compromised hosts and quickly secure their networks.

As our Threat Prevention appliances are typically deployed in-line with network traffic, they analyze traffic through the following four major phases.

Fast Path Blocking. To maintain high network throughput and leverage known threat data, our Threat Prevention appliances utilize our proprietary database of threat intelligence as well as third-party threat data feeds to perform identification of known threats. If the traffic is identified as malicious, it is blocked immediately. If the traffic is not identified as malicious, it is passed to our custom anomaly detector. Threat intelligence includes behavioral information about the threat, versus a specific byte-by-byte fingerprint found with signatures. This helps us to guard against threats that can evolve over time.

Line Rate Anomaly Detection. Traffic that is not blocked in our fast path blocking phase is passed to our proprietary anomaly detector. The anomaly detector is designed to identify any remotely suspicious network flows. We have custom built our anomaly detector to deliver high levels of accuracy while preventing any threats from being missed. If any suspicious attributes are detected, the flow is passed on to the virtual execution environment.

MVX Execution. Through a pre-configured, instrumented virtual analysis environment, our MVX engine fully executes suspicious objects and flows to allow deep inspection of common file formats, email attachments, and Web objects. Newly discovered malware is installed and executed to completion within our MVX engine so that it is forensically analyzed, tracked and blocked. Analysis of malware is automated to create dynamic blocking of inbound attacks and its outbound transmissions.

Notification. If a threat is identified in the virtual environment, the associated DTI gained in the process is shared with other FireEye appliances on the network through our CMS appliance and globally via our DTI cloud.

Customers

Our customer base has grown from over 450 end-customers at the end of 2011 to over 1,900 end-customers as of December 31, 2013 in more than 60 countries, including more than 130 of the Fortune 500. We provide products and subscriptions to customers of varying sizes, including enterprises, governmental agencies and

educational and nonprofit organizations. Our customers include leading enterprises in a diverse set of industries, including telecommunications providers, financial services entities, Internet search engines, social networking sites, stock exchanges, electrical grid operators, networking vendors, oil and gas companies and leading U.S. and international governmental agencies. Our business is not dependent on any particular end-customer as no end-customer represented more than 10% of our revenue for any of the years ended December 31, 2011, 2012 or 2013. Accuvant, one of our resellers, accounted for approximately 12% and 10% of our revenue for each of the years ended December 31, 2011 and 2012, respectively. For the year ended December 31, 2013, Carahsoft Technology Corp., one of our distributors, and Accuvant accounted for approximately 11% and 11% of our revenue, respectively.

Customer Case Studies

The following are examples of customers successfully deploying our platform to protect their organizations against next-generation cyber attacks:

Fortune 500 Global Manufacturer

Problem: As a global manufacturer with annual sales of over $20 billion and more than 100,000 employees, this enterprise was increasingly targeted with advanced malware, zero-day, and other next-generation threats. This enterprise needed a way to identify and combat these attacks across a number of distributed properties, including those of recently acquired companies. As a result, to be viable, any solution needed to be not only effective, but also easy to deploy and efficient to manage.

Solution: With our virtual machine-based security solution, this global manufacturer can detect and block a broad range of cyber-attacks, including advanced malware, spear phishing and other next-generation threats. Our Web Threat Prevention appliance and Email Threat Prevention appliance were deployed across existing corporate offices, and now, before an acquired company s networks are integrated with the enterprise, the enterprise deploys our solution to ensure newly acquired properties do not introduce new vulnerabilities or compromise the enterprise s IT security. Since deployment, our solution identified over 10,000 malicious events and callback communications that circumvented and were undetected by the enterprise s legacy, signature-based systems, including approximately 20 APT attacks. Security professionals within the enterprise realized the value of our solution almost immediately upon deployment. As a result of this success, after installing our Web Threat Prevention appliance and CMS appliance in 2010, the enterprise subsequently purchased our Email Threat Prevention appliance and additional Web Threat Prevention appliances in 2011. As of December 31, 2012, the aggregate price of the products, subscriptions and services purchased by this manufacturer from us was approximately 2.7x the amount it initially purchased from us in 2010.

Global Telecommunications Enterprise

Problem: As one of the largest global telecom companies, this enterprise was the target of an onslaught of cyber-attacks. Protecting customer data and intellectual property was vital, yet the enterprise s existing security architecture was ill-equipped to detect the multi-vector, multi-phased attacks that were being encountered.

Solution: The enterprise started by purchasing our Web Threat Prevention appliance in the fall of 2012. It quickly determined that it needed broader protection and subsequently purchased our Email Threat Prevention appliance and CMS appliance. Working together, these appliances detect threats on a daily basis that were not being discovered by the enterprise s signature-based security solutions alone. Our solution has

identified more than 200,000 Web and email threats and over 1,000 sophisticated APT attacks. Given the value the enterprise has seen delivered, it has begun to offer its own customers a security service that leverages our solution.

Global Information Technology and Electronics Company

Problem: As one of the largest information technology and electronics companies in the world, this enterprise had critical intellectual property that needed to be protected. The security team was concerned that the

enterprise s existing security architecture was missing advanced attacks that were exploiting unknown, zero-day vulnerabilities. As a result, the enterprise was increasingly exposed to cyber attacks that it believed could have a devastating impact on its business.

Solution: The enterprise has leveraged our Web Threat Prevention appliance and Email Threat Prevention appliance to ensure real-time protection of its corporate network. In its initial testing of our solution, the enterprise s security team immediately identified hundreds of breached systems from which calls were being made to servers outside of the enterprise s networks. The enterprise was also able to immediately detect an APT attack that had infiltrated its network and had been missed by the enterprise s prior defenses. Since deploying our solution, the enterprise has identified thousands of advanced threats that had not been detected by its prior defenses.

Backlog

Each order for services for multiple years is billed shortly after receipt of the order and is included in deferred revenue. The timing of revenue recognition for services may vary depending on the contractual service period or when the services are rendered. Products are shipped and billed shortly after receipt of an order. We do not believe that our product backlog at any particular time is meaningful because it is not necessarily indicative of future revenue in any given period, as such orders may be delayed. Additionally, the majority of our product revenue comes from orders that are received and shipped in the same quarter.

Sales and Marketing

Sales. Our sales organization consists of a direct sales team and channel partners who work in collaboration with our direct sales team to identify new sales prospects, sell products, subscriptions and services, and provide post-sale support. Our direct field sales team is responsible for securing enterprise and government accounts globally. Our direct inside sales organization is responsible for securing medium and smaller organizations that are focused on protecting key assets. We also recently built a strategic account management team to support and expand sales within our customer base. Our sales cycle varies by industry, but can last several months, although some deals close in only a few weeks given the typically shorter deployment time of our products as compared to traditional network security products. Our incident response engagements are generally sold through inbound inquiries from customers that have recently experienced a breach. The sales cycle for these engagements is typically a few days. We also have a dedicated team focused on the channel that works with our direct sales organization to manage the relationships with our channel partners and work with our channel partners in winning and supporting customers. We believe this direct-touch sales approach allows us to leverage the benefits of the channel as well as maintain face-to-face connectivity with our customers, including key enterprise accounts. We expect to continue to grow our sales headcount in all markets, particularly in countries where we currently do not have a direct sales presence. In our most recent quarter, nearly a third of our engagements with prospects have been led by channel partners.

Our sales organization is supported by sales engineers with deep technical domain expertise who are responsible for pre-sales technical support, solutions engineering for our customers, proof of concept work and technical training for our channel partners. We believe that, by providing a proof of concept to potential customers, we are able to contrast the effectiveness of our platform versus our competitors in identifying suspicious and potentially malicious software code in their actual IT environments. Our sales engineers also act as the liaison between customers and our marketing and product development organizations.

Marketing. Our marketing is focused on building our brand reputation and the market awareness of our platform, driving customer demand and a strong sales pipeline, and working with our channel partners around the globe. Our marketing team consists primarily of corporate marketing, channel marketing, account/lead development, operations, and corporate communications. Marketing activities include demand generation, advertising, managing our corporate Website and partner portal, trade shows and conferences, press and analyst relations, and customer

awareness. We are also actively engaged in driving global thought leadership programs

Table of Contents

through blogs and media and developing rich content such as the global cyber maps and report released in the second quarter of 2013. In 2011, we started releasing a semi-annual threat report, called *FireEye Advanced Threat Report*, the industry s first report exclusively focused on the next-generation threat landscape.

Technology Alliance Partners

Given our role in our customer networks, we maintain a large technology alliance network with other enterprise technology vendors. These vendors include service providers and consulting firms, managed security service providers, network appliance vendors, enterprise hardware manufacturers, enterprise infrastructure software vendors, and threat intelligence firms. The list below contains a representative subset of our broader technology alliance network:

- Instrumentation partners, including Gigamon, VSS Monitoring (acquired by Danaher Corporation in June 2012) and Ixia;
- Endpoint partners, including Guidance Software, Bit9 and Verdasys;
- Analysis/Security Information & Event Management partners, including Radar, a subsidiary of IBM, RSA, a subsidiary of EMC, LogRhythm, ArcSight, a subsidiary of HP, and Splunk; and
- Mitigation partners, including Imperva, Infoblox, Bradford Networks, NetCitadel, ForeScout and OpenDNS.

Government Affairs

We maintain relationships with several governments around the globe. Our thought leadership in protection against next-generation threats has helped to shape the legislative, regulatory and policy environment to better enhance these governments individual and collective cyber posture. As part of this effort, we contribute to the evolving standard-making processes and help define best practices in various jurisdictions. We also identify future needs and requirements and develop technologies in concert with government entities. In the United States, David G. DeWalt, our Chief Executive Officer, is a member of President Obama s National Security Telecommunications Advisory Committee, which provides recommendations to the President on how to assure vital telecommunications links through any event or crisis, and help the nation maintain a reliable, secure and resilient national communications posture. In addition, we are a member of the Information Technology Sector Coordination Council, which is the primary vehicle for providing sector input to the United States Government on information technology related critical infrastructure protection public policy issues. Through these and related activities, we engage on the front lines of the threat landscape and use that knowledge and insight to improve the efficacy of our solutions.

Manufacturing

The manufacturing of our security products is outsourced to third-party contract manufacturers. This approach allows us to reduce our costs as it reduces our manufacturing overhead and inventory and also allows us to adjust more quickly to changing customer demand. Our manufacturing partners assemble our products using design specifications, quality assurance programs, and standards that we establish, and they procure components and assemble our products based on our demand forecasts. These forecasts represent our estimates of future demand for our

products based upon historical trends and analysis from our sales and product management functions as adjusted for overall market conditions.

Our primary contract manufacturer is Flextronics Telecom Systems, Ltd., or Flextronics. The manufacturing agreement we have entered into with Flextronics does not provide for any minimum purchase commitments and has an initial term of one year, which is automatically renewed for one-year terms, unless either party gives written notice to the other party not less than 90 days prior to the last day of the applicable term. Additionally, this agreement may be terminated by either party (i) with advance written notice provided to the other party,

Table of Contents

subject to certain notice period limitations, or (ii) with written notice, subject to applicable cure periods, if the other party has materially breached its obligations under the agreement.

Research and Development

We invest substantial resources in research and development to enhance our virtual execution engine, build add-on functionality and improve our core technology. We believe that both hardware and software are critical to expanding our leadership in the security industry. Our engineering team has deep networking and security expertise and works closely with customers to identify their current and future needs. In addition to our focus on hardware and software, our research and development team is focused on research into next-generation threats, which is required to respond to the rapidly changing threat landscape.

Research and development expense totaled $7.3 million, $16.5 million and $66.0 million for 2011, 2012 and 2013, respectively. We plan to continue to significantly invest in resources to conduct our research and development effort.

Competition

We operate in the intensely competitive IT security market that is characterized by constant change and innovation. Changes in the threat landscape and broader IT infrastructures result in evolving customer requirements for the protection from next-generation threats. Several vendors have both recently introduced new products to compete with our solutions and are incorporating features to compete with our products. Our current and potential future competitors fall into six general categories:

- large networking vendors such as Cisco and Juniper that may emulate or integrate features similar to ours into their own products;
- large companies such as Intel, IBM and HP that have acquired large IT security specialist vendors in recent years and have the technical and financial resources to bring competitive solutions to the market;
- independent security vendors such as Sourcefire (which was recently acquired by Cisco), Palo Alto Networks and Trend Micro that offer products that claim to perform similar functions to our platform;
- small and large companies that offer point solutions that compete with some of the features present in our platform;
- providers of traditional IT security solutions, such as Symantec, that we may compete with in the future; and
- other providers of incident response services.

As our market grows and new IT budgets are created to support next-generation threat protection, it will attract more highly specialized vendors as well as larger vendors that may continue to acquire or bundle their products more effectively.

The principal competitive factors in our market include:

- ability to detect next-generation threats by overcoming the limitations of signature-based approaches;
- efficacy of the virtual machine technology in terms of detecting the maximum number of threats;
- scalability, throughput and overall performance of the virtual machine technology;
- visibility into all stages of an attack, especially the exploit phase;
- ability to achieve low false-positive rates;
- breadth and richness of the shared threat data the appliances have access to;

Table of Contents

- ability to process all data entering a network on premise;
- brand awareness and reputation;
- strength of sales and marketing efforts;
- product extensibility and ability to integrate with other technology infrastructures;
- price and total cost of ownership; and
- our ability to provide a comprehensive solution of products and services for detecting, preventing and resolving advanced cybersecurity threats.

We believe we compete favorably with our competitors on the basis of these factors as a result of the features and performance of our platform, the ease of integration of our products with technological infrastructures, and the relatively low total cost of ownership of our products. However, many of our competitors have substantially greater financial, technical and other resources, greater name recognition, larger sales and marketing budgets, deeper customer relationships, broader distribution, and larger and more mature intellectual property portfolios.

Intellectual Property

Our success depends in part upon our ability to protect our core technology and intellectual property. We rely on, among other things, patents, trademarks, copyrights and trade secret laws, confidentiality safeguards and procedures, and employee non-disclosure and invention assignment agreements to protect our intellectual property rights. We have 16 U.S. issued patents and 78 patent applications pending in the United States. We also have a number of foreign counterparts of these patent applications, consisting of seven pending applications under the Patent Cooperation Treaty, three pending application in the European Patent Office and another two in Japan. Our issued patents expire between 2025 and 2030. We cannot assure you whether any of our patent applications will result in the issuance of a patent or whether the examination process will result in patents of valuable breadth or applicability. In addition, any patents that may issue may be contested, circumvented, found unenforceable or invalidated, and we may not be able to prevent third parties from infringing them. We also license software from third parties for integration into our products, including open source software and other software available on commercially reasonable terms.

We control access to and use of our proprietary software, technology and other proprietary information through the use of internal and external controls, including contractual protections with employees, contractors, end-customers and partners, and our software is protected by U.S. and international copyright, patent and trade secret laws. Despite our efforts to protect our software, technology and other proprietary information, unauthorized parties may still copy or otherwise obtain and use our software, technology and other proprietary information. In addition, we intend to expand our international operations, and effective patent, copyright, trademark, and trade secret protection may not be available or may be limited in foreign countries.

Our industry is characterized by the existence of a large number of patents and frequent claims and related litigation regarding patent and other intellectual property rights. If we become more successful, we believe that competitors will be more likely to try to develop products that are similar to ours and that may infringe our proprietary rights. It may also be more likely that competitors or other third parties will claim that our products infringe their proprietary rights. In particular, large and established companies in the IT security industry have extensive patent

portfolios and are regularly involved in both offensive and defensive litigation. From time-to-time, third parties, including certain of these large companies and non-practicing entities, may assert patent, copyright, trademark, and other intellectual property rights against us, our channel partners, or our end-customers, whom our standard license and other agreements obligate us to indemnify against such claims. Successful claims of infringement by a third party, if any, could prevent us from distributing certain products or performing certain services, require us to expend time and money to develop non-infringing solutions, or force us to pay substantial damages (including, in the United States, treble damages if we are found to have willfully

Table of Contents

infringed patents), royalties or other fees. We cannot assure you that we do not currently infringe, or that we will not in the future infringe, upon any third-party patents or other proprietary rights. For example, we are currently a party to claims alleging, among other things, patent infringement, which are in the early stages of litigation. See *Risk Factors Risks Related to Our Business and Our Industry Claims by others that we infringe their proprietary technology or other rights could harm our business* for additional information.

Employees

As of December 31, 2013, we had 1,679 full-time employees. None of our employees is represented by a labor organization or is a party to any collective bargaining arrangement. We have never had a work stoppage, and we consider our relationship with our employees to be good.

Facilities

We currently lease approximately 170,000 square feet of space for our corporate headquarters in Milpitas, California under lease agreements that expire on various dates through 2018. We maintain additional offices throughout the United States and various international locations, including Australia, Dubai, India, Ireland, Japan, South Korea, Singapore, Taiwan, Turkey and the United Kingdom. We believe that our current facilities are adequate to meet our ongoing needs, and that, if we require additional space, we will be able to obtain additional facilities on commercially reasonable terms.

Legal Proceedings

We are a party to litigation and subject to claims incident to the ordinary course of business. Although the results of litigation and claims cannot be predicted with certainty, we currently believe that the final outcome of these matters will not have a material adverse effect on our business. Regardless of the outcome, litigation can have an adverse impact on us because of defense and settlement costs, diversion of management resources and other factors.

Table of Contents

MANAGEMENT

Executive Officers and Directors

The following table provides information regarding our executive officers and directors:

Name	Age	Position(s)
David G. DeWalt	49	Chief Executive Officer and Chairman of the Board
Ashar Aziz	55	Founder, Chief Technology Officer, Chief Strategy Officer and Vice Chairman of the Board
Kevin R. Mandia	43	Senior Vice President and Chief Operating Officer
Michael J. Sheridan	49	Senior Vice President and Chief Financial Officer
Alexa King	46	Senior Vice President, General Counsel and Secretary
Jeffrey C. Williams	47	Senior Vice President, Sales
Bahman Mahbod	54	Senior Vice President, Engineering
Ronald E. F. Codd[(1)(2)]	58	Director
William M. Coughran Jr.[(2)(3)]	61	Director
Gaurav Garg[(1)]	48	Director
Promod Haque[(2)(3)]	65	Director
Robert F. Lentz[(1)]	61	Director
Enrique Salem[(3)]	48	Director

(1) Member of our audit committee.
(2) Member of our nominating and corporate governance committee.
(3) Member of our compensation committee.

Executive Officers

David G. DeWalt has served as our Chief Executive Officer since November 2012 and has served as our Chairman of the Board since May 2012. Prior to joining FireEye, Mr. DeWalt served as President, Chief Executive Officer and director of McAfee, Inc., a provider of antivirus software and intrusion prevention solutions, from April 2007 until February 2011 when McAfee was acquired by Intel Corporation. Mr. DeWalt served as President of McAfee, a wholly-owned subsidiary of Intel, from February 2011 to August 2011. From December 2003 to March 2007, Mr. DeWalt held various positions at EMC Corporation, a developer and provider of information infrastructure technology and solutions, including Executive Vice President, EMC Software Group and President of EMC s Documentum and Legato Software divisions. Prior to joining EMC, Mr. DeWalt served as President and Chief Executive Officer of Documentum, Inc. from July 2001 to December 2003, Executive Vice President and Chief Operating Officer of Documentum from October 2000 to July 2001 and Executive Vice President and General Manager, eBusiness Unit, of Documentum from August 1999 to October 2000. Mr. DeWalt has served on the board of directors of Delta Air Lines, Inc. since November 2011. Mr. DeWalt also serves on the board of directors of Five9, Inc. Mr. DeWalt served on the board of directors of Polycom, Inc. from November 2005 to May 2013 and as its Chairman of the Board from May 2010 to May 2013 and served on the board of directors of Jive Software, Inc. from February 2011 to April 2013. Mr. DeWalt holds a B.S. in Computer Science from the University of Delaware. Our board of directors believes that Mr. DeWalt possesses specific attributes that qualify him to serve as a director, including the perspective and experience he brings as our Chief Executive Officer and his extensive senior management expertise in the network security

industry.

Table of Contents

Ashar Aziz founded FireEye in 2004 and served as our Chief Executive Officer until November 2012. He has served as our Vice Chairman of the Board, Chief Technology Officer and Chief Strategy Officer since November 2012 and as a member of our board of directors since February 2004. Prior to FireEye, Mr. Aziz founded Terraspring, Inc., a data center automation and virtualization company acquired by Sun Microsystems, Inc., in November 2002 and served as Chief Technology Officer of its N1 program until October 2003. Prior to Terraspring, Inc., Mr. Aziz spent 12 years at Sun Microsystems as a distinguished engineer focused on networking and network security. Mr. Aziz holds an S.B. in Electrical Engineering and Computer Science from Massachusetts Institute of Technology and an M.S. in Electrical Engineering and Computer Science from the University of California, Berkeley, where he received the U.C. Regents Fellowship. Our board of directors believes that Mr. Aziz possesses specific attributes that qualify him to serve as a director, including the perspective and experience he brings as our founder and former Chief Executive Officer and as one of our largest stockholders, as well as his extensive experience with technology companies.

Kevin R. Mandia has served as our Senior Vice President and Chief Operating Officer since our acquisition of Mandiant in December 2013. Prior to joining FireEye, Mr. Mandia was the chief executive officer of Mandiant and had served in that capacity since he founded Mandiant in 2004. Prior to forming Mandiant, Mr. Mandia served as the director of computer forensics at Foundstone (later acquired by McAfee Corporation) from 2000 to 2003 and as the director of information security for Sytex (later acquired by Lockheed Martin) from 1998 to 2000. From 1993 to 2000, Mr. Mandia was an officer in the United States Air Force, where he served in various capacities, including as a computer security officer in the 7th Communications Group at the Pentagon, and later as a special agent in the Air Force Office of Special Investigations (AFOSI). Mr. Mandia holds a B.S. in Computer Science from Lafayette College and an M.S. in Forensic Science from The George Washington University. In 2011, Mr. Mandia was named Ernst & Young Entrepreneur of the Year for the Greater Washington area. He completed the Harvard Business School s Owner/President Management Program in February 2013. Mr. Mandia has taught graduate level courses at Carnegie Melon University and The George Washington University and has co-authored two books on responding to security breaches, Incident Response: Performing Computer Forensics (McGraw-Hill, 2003) and Incident Response: Investigating Computer Crime (McGraw-Hill, 2001).

Michael J. Sheridan has served as our Senior Vice President and Chief Financial Officer since June 2011. Prior to joining FireEye, Mr. Sheridan was Chief Financial Officer at Mimosa Systems, Inc., a provider of enterprise content archiving systems, from 2009 until its acquisition by Iron Mountain, Inc. in 2010. Prior to Mimosa Systems, Inc., Mr. Sheridan was Chief Financial Officer of Playlist, Inc., a social media and Internet company, from 2008 to 2009, Facebook Inc., a social media and Internet company, from 2006 to 2007, IGN Entertainment, Inc., a media and entertainment company (acquired by News Corporation in 2005), from 2004 to 2006, and SonicWALL, Inc., a network security and data protection company, from 1999 to 2003. Mr. Sheridan received a B.S. in Commerce from Santa Clara University.

Alexa King has served as our Senior Vice President, General Counsel and Secretary since April 2012. Prior to joining FireEye, Ms. King was Vice President, General Counsel and Secretary of Aruba Networks, Inc., a provider of enterprise wireless network software and hardware from December 2005 to April 2012. From 2000 to 2005, Ms. King served as Senior Director of Legal at Siebel Systems, Inc. a software company, and her early career included working at Pillsbury Madison & Sutro (now Pillsbury Winthrop) and Fenwick & West. Additionally, Ms. King served as founding director of Pathbrite, Inc. (f/k/a RippleSend, Inc.) from 2008 to 2009 and as advisor from 2009 to 2011. Ms. King graduated magna cum laude from Harvard College with a degree in Eastern European Studies and received her J.D. from the University of California, Berkeley, Boalt Hall School of Law, where she was named to the Order of the Coif.

Jeffrey C. Williams has served as our Senior Vice President, Sales since March 2010. He also served as a member of our advisory board from April 2006 to February 2010. Prior to joining FireEye, Mr. Williams was vice president of sales at Cisco Systems, Inc., a technology manufacturing and sales company, from April 2003 to January 2010. Prior to Cisco Systems, Mr. Williams managed sales for IronPort Systems, Inc. prior to its

acquisition by Cisco Systems in June 2007. Prior to IronPort, Mr. Williams was Vice President of Sales at IntruVert Networks, Inc., a next-generation IPS company which was acquired by McAfee, from February 2002 to April 2003. Prior to IntruVert Networks, Mr. Williams was Vice President of Sales of Abeona Networks, Inc. from January 2001 to January 2002 and at GlobalCenter Inc., which was acquired by Exodus Communications, from February 1990 to January 2001. Additionally, Mr. Williams served on the board of directors of Meraki, Inc. from 2010 until its acquisition by Cisco Systems in 2012. He holds a B.S. in Marketing from California State University, Chico.

Bahman Mahbod has served as our Senior Vice President, Engineering since February 2012, and as our Vice President of Engineering and Security Research from October 2007 to February 2012. Prior to joining FireEye, Mr. Mahbod served as Head of Server Engineering, Quality Assurance and Technical Publications at Gemini Mobile Technologies, Inc., a provider of infrastructure and mobile messaging software, from 2005 to 2007 and Vice President of Engineering, Network Operations and Client Services at FaceTime Communications (now Actiance), a provider of extensible real-time security and management solutions, from 1999 to 2005. Prior to that, Mr. Mahbod held various leadership positions at IBM Corporation, Sybase, Inc., Vantive Inc. and Bell-Northern Research Co. Mr. Mahbod holds a B.S. in Computer Science from the University of California, Santa Barbara.

Non-Employee Directors

Ronald E. F. Codd has served as a member of our board of directors since July 2012. Mr. Codd has been an independent business consultant since April 2002. From January 1999 to April 2002, Mr. Codd served as President, Chief Executive Officer and a director of Momentum Business Applications, Inc., an enterprise software company. From September 1991 to December 1998, Mr. Codd served as Senior Vice President of Finance and Administration and Chief Financial Officer of PeopleSoft, Inc., a provider of human resource management systems. Mr. Codd has served on the board of directors of ServiceNow, Inc., Rocket Fuel Inc., and Veeva Systems Inc. since February 2012. Additionally, Mr. Codd previously served on the boards of directors of numerous information technology companies, including most recently DemandTec, Inc., Interwoven, Inc. and Data Domain, Inc. Mr. Codd holds a B.S. in Accounting from the University of California, Berkeley and an M.M. in Finance and M.I.S. from the Kellogg Graduate School of Management at Northwestern University. Our board of directors believes that Mr. Codd possesses specific attributes that qualify him to serve as a director, including his extensive management and software industry experience, and his experience in finance.

William M. Coughran Jr. has served as a member of our board of directors since July 2012. Mr. Coughran has been a member of Sequoia Capital, a venture capital firm, since October 2011. He currently serves on the board of directors of multiple private companies, and he served on the board of directors of Clearwell Systems, Inc. from March 2005 to June 2011, when it was acquired by Symantec, Inc. Prior to joining Sequoia Capital, Mr. Coughran held a number of roles at Google Inc. from April 2003 to September 2011, including Senior Vice President of Engineering. At Google, he was responsible for security efforts as well as serving on the executive committee and as an advisor to the founders and Eric Schmidt. Prior to Google, Mr. Coughran co-founded Entrisphere, Inc., a telecom equipment vendor, and served as its initial Chief Executive Officer and in other roles from November 1999 to December 2002. From 1980 to 1999, Mr. Coughran held a number of roles at Bell Labs, Inc. (originally part of AT&T, Inc. and then Lucent Technologies, Inc.), including vice president of the Computing Sciences Research Center, known for key developments in operating and distributed systems as well as early work in networked computer security. Mr. Coughran has held adjunct and visiting faculty roles at Stanford University, Duke University, and ETH Zürich. Mr. Coughran has a B.S. and M.S. in Mathematics from California Institute of Technology and an M.S. and Ph.D. in Computer Science from Stanford University. Our board of directors believes that Mr. Coughran possesses specific attributes that qualify him to serve as a director, including his extensive experience with technology companies and his experience as an investment professional.

Gaurav Garg has served as a member of our board of directors since September 2004. Mr. Garg co-founded and has been a managing member of Wing Venture Partners, a venture capital firm, since June 2013. He has served on the board of directors of Ruckus Wireless, Inc. since August 2002. Mr. Garg also currently serves

124

on the board of directors of a number of privately held technology companies, including MobileIron and Jasper Wireless. From May 2001 to June 2010, Mr. Garg was a non-managing member at Sequoia Capital, a venture capital firm. Prior to joining Sequoia Capital, Mr. Garg was a founder, board member and Senior Vice President of Product Management at Redback Networks, Inc., a telecommunications equipment company acquired by Ericsson, Inc. in 2007. Prior to Redback Networks, Mr. Garg held various engineering positions at SynOptics Communications, Inc. and Bay Networks, Inc., both computer network equipment vendors. Mr. Garg holds a B.S. and M.S. in Electrical Engineering and a B.S. in Computer Science, all from Washington University in St. Louis. Our board of directors believes that Mr. Garg possesses specific attributes that qualify him to serve as a director, including his extensive experience with technology and networking companies as an investment professional, board member, company founder, and senior executive.

Promod Haque has served as a member of our board of directors since March 2005. Mr. Haque has been a managing partner of Norwest Venture Partners, a venture capital firm, since 1990 and currently serves as senior managing partner. He has served on the board of directors of Cyan, Inc. since April 2007. Mr. Haque also currently serves on the boards of directors of several privately held companies, including Apigee, Inc. and PCH International, Inc., and previously served on the board of directors of Persistent Systems Limited from November 2005 to November 2010, and as Chairman of the Board of Veraz Networks, Inc., a provider of application, control and bandwidth optimization solutions, from July 2001 until October 2010, when it merged with Dialogic Corporation. Mr. Haque holds a B.S. in Electrical Engineering from the University of Delhi, India, an M.B.A. from the Kellogg Graduate School of Management at Northwestern University, and a Ph.D. in Electrical Engineering from Northwestern University. Our board of directors believes that Mr. Haque possesses specific attributes that qualify him to serve as a director, including his substantial experience as an investment professional and his extensive experience with technology and networking companies.

Robert F. Lentz has served as a member of our board of directors since March 2010. Mr. Lentz has served as the President of Cyber Security Strategies since October 2009. He served as the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance in the Office of the Assistant Secretary of Defense, Networks and Information Integration/Chief Information Officer from November 2007 to October 2009. Since November 2000, he has also served as the Chief Information Security Officer for the U.S. Department of Defense. He previously worked at the National Security Agency from 1975 to 2000, where he served in the first National Computer Security Center as Chief of Network Security. Mr. Lentz has served as a member of the board of directors of Sypris Solutions, Inc. since July 2012, as well as on the board of directors of two private companies and as an advisor to several other technology companies. Mr. Lentz holds a B.A. in History and Social Science from St. Mary s College and an M.S. in National Strategy from National Defense University. Our board of directors believes that Mr. Lentz possesses specific attributes that qualify him to serve as a director, including his substantial experience in the security industry, his extensive experience with the U.S. federal government and breadth of knowledge in international cyber security.

Enrique Salem has served as a member of our board of directors since February 2013. Mr. Salem was president, Chief Executive Officer and a director of Symantec Corporation, a provider of information security, storage and systems management solutions, from April 2009 until July 2012. Mr. Salem was Chief Operating Officer of Symantec Corporation from January 2008 to April 2009, group President, Worldwide Sales and Marketing from April 2007 to January 2008, group President, Consumer Products from May 2006 to April 2007, Senior Vice President, Consumer Products and Solutions from February 2006 to May 2006, Senior Vice President, Security Products and Solutions from January 2006 to February 2006, and Senior Vice President, Network and Gateway Security Solutions from June 2004 to February 2006. Prior to Symantec, from April 2002 to June 2004, Mr. Salem served as President and Chief Executive Officer of Brightmail, Inc., an email filtering company, prior to its acquisition by Symantec in 2004. Mr. Salem also held senior leadership roles at Oblix Inc., Ask Jeeves Inc., Peter Norton Computing, Inc. and Security Pacific Merchant Bank. In March 2011, he was appointed to President Barack Obama s Management Advisory Board. Mr. Salem has been a director of Automatic Data Processing, Inc. since January 2010 and previously served on the board of directors of Symantec Corporation from April 2009 to July 2012. He received the Estrella Award from the Hispanic IT Executive

Table of Contents

Council in 2010 and was named Entrepreneur of the Year in 2004 by Ernst & Young. Mr. Salem holds an A.B. in Computer Science from Dartmouth College. Our board of directors believes that Mr. Salem possesses specific attributes that qualify him to serve as a director, including his extensive leadership experience, including oversight of global operations, as well as a strong background in information technology, data security, compliance and systems management.

Our executive officers are appointed by our board of directors and serve until their successors have been duly elected and qualified. There are no family relationships among any of our directors or executive officers.

Code of Business Conduct and Ethics

Our board of directors has adopted a code of business conduct and ethics that applies to all of our employees, officers and directors, including our Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, and other executive and senior financial officers. The full text of our code of business conduct and ethics is available on our Website at www.fireeye.com. We intend to post any amendment to our code of business conduct and ethics, and any waivers of such code for directors and executive officers, on the same Website. The information on our Website is not incorporated by reference into this prospectus.

Board Composition

Our business affairs are managed under the direction of our board of directors, which is currently composed of eight members. Six of our directors are independent within the meaning of the independent director guidelines of The NASDAQ Stock Market. Our board of directors is divided into three classes with staggered three-year terms. At each annual meeting of stockholders, the successors to the directors whose terms then expire will be elected to serve from the time of election and qualification until the third annual meeting following their election. Our directors are divided among the three classes as follows:

- the Class I directors are Messrs. Coughran, Garg and Haque, and their terms will expire at the annual meeting of stockholders to be held in 2014;
- the Class II directors are Messrs. Aziz, DeWalt and Lentz, and their terms will expire at the annual meeting of stockholders to be held in 2015; and
- the Class III directors are Messrs. Codd and Salem, and their terms will expire at the annual meeting of stockholders to be held in 2016.

Each director s term will continue until the election and qualification of his successor, or his earlier death, resignation, or removal. We expect that any increase or decrease in the number of directors will be distributed among the three classes so that, as nearly as possible, each class will consist of one-third of the directors. The classification of our board of directors may have the effect of delaying or preventing changes in our management or a change in control of our company. See Description of Capital Stock Anti-Takeover Effects of Delaware Law and Our Amended and Restated Certificate of Incorporation and Amended and Restated Bylaws for a discussion of other anti-takeover provisions found in our amended and restated certificate of incorporation and amended and restated bylaws.

Director Independence

Our common stock is listed on The NASDAQ Global Select Market. Under the rules of The NASDAQ Stock Market, independent directors must comprise a majority of a listed company s board of directors within a specified period of time after the completion of such company s initial public offering. In addition, the rules of The NASDAQ Stock Market require that, subject to specified exceptions, each member of a listed company s audit, compensation, and nominating and corporate governance committees be independent. Under the rules of The NASDAQ Stock Market, a director will only qualify as an independent director if, in the opinion of that company s board of directors, that director does not have a relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a director.

Table of Contents

Audit committee members must also satisfy the independence criteria set forth in Rule 10A-3 under the Securities Exchange Act of 1934, as amended, or the Exchange Act. In order to be considered independent for purposes of Rule 10A-3, each member of the audit committee of a listed company may not, other than in his or her capacity as a member of such committee, the board of directors, or any other board committee: (i) accept, directly or indirectly, any consulting, advisory, or other compensatory fees from the listed company or any of its subsidiaries; or (ii) be an affiliated person of the listed company or any of its subsidiaries.

Our board of directors has undertaken a review of the independence of each director and considered whether such director has a material relationship with us that could compromise his ability to exercise independent judgment in carrying out his responsibilities. As a result of this review, our board of directors has determined that Messrs. Codd, Coughran, Garg, Haque, Lentz and Salem are independent directors as defined under the applicable rules and regulations of the Securities and Exchange Commission, or SEC, and the listing requirements and rules of The NASDAQ Stock Market.

Committees of the Board of Directors

Our board of directors has established an audit committee, a compensation committee, and a nominating and corporate governance committee, each of which has the composition and responsibilities described below. Members serve on these committees until their resignation or until otherwise determined by our board of directors.

Audit Committee

Our audit committee is comprised of Ronald E. F. Codd, Gaurav Garg and Robert F. Lentz, each of whom is a non-employee member of our board of directors. Mr. Codd is the chair of our audit committee. Our board of directors has determined that each of the members of our audit committee satisfies the requirements for independence and financial literacy under the rules and regulations of The NASDAQ Stock Market and the SEC, including Rule 10A-3. Our board of directors has also determined that Mr. Codd qualifies as an audit committee financial expert as defined in the SEC rules and satisfies the financial sophistication requirements of The NASDAQ Stock Market. This designation does not impose on Mr. Codd any duties, obligations or liabilities that are greater than those generally imposed on members of our audit committee and our board of directors. Our audit committee is responsible for, among other things:

- selecting and hiring our registered public accounting firm;
- evaluating the performance and independence of our registered public accounting firm;
- approving the audit and pre-approving any non-audit services to be performed by our independent registered public accounting firm;
- reviewing the adequacy and effectiveness of our internal control policies and procedures and our disclosure controls and procedures;
- overseeing procedures for the treatment of complaints on accounting, internal accounting controls or audit matters;

reviewing and discussing with management and the independent registered public accounting firm the results of our annual audit, our quarterly financial statements and our publicly filed reports;

reviewing and approving related person transactions; and

preparing the audit committee report that the SEC requires in our annual proxy statement.

Compensation Committee

Our compensation committee is comprised of William M. Coughran Jr., Promod Haque and Enrique Salem, each of whom is a non-employee member of our board of directors. Mr. Salem is the chair of our compensation committee. Our board of directors has determined that each member of our compensation committee meets the

Table of Contents

requirements for independence under the rules of The NASDAQ Stock Market and the SEC, is a non-employee director within the meaning of Rule 16b-3 under the Exchange Act and is an outside director within the meaning of Section 162(m) of the Internal Revenue Code of 1986, or the Code. Our compensation committee is responsible for, among other things:

- reviewing and approving our Chief Executive Officer s and other executive officers annual base salaries; incentive compensation plans, including the specific goals and amounts; equity compensation, employment agreements, severance arrangements and change in control agreements; and any other benefits, compensation or arrangements; provided that any approvals relating to the Chief Executive Officer s compensation will be subject to the ratification of our entire board of directors, with any non-independent directors abstaining;
- administering our equity compensation plans;
- overseeing our overall compensation philosophy, compensation plans and benefits programs; and
- preparing the compensation committee report that the SEC requires in our annual proxy statement.

Nominating and Corporate Governance Committee

Our nominating and corporate governance committee is comprised of Ronald E. F. Codd, William M. Coughran Jr. and Promod Haque, each of whom is a non-employee member of our board of directors. Mr. Coughran is the chair of our nominating and corporate governance committee. Our board of directors has determined that each member of our nominating and corporate governance committee meets the requirements for independence under the rules of The NASDAQ Stock Market. Our nominating and corporate governance committee is responsible for, among other things:

- evaluating and making recommendations regarding the composition, organization, and governance of our board of directors and its committees;
- evaluating and making recommendations regarding the creation of additional committees or the change in mandate or dissolution of committees;
- reviewing and making recommendations with regard to our corporate governance guidelines and compliance with laws and regulations; and
- reviewing and approving conflicts of interest of our directors and corporate officers, other than related person transactions reviewed by the audit committee.

We have posted the charters of our audit, compensation and nominating and corporate governance committees on our Website at www.fireeye.com, and we intend to post any amendments to such charters that may be adopted from time to time on the same Website. Our board of directors may from time to time establish other committees.

Compensation Committee Interlocks and Insider Participation

None of the members of our compensation committee is or has been an officer or employee of our company. None of our executive officers currently serves, or in the past year has served, as a member of the board of directors or compensation committee, or other board committee performing equivalent functions, of any entity that has one or more executive officers serving on our compensation committee or our board of directors. We have had a compensation committee since November 2012. Prior to establishing the compensation committee, our full board of directors made decisions relating to the compensation of our executive officers.

Table of Contents

Director Compensation

We do not currently have a formal policy with respect to compensation payable to our non-employee directors for service as directors. Our non-employee directors do not currently receive, and did not receive during 2013, any cash compensation for their services as directors or as board committee members. Our board of directors has, however, granted equity awards from time to time to non-employee directors who are not affiliated with our venture fund investors as compensation for their service as directors.

The table below shows equity compensation earned by our non-employee directors during 2013.

Director Compensation Table

Name[1]	Option Awards ($)[2]	Total ($)
Ronald E. F. Codd[3]		
William M. Coughran Jr.		
Enrique Salem[4]	682,093	682,093
Gaurav Garg[5]		
Promod Haque		
Robert F. Lentz[6]		

(1) Except as described in the footnotes below, no non-employee director held options to purchase shares of our common stock or unvested stock awards as of December 31, 2013.

(2) The amount reported in this column represents the aggregate grant date fair value of the awards as computed in accordance with Financial Accounting Standard Board Accounting Standards Codification Topic 718. The assumptions used in calculating the grant date fair value of the awards reported in this column are set forth in the notes to our audited consolidated financial statements included elsewhere in this prospectus.

(3) As of December 31, 2013, Mr. Codd held an option to purchase 125,000 shares of common stock at an exercise price of $2.48 per share, and the Codd Revocable Trust dtd March 6, 1998 held 36,459 shares of restricted common stock that remained subject to a right of repurchase by us as of such date.

(4) As of December 31, 2013, Mr. Salem held 200,000 shares of restricted common stock that remained subject to a right of repurchase by us as of such date.

(5) As of December 31, 2013, Mr. Garg s affiliated entities held 151,729 shares of restricted common stock that remained subject to a right of repurchase by us as of such date.

(6) As of December 31, 2013, Mr. Lentz held an option to purchase 430,382 shares of common stock at an exercise price of $0.07 per share.

See Executive Compensation for information about the compensation of directors who are also our employees.

Table of Contents

EXECUTIVE COMPENSATION

Summary Compensation Table

The following table provides information regarding the compensation awarded to, or earned by, our executive officers, including each of our named executive officers, during 2012 and 2013.

Name and Principal Position	Year	Salary ($)	Bonus ($)[1]	Stock Awards ($)[2][3]	Option Awards ($)[2]	Non-Equity Incentive Plan Compensation ($)[4]	Total ($)
David G. DeWalt,	2013	350,000	190,000		431,177		971,177
	2012	42,424	23,562	3,576,032[5]	2,390,756		6,032,774
Chief Executive Officer							
Ashar Aziz,	2013	300,000				152,869	452,869
Chief Technology Officer, Chief Strategy Officer, and Former Chief Executive Officer	2012	300,000	171,000		1,916,037		2,387,037
Jeffrey C. Williams,	2013	226,042	150,000	302,495		190,636	869,173
Senior Vice President, Sales	2012	200,000	150,000			336,202	686,202
Alexa King,	2013	250,000		302,495		106,227	658,722
Senior Vice President, General Counsel and Secretary	2012	177,083	40,403		436,885		654,371
Bahman Mahbod,	2013	250,000		302,495		104,414	656,909
Senior Vice President, Engineering	2012	246,932	57,000		124,813		428,745
Michael J. Sheridan,	2013	265,000		302,495		147,712	715,207
Senior Vice President and Chief Financial Officer	2012	265,000	94,536				359,536
Kevin R. Mandia,	2013						
Senior Vice President and Chief Operating Officer[6]							

(1) Represents amounts paid as a discretionary bonus to our executive officers, including our named executive officers, for exemplary performance in 2012 as compared with our 2012 operating plan.

(2) The amounts in this column represent the aggregate grant date fair value of the award as computed in accordance with Financial Accounting Standard Board Accounting Standards Codification Topic 718. The assumptions used in calculating the grant date fair value of the awards reported in this column are set forth in the notes to our audited consolidated financial statements included elsewhere in this prospectus.

(3) In February 2014, our board of directors granted restricted stock units covering up to 41,250 shares of our common stock to Mr. Aziz, restricted stock units covering up to 82,500 shares of our common stock to Mr. Williams, restricted stock units covering up to 53,125 shares of our common stock to Ms. King, restricted stock units covering up to 55,000 shares of our common stock to Mr. Mahbod, and restricted stock units covering up to 48,125 shares of our common stock to Mr. Sheridan. In addition, in March 2014, our board of directors granted restricted stock units covering up to 187,500 shares of our common stock to Mr. DeWalt. All of these restricted stock units are subject to performance-based and/or time-based vesting schedules.

130

Table of Contents

(4) For 2013, represents amounts paid under the Employee Incentive Plan. For 2012, represents amounts paid to Mr. Williams under his Master Commission Plan.

(5) Represents the grant date fair value of stock awards granted to Mr. DeWalt in his capacity as our Chief Executive Officer. For information regarding additional equity awards received by Mr. DeWalt during 2012 in his capacity as a member of our board of directors and as Chairman of the Board, see the disclosure under Management Director Compensation Director Compensation Table in our prospectus dated September 20, 2013, as filed with the SEC pursuant to Rule 424(b)(3).

(6) Mr. Mandia was appointed as our Senior Vice President and Chief Operating Officer on December 30, 2013 and accordingly received no compensation from us during 2013.

Bonus and Non-Equity Incentive Plan Compensation

Discretionary Bonus

Mr. DeWalt, our Chief Executive Officer and Chairman of the Board, and Mr. Williams, our Senior Vice President, Sales, each received discretionary bonuses for exemplary individual performance in 2013 and for company performance in 2013 as compared to our 2013 operating plan. These discretionary bonuses were not paid pursuant to any formal plan document.

Non-Equity Incentive Plan Compensation

Our compensation committee has adopted the Employee Incentive Plan, or the Bonus Plan. See the disclosure under Employee Incentive Plan for additional information.

2013 Performance Targets under Employee Incentive Plan Non-Sales Executives

For 2013, our compensation committee approved the performance targets under the Bonus Plan for each of our executive officers other than Messrs. Williams, Mandia and DeWalt. For 2013, the compensation committee set commission-based targets for Mr. Williams, as described below, and Mr. Mandia was not employed with us for most of 2013.

Under the Bonus Plan, each eligible participant has an opportunity to earn semi-annual payments, subject to our achievement of corporate performance goals and the participant s achievement of individual goals. For 2013, the relative weight of each performance element was 75% corporate and 25% individual, and our corporate-level goals were certain targets for bookings, EBITDA and new customers.

For 2013, each of these corporate goals was equally weighted. The minimum level of achievement for each corporate component is 80%, which corresponds to a 75% payout for that component. If achievement for a component is 120% or greater, then the corresponding payout for that component is 140%. The payout is scaled for achievement between 80% and 120%. Our compensation committee reserves the right to adjust the corporate performance target in the case of a merger, acquisition or such other unforeseeable future event occurs.

With respect to individual goals, the amount of achievement and payout is determined based on our Chief Executive Officer s assessment of achievement. Payout for the individual performance component can be up to 200%.

The compensation committee reserves the right to increase or decrease (including to zero) the amount of any payout to a participant.

Table of Contents

For 2013, the target incentive amounts and the aggregate annual payments earned by our executive officers under the Bonus Plan were as follows:

Executive Officer	Annual Target Award Opportunity	Actual Annual Award Amount
Ashar Aziz	$ 150,000	$152,869
Alexa King.	100,000	106,227
Bahman Mahbod	100,000	104,414
Michael J. Sheridan	135,000	147,712

2013 Performance Targets under Employee Incentive Plan Sales Executive

For 2013, our compensation committee approved commission-based performance targets for Mr. Williams under the Bonus Plan. These commissions were calculated by multiplying his effective commission rate by the value of our bookings. Certain types of orders were eligible for additional bonuses at an increased commission rate. In addition, the compensation committee provided that (i) Mr. Williams effective commission rate would be accelerated if he exceeded his annual bookings target and (ii) commissions would not be subject to a cap and would be paid prior to the end of the month following the close of the month in which the commissions were earned.

For 2013, the target incentive amount and the aggregate annual payment earned by Mr. Williams under the Bonus Plan were as follows:

Executive Officer	Annual Target Award Opportunity	Actual Annual Award Amount
Jeffrey C. Williams	$ 200,000	$190,636

Employment Agreements for Executive Officers

David G. DeWalt

Effective November 19, 2012, we entered into an amended and restated offer letter with David G. DeWalt, our Chief Executive Officer and Chairman of the Board. The offer letter has no specific term and provides that Mr. DeWalt is an at-will employee. Mr. DeWalt s current annual base salary is $350,000, and he is eligible for annual target incentive payments of $350,000 for 2014. Mr. DeWalt s offer letter was subsequently amended in August 2013.

In connection with Mr. DeWalt s commencement of employment as our Chief Executive Officer, the vesting schedule of each of Mr. DeWalt s equity awards was amended and restated to vest from and after the date Mr. DeWalt became our Chief Executive Officer, as follows:

Mr. DeWalt s restricted stock award covering 269,686 shares of common stock granted on May 1, 2012 vests as to 1/48th of the shares subject to the award each month beginning in May 2012, subject to his continuous service as a member of our board of directors on each such vesting date.

Mr. DeWalt s restricted stock award covering 377,560 shares of common stock granted on May 1, 2012 vests as to 1/7th of the shares subject to the award each month beginning in May 2012, subject to his continuous service as our Chairman of the Board on each such vesting date.

Mr. DeWalt s restricted stock award covering 431,497 shares of common stock granted on May 1, 2012 vests as to 100% of the shares subject to the award on the date that is six months following the date Mr. DeWalt became our Chief Executive Officer, subject to his continuous service as our Chief Executive Officer on such vesting date.

Mr. DeWalt s restricted stock award covering 836,026 shares of common stock granted on May 1, 2012 vests as to 100% of the shares subject to the award on the first anniversary of the date Mr. DeWalt became our Chief Executive Officer, subject to his continuous service as our Chief Executive Officer on such date.

Mr. DeWalt s restricted stock award covering 350,591 shares of common stock granted on May 1, 2012 vests as to 1/5th of the shares subject to the award each month beginning on the last day of the month following the first anniversary of the date Mr. DeWalt became our Chief Executive Officer, subject to his continuous service as our Chief Executive Officer on each such vesting date.

Mr. DeWalt s stock option to purchase 2,157,486 shares of our common stock granted on May 1, 2012 vests in 31 equal monthly installments beginning on the last day of the 18th month following the date Mr. DeWalt became our Chief Executive Officer, subject to his continuous service as our Chief Executive Officer on each such vesting date.

Mr. DeWalt s stock option to purchase 41,000 shares of our common stock granted on June 15, 2012 vests as to 1/48th of the shares subject to the award each month beginning on the date Mr. DeWalt became our Chief Executive Officer, subject to his continuous service as our Chief Executive Officer on each such vesting date.

In August 2013, Mr. DeWalt s offer letter was amended to provide that any of Mr. DeWalt s rights to severance, equity acceleration and/or change of control benefits under his offer letter would be superseded by eligibility for severance benefits under our Change of Control Severance Policy for Officers. See the disclosure under Change of Control Severance Policy for Officers for additional information.

The description above does not purport to be complete and is qualified in its entirety by the provisions of Mr. DeWalt s offer letter, as amended, a copy of which has been filed as an exhibit to the registration statement of which this prospectus is a part.

Ashar Aziz

Effective November 19, 2012, we entered into an offer letter with Ashar Aziz, our founder, Vice Chairman of the Board, Chief Technology Officer and Chief Strategy Officer. The offer letter has no specific term and provides that Mr. Aziz is an at-will employee. Mr. Aziz s current annual base salary is $300,000, and he is eligible for annual target incentive payments of $150,000 each year.

In connection with Mr. Aziz s transition from our Chief Executive Officer to our Chief Technology Officer and Chief Strategy Officer, the offer letter clarified and confirmed the vesting schedule of each of Mr. Aziz s equity awards as follows:

Mr. Aziz s stock option to purchase 2,170,794 shares of common stock granted on December 28, 2009 vests as to 38,441 shares subject to the award each month beginning on June 25, 2009 until fully vested.

Mr. Aziz s stock option to purchase 856,218 shares of common stock granted on June 25, 2010 vests as to 15,162 shares subject to the award each month beginning on June 25, 2009 until fully vested.

Mr. Aziz s stock option to purchase 926,640 shares of common stock granted on May 27, 2011 vests as to 19,305 shares subject to the award each month beginning on June 1, 2011 until fully vested.

Mr. Aziz s stock option to purchase 555,984 shares of common stock granted on May 27, 2011 vests as to 11,583 shares subject to the award each month beginning on December 29, 2012 until fully vested.

Mr. Aziz s stock option to purchase 1,618,439 shares of common stock granted on March 30, 2012 vested as to 36,782 shares subject to the award on November 26, 2012 and December 26, 2012, vested as to 12,260 shares on the 26th of each month from January 2013 through June 2013, and then vests as to 36,782 shares on the 26th of each month until fully vested.

Mr. Aziz s stock option to purchase 484,425 shares of common stock granted on May 25, 2012 vested on November 19, 2012, the date Mr. DeWalt became our Chief Executive Officer.

The vesting terms described above as to Mr. Aziz are all subject to Mr. Aziz s continuous service with us on each vesting date. Pursuant to the terms of the offer letter, effective as of the date Mr. DeWalt joined us as our Chief Executive Officer, 500,000 of the unvested shares subject to the equity awards described above vested on a pro rata basis across all such awards. See Outstanding Equity Awards at Fiscal Year-End for a description of the vesting of Mr. Aziz s equity awards as of December 31, 2013 after giving effect to the acceleration described in the preceding sentence.

In addition to the vesting acceleration described above, Mr. Aziz s offer letter also provides for the vesting acceleration of his equity awards as follows:

Upon the effectiveness of our initial public offering and the public trading of our common stock while Mr. Aziz is an employee or director, 500,000 of the unvested shares subject to his equity awards will vest.

If Mr. Aziz remains an employee or director on the six-month anniversary of the effectiveness of our initial public offering, 500,000 of the unvested shares subject to his equity awards will vest.

If, prior to the expiration of the underwriter-imposed lock-up agreement in connection with our initial public offering, Mr. Aziz is subject to a termination of employment without cause, then subject to his execution of a release of claims, the unvested shares subject to his equity awards will vest as if Mr. Aziz had completed an additional 12 months of employment following the date of his termination of employment. Also, if Mr. Aziz is entitled to such vesting acceleration and is not maintained as a director through the later of the expiration of the underwriter-imposed lock-up agreement in connection with our initial public offering and our first annual meeting as a public company, then the unvested shares subject to his equity awards will vest as if Mr. Aziz had completed an additional 12 months of service following his termination date.

If we are subject to a change in control when Mr. Aziz is not an employee but is a director, then 100% of his unvested equity awards will vest.

If we are subject to a change in control when Mr. Aziz is an employee and Mr. Aziz subsequently terminates his employment, then, subject to his execution of a release of claims, Mr. Aziz s equity awards will vest as if Mr. Aziz had completed an additional 24 months of employment following his termination of employment date.

Mr. Aziz s offer letter provides that, if prior to the expiration of the underwriter-imposed lock-up agreement in connection with our initial public offering, Mr. Aziz is terminated without cause either prior to, or more than 24 months following, a change in control, then, subject to the execution of a release of claims, Mr. Aziz will receive continuing payment of his base salary for a period of 12 months. If, prior to the expiration of the underwriter imposed lock-up agreement in connection with our initial public offering, Mr. Aziz s employment is terminated without cause or for good reason, in each case within 24 months following a change in control, then, subject to the execution of a release of claims, Mr. Aziz will receive continuing payment of his base salary for a period of 12 months and a payment equal to Mr. Aziz s annual target bonus.

Mr. Aziz had entered into certain promissory notes with us in connection with the purchase of our common stock. In connection with his transition, the term of these notes were modified so that their term extended until the first to occur of (i) December 31, 2017 or (ii) (a) the day prior to the date we file our registration statement in connection with our initial public offering, (b) the date we are acquired by a company whose stock is publicly traded and the notes would violate applicable law, or (c) the date we determine that the notes would be a violation of Section 402 of the Sarbanes-Oxley Act. All promissory notes have been repaid in full as described in greater detail under the heading Certain

Relationships and Related Party Transactions Loans to Executive Officers.

Table of Contents

The description above does not purport to be complete and is qualified in its entirety by the provisions of Mr. Aziz s offer letter, a copy of which has been filed as an exhibit to the registration statement of which this prospectus is a part.

Kevin R. Mandia

Effective December 30, 2013, we entered into an offer letter with Kevin R. Mandia, our Senior Vice President and Chief Operating Officer. The offer letter is for no specific term and provides that Mr. Mandia is an at-will employee. Mr. Mandia s current annual base salary is $260,000, and he is eligible for annual target incentive payments based on the achievement of certain individual performance objectives and company success metrics to be determined by us after consultation with Mr. Mandia. Mr. Mandia is also eligible for severance benefits under our Change of Control Severance Policy for Officers.

Pursuant to the terms of the offer letter, Mr. Mandia agreed that we would impose vesting requirements on a portion of the shares of our common stock that were issued to him as stock consideration as part of our acquisition of Mandiant and that would otherwise have been fully vested shares of our common stock. As a result, we imposed the following vesting requirements on 469,813 shares of our common stock issued to Mr. Mandia upon the closing of the acquisition: one half of the total shares of revested stock shall vest on each anniversary of the closing of the acquisition, subject to Mr. Mandia s continued status as a service provider to us on each such date. If Mr. Mandia s status as a service provider to us is terminated prior to full vesting, then any unvested portion of the revested shares will be immediately forfeited to us without consideration. Notwithstanding the foregoing, if we terminate Mr. Mandia s service without cause (as defined in our Change of Control Severance Policy for Officers) or breach the terms of his offer letter, the vesting of such revested shares automatically accelerates in full. The terms and conditions of the revested stock are also set forth in a consideration holdback agreement between Mr. Mandia and us.

The offer letter also contains certain covenants regarding activities that Mr. Mandia cannot engage in while providing services to us. In addition, Mr. Mandia entered into a key employee non-competition agreement, or non-competition agreement, with us, which provides that he will not, for a period of time equal to the later of (a) the period commencing on December 30, 2013 and ending on the second anniversary of such date, or (b) only if he does not work in California, the period commencing on December 30, 2013 and ending 18 months after the termination of his employment or consulting agreement with us or any of our affiliates, compete with us by engaging in any competing business purpose (as defined in the non-competition agreement) in the restricted territory (as defined in the non-competition agreement). The non-competition agreement also contains standard non-solicitation provisions, preventing Mr. Mandia from (i) soliciting any of our employees (including former Mandiant employees) or consultants to leave his or her employment and (ii) asking any of our employees (including former Mandiant employees) or consultants to engage in any activity which Mr. Mandia is prohibited from engaging in under the terms of the non-competition agreement.

Jeffrey C. Williams

Effective August 1, 2013, we entered into a confirmatory offer letter with Jeffrey C. Williams, our Senior Vice President, Sales. The offer letter is for no specific term and provides that Mr. Williams is an at-will employee. Mr. Williams current annual base salary is $225,000, and he is eligible for annual target incentive payments equal to $225,000 for 2014. Mr. Williams is also eligible for severance benefits under our Change of Control Severance Policy for Officers.

Alexa King

Effective August 1, 2013, we entered into a confirmatory offer letter with Alexa King, our Senior Vice President, General Counsel and Secretary. The offer letter is for no specific term and provides that Ms