

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.

Edgar Filing: FireEye, Inc. - Form 424B4

PRICE \$82.00 A SHARE

	<i>Underwriting</i>			
	<i>Price to</i>	<i>Discounts and</i>	<i>Proceeds to</i>	
	<i>Public</i>	<i>Commissions⁽¹⁾</i>	<i>FireEye</i>	<i>Proceeds to Selling</i>
				<i>Stockholders</i>
<i>Per Share</i>	\$82.00	\$2.46	\$79.54	\$79.54
<i>Total</i>	\$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
UBS INVESTMENT BANK
PACIFIC CREST SECURITIES

BARCLAYS

J.P. MORGAN
DEUTSCHE BANK SECURITIES

GOLDMAN, SACHS & CO.
CITIGROUP
NOMURA

March 6, 2014

Table of Contents

Table of Contents

Table of Contents**TABLE OF CONTENTS**

	Page
<u>Prospectus Summary</u>	1
<u>Risk Factors</u>	15
<u>Special Note Regarding Forward-Looking Statements</u>	45
<u>Market and Industry Data</u>	47
<u>Use of Proceeds</u>	48
<u>Market Price of Common Stock</u>	48
<u>Dividend Policy</u>	48
<u>Capitalization</u>	49
<u>Dilution</u>	51
<u>Selected Consolidated Financial Data</u>	53
<u>Management's Discussion and Analysis of Financial Condition and Results of Operations</u>	56
<u>Business</u>	97
	Page
<u>Management</u>	122
<u>Executive Compensation</u>	130
<u>Certain Relationships and Related Party Transactions</u>	152
<u>Principal and Selling Stockholders</u>	156
<u>Description of Capital Stock</u>	164
<u>Shares Eligible for Future Sale</u>	168
<u>Material U.S. Federal Income Tax Consequences to Non-U.S. Holders</u>	171
<u>Underwriters</u>	175
<u>Legal Matters</u>	183
<u>Experts</u>	183
<u>Where You Can Find Additional Information</u>	183
<u>Index to Consolidated Financial Statements</u>	F-1

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.

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

Table of Contents

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,

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.

Edgar Filing: FireEye, Inc. - Form 424B4

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.

Table of Contents

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.

7

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;

Edgar Filing: FireEye, Inc. - Form 424B4

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

Edgar Filing: FireEye, Inc. - Form 424B4

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

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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;

Edgar Filing: FireEye, Inc. - Form 424B4

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

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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.

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.

Table of Contents

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

Table of Contents

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

Table of Contents

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

Table of Contents

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.

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.

Edgar Filing: FireEye, Inc. - Form 424B4

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;

Edgar Filing: FireEye, Inc. - Form 424B4

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;

Table of Contents

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

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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.

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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.

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;

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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.

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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.

Edgar Filing: FireEye, Inc. - Form 424B4

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

Table of Contents

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 words and 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;

Edgar Filing: FireEye, Inc. - Form 424B4

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.

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;

Edgar Filing: FireEye, Inc. - Form 424B4

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