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

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

PROSPECTUS

14,000,000 Shares

COMMON STOCK

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

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

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

PRICE $82.00 A SHARE

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

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

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

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

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

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

March 6, 2014

Table of Contents

Table of Contents

Table of Contents

TABLE OF CONTENTS

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

1

Table of Contents

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

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

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

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

Industry Background

Organizations Are Spending Billions On Legacy Signature-Based Security Technologies

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

2

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.

3

Table of Contents

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

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

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

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

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

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

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

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

4

Table of Contents

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

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

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

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

Our Solution

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

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

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

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

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

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.

6

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

Our Competitive Strengths

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

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

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

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

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

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

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

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

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

Table of Contents

Our Strategy

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

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

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

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

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

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

Risks Associated With Our Business

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

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

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

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

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

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

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

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

Table of Contents

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

Corporate Information

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

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

Emerging Growth Company

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

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

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

Table of Contents

THE OFFERING

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

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

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

Table of Contents

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

SUMMARY CONSOLIDATED FINANCIAL DATA

The summary consolidated statements of operations data presented below for the years ended December 31, 2011, 2012 and 2013 are derived from audited consolidated financial statements included elsewhere in this prospectus. The following summary consolidated financial data should be read with &#1