

FireEye, Inc.  
Form 10-K  
March 03, 2014

UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
Washington, D.C. 20549

FORM 10-K

(Mark One)

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2013

or

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from \_\_\_\_\_ to \_\_\_\_\_

Commission File Number 001-36067

FireEye, Inc.  
(Exact name of registrant as specified in its charter)

Delaware  
(State or other jurisdiction of  
incorporation or organization)

20-1548921  
(I.R.S. Employer  
Identification Number)

1440 McCarthy Blvd.  
Milpitas, CA 95035  
(408) 321-6300

(Address, including zip code, and telephone number, including area code, of registrant's principal executive offices)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Name of each exchange on which registered
Common Stock, par value \$0.0001 per share	The NASDAQ Global Select Market

Securities registered pursuant to Section 12(g) of the Act:

None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes  No

Edgar Filing: FireEye, Inc. - Form 10-K

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Securities Exchange Act of 1934 (the "Exchange Act"). Yes  No

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes  No

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes  No

Indicate by a check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K.

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of "large accelerated filer," "accelerated filer" and "smaller reporting company" in Rule 12b-2 of the Exchange Act. (Check one):

---

Large accelerated  
filer

Accelerated filer

Non-accelerated  
filer

(Do not check if a smaller reporting company)

Smaller reporting  
company

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes  
.. No

As of June 30, 2013, the last business day of the registrant's most recently completed second fiscal quarter, there was no established public market for the registrant's common stock and, therefore, the registrant cannot calculate the aggregate market value of its common stock held by non-affiliates as of such date. At September 30, 2013, the aggregate market value of the registrant's common stock held by non-affiliates based upon the closing price of such shares on The NASDAQ Global Select Market on such date was approximately \$1.8 billion. Shares of common stock held by each executive officer, director and by each person who owns 5% or more of the outstanding common stock have been excluded in that such persons may be deemed to be affiliates. This determination of affiliate status is not necessarily a conclusive determination for other purposes.

The number of outstanding shares of the registrant's common stock was 137,896,790 as of February 27, 2014.

#### DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement for the 2014 Annual Meeting of Stockholders to be filed with the Securities and Exchange Commission within 120 days after the end of the registrant's fiscal year ended December 31, 2013 are incorporated by reference into Part III of this Annual Report on Form 10-K.

---

	Page
<u>PART I</u>	
<u>Item 1. Business</u>	<u>6</u>
<u>Item 1A. Risk Factors</u>	<u>17</u>
<u>Item 1B. Unresolved Staff Comments</u>	<u>39</u>
<u>Item 2. Properties</u>	<u>39</u>
<u>Item 3. Legal Proceedings</u>	<u>40</u>
<u>Item 4. Mine Safety Disclosures</u>	<u>40</u>
<u>PART II</u>	
<u>Item 5. Market for Registrant's Common Equity, Related Stockholder Matters, and Issuer Purchases of Equity Securities</u>	<u>41</u>
<u>Item 6. Selected Consolidated Financial Data</u>	<u>44</u>
<u>Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations</u>	<u>46</u>
<u>Item 7A. Quantitative and Qualitative Disclosures About Market Risk</u>	<u>67</u>
<u>Item 8. Financial Statements and Supplementary Data</u>	<u>67</u>
<u>Item 9. Changes in and Disagreements With Accountants on Accounting and Financial Disclosure</u>	<u>102</u>
<u>Item 9A. Controls and Procedures</u>	<u>102</u>
<u>Item 9B. Other Information</u>	<u>103</u>
<u>PART III</u>	
<u>Item 10. Directors, Executive Officers, and Corporate Governance</u>	<u>103</u>
<u>Item 11. Executive Compensation</u>	<u>103</u>
<u>Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</u>	<u>104</u>
<u>Item 13. Certain Relationships and Related Transactions and Director Independence</u>	<u>104</u>
<u>Item 14. Principal Accountant Fees and Services</u>	<u>104</u>
<u>PART IV</u>	
<u>Item 15. Exhibits and Financial Statement Schedules</u>	<u>104</u>
<u>Signatures</u>	<u>105</u>
<u>Exhibit Index</u>	<u>106</u>

---

## SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K, including the sections entitled “Business,” “Risk Factors,” and “Management’s Discussion and Analysis of Financial Condition and Results of Operations,” 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,” “could,” “would,” “project,” “plan” “expect,” the negative and plural forms of these words and similar expressions that convey uncertainty of future events or outcomes are intended to identify forward-looking statements. These forward-looking statements include, but are not limited to, statements concerning the following:

- the evolution of the threat landscape facing our customers and prospects;
- our ability to educate the market regarding the advantages of our virtual machine-based security solution;
- our ability to maintain an adequate rate of revenue growth;
- our future financial and operating results;
- our business plan and our ability to effectively manage our growth and associated investments;
- beliefs and objectives for future operations;
- our ability to expand our leadership position in advanced network security;
- our ability to attract and retain customers;
- our ability to further penetrate our existing customer base;
- our expectations concerning renewal rates for subscriptions and services by existing customers;
- our ability to maintain our competitive technological advantages against new entrants in our industry;
- our ability to timely and effectively scale and adapt our existing technology;
- our ability to innovate new products and bring them to market in a timely manner;
- our ability to maintain, protect, and enhance our brand and intellectual property;
- our ability to expand internationally;
- the reorganization of our corporate structure and intercompany relationships and our ability to improve our overall effective tax rate;
- the effects of increased competition in our market and our ability to compete effectively;
- cost of revenue, including changes in costs associated with production, manufacturing and customer support;
- operating expenses, including changes in research and development, sales and marketing, and general and administrative expenses;
- anticipated income tax rates;
- sufficiency of cash to meet cash needs for at least the next 12 months;
- our ability to maintain our good standing with the United States and international governments and capture new contracts;
- costs associated with defending intellectual property infringement and other claims, such as those claims discussed in “Business—Legal Proceedings”;
- our expectations concerning relationships with third parties, including channel partners and logistics providers;
- 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” included in Part I, Item 1A and elsewhere in this Annual Report on Form 10-K. 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 Annual Report on Form 10-K 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 Annual Report on Form 10-K to conform these statements to actual results or to changes in our expectations, except as required by law.

---

You should read this Annual Report on Form 10-K and the documents that we reference in this Annual Report on Form 10-K and have filed with the SEC as exhibits to this Annual Report on Form 10-K with the understanding that our actual future results, levels of activity, performance and events and circumstances may be materially different from what we expect.

---

## PART I

### Item 1. Business

#### General

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

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

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

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

Second, Mandiant brings significant depth in intelligence on next-generation attacks, which is continually gathered from ongoing monitoring of more than two million endpoints and by incident response and remediation teams that



serve on the front lines combating the most advanced attacks. When this depth of threat intelligence is paired with the breadth of the FireEye real-time threat intelligence gathered from more than two million virtual machines, organizations will have robust detection and contextual information about attempted attacks, including the level of risk, the identity of the attackers, and the intended target of the attacks.

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

Our platform is delivered through a family of software-based appliances and includes our cloud subscription services as well as support and maintenance services. Our principal threat prevention appliance families address four critical vectors of attack: Web, email, file and mobile. We also provide a family of threat prevention appliances that enable rapid identification and remediation of attacks that have penetrated and are residing on an organization's endpoints, such as desktop computers, laptops, or mobile devices. Our management appliances serve as a central nervous system unifying reporting and configuration, while monitoring and correlating attacks that simultaneously cross multiple vectors of the network, thereby increasing the efficacy of our security platform. Our

management appliances enable us to share intelligence regarding threats at a local implementation level and also across the organization. In addition, we enhance the efficacy of our solution by sharing with customers anonymized global threat data through our DTI cloud. We also offer a forensic analysis appliance that provides IT security analysts with the ability to test, characterize and conduct forensic examinations on next-generation cyber attacks by simulating their execution path with our virtual machine technology. Our cloud-based mobile threat prevention platform identifies and stops mobile threats by analyzing mobile applications within our MVX engine. Finally, we offer incident response and managed services to assist our customers who have been breached as part of our full service solution to combat advanced threats.

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

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

For 2013, 2012 and 2011, our revenue was \$161.6 million, \$83.3 million and \$33.7 million, respectively, representing year-over-year growth of 94% for 2013, 148% for 2012 and 186% for 2011, and our net losses were \$120.6 million, \$35.8 million and \$16.8 million, respectively.

We primarily market and sell our virtual machine-based security platform to Global 2000 companies in a broad range of industries and governments worldwide. Our business is geographically diversified, with 72% of our total revenue from the Americas, 14% from Europe, the Middle East, and Africa (EMEA), and 10% from Asia Pacific and Japan (APAC) in 2013. As of December 31, 2013, we had over 1,900 end-customers, including over 130 of the Fortune 500.

We were incorporated in Delaware in February 2004 under the name NetForts, Inc., and changed our name to FireEye, Inc. in September 2005. Our principal executive offices are located at 1440 McCarthy Blvd, Milpitas, California 95035, and our telephone number is (408) 321- 6300. Our website is [www.fireeye.com](http://www.fireeye.com). Information contained on, or that can be accessed through, our website is not incorporated by reference into this report, and you should not consider information on our website to be part of this report. Our Annual Report on Form 10-K, Quarterly Report on Form 10-Q, Current Reports on Form 8-K and amendments to reports filed or furnished pursuant to Sections 13(a) and 15(d) of the Securities Exchange Act of 1934, as amended, are available free of charge on the Investors portion of our web site as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC.

We are organized and operate in a single segment. See "Management's Discussion and Analysis of Financial Condition and Results of Operations" included in Part II, Item 7 of this report.

## Our Products and Services

### Products

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

7

---

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

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

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

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

**Forensic Analysis System.** Our Forensic Analysis System provides powerful auto-configured test environments to allow forensics teams to manually execute and inspect advanced malware, zero-day, and other advanced cyber attacks embedded in files, email attachments, and Web objects. The Forensic Analysis System inspects single files or batches of files for malware and tracks outbound connection attempts across multiple protocols. In virtual execution mode, the Forensic Analysis System analyzes the execution path of a particular malware sample to generate a dynamic and anonymized profile that can be distributed to other FireEye appliances on the network. Malware attack profiles

include identifiers of malware code, exploit URLs, and other sources of infections and attacks. To fully analyze the behavior of every unknown file, the Forensic Analysis System provides full malware life cycle analysis. While the Forensic Analysis System is not required for deployments, our larger customers typically purchase the product to enable advanced and deeper analysis of potential malicious software outside of the real-time traffic scanning done by our Threat Prevention appliances.

Endpoint Threat Prevention System. Our Endpoint Threat Prevention System is an appliance and endpoint agent-based system that equips security organizations to confidently detect, analyze and resolve security incidents in a fraction of the time it takes using conventional approaches. The Endpoint Threat Prevention System enables security operations teams to connect the dots between security incidents in their networks and endpoints to provide the holistic picture required to find and scope security breaches as they are unfolding. In addition to applying proprietary intelligence to sweep for indicators of compromise, or IOCs, our Endpoint Prevention System automatically investigates alerts generated by FireEye products, SIEM, log management and other network security solutions, to identify the specific devices that have been impacted and assess the potential risk. Security

operations teams receive the information they need, when they need it, to make rapid, accurate decisions about potential incidents. When a suspected incident is confirmed, the endpoints involved can be contained with a single click to deny the attacker access while still allowing forensic investigations to continue.

## Subscription and Services

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

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

**Email Threat Prevention Attachment/URL Engine.** Our Email Threat Prevention Attachment/URL engine analyzes email attachments and URLs embedded in emails for next-generation threats. Customers who purchase the Email Threat Prevention appliance are also required to purchase a one or three year subscription to our Email Threat Prevention Attachment/URL engine.

## Security-as-a-Service Offerings.

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

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

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

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

Incident response and related consulting services. We have a team of cyber security experts that can quickly respond to customers that have experienced a breach and help them understand the scope of the incident and quickly remediate the attack. Our cyber security experts will inform customers who is behind the attack (i.e., organized crime, nation state or malicious insider) and how much damage was done, and will work with them to recover from the incident while minimizing the impact of the event on the organization. We have performed hundreds of successful computer security investigations

across all industries, organization sizes and technical environments. As part of our services, we can help customers organize their own security programs, help with litigation support and forensics, and assist with threat and vulnerability assessments.

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

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

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



Edgar Filing: FireEye, Inc. - Form 10-K

Product Category	Models / Types	Key Features	Subscriptions
Web Threat Prevention	NX 900	<ul style="list-style-type: none"> <li>• 1U to 2U Rack-mount</li> <li>• 10Mbps to 4 Gbps throughput</li> <li>• 150—40,000 users</li> <li>• Broad Web object support</li> </ul>	• DTI
	NX 1400		
	NX 2400		
	NX 4400		
	NX 4420		
	NX 7400		
Email Threat Prevention	NX 7420	<ul style="list-style-type: none"> <li>• 1U to 2U Rack-mount</li> <li>• Email quarantine</li> <li>• Anti-Virus integration</li> <li>• Spear phishing security</li> </ul>	<ul style="list-style-type: none"> <li>• DTI</li> <li>• Email Threat Prevention Attachment/URL Engine</li> </ul>
	NX 1000		
	EX 3400		
	EX 5400		
File Threat Prevention	EX 8400	<ul style="list-style-type: none"> <li>• 1U to 2U Rack-mount</li> <li>• File quarantine</li> <li>• Deep file analysis</li> <li>• Anti-virus integration</li> <li>• Broad file type support</li> </ul>	• DTI
	EX8420		
Central Management	FX 5400	<ul style="list-style-type: none"> <li>• U to 2U Rack-mount</li> <li>• Threat Prevention Appliance management</li> <li>• Blended attack correlation</li> <li>• SIEM Integration</li> <li>• Detailed reporting</li> </ul>	
	FX 8400		
	CM 4400		
Forensic Analysis	CM 7400	<ul style="list-style-type: none"> <li>• 1U to 2U Rack-mount</li> <li>• Full threat lifecycle analysis</li> <li>• Sandbox and honeypot modes</li> <li>• Broad file type support</li> </ul>	• DTI
	CM 9400		
Endpoint Threat Prevention	AX 5400	<ul style="list-style-type: none"> <li>• Endpoint validation for advanced threats</li> <li>• One-click containment across all endpoints • Agent Anywhere™ technology to monitor within and outside corporate network</li> </ul>	
	AX 8400		

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

### Our Technology

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

Custom Anomaly Detector. Commercial anomaly detectors are common place in IT security. While such anomaly detectors are the foundation for IPS solutions, they generate a significant number of false positives, making their efficacy in detecting IT security threats challenging. We have custom built our anomaly detector with a focus on helping to filter potentially suspicious data from benign traffic. This filtering allows for most normal traffic to pass

through and any other traffic to be executed in our virtual machine. While our virtual machine can ultimately process all traffic, using an anomaly detector helps to increase network throughput and limit the amount of traffic that requires virtual execution. We are constantly improving the efficacy of our anomaly detector as we discover new threats in our virtual machine. Our anomaly detector also receives updates from our DTI cloud in the attributes, or markers, it looks for when inspecting potentially suspicious data. Uniquely, because the line rate anomaly detector is designed to feed suspicious flows to our MVX engine, it can focus on minimizing missed attacks by aggressively categorizing traffic as suspicious. Any potential false alerts in the output of this system are automatically weeded out by our MVX engine, which confirms whether a suspicious flow or object is malicious. Because we first identify suspicious flows with our line rate anomaly detector and then, through a separate

process, use our MVX engine to determine whether such suspicious flows are malicious, our solution is able to achieve negligible false-positive rates and missed attacks, which are the desired results of the ideal detection engine. Proprietary MVX Engine. Our appliances utilize a proprietary virtual execution engine to execute potentially suspicious software code. We have built our virtual execution engine to take advantage of advances in multi-core processing and run on many-core network processors. As we do not use a commercially available virtual machine, we are not encumbered by any incremental overhead beyond the execution of our environments and the detection of threats. We are also free to make modifications to the code base of our virtual execution engine, which our competitors are not able to do. Our virtual execution engine mimics operating systems and configurations of several user devices, including several popular operating systems, applications and Web browsers. Once the unknown software code is loaded into this environment, our engine monitors the software's behavior. Using a proprietary behavior analysis technology, our appliances determine if the actions the code is taking in the virtual environment are malicious or benign. We have developed our MVX engine over the past 9 years to provide high performance next-generation threat protection while maintaining high threat detection efficacy, negligible false-positive rates, and minimal impact on network performance.

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

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

Evolved Network Security Architecture. Our appliances are designed to operate as part of a comprehensive architecture to defend networks against next-generation threats. This allows appliances to be deployed at the right vectors and have visibility into the traffic streams necessary to detect and block next-generation threats. The ability to monitor all traffic and file stores is critical to detecting next-generation threats that will enter through multiple vectors and move laterally across the network. This is impossible for legacy network security providers to achieve with architectures that were built around traditional threats and file scanning and don't have visibility into the traffic sources next-generation threats utilize during attacks.

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

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

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

MVX Execution. Through a pre-configured, instrumented virtual analysis environment, our MVX engine fully executes suspicious objects and flows to allow deep inspection of common file formats, email attachments, and Web

objects. Newly discovered malware is installed and executed to completion within our MVX engine so that it is forensically analyzed, tracked and blocked. Analysis of malware is automated to create dynamic blocking of inbound attacks and its outbound transmissions.

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

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

based intelligence so customers can confirm the scope of the attack, identify and contain all compromised hosts and quickly secure their networks.

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

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

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

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

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

## Customers

Our customer base has grown from approximately 450 end-customers at the end of 2011 to over 1,900 end-customers as of December 31, 2013 in more than 60 countries, including more than 130 of the Fortune 500. We provide products and subscriptions to customers of varying sizes, including enterprises, governmental agencies and educational and nonprofit organizations. Our customers include leading enterprises in a diverse set of industries, including telecommunications providers, financial services entities, Internet search engines, social networking sites, stock exchanges, electrical grid operators, networking vendors, oil and gas companies and leading U.S. and international governmental agencies. Our business is not dependent on any particular end-customer as no end-customer represented more than 10% of our revenue for any of the years ended December 31, 2013, 2012 and 2011. For the year ended December 31, 2013, Accuvant and Carahsoft, two of our resellers, accounted for approximately 11% and 11% of our revenue, respectively. Accuvant accounted for approximately 10% of our revenue for the year ended December 31, 2012.

## Backlog

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

## Sales and Marketing

Sales. Our sales organization consists of a direct sales team and channel partners who work in collaboration with our direct sales team to identify new sales prospects, sell products, subscriptions and services, and provide post-sale support. Our direct field sales team is responsible for securing enterprise and government accounts globally. Our direct inside sales organization is responsible for securing medium and smaller organizations that are focused on protecting key assets. We also recently built a strategic account management team to support and expand sales within our customer base. Our sales cycle varies by industry, but can last several months, although some deals close in only a few weeks given the typically shorter deployment time of our products as compared to traditional network security products. We also have a dedicated team focused on the channel, who work with our direct sales organization to manage the relationships with our channel partners and work with our channel partners in winning and supporting customers. We believe this direct-touch sales approach allows us to leverage the benefits of the channel as well as maintain face-to-face connectivity with our customers, including key enterprise accounts. We expect to continue to grow our sales headcount in all markets, particularly

in countries where we currently do not have a direct sales presence. In our most recent quarter, nearly a third of our engagements with prospects have been led by channel partners.

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

**Marketing.** Our marketing is focused on building our brand reputation and the market awareness of our platform, driving customer demand and a strong sales pipeline, and working with our channel partners around the globe. Our marketing team consists primarily of corporate marketing, channel marketing, account/lead development, operations, and corporate communications. Marketing activities include demand generation, advertising, managing our corporate Website and partner portal, trade shows and conferences, press and analyst relations, and customer awareness. We are also actively engaged in driving global thought leadership programs through blogs and media and developing rich content such as the global cyber maps and report released in the second quarter of 2013. In 2011, we started releasing a semi-annual threat report, called FireEye Advanced Threat Report, the industry's first report exclusively focused on the next-generation threat landscape.

#### Technology Alliance Partners

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

- Network Monitoring vendors, including Gigamon, Solera Networks (acquired by Blue Coat Systems, Inc. in May 2013) and VSS Monitoring (acquired by Danaher Corporation in June 2012);
- Security Information & Event Management vendors, including RSA, a subsidiary of EMC, ArcSight, a subsidiary of HP, and Q1 Labs, a subsidiary of IBM, and Splunk;
- Network Equipment vendors, including Blue Coat and Juniper Networks;
- Forensic software vendors, including Guidance Software; and
- Web Application Firewall vendors, including Imperva.

#### Government Affairs

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

## Manufacturing

The manufacturing of our security products is outsourced to a single third-party contract manufacturer. This approach allows us to reduce our costs as it reduces our manufacturing overhead and inventory and also allows us to adjust more quickly to changing customer demand. Our manufacturing partner assembles our products using design specifications, quality assurance programs, and standards that we establish, and it procures components and assembles our products based on our demand forecasts. These forecasts represent our estimates of future demand for our products based upon historical trends and analysis from our sales and product management functions as adjusted for overall market conditions.



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

#### Research and Development

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

Research and development expense totaled \$66.0 million, \$16.5 million and \$7.3 million for the years ended December 31, 2013, 2012 and 2011, respectively. We plan to continue to significantly invest in resources to conduct our research and development effort.

#### Competition

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

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

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

The principal competitive factors in our market include:

- ability to detect next-generation threats by overcoming the limitations of signature-based approaches;
- efficacy of the virtual machine technology in terms of detecting the maximum number of threats;
- scalability, throughput and overall performance of the virtual machine technology;
- visibility into all stages of an attack, especially the exploit phase;
- ability to achieve low false-positive rates;
- breadth and richness of the shared threat data the appliances have access to;

- ability to process all data entering a network on premise;
- brand awareness and reputation;
  - strength of sales and marketing efforts;
- product extensibility and ability to integrate with other technology infrastructures;
- price and total cost of ownership; and
  - our ability to provide a comprehensive solution of products and services for detecting, preventing and resolving advanced cybersecurity threats.

We believe we compete favorably with our competitors on the basis of these factors as a result of the features and performance of our platform, the ease of integration of our products with technological infrastructures, and the relatively low total cost of ownership of our products. However, many of our competitors have substantially greater financial, technical and other resources, greater name recognition, larger sales and marketing budgets, deeper customer relationships, broader distribution, and larger and more mature intellectual property portfolios.

## Intellectual Property

Our success depends in part upon our ability to protect our core technology and intellectual property. We rely on, among other things, patents, trademarks, copyrights and trade secret laws, confidentiality safeguards and procedures, and employee non-disclosure and invention assignment agreements to protect our intellectual property rights. We have 16 U.S. issued patents and 78 patent applications pending in the United States. We also have a number of foreign counterparts of these patent applications, consisting of two pending applications under the Patent Cooperation Treaty, a pending application in the European Patent Office and another in Japan. Our issued patents expire between 2025 and 2030. We cannot assure you whether any of our patent applications will result in the issuance of a patent or whether the examination process will result in patents of valuable breadth or applicability. In addition, any patents that may issue may be contested, circumvented, found unenforceable or invalidated, and we may not be able to prevent third parties from infringing them. We also license software from third parties for integration into our products, including open source software and other software available on commercially reasonable terms.

We control access to and use of our proprietary software, technology and other proprietary information through the use of internal and external controls, including contractual protections with employees, contractors, end-customers and partners, and our software is protected by U.S. and international copyright, patent and trade secret laws. Despite our efforts to protect our software, technology and other proprietary information, unauthorized parties may still copy or otherwise obtain and use our software, technology and other proprietary information. In addition, we intend to expand our international operations, and effective patent, copyright, trademark, and trade secret protection may not be available or may be limited in foreign countries.

Our industry is characterized by the existence of a large number of patents and frequent claims and related litigation regarding patent and other intellectual property rights. If we become more successful, we believe that competitors will be more likely to try to develop products that are similar to ours and that may infringe our proprietary rights. It may also be more likely that competitors or other third parties will claim that our products infringe their proprietary rights. In particular, large and established companies in the IT security industry have extensive patent portfolios and are regularly involved in both offensive and defensive litigation. From time-to-time, third parties, including certain of these large companies and non-practicing entities, may assert patent, copyright, trademark, and other intellectual property rights against us, our channel partners, or our end-customers, whom our standard license and other agreements obligate us to indemnify against such claims. Successful claims of infringement by a third party, if any, could prevent us from distributing certain products or performing certain services, require us to expend time and money to develop non-infringing solutions, or force us to pay substantial damages (including, in the United States, treble damages if we are found to have willfully infringed patents), royalties or other fees. We cannot assure you that we do not currently infringe, or that we will not in the future infringe, upon any third-party patents or other proprietary rights. For example, we are currently a party to claims alleging, among other things, patent infringement, which are in the early stages of litigation. See “Risk Factors—Risks Related to Our Business and Our Industry—Claims by others that we infringe their proprietary technology or other rights could harm our business” for additional information.

## Employees

As of December 31, 2013, we had 1,678 full-time employees. None of our employees is represented by a labor organization or is a party to any collective bargaining arrangement. We have never had a work stoppage, and we consider our relationship with our employees to be good.

## Facilities

We currently lease approximately 170,000 square feet of space for our corporate headquarters in Milpitas, California under lease agreements that expire at various dates through 2018. We maintain additional offices throughout the

United States and various international locations, including Australia, Dubai, India, Ireland, Japan, South Korea, Singapore, Taiwan, Turkey and the United Kingdom. We believe that our current facilities are adequate to meet our ongoing needs, and that, if we require additional space, we will be able to obtain additional facilities on commercially reasonable terms.

#### Legal Proceedings

We are a party to litigation and subject to claims incident to the ordinary course of business. Although the results of litigation and claims cannot be predicted with certainty, we currently believe that the final outcome of these matters will not have a material adverse effect on our business. Regardless of the outcome, litigation can have an adverse impact on us because of defense and settlement costs, diversion of management resources and other factors.

#### Item 1A. Risk Factors

Our operations and financial results are subject to various risks and uncertainties including those described below. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, also may become important factors that affect us. If any of the following risks or others not specified below materialize, our business, financial condition and results of operations could be materially adversely affected. In that case, the trading price of our common stock could decline.

##### Risks Related to Our Business and Our Industry

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

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

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

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

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

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

17

---

- 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.

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.

18

---



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

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

Our headcount increased from more than 175 employees as of December 31, 2011 to over 1,600 employees as of December 31, 2013. We expect our headcount to continue to grow rapidly. In addition, our number of end-customers increased from more than 425 to more than 1,900 over the same period. This rapid growth has placed significant demands on our management and our operational and financial infrastructure. To improve our infrastructure, we have recently implemented a new enterprise resource planning system, including revenue recognition and management software, and we plan to implement additional systems. There is no assurance that we will be able to successfully scale improvements to our enterprise resource planning system or other systems and processes in a manner that keeps pace with our growth or that such systems will be effective in preventing or detecting errors, omissions or fraud.

As part of our efforts to improve our internal systems, processes and controls, we have licensed technology from third parties. The support services available for such third-party technology is outside of our control and may be negatively affected by consolidation in the software industry. In addition, if we do not receive adequate support for the software underlying our systems, processes and controls, our ability to provide products and services to our customers in a timely manner may be impaired, which may cause us to lose customers, limit us to smaller deployments of our platform or increase our technical support costs.

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

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

These and other improvements in our systems and controls will require significant capital expenditures and the allocation of valuable management and employee resources. If we fail to implement these improvements effectively, our ability to manage our expected growth, ensure uninterrupted operation of key business systems and comply with

the rules and regulations applicable to public reporting companies would be impaired, and our business, financial condition and results of operations would be harmed.

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

Our revenue depends significantly on general economic conditions and the demand for products in the IT security market. Economic weakness, customer financial difficulties, and constrained spending on IT security may result in decreased revenue and earnings. Such factors could make it difficult to accurately forecast our sales and operating results and could negatively affect our ability to provide accurate forecasts to our contract manufacturers and manage our contract manufacturer relationships and other expenses. In addition, concerns regarding the impact of the U.S. federal sequestration on the IT budgets of various agencies of the U.S. government, as well as continued budgetary challenges in the United States and Europe and geopolitical turmoil in many parts of the world have and may continue to put pressure on global economic conditions and overall spending on IT security. Currently, most enterprises and governments have not allocated a fixed portion of their budgets to protect against next-generation advanced cyber attacks. If we do not succeed in convincing

customers that our platform should be an integral part of their overall approach to IT security and that a fixed portion of their annual IT budgets should be allocated to our platform, general reductions in IT spending by our customers are likely to have a disproportionate impact on our business, results of operations and financial condition. General economic weakness may also lead to longer collection cycles for payments due from our customers, an increase in customer bad debt, restructuring initiatives and associated expenses, and impairment of investments. Furthermore, the continued weakness and uncertainty in worldwide credit markets, including the sovereign debt situation in certain countries in the European Union, may adversely impact the ability of our customers to adequately fund their expected capital expenditures, which could lead to delays or cancellations of planned purchases of our platform.

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

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

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

- our ability to attract and retain new customers;
- the budgeting cycles, seasonal buying patterns and purchasing practices of customers;
- the timing of shipments of our products and length of our sales cycles;
- changes in customer or reseller requirements or market needs;
- changes in the growth rate of the IT security market, particularly the market for threat protection solutions like ours that target next-generation advanced cyber attacks;
- the timing and success of new product and service introductions by us or our competitors or any other change in the competitive landscape of the IT security market, including consolidation among our customers or competitors;
- the level of awareness of IT security threats, particularly advanced cyber attacks, and the market adoption of our platform;
- deferral of orders from customers in anticipation of new products or product enhancements announced by us or our competitors;
- our ability to successfully expand our business domestically and internationally;
- reductions in customer renewal rates for our subscriptions;
- decisions by organizations to purchase IT security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
  - any disruption in, or termination of, our relationship with channel partners;
- decreases in our customers' subscription renewal rates;
- our inability to fulfill our customers' orders due to supply chain delays or events that impact our manufacturers or their suppliers;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our products, subscriptions and services, or confronting our key suppliers, particularly our sole source suppliers, which could disrupt our supply chain;
- the cost and potential outcomes of existing and future litigation;
- seasonality in our business;
- general economic conditions, both domestic and in our foreign markets;

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

20

---

- 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.

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 \$120.6 million, \$35.8 million and \$16.8 million in the years ended December 31, 2013, 2012 and 2011, 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 their fiscal years. For example, we have historically recorded our highest level of revenue in our fourth quarter, which we believe corresponds to the fourth quarter of a majority of our customers. Similarly, we have historically recorded our second-highest level of revenue in our third quarter, which corresponds to the fourth quarter of U.S. federal agencies and other customers in the U.S. federal government. In addition, our rapid growth rate over the last couple years may have made seasonal fluctuations more difficult to detect. If our rate of growth slows over time, seasonal or cyclical variations in our operations may become more pronounced, and our business, results of operations and financial position may be adversely affected.

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

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

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

• greater name recognition, longer operating histories and larger customer bases;

• larger sales and marketing budgets and resources;

• broader distribution and established relationships with channel and distribution partners and customers;

• greater customer support resources;

• greater resources to make acquisitions;

• lower labor and research and development costs;

• larger and more mature intellectual property portfolios; and

• substantially greater financial, technical and other resources.

In addition, some of our larger competitors have substantially broader product offerings and may be able to leverage their relationships with distribution partners and customers based on other products or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing our products, subscriptions and services, including by selling at zero or negative margins, product bundling or offering closed technology platforms. Potential customers may also prefer to purchase from their existing suppliers rather than a new supplier regardless of product performance or features. As a result, even if the features of our platform are superior, customers may not purchase our products. In addition, new innovative start-up companies, and larger companies that are making significant investments in research and development, may invent similar or superior products and technologies that compete with our platform. Our current and potential competitors may also establish cooperative relationships among themselves or with third parties that may further enhance their resources. If we are unable to compete successfully, or if competing successfully requires us to take costly actions in response to the actions of our competitors, our business, financial condition and results of operations could be adversely affected.

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

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



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

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

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

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

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.

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.

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:

- loss of existing or potential customers or channel partners;
- delayed or lost revenue;
- delay in attaining, or the failure to attain, market acceptance;
- the expenditure of significant financial and product development resources in efforts to analyze, correct, eliminate, or work around errors or defects, to address and eliminate vulnerabilities, or to identify and ramp up production with alternative third-party manufacturers;
-

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

harm to our reputation or brand; and

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

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

We believe that our intellectual property is an essential asset of our business. We rely on a combination of patent, copyright, trademark and trade secret laws, as well as confidentiality procedures and contractual provisions, to establish and protect our intellectual property rights in the United States and abroad. The efforts we have taken to protect our intellectual property may not be sufficient or effective, and our trademarks, copyrights and patents may be held invalid or unenforceable. Any U.S. or other patents issued to us may

not be sufficiently broad to protect our proprietary technologies, and given the costs of obtaining patent protection, we may choose not to seek patent protection for certain of our proprietary technologies. We may not be effective in policing unauthorized use of our intellectual property, and even if we do detect violations, litigation may be necessary to enforce our intellectual property rights. Any enforcement efforts we undertake, including litigation, could be time-consuming and expensive, could divert management's attention and may result in a court determining that our intellectual property rights are unenforceable. If we are not successful in cost-effectively protecting our intellectual property rights, our business, financial condition and results of operations could be harmed.

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

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

Although third parties may offer a license to their technology or other intellectual property, the terms of any offered license may not be acceptable, and the failure to obtain a license or the costs associated with any license could cause our business, financial condition and results of operations to be materially and adversely affected. In addition, some licenses may be non-exclusive, and therefore our competitors may have access to the same technology licensed to us. If a third party does not offer us a license to its technology or other intellectual property on reasonable terms, or at all, we could be enjoined from continued use of such intellectual property. As a result, we may be required to develop alternative, non-infringing technology, which could require significant time (during which we could be unable to continue to offer our affected products, subscriptions or services), effort, and expense and may ultimately not be successful. Furthermore, a successful claimant could secure a judgment or we may agree to a settlement that prevents us from distributing certain products, providing certain subscriptions or performing certain services or that requires us to pay substantial damages, royalties or other fees. Any of these events could harm our business, financial condition and results of operations.

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

We incorporate technology from third parties into our products. We cannot be certain that our suppliers and licensors are not infringing the intellectual property rights of third parties or that the suppliers and licensors have sufficient rights to the technology in all jurisdictions in which we may sell our products. Some of our agreements with our suppliers and licensors may be terminated for convenience by them. If we are unable to obtain or maintain rights to any of this technology because of intellectual property infringement claims brought by third parties against our suppliers and licensors or against us, or if we are unable to continue to obtain such technology or enter into new

agreements on commercially reasonable terms, our ability to develop and sell products, subscriptions and services containing such technology could be severely limited, and our business could be harmed. Additionally, if we are unable to obtain necessary technology from third parties, including certain sole suppliers, we may be forced to acquire or develop alternative technology, which may require significant time, cost and effort and may be of lower quality or performance standards. This would limit and delay our ability to offer new or competitive products and increase our costs of production. If alternative technology cannot be obtained or developed, we may not be able to offer certain functionality as part of our products, subscriptions and services. As a result, our margins, market share and results of operations could be significantly harmed.

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

Our products and subscriptions contain software modules licensed to us by third-party authors under “open source” licenses. The use and distribution of open source software may entail greater risks than the use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code. Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon the type of open source software we use. If we combine our proprietary software with open source software in a certain



manner, we could, under certain open source licenses, be required to release the source code of our proprietary software to the public. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us.

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

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.

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 45%, 37% and 26% for the years ended December 31, 2013, 2012 and 2011, 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 quarter will not be fully reflected in revenue in that quarter but will negatively affect our revenue in future quarters. Accordingly, the effect of significant downturns in new or renewed sales of our subscriptions or services is not reflected in full in our results of operations until future periods. Also, it is difficult for us to rapidly increase our subscription revenue through additional sales in any period, as revenue from new and renewal subscription contracts must be recognized ratably over the applicable service period. Furthermore, any increases in the average term of subscriptions contracts would result in revenue for those subscription contracts being recognized over longer periods of time.

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

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

selling to governmental agencies can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;

government certification requirements applicable to our products may change and in doing so restrict our ability to sell into the U.S. federal government sector until we have attained the revised certification;

government demand and payment for our products and services may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our products and services;

we sell our platform to governmental agencies through our indirect channel partners, and these agencies may have statutory, contractual or other legal rights to terminate contracts with our distributors and resellers for convenience or due to a default, and any such termination may adversely impact our future results of operations;

governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and results of operations, or institute fines or civil or criminal liability if the audit uncovers improper or illegal activities; and

governments may require certain products to be manufactured in the United States and other relatively high-cost manufacturing locations, and we may not manufacture all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies.

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

Once our platform is deployed within our customers' networks, our customers depend on our technical and other support services, as well as the support of our channel partners, to resolve any issues relating to the implementation and maintenance of our platform. If we or our channel partners do not effectively assist our customers in deploying our platform, succeed in helping our customers quickly resolve post-deployment issues, or provide effective ongoing support, our ability to sell additional products, subscriptions or services as part of our platform to existing customers would be adversely affected and our reputation with potential customers could be damaged. Many larger organizations have more complex networks and require higher levels of support than smaller customers. If we fail to meet the requirements of our larger customers, it may be more difficult to execute on our strategy of upselling and cross selling with these customers. Additionally, if our channel partners do not effectively provide support to the satisfaction of our customers, we may be required to provide this level of support to those customers, which would require us to hire additional personnel and to invest in additional resources. We are also in the process of expanding our professional services organization. It can take significant time and resources to recruit, hire, and train qualified technical support and professional services employees. We may not be able to hire such resources fast enough to keep up with demand, particularly when the sales of our platform exceed our internal forecasts. To the extent that we or our channel partners are unsuccessful in hiring, training, and retaining adequate support resources, our ability and the ability of our channel partners to provide adequate and timely support to our customers will be negatively impacted, and our customers' satisfaction with our platform will be adversely affected. Additionally, to the extent that we need to rely on our sales engineers to provide post-sales support while we are ramping our professional services organization, our sales productivity will be negatively impacted, which would harm our results of operations.

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

The sales prices for our products, subscriptions and services may decline for a variety of reasons, including competitive pricing pressures, discounts, a change in our mix of products and subscriptions, anticipation of the introduction of new products or subscriptions, or promotional programs. Competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the

price of products or subscriptions that compete with ours or may bundle them with other products and subscriptions. Additionally, although we price our products and subscriptions worldwide in U.S. dollars, currency fluctuations in certain countries and regions may negatively impact actual prices that partners and customers are willing to pay in those countries and regions. Furthermore, we anticipate that the sales prices and gross profits for our products will decrease over product life cycles. We cannot assure you that we will be successful in developing and introducing new offerings with enhanced functionality on a timely basis, or that our new product and subscription offerings, if introduced, will enable us to maintain our prices and gross profits at levels that will allow us to maintain positive gross margins and achieve profitability.

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

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

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

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 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.

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

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

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

We intend to continue to make investments to support our business growth and may require additional funds to respond to business challenges, including the need to develop new products and enhancements to our platform, improve our operating infrastructure or acquire complementary businesses and technologies. Accordingly, we may need to engage in equity or debt financings to secure

additional funds. If we raise additional equity financing, our stockholders may experience significant dilution of their ownership interests and the per share value of our common stock could decline. Furthermore, if we engage in debt financing, the holders of debt would have priority over the holders of common stock, and we may be required to accept terms that restrict our ability to incur additional indebtedness. We may also be required to take other actions that would otherwise be in the interests of the debt holders and force us to maintain specified liquidity or other ratios, any of which could harm our business, results of operations, and financial condition. If we need additional capital and cannot raise it on acceptable terms, we may not be able to, among other things:

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

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

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

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

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

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

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

We have a limited history of marketing, selling, and supporting our platform internationally. As a result, we must hire and train experienced personnel to staff and manage our foreign operations. To the extent that we experience

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

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

- greater difficulty in enforcing contracts and managing collections, as well as longer collection periods;
  - higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for our international operations;
  - fluctuations in exchange rates between the U.S. dollar and foreign currencies in markets where we do business;
  - management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of our platform that may be required in foreign countries;
- greater risk of unexpected changes in regulatory practices, tariffs, and tax laws and treaties;
  - compliance with anti-bribery laws, including, without limitation, compliance with the U.S. Foreign Corrupt Practices Act of 1977, as amended, the U.S. Travel Act and the UK Bribery Act 2010, violations of which could lead to significant fines, penalties and collateral consequences for our company;
  - heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;
  - the uncertainty of protection for intellectual property rights in some countries;
  - general economic and political conditions in these foreign markets;
  - foreign exchange controls that might prevent us from repatriating cash earned outside the United States;
  - political and economic instability in some countries; and
  - double taxation of our international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which we operate.

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

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

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

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

Our products are subject to U.S. export controls, specifically the Export Administration Regulations and economic sanctions enforced by the Office of Foreign Assets Control. We incorporate standard encryption algorithms into our products, which, along with the underlying technology, may be exported outside of the U.S. only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of an encryption registration and classification request. Furthermore, U.S. export control laws and economic sanctions prohibit the shipment of certain products and services to countries, governments, and persons targeted by U.S. sanctions. While we have taken precautions to prevent our products and services from being exported in violation of these laws, in certain instances in the past we shipped our encryption products prior to obtaining the required export authorizations and/or submitting the required requests, including a classification request and request for an encryption registration number, resulting in an inadvertent violation of U.S. export control laws. As a result, in February 2013, we filed a Voluntary Self Disclosure with the U.S. Department of Commerce's Bureau of Industry and Security, or BIS, concerning these potential violations. In June 2013, BIS notified us that it had completed its review

of this matter and closed its review with the issuance of a warning letter. No monetary penalties were assessed. Even though we take precautions to ensure that our channel partners comply with all relevant regulations, any

failure by our channel partners to comply with such regulations could have negative consequences, including reputational harm, government investigations and penalties.

In addition, various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our products or could limit our customers' ability to implement our products in those countries. Changes in our products or changes in export and import regulations may create delays in the introduction of our products into international markets, prevent our customers with international operations from deploying our products globally or, in some cases, prevent the export or import of our products to certain countries, governments or persons altogether. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such regulations, could result in decreased use of our products by, or in our decreased ability to export or sell our products to, existing or potential customers with international operations. Any decreased use of our products or limitation on our ability to export or sell our products would likely adversely affect our business, financial condition and results of operations.

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

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

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

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

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

regulations, they will likely result in additional costs and may increase penalties associated with violations or require us to change the content of our products or how they are manufactured, which could have a material adverse effect on our business, results of operations and financial condition.

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

Recent changes to U.S. tax laws, including limitations on the ability of taxpayers to claim and utilize foreign tax credits and the deferral of certain tax deductions until earnings outside of the United States are repatriated to the United States, as well as changes to U.S. tax laws that may be enacted in the future, could impact the tax treatment of our foreign earnings. Due to expansion of our international business activities, any changes in the U.S. taxation of such activities may increase our worldwide effective tax rate and adversely affect our financial condition and operating results.

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



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

We could be subject to additional tax liabilities.

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

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

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

#### Risks Related to 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 February 28, 2014 was \$85.64 per share. The trading price of our common stock may fluctuate widely in response to various factors, some of which are beyond our control. These factors include:

- announcements of new products, services or technologies, commercial relationships, acquisitions or other events by us or our competitors;

changes in how customers perceive the effectiveness of our platform in protecting against advanced cyber attacks or other reputational harm;

publicity concerning cyber attacks in general or high profile cyber attacks against specific organizations;

price and volume fluctuations in the overall stock market from time to time;

significant volatility in the market price and trading volume of technology companies in general and of companies in the IT security industry in particular;

fluctuations in the trading volume of our shares or the size of our public float;

actual or anticipated changes or fluctuations in our results of operations;

whether our results of operations and, in particular, our revenue growth rates meet the expectations of securities analysts or investors;

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

litigation involving us, our industry, or both;

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

general economic conditions and trends;

major catastrophic events;

sales of large blocks of our common stock; or

departures of key personnel.

In addition, if the market for technology stocks or the stock market in general experiences a loss of investor confidence, the trading price of our common stock could decline for reasons unrelated to our business, results of operations or financial condition. The trading price of our common stock might also decline in reaction to events that affect other companies in our industry even if these events do not directly affect us. In the past, following periods of volatility in the market price of a company's securities, securities class action litigation has often been brought against that company. If our stock price is volatile, we may become the target of securities litigation. Securities litigation could result in substantial costs and divert our management's attention and resources from our business. This could have a material adverse effect on our business, results of operations and financial condition.

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

The market price of shares of our common stock could decline as a result of substantial sales of our common stock, particularly sales by our secondary offering, our directors, executive officers, employees and significant stockholders, a large number of shares of our common stock becoming available for sale, or the perception in the market that holders of a large number of shares intend to sell their shares. As of December 31, 2013, we had outstanding 137,757,512 shares of our common stock.

As a result of lock-up agreements entered into by certain stockholders in connection with our initial public offering and planned secondary offering and certain transfer restrictions under our insider trading policy, 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:

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 our planned secondary offering, assuming the prior effectiveness of the resale registration statement for former stockholders of Mandiant; and

1,927 shares will be eligible for sale in the public market on June 30, 2014.



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

In addition, holders of up to approximately 84,310,480 shares of our common stock (excluding shares expected to be sold by certain selling stockholders in connection with our planned secondary offering), or 58.5% of our total outstanding common stock, based on shares outstanding as of December 31, 2013, will be entitled to rights with respect to registration of these shares under the Securities Act pursuant to an investors' rights agreement. If these holders of our common stock, by exercising their registration rights, sell a large number of shares, they could adversely affect the market price for our common stock. If we file a registration statement for the purpose of selling additional shares of common stock to raise capital and are required to include shares held by these holders pursuant to the exercise of their registration rights, our ability to raise capital may be impaired. Furthermore, all of our executive officers and certain of our directors have adopted, and other directors may in the future adopt, written plans, known as "Rule 10b5-1 Plans," under which they have contracted, or may in the future contract, with a broker to sell shares of our common stock on a periodic basis to diversify their assets and investments. Sales of substantial amounts of our common stock in the public market 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.

As of December 31, 2013, our directors, executive officers and each of our stockholders who owns greater than 5% of our outstanding common stock, in the aggregate, beneficially own approximately 64.5% of the total outstanding shares of our common stock. 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 do not intend to pay dividends for the foreseeable future.

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

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 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;

- 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 <sup>2</sup>/<sub>3</sub>% 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.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

39

---

Our corporate headquarters is located in Milpitas, California where we currently lease approximately 170,000 square feet of space under lease agreements that expire at various dates through 2018. We maintain additional offices throughout the United States and various international locations, including Australia, Dubai, India, Ireland, Japan, South Korea, Singapore, Taiwan, Turkey and the United Kingdom. We believe that our current facilities are adequate to meet our ongoing needs, and that, if we require additional space, we will be able to obtain additional facilities on commercially reasonable terms.

Item 3. Legal Proceedings

The information set forth under "Litigation" in Note 7 contained in the "Notes to Consolidated Financial Statements" in Item 8 of Part II of this Annual Report on Form 10-K is incorporated herein by reference.

Item 4. Mine Safety Disclosures

Not applicable.

## PART II

## Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

## Market Information

Our common stock, \$0.0001 par value per share, began trading on The NASDAQ Global Select Market on September 20, 2013, where its prices are quoted under the symbol "FEYE."

## Holders of Record

As of December 31, 2013, there were 352 holders of record of our common stock. Because many of our shares are held by brokers and other institutions on behalf of stockholders, we are unable to estimate the total number of stockholders represented by these record holders.

## Price Range of Our Common Stock

The following table sets forth the reported high and low sales prices of our common stock for the periods indicated, as regularly quoted on The NASDAQ Global Select Market:

Year Ended December 31, 2013:	High	Low
Third Quarter (from September 20 , 2013)	\$44.89	\$35.25
Fourth Quarter	\$44.55	\$33.30

## Stock Performance Graph

The following performance graph shall not be deemed "filed" for purposes of Section 18 of the Exchange Act or otherwise subject to the liabilities under that Section, and shall not be deemed to be incorporated by reference into any of our filings under the Securities Act or the Exchange Act, except as shall be expressly set forth by specific reference in such filing.

The following graph compares the cumulative total return of our common stock with the total return for the Standard & Poor's 500 Index and the Standard & Poor's Information Technology Index from September 20, 2013 (the date our common stock commenced trading on The NASDAQ Global Select Market) through December 31, 2013. The graph assumes that \$100 was invested on September 20, 2013 in our common stock, the Standard & Poor's 500 Index and the Standard & Poor's Information Technology Index, and assumes reinvestment of any dividends. The stock price performance on the following graph is not necessarily indicative of future stock price performance.

	September 20, 2013	September 30, 2013	October 31, 2013	November 30, 2013	December 31, 2013
FireEye, Inc.	\$100.00	\$115.36	\$105.28	\$106.58	\$121.14
S&P 500	\$100.00	\$103.14	\$107.88	\$111.16	\$113.98
S&P Information Technology	\$100.00	\$102.88	\$107.61	\$111.88	\$116.52

#### Dividend Policy

We have never declared or paid, and do not anticipate declaring or paying in the foreseeable future, any cash dividends on our capital stock. Any future determination as to the declaration and payment of dividends, if any, will be at the discretion of our board of directors, subject to applicable laws, and will depend on then existing conditions, including our financial condition, operating results, contractual restrictions, capital requirements, business prospects, and other factors our board of directors may deem relevant.

#### Recent Sales of Unregistered Securities

During the fiscal year ended December 31, 2013, we sold the following unregistered securities:

##### Sales of Convertible Preferred Stock

In January 2013, we sold an aggregate of 474,380 shares of Series F convertible preferred stock to a total of 15 accredited investors at a purchase price of approximately \$10.53 per share, for an aggregate purchase price of approximately \$5.0 million.

#### Option and Common Stock Issuances

From January 1, 2013 through September 20, 2013 (the date of the filing of our registration statement on Form S-8, File No. 333-191299), pursuant to the terms of our 2008 Stock Plan and our 2013 Equity Incentive Plan, we granted to our officers, directors, employees, consultants and other service providers options to purchase an aggregate of 12,754,194 shares of our common stock at exercise prices ranging from \$5.44 to \$20.00 per share.

From January 1, 2013 through September 20, 2013 (the date of the filing of our registration statement on Form S-8, File No. 333-191299), pursuant to the terms of our 2008 Stock Plan, we granted to certain officers restricted stock units covering up to an aggregate of 565,500 shares of our common stock in exchange for services.

From January 1, 2013 through September 20, 2013 (the date of the filing of our registration statement on Form S-8, File No. 333-191299), pursuant to the terms of our 2004 Stock Option Plan and our 2008 Stock Plan, we issued and sold to our officers, directors, employees, consultants and other service providers an aggregate of 6,189,368 shares of our common stock upon the exercise of options at exercise prices ranging from \$0.05 to \$7.93 per share, for an aggregate exercise price of \$5.4 million.

From January 1, 2013 through September 20, 2013 (the date of the filing of our registration statement on Form S-8, File No. 333-191299), we issued an aggregate of 316,492 shares of our restricted common stock in exchange for services.

On October 1, 2013, we issued 299,160 shares of common stock to an accredited investor upon the cashless net exercise of two outstanding warrants based on a weighted-average exercise price of approximately \$0.67 per share.

None of the foregoing transactions involved any underwriters, underwriting discounts or commissions, or any public offering. We believe the offers, sales, and issuances of the above securities were exempt from registration under the Securities Act by virtue of (i) Section 4(a)(2) of the Securities Act (or Regulation D promulgated thereunder) as transactions not involving a public offering, (ii) Rule 701 promulgated under the Securities Act as transactions pursuant to compensatory benefit plans or contracts relating to compensation as provided under such rule, or (iii) Regulation S promulgated under the Securities Act as transactions made outside of the United States. The recipients of the securities in each of these transactions represented their intentions to acquire the securities for investment only and not with a view to or for sale in connection with any distribution thereof, and appropriate legends were placed upon the stock certificates or book-entry positions representing the shares issued in these transactions. All recipients had adequate access, through their relationships with us, to information about us. The sales of these securities were made without any general solicitation or advertising.

On September 25, 2013, in connection with the completion of our initial public offering, all 64,589,760 shares of our then-outstanding shares of preferred stock were automatically converted into 74,221,533 shares of common stock. The issuance of such shares was exempt from the registration requirements of the Securities Act in reliance on Section 3(a)(9) and Section 4(a)(2) of the Securities Act. We received no additional consideration for such automatic conversions.

In addition to the securities described above, we have issued securities in connection with the following acquisitions:

- On September 3, 2013, we issued 222,500 shares of our common stock as partial consideration for the acquisition of three entities affiliated with each other.

•On December 30, 2013, we issued 16,920,709 shares of our common stock as partial consideration for the acquisition of Mandiant Corporation.

None of the foregoing transactions with respect to the acquisitions involved any underwriters, underwriting discounts or commissions, or any public offering. We believe that such offers, sales and issuances of the above securities in connection with the foregoing acquisitions were exempt from registration under the Securities Act by virtue of Regulation D promulgated thereunder, as transactions by an issuer not involving a public offering.

#### Use of Proceeds

On September 25, 2013, we closed our initial public offering, or IPO, in which we sold 17,450,000 shares of common stock at a price to the public of \$20.00 per share (inclusive of 2,275,000 shares of common stock from the full exercise of the over-allotment option granted to the underwriters). The aggregate offering price for shares sold in the offering was \$349.0 million. The offer and sale of all of the shares in the IPO were registered under the Securities Act pursuant to registration statements on Form S-1 (File Nos. 333-190338 and 333-191275), which were declared or became effective on September 19, 2013. We raised approximately \$321.0 million in net

proceeds after deducting underwriting discounts and commissions of approximately \$24.4 million and other offering expenses of approximately \$3.6 million. The underwriters of that offering were Morgan Stanley & Co. LLC, Goldman Sachs & Co., J.P. Morgan Securities LLC, Barclays Capital Inc., Merrill Lynch, Pierce, Fenner & Smith Incorporated, UBS Securities LLC, and Nomura Securities International, Inc. No payments were made by us to directors, officers or persons owning ten percent or more of our common stock or to their associates, or to our affiliates, other than payments in the ordinary course of business to officers for salaries. There has been no material change in our planned use of proceeds from our IPO as described in our final prospectus filed with the SEC on September 20, 2013 pursuant to Rule 424(b) under the Securities Act, except that we used approximately \$106.5million of such proceeds to fund our acquisition of Mandiant in December 2013. David DeWalt, our Chief Executive Officer and Chairman of our board of directors, and Kevin Mandia, our Senior Vice President and Chief Operating Officer, were stockholders of Mandiant and received aggregate cash consideration of approximately \$3.9 million and approximately \$19.9 million, respectively, in connection with such acquisition.

#### Issuer Purchases of Equity Securities

There were no repurchases of equity securities by us during the fourth quarter of 2013.

#### Securities Authorized for Issuance Under Equity Compensation Plans

See Item 12 of Part III of this report regarding information about securities authorized for issuance under our equity compensation plans.

#### Item 6. Selected Consolidated Financial Data

The following selected historical financial data below should be read in conjunction with Item 7, "Management's Discussion and Analysis of Financial Condition and Results of Operations," our financial statements, and the related notes appearing in Item 8, "Financial Statements and Supplementary Data," of this Annual Report on Form 10-K to fully understand factors that may affect the comparability of the information presented below.

The statements of operations data for the years ended December 31, 2013, 2012, and 2011 and the balance sheet data as of December 31, 2013 and 2012 are derived from our audited financial statements appearing in Item 8, "Financial Statements and Supplementary Data," of this Annual Report on Form 10-K. The statements of operations for the years ended December 31, 2010 and 2009 and the balance sheet data as of December 31, 2011, 2010 and 2009 are derived from audited financial statements not included in this Annual Report on Form 10-K. Our historical results are not necessarily indicative of the results to be expected in the future.



Edgar Filing: FireEye, Inc. - Form 10-K

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

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

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

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

## Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with our financial statements and related notes appearing elsewhere in this Annual Report on Form 10-K. In addition to historical financial information, the following discussion contains forward-looking statements that reflect our plans, estimates and beliefs. Our actual results could differ materially from those contained in or implied by any forward-looking statements. Factors that could cause or contribute to these differences include those under "Risk Factors" included in Part I, Item 1a or in other parts of this report.

### Overview

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

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

threat protection against next-generation cyber attacks.

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

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

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

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

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

On December 30, 2013, we acquired privately held Mandiant Corporation, or Mandiant, the leading provider of advanced endpoint security products and security incident response management solutions. We believe this combination creates the industry's leading advanced threat protection vendor with the ability to detect, prevent and resolve cyber attacks at every stage of the attack life cycle. Under the terms of the merger agreement governing the transaction, we delivered to the former security holders of Mandiant merger consideration with an aggregate value equal to approximately \$1,020.3 million, consisting of approximately \$106.5 million in net cash and an aggregate of 21.5 million shares and options to purchase shares of our common stock. The results of operations of Mandiant have been included in our consolidated statements of operations since December 30, 2013, the acquisition date. The balance sheet as of December 31, 2013 reflects items assumed from the Mandiant acquisition.

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

We have experienced rapid growth and increased demand for our products over the last few years. To manage any future growth effectively, we must continue to improve and expand our information technology and financial infrastructure, our operating and administrative systems and controls, and our ability to manage headcount, capital, and processes in an efficient manner. Additionally, we face intense competition in our market, and to succeed, we need to innovate and offer products that are differentiated from existing infrastructure products, as well as effectively hire, retain, train, and motivate qualified personnel and senior management. If we are unable to successfully address these challenges, our business, operating results, and prospects could be adversely affected.

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

Our Business Model

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

upon shipment. Finally, we recently introduced our File Threat Prevention appliance in the second quarter of 2012, and as a result, revenue from our File Threat Prevention product represents a small percentage of our product revenue.

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

### Key Business Metrics

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

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

Deferred revenue. Our deferred revenue consists of amounts that have been invoiced but have not yet been recognized as revenue as of the period end. For the year ended December 31, 2013, deferred revenue includes the addition of \$16.1 million of deferred revenue assumed in connection with the Mandiant acquisition. For the year ended December 31, 2012, deferred revenue includes the addition of \$16.1 million of deferred revenue assumed in connection with the Mandiant acquisition. The majority of our deferred revenue consists of the unamortized balance of revenue from sales of our Email MPS product, subscriptions to our DTI cloud and Email MPS 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 noncurrent 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 noncurrent. We monitor our deferred revenue balance because it represents a significant portion of revenue to be recognized in future periods.

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

	Year Ended December 31,		
	2013	2012	2011
	(in thousands)		
Revenue	\$161,552	\$83,316	\$33,658
Deferred revenue, end of period	187,514	76,406	30,102
Less: deferred revenue, beginning of period	76,406	30,102	6,266
Less: Mandiant deferred revenue assumed	16,099	—	—
Billings ( non-GAAP)	\$256,561	\$129,620	\$57,494

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

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

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

#### Factors Affecting our Performance

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



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

Our growth strategy contemplates increased sales and marketing investments internationally. Newly hired sales and marketing resources will require several months to establish prospect relationships and drive overall sales productivity. In addition, sales teams in international regions will face local markets that have not had significant market education about advanced security threats that our platform addresses. All of these factors will influence timing and overall levels of sales productivity, impacting the rate at which we will be able to convert prospects to sales and drive revenue growth.

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

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

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

## Components of Operating Results

### Revenue

We generate revenue from the sales of our products, subscriptions and services. As discussed further in “—Critical Accounting Policies and Estimates—Revenue Recognition” under “Management’s Discussion and Analysis of Financial Condition and Results of Operations” below, revenue is recognized when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed or determinable, and collectability is reasonably assured.

Our total revenue consists of the following:

**Product revenue.** Our product revenue is generated from sales of our appliances. For our Web MPS, File MPS, MAS and CMS appliances, we recognize product revenue at the time of shipment, provided that all other revenue recognition criteria have been met. For our Email MPS appliances, we recognize product revenue ratably over the longer of the contractual term of the subscription service or the estimated period the customer is expected to benefit from the product.

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

#### Cost of Revenue

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

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

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

#### Gross Margin

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

#### Operating Expenses

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

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

Sales and marketing. Sales and marketing expense consists primarily of personnel costs, incentive commission costs and allocated overhead. We expense commission costs as incurred. Sales and marketing expense also includes costs for market development programs, promotional and other marketing activities, travel, office equipment, depreciation of proof-of-concept evaluation units and outside consulting costs. We expect sales and marketing expense to continue to increase in absolute dollars as we increase the size of our sales and marketing organizations and expand our international operations, although such expense may fluctuate as a percentage of total revenue.

General and administrative. General and administrative expense consists of personnel costs, professional services and allocated overhead. General and administrative personnel include our executive, finance, human resources, facilities and legal organizations. Professional services consist primarily of legal, auditing, accounting and other consulting costs. We expect general and administrative expense to continue to increase in absolute dollars as we have recently incurred, and expect to continue to incur, additional general and administrative expenses as we grow our operations and comply with public company regulations, including higher legal, corporate insurance, and accounting expenses.

#### Interest Income

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

#### Interest Expense

Interest expense consists of interest on our outstanding debt. See Note 6 to our consolidated financial statements included elsewhere in this Annual Report on Form 10-K for more information about our debt.

#### Other Expense, Net

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

**Provision for (Benefit from) Income Taxes**

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

## Results of Operations

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

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

Edgar Filing: FireEye, Inc. - Form 10-K

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

Comparison of the Years Ended December 31, 2013 and 2012

Revenue

	Year Ended December 31,		2012	% of Total Revenue	Change	2011	% of Total Revenue	Change	2010
	2013	2012							
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%	Amount	%	Amount
	(Dollars in thousands)								
Revenue:									
Product	\$88,253	55	% \$52,265	63	% \$35,988	69	%		
Subscription and services	73,299	45	% 31,051	37	% 42,248	136	%		
Total revenue	\$161,552	100	% \$83,316	100	% \$78,236	94	%		
Revenue by geographic region:									
United States	\$116,730	72	% \$66,556	80	% \$50,174	75	%		
EMEA	22,845	14	% 6,628	8	% 16,217	245	%		
APAC	16,004	10	% 6,488	8	% 9,516	147	%		
Other	5,973	4	% 3,644	4	% 2,329	64	%		
Total revenue	\$161,552	100	% \$83,316	100	% \$78,236	94	%		

Total revenue increased by \$78.2 million, or 94%, during the year ended December 31, 2013 compared to the year ended December 31, 2012. The increase in product revenue was primarily driven by growth in our installed base of customers, which grew from 927 as of December 31, 2012 to 1,964 as of December 31, 2013, as well as follow-on purchases from customers expanding their initial deployments of our product portfolio. Our Web Threat Prevention

product continued to account for the largest portion of our product revenue as customers that purchase our product portfolio generally purchase more Web Threat Prevention appliances than Email Threat Prevention or File Threat Prevention appliances, reflecting the fact that their networks typically have more Web entry points than email or file entry points to protect. In addition, revenue associated with our Web Threat Prevention product is recognized upon shipment whereas revenue associated with our Email Threat Prevention product is recognized ratably over the longer of the contractual term or the estimated period the customer is expected to benefit from the product.



Revenue from the amortization of deferred subscription and services revenue related to initial customer purchases was \$55.1 million and \$25.1 million for the years ended December 31, 2013 and 2012, respectively. Revenue from the amortization of deferred subscription and services revenue related to renewals was \$18.0 million and \$6.0 million for the years ended December 31, 2013 and 2012, respectively. Given our high renewal rate and increasing base of customers, we expect revenue from the amortization of deferred subscription and services revenue related to renewals to increase as a percentage of our total revenue from deferred subscription and services revenue. Our renewal rate for subscription and services agreements expiring in the 12 months ended December 31, 2013 was in excess of 90%.

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

#### Cost of Revenue and Gross Margin

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

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

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

#### Operating Expenses

	Year Ended December 31, 2013		2012		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Operating expenses:						
Research and development	\$66,036	41 %	\$16,522	20 %	\$49,514	300 %
Sales and marketing	167,466	104	67,562	81	99,904	148
General and administrative	52,503	32	15,221	18	37,282	245
Total operating expenses	\$286,005	177 %	\$99,305	119 %	\$186,700	188 %

Includes stock-based compensation  
expense of:

Research and development	\$6,958	\$1,465
Sales and marketing	10,748	1,672
General and administrative	8,342	3,536
Total	\$26,048	\$6,673

Research and Development

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

#### Sales and Marketing

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

#### General and Administrative

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

#### Interest Income

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

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

#### Interest Expense

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

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

#### Other Expense, Net

	Year Ended December 31,	Change
--	-------------------------	--------

Edgar Filing: FireEye, Inc. - Form 10-K

	2013	2012	Amount	%
	(Dollars in thousands)			
Other expense, net	\$(7,257 )	\$(2,572 )	\$(4,685 )	182 %

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

Provision for (Benefit from) Income Taxes

	Year Ended December 31,	
	2013	2012
	(Dollars in thousands)	
Provision for (benefit from) income taxes	\$ (59,297 )	\$ (965 )
Effective tax rate	33 %	3 %

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

Comparison of the Years Ended December 31, 2012 and 2011

Revenue

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

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

Revenue from the amortization of deferred subscription and services revenue related to initial customer purchases was \$25.1 million and \$7.6 million for the years ended December 31, 2012 and 2011, respectively. Revenue from the amortization of deferred subscription and services revenue related to renewals was \$6.0 million and \$1.2 million for the years ended December 31, 2012 and 2011, respectively. Our renewal rate for subscription and services agreements that expired in 2012 and 2011 was in excess of 90%.



## Cost of Revenue and Gross Margin

	Year Ended December 31,		Gross Margin	Change
	2012	2011		
	Amount	Amount	Gross Margin	Amount
(Dollars in thousands)				
Cost of revenue:				
Product	\$14,467	\$5,690		\$8,777
Subscription and services	3,163	1,590		1,573
Total cost of revenue	\$17,630	\$7,280		\$10,350
Gross margin:				
Product			72 %	77 %
Subscription and services			90 %	82 %
Total gross margin			79 %	78 %

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

## Operating Expenses

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

## Research and Development

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

## Sales and Marketing

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



## General and Administrative

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

## Interest Income

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

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

## Interest Expense

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

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

## Other Expense, Net

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

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

## Provision for (Benefit from) Income Taxes

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

The increase in provision for (benefit from) income taxes during the year ended December 31, 2012 compared to the year ended December 31, 2011 was primarily due to a reduction in the valuation allowance resulting from recording a

deferred tax liability on acquisition related intangibles for which no tax benefit will be derived partially offset by an increase in pre-tax income related to international operations.

#### Quarterly Results of Operations

The following unaudited quarterly statements of operations data for each of the eight quarters in the period December 31, 2013 have been prepared on a basis consistent with our audited annual financial statements included in this Annual Report on Form 10-K and include, in our opinion, all normal recurring adjustments necessary for the fair presentation of the financial information contained in

58

---

Edgar Filing: FireEye, Inc. - Form 10-K

those statements. Our historical results are not necessarily indicative of the results that may be expected in the future. The following quarterly financial data should be read in conjunction with our audited financial statements and the related notes included in this Annual Report on Form 10-K.

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

#### Quarterly Revenue Trends

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

#### Quarterly Gross Margin Trends

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

increase in cost of subscription and services revenue relating to increased personnel costs in customer support.

#### Quarterly Expense Trends

Total operating expenses increased year-over-year for all periods presented primarily due to the addition of personnel in connection with the expansion of our business our continuous investment in system infrastructures required to manage our growth and develop and promote our products and services. Research and development expense increased sequentially over the periods as we increased our headcount to support continued investment in our future product and subscription and services offerings. Sales and marketing expense increased significantly in the three months ended December 31, 2011 compared to the three months ended September 30, 2011,

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

#### Liquidity and Capital Resources

	As of December 31, 2013	As of December 31, 2012	
	(In thousands)		
Cash and cash equivalents	\$173,918	\$60,200	
	Year Ended		
	December 31,		
	2013	2012	2011
	(In thousands)		
Cash provided by (used in) operating activities	\$(69,762 )	\$21,500	\$5,111
Cash used in investing activities	(148,469 )	(20,215 )	(5,224 )
Cash provided by financing activities	331,949	48,239	3,124
Net increase in cash and cash equivalents			