FireEye, Inc.
Form 10-K
February 26, 2016

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

FORM 10-K

(Mark One)
x ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended December 31, 2015

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	20-1548921
(State or other jurisdiction of incorporation or organization)	(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 x No ¨

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 x

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 x 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 x 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	x	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 x

As of June 30, 2015, the last business day of the registrant’s most recently completed second fiscal quarter, the aggregate market value of the registrant’s common stock held by non-affiliates was approximately $7.0 billion, based on the closing price of such stock reported for such date on The NASDAQ Global Select Market. This calculation does not reflect a determination that persons are affiliates for any other purposes.

The number of outstanding shares of the registrant’s common stock was 165,949,541 as of February 24, 2016.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant’s Proxy Statement for the 2016 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, 2015 are incorporated by reference into Part III of this Annual Report on Form 10-K.

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,” “i “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 and to expand our solutions footprint within each of these customers;
- our expectations concerning renewal rates for subscriptions and services by existing customers, including our expectation that revenue from such renewals will increase as a percentage of our total revenue from subscriptions and services;
- 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 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 generate cash flows from operations and free cash flows;
- our ability to capture new, and renew existing, contracts with the United States and international governments;
- 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;
- 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 cybersecurity solution for detecting, preventing, analyzing and resolving today's advanced cyber-attacks that evade legacy signature-based security products. Our cybersecurity solutions combine our purpose-built virtual-machine technology, threat intelligence, and advanced security expertise in a suite of products and services that reduces our customers' exposure to attacks by enabling accurate detection and rapid response. Our proprietary virtual machine-based technology delivers high efficacy detection and prevention, while also scaling in response to ever-increasing network performance requirements, to provide real-time protection to enterprises and governments worldwide. Our analysis and forensic solutions, threat intelligence subscriptions, managed services, compromise assessments, incident response and consulting services complement our threat prevention products to help organizations adapt their security profile as threats evolve. This adaptive approach to cybersecurity represents a paradigm shift in how IT security has been conducted since the earliest days of the information technology industry. We believe it is imperative for organizations to invest in this new approach to protect their critical assets from the global pandemic of cybercrime, hacktivism, cyber espionage and cyber warfare.

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 modern attacks are built on dynamic, stealthy and targeted malware that penetrates defenses in multiple stages and through multiple entry points of an IT network. These highly targeted, "single-use" cyber-attacks easily circumvent security solutions that rely on pattern-matching detection technologies. Additionally, because legacy solutions reference outdated signatures of past threats, they also generate a high number of false-positive alerts.

To address the shortcomings of signature-based security solutions, we developed a new threat prevention platform based on our purpose-built, virtual machine-based detection engine, MVX. Our comprehensive platform combines our MVX virtual execution engine and our cloud-based threat intelligence network to identify previously unknown threats and protect organizations at all stages of the attack lifecycle and across all primary threat vectors, including Web, email, file, endpoint and mobile.

Our over ten years of research and development in proprietary virtual machine technology, anomaly detection and associated heuristic, or experience-based, algorithms enables MVX to provide real-time, dynamic threat protection without the use of signatures while delivering high efficacy and network performance. Our MVX engine detonates, or "runs," Web objects, executable code, suspicious attachments and files within virtual environments to detect and block the full array of modern 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 correlated with other FireEye products within the organization through our management platform and 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, a leading provider of advanced endpoint security products and professional service solutions. FireEye and Mandiant have been strategic partners with integrated product offerings since April 2012. We believe the combination of the two companies created 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, analyzing and resolving advanced cybersecurity threats across four distinct disciplines:

- First, Mandiant provided endpoint-based threat detection, forensic and response solutions, and we have continued to develop Mandiant's endpoint technology as part of our comprehensive security platform. The integration of threat intelligence from our endpoint products with our web, email, file and mobile platforms increases security teams' visibility into attacks and enables 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 and threat actors, which is continually gathered from ongoing monitoring of more than six million endpoints and through compromise assessments, 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 ten million virtual machines every hour, 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. This role as first responder to high profile breaches fosters a trusted advisor relationship with organizations and enables long term strategic relationships.

- Fourth, Mandiant brought 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, and was the basis for our FireEye-as-a-Service advanced security-as-a-service offering.

Our cybersecurity platform includes a family of software-based appliances, endpoint agents, cloud-based subscription services, support and maintenance, and professional consulting services. Our principal threat prevention appliance families address critical vectors of attack: Web, email, file, endpoint and mobile. We also offer a cloud-based email threat prevention solution that can be deployed either standalone or in conjunction with our appliance-based email solution. 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 cross-correlate intelligence regarding threats detected at the local implementation level with other FireEye appliances deployed across the organization to block multi-vector attacks and the exfiltration of critical data.

We maintain the efficacy of our solution by distributing our global threat intelligence through our DTI cloud. We also offer a cloud-based threat analysis platform that allows IT security analysts to analyze and prioritize attack alerts from security devices utilizing our repository of dynamic and contextual threat intelligence.

We also provide a family of forensic and analysis appliances and agents to enable investigation and remediation of breaches. Our endpoint forensics solution enables rapid identification and remediation of attacks that have penetrated an organization's defenses and are residing on an organization's endpoints, such as desktop computers, laptops or mobile devices. Our network forensics solution pairs high performance packet capture of network data with analysis tools to aid investigation efforts. We also offer a malware 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 both incident response services to assist our customers who have been breached and compromise assessments, security program assessments and consulting services to help customers build and maintain their security programs. Additionally, we offer our FireEye-as-a-Service subscription services for management of FireEye devices and comprehensive monitoring of attacks based on our threat intelligence and security expertise.

Our sales model consists of direct and inside sales teams 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, compromise assessment and security program assessment 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, 2015, we had over 4,400 end-customers, including more than 680, or approximately 34%, of the Forbes Global 2000. 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 2015, 2014 and 2013, our revenue was $623.0 million, $425.7 million and $161.6 million, respectively, representing year-over-year growth of 46% for 2015, 163% for 2014 and 94% for 2013, and our net losses were $539.2 million, $443.8 million and $120.6 million, respectively.

We primarily market and sell our intelligence-led security platform to enterprise companies in a broad range of industries and to national, regional and local governments worldwide. Our business is geographically diversified, with 70% of our total revenue from the United States, 13% from Europe, the Middle East, and Africa (EMEA), 12% from Asia Pacific and Japan (APAC), and 5% from other regions in 2015. See Note 16 contained in "Notes to Consolidated Financial Statements" in Item 8 of Part II of this Annual Report on Form 10-K for more information about customers and revenue and assets by geographic region.

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. 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 Reports 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 Annual Report on Form 10-K.

Our Products, Subscriptions and Services

Products

- Threat Prevention Platform. Our Threat Prevention Platform consists of vector-specific appliance and cloud-based solutions that provide comprehensive advanced threat protection, from network to endpoint, for both inbound and outbound network traffic that may contain sensitive information. Our portfolio of Threat Prevention solutions includes the following appliances covering the Web, email, endpoint, file and mobile threat vectors:
- Network Threat Prevention Platform (NX Series). Our Network Security NX Series appliances scale from 10 Mbps to multiple gigabits of throughput and are deployed in-line at enterprise Internet access points to analyze all web traffic. Utilizing our MVX engine, these appliances identify and block cyber threats deeply embedded inside web traffic, create real-time protection descriptors with the identification of new 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. Using our MVX engine, our Network Security platform confirms zero-day attacks, generates real-time security intelligence and captures dynamic callback destinations to defend against attacks. 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. 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. In June 2014, we added intrusion prevention systems functionality (IPS) to our Network Threat Prevention Platform to allow organizations to consolidate advanced threat prevention with traditional signature-based network security. This allows an organization to optimize security spending, reduce false positives to illuminate actual attacks, and enable compliance. In September 2014, we introduced the NX 7500 with support for Windows and Mac OSX on the same appliance. In February 2015, we introduced the NX 4400 to bridge performance requirements from 1 gigabit to multiple gigabits, and in October 2015, we added decryption capabilities to enable visibility into encrypted network traffic.
- Email Threat Prevention Platform (EX Series and ETP). Our Email Threat Prevention appliances (EX series) and cloud-based solutions (ETP) detect and stop advanced attacks that exploit unknown operating system, browser, and application vulnerabilities as well as malicious code and attachments included in emails. Using our MVX engine, both the appliance and cloud-based solutions analyze email content as well as email attachments, including all common file and archive formats. In particular, our Email Threat Prevention solutions secure networks against spear phishing emails, which bypass traditional anti-spam and reputation-based technologies. Spear phishing attacks use individually targeted content to trick users into clicking on a malicious link or opening a document, and are frequently used by cybercriminals to extract sensitive information such as user IDs and passwords. Our MVX engine actively executes, and is able to quickly identify, links to compromised websites and malicious attachments and blocks spear-phishing emails.
- Endpoint Threat Prevention Platform (HX Series). Our Endpoint Threat Prevention Platform is an appliance and endpoint agent system that equips security organizations to detect, analyze and resolve security incidents on desktops, laptops and other end-user devices using the threat detection algorithms of the MVX engine. Threat intelligence and alerts are correlated between our Network Threat Prevention and Endpoint Threat Prevention platforms to provide visibility across an organization and enable rapid containment. Additionally, the HX agent collects forensic data necessary for investigation and analysis of attacks. Our Endpoint Threat Prevention can be configured to sweep for indicators of compromise at regular intervals to identify new attacks and compromised devices and is a component of our FireEye-as-a-Service offering. In November 2015, we introduced HX Endpoint 3.0 with enterprise search and live response, enabling organizations to rapidly search for new threats across as many as 100,000 endpoints.
- File Content Security (FX Series). Our FX Series appliances analyze network file servers to detect and quarantine malicious software brought into the network through technologies that bypass traditional security solutions, such as online file sharing and associated collaboration tools. 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 FX Series appliances perform recursive, scheduled, and on-demand scanning of accessible network file servers to continuously identify and quarantine resident threats.

Mobile Threat Prevention (MX Series). Our Mobile Threat Prevention product allows organizations to identify malicious mobile apps and assess risk levels for other apps for Android and Apple devices. Using our MVX technology, we have threat intelligence from more than nine million mobile applications and assigned security and privacy risk levels for each. Our Mobile Threat Prevention platform includes a downloadable app and a management solution that can integrate with a number of the major mobile device management solutions. The management solution is available as an on-premise appliance or a cloud-based solution.

- Security Management Products

Central Management System. Our Central Management System, or CMS, unifies reporting, configuration, and threat intelligence sharing and manages the overall deployment of the components of our Threat Prevention Platform. CMS appliances distribute threat intelligence from the DTI cloud and provide cross-enterprise threat data correlation to identify and block blended attacks across multiple attack vectors. CMS consolidates the management and reporting of activities in a unified security dashboard to provide a real-time view of an organization's security profile. Customers generally purchase this appliance when they need to manage multiple FireEye appliances.

- Security Analysis Products

Threat Analytics Platform (TAP). Our Threat Analytics Platform, or TAP, is a cloud-based solution that enables security teams to identify and effectively respond to cyber threats by correlating enterprise-generated security event data from any security product with real-time threat intelligence from FireEye. The platform is designed to scale by keeping as much data online and searchable as business needs demand. Search results can be exported from the user interface for use in other incident response management tools as needed.

Malware Analysis System (AX Series). Our AX Series of appliances provide a secure environment to test, replay, characterize and document advanced malicious activities by allowing security teams to manually execute and inspect advanced malware, zero-day, and other advanced cyber-attacks embedded in files, email attachments, and Web objects. Using our MVX engine, AX 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. 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.

- Security Forensics Products

Network Forensics Platform (PX Series). Our Network Forensics Platform appliances complement our Threat Prevention Platform by capturing and indexing full packets at extremely rapid speeds to allow organizations to investigate and resolve security incidents. Using our Network Forensics Platform in conjunction with our Threat Prevention Platform, security analysts can detect threats and view specific packets and sessions before, during, and after the attack to confirm what may have triggered a malware download or callback. This information can be used for rapid response and to develop future protective strategies.

Investigation Analysis System (AI Series). Our Investigative Analysis System provides a centralized, easy-to-use analytical interface to the Network Forensics Platform to provide data visualization and in-depth analytics to security analysts in a single centralized dashboard. Our Investigation Analysis System supports a number of configurations for single node and distributed architectures to optimize bandwidth and performance of metadata aggregation, queries, and analytics.

- Mandiant Intelligent Response (MIR). The MIR endpoint forensics product enables remote investigation of endpoints and allows security teams to collect targeted forensic data for identification of attacker behavior, tools and techniques.

Subscription and Services

- Product Subscriptions
- Threat Intelligence Subscriptions

Dynamic Threat Intelligence Cloud (DTI). Our Dynamic Threat Intelligence, or DTI, cloud interconnects FireEye appliances deployed within customer networks, technology partner networks, and service providers around the world to gather and share real-time threat intelligence. Our DTI cloud is a bi-directional system that collects threat intelligence from our appliances, our global threat gathering network and our security labs, and distributes updated intelligence throughout our installed base of customers to provide real-time detection of advanced attacks. The network effects of a globally distributed, automated threat analysis network improve the efficacy of our Threat

Prevention Platform and differentiate our security solutions. Customers are required to purchase either a one or three year subscription to our DTI cloud as part of their initial appliance purchase.

Advanced Threat Intelligence (ATI). Our Advanced Threat Intelligence augments our Dynamic Threat Intelligence with contextual information on threats and threat actors, including information on the identity of the attacker, likely motives, and details on attack patterns. This information can be used to search for additional compromises and enhance protective measures to prevent future attacks. ATI is an optional upgrade to our DTI Cloud subscription.
Advanced Threat Intelligence Plus (ATI+). ATI+ adds comprehensive dossiers, trends, news, and analysis on advanced cyber threat groups as well as profiles of targeted industries and information about the types of data threat groups are targeting. It also includes community threat sharing, which allows organizations to share threat intelligence with trusted partners to develop personalized community cyber defenses. Customers at this level can also benefit from our 24/7/365 critical alert and detection efficacy monitoring.
Email Threat Prevention Attachment/URL Engine. Our Email Threat Prevention Attachment/URL engine analyzes email attachments and URLs embedded in emails for threats. Customers who purchase the Email Threat Prevention appliance are also required to purchase one or three year subscriptions to our DTI cloud and the Email Threat Prevention Attachment/URL engine.
Email Threat Prevention Cloud (ETP). Our cloud-based Email Threat Prevention solution (ETP) is a software-as-a-service (SaaS) offering that protects cloud-based mailboxes from advanced threats using our MVX engine and provides anti-spam and anti-virus protection. ETP can be used to complement and extend our FireEye EX Series appliances, whereby the incoming emails are analyzed and quarantined by the anti-spam, anti-virus engine in the cloud to thwart known threats while the on-premise EX Series combats the advanced unknown threats and zero-day attacks. Subscriptions to the DTI cloud and Email Threat Prevention Attachment/URL engine are included in the per mailbox price of ETP.
Mobile Threat Prevention (MTP). Our Mobile Threat Prevention solution uses the MVX engine to analyze a combination of semantic, dynamic, and behavioral characteristics to provide a comprehensive risk assessment of mobile applications for Apple iOS and Android devices, and includes an MTP App, MTP Management and MTP Analysis. The MTP App is a lightweight mobile app that alerts mobile users to threats, communicates with the MTP Management appliance to display the threat scores of mobile apps, details malicious or unwanted behavior within each app, and examines factors associated with endpoint device compromise. MTP Management is a hybrid cloud offering that works with the MTP App to enable an enterprise-wide view into mobile device compromise and a customizable enforcement option. MTP Analysis is a standalone subscription that provides for deeper on-demand app forensics and analysis by security analysts.

- Security-as-a-Service Offerings

FireEye-as-a-Service. Our FireEye-as-a-Service offering includes our Network Security Platform and our Endpoint Security Platform solutions, managed by our security experts through our security operations centers around the world. Using automated techniques and our advanced threat intelligence, our analysts monitor and analyze network traffic, regularly sweep enterprise endpoints for new malware, and actively hunt for new attacks and adversaries. Customers receive detailed analyses of threats with the context necessary to assess risk and prioritize action, as well as recommendations for containment and response.

- Customer Support and Consulting Services

Incident response, compromise assessments and related consulting services. We have a team of cybersecurity experts to quickly respond to customers that have experienced a breach and help them understand the scope of the incident and quickly remediate the attack. Our cybersecurity 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 security investigations across all industries, organization sizes and technical environments. As part of our services, we can help customers scope their own security programs, provide litigation support and forensic analysis. Our cybersecurity experts also perform compromise assessments to analyze network, endpoint and log data to identify indications of present or historical attacker activity. These consulting services are marketed under the Mandiant brand.

- Training and professional services. We offer training services to our customers and channel partners through our training department and authorized training partners. These services are designed to provide education regarding implementation, use and functionality, and maintenance and support of our products. We also provide training on

managing the stages of our sales cycle for our channel partners. We offer professional services to customers for large implementations where expert technical resources are required. We provide professional services both directly to our customers, and indirectly through our authorized partners, who provide similar services to the end-customer.

- 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 to help customers solve technical challenges that they may encounter. In addition to post-sales support activities, our support organization works with our product management and engineering teams 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. We offer multiple appliance models, each with various features and capabilities. All our appliance products require subscriptions to threat intelligence and support, which are typically priced as a percentage of the appliance price in one or three year subscriptions. FireEye-as-a-Service and cloud-based offerings are offered in one or three year subscriptions and are typically priced based on appropriate use metrics. We typically invoice customers for the full term of the subscription up front.

For contributions to total revenue by significant class of revenues, see "Management's Discussion and Analysis of Financial Condition and Results of Operations" included in Part II, Item 7 of this Annual Report on Form 10-K.

Our Technology

Our MVX multi-vector execution engine has been built from the ground up to address today's modern threats, and is the key threat detection technology underlying our platform and threat intelligence network. Our foundational technologies in the MVX engine are: (i) line rate anomaly detection, (ii) proprietary virtual execution, (iii) exploit stage monitoring, (iv) cross correlation, (v) evolved network security architecture, and (vi) advanced endpoint validation and containment. We have built our technology over 10 years of research and development, and we believe it represents a significant competitive advantage for us. In 2015, we completed a multi-year effort to re-architect the MVX engine that increased overall analysis speed by three-fold and increased detection capacity by five-fold.

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 rapidly and accurately filtering potentially suspicious data from benign traffic, using algorithms based on real-time threat intelligence delivered through our DTI cloud. This filtering allows benign traffic to pass through and forwards suspicious traffic to the MVX detonation chamber to be executed in the target environment. While our virtual machine can process all traffic, using an anomaly detector helps 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 addition to updates from MVX, our anomaly detector also receives updates from our DTI cloud in the attributes, or markers, it looks for when inspecting potentially suspicious data based on our global threat intelligence network. Our line rate anomaly detector minimizes missed attacks (false negatives) by aggressively categorizing traffic as suspicious. 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 Virtual Execution. 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 technology, 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 rapid modifications to the code base of our virtual execution engine as attackers develop new evasion techniques, which our competitors are not able to do. Our virtual execution engine is capable of mimicking thousands of combinations of operating systems and user configurations, including several popular operating systems, applications and Web browsers. Once suspicious software code identified by the custom anomaly detector is loaded into the target environment, our MVX engine monitors the software’s behavior. Using a proprietary behavior analysis technology, MVX determines if the actions the code is taking in the virtual environment are malicious or benign. We have developed our MVX engine over the past 10 years to provide high performance threat protection through high 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 through a vulnerability in the software. The exploit object can be embedded in any piece of content, such as an ordinary Web page. This stage of the attack is invisible to network security technologies that are focused on examining files and executables once they are written to the hard drive on a host computer. Today's threats often encrypt the malware file they download, making detection impossible unless the attack has been monitored at the exploit phase. We are able to detect new exploits by running suspicious software through our MVX virtual execution engine. Additionally, MVX collects the encryption key necessary to properly execute the subsequent malware in a virtual environment.

Multi-Vector Cross Correlation. Our appliances, when deployed with the CMS appliance, communicate threat information between appliances in real-time as well as receive updates from our DTI cloud. This awareness allows our appliances, which are specific to threat vectors, to prevent sophisticated multi-vector threats, particularly blended attacks. This cross-fertilization of attack information enables our appliances to piece together separate and seemingly benign components to identify and block a blended or multi-vector attack.

Evolved Network Security Architecture. Our solutions are designed to operate as part of a comprehensive architecture to defend networks against today's advanced 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, which do not have visibility into the traffic sources today's advanced threats utilize during attacks.

Advanced Endpoint Validation and Containment. Our Endpoint Threat Prevention System is a hybrid appliance and endpoint agent-based solution that enables real-time, automated validation and investigation of security incidents across thousands of endpoints. Our Endpoint Threat Prevention technology 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 security analysts can confirm the scope of the attack, identify and contain all compromised hosts, and quickly secure their networks from further attack.

The Endpoint Threat Prevention Platform also enables security operations teams to correlate network and endpoint attack activity and threat intelligence. Organizations can automatically investigate alerts generated by other FireEye Threat Prevention Platforms, log management and network security products, apply proprietary intelligence from FireEye, or sweep for IOCs, to identify the devices that have been compromised and contain compromised endpoints with a single click using our Agent Anywhere technology. Our endpoint validation and containment technologies include:

- Automatic creation of indicators of compromise coupled with rapid enterprise-wide search. Security teams are able to generate search parameters based on new threat intelligence, query tens or hundreds of thousands of endpoints to identify critical issues, and contain compromised hosts in a matter of minutes.
- Agent Anywhere. Investigate any endpoint event even when the device is disconnected from the network.
- Unified endpoint dashboard. In addition, our Endpoint Threat Prevention platform provides a unified dashboard that allows administrators to view malicious activity both on conventional endpoints like PCs as well as mobile devices.

Customers

Our customer base has grown from approximately 450 end-customers at the end of 2011 to over 4,400 end-customers as of December 31, 2015, including 680 of the Forbes Global 2000. We provide products, subscriptions and services 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, healthcare and pharmaceutical 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, 2015, 2014 or 2013. For the years ended December 31, 2015, 2014 and 2013, one reseller represented 13%, 11% and 11%, respectively, of our total revenue. For the year ended December 31, 2013, another reseller also represented 11% of our total revenue. For the year ended December 31, 2015, one distributor represented 17% of our total revenue. No distributor represented 10% or greater of our total revenue for the years ended December 31, 2014 and 2013.

Backlog

Orders for subscriptions and services for multiple years are typically billed in their entirety shortly after receipt of the order and are included in deferred revenue. The timing of revenue recognition for subscriptions and 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. The majority of our product revenue comes from orders that are received and shipped in the same quarter. 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 the fulfillment of such orders may be delayed.

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 and can last multiple months, although some transactions can close in a few weeks when an active breach is discovered.

We also have a dedicated team focused on channel sales who manage the relationships with our value-added reseller and distributor partners and work with these channel partners in winning and supporting customers. We believe this direct-touch sales approach allows us to leverage the benefits of broader market coverage provided by a reseller channel as well as maintain a face-to-face connection with our customers, including key enterprise accounts.

We have also cultivated alliances with non-traditional partners to generate customer referrals and extend our technologies and sales coverage to new segments. These relationships include relationships with insurance providers, large systems integrators and managed service providers, and we have engaged in joint solution development with leading providers of engineering services and payment systems.

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.

As part of our sales strategy, we often provide prospective customers with our products for a short-term evaluation period. In such cases, 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 three years, and we often discover incidents of next-generation threats 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 at a lower total cost of ownership compared to many other security solutions.

Marketing. Our marketing is focused on building our brand reputation and market awareness for 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, product launch activities, 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 threat reports.

Technology Alliance Partners

FireEye has built a robust ecosystem of Technology Alliance Partners who, through integration and joint go-to-market efforts, extend the breadth and depth of cybersecurity and protection customers gain from FireEye. Spanning multiple technology categories, including network monitoring vendors, security information and event management vendors, network equipment vendors, forensic software vendors and web application firewall vendors, these partnerships provide for threat intelligence sharing, cross-vendor integrations, and joint solution development. By helping to ease the complications that organizations face when implementing multi-layered security solutions, our technology alliances facilitate integrated solution design, accelerate the time to realize value, and enhance our role as a strategic security partner.

Government Affairs

We maintain relationships with several governments around the globe. Our thought leadership in defending 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, help define best practices in various jurisdictions and help organizations of all sizes better understand the cyber threat landscape. We also help governments identify future needs and requirements. 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. Through these and related activities, we engage on the front lines of emerging cybersecurity related public policy and use our knowledge and insight to improve the cybersecurity of our government and industry customers.

Manufacturing

The manufacturing of our security products is outsourced to principally one 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 had an initial term of one year and automatically renews 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 to our products and improve our core technologies. We believe that hardware, software and cloud-based technologies are critical to expanding our leadership in the security industry. Our engineering teams have deep networking and security expertise and work closely with our customers to identify their current and future needs. Additionally, our Mandiant consultants use our products in their incident response and compromise assessment engagements and provide continual feedback to our engineering teams on product performance, detection efficacy, evasion techniques and attack trends.

In addition to our focus on platform expansion and enhancement, our research and development teams are focused on developing automation tools and machine learning techniques to reduce the time to discover and distribute new threat intelligence, as well as generate efficiencies in our services offerings. We are also investing in security platform management capabilities to provide unified reporting and security orchestration features to customers in a single dashboard.

We maintain research and development activities across the globe with teams located in Germany, India, Ireland, Japan, Singapore and the United States.

Research and development expense totaled $279.5 million, $203.2 million and $66.0 million for the years ended December 31, 2015, 2014 and 2013, respectively.

Competition

We operate in the intensely competitive IT security market which is characterized by constant change and innovation. Changes in the threat landscape and broader IT infrastructures result in evolving customer requirements for security. Several vendors have either introduced new products or incorporated new features into existing products that compete with our solutions. Our current and potential future competitors fall into six general categories:

- large networking vendors such as Cisco and Juniper that may emulate or integrate features similar to ours into their own products;
- large companies such as Intel, IBM and HPE 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 Palo Alto Networks and Trend Micro that offer products that claim to perform similar functions to our platform;
- small and large companies, including new entrants, 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 and compromise assessment services.

As our market grows and IT budgets are allocated to support protection from advanced threats, 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 deliver the combination of technology, intelligence and expertise necessary to combat the current threat landscape;
- ability to detect current threats by overcoming the limitations of signature-based approaches, while maintaining a low rate of false-positive alerts;
- scalability, throughput and overall performance of the virtual machine technology;

- visibility into all stages of an attack, especially the exploit phase;
- breadth and richness of the shared threat intelligence, including threat intelligence on cyber crime, cyber espionage, hacktivism, attacks on critical infrastructure and nation-state attacks;

- flexible deployment options, including on-premise appliances, software in the cloud, or a hybrid of both;
- brand awareness and reputation;
- strength of sales and marketing efforts;
- product extensibility and ability to integrate with other technologies in the network infrastructure;
- ease of use;
- price and total cost of ownership; and
- ability to provide an orchestrated solution of products and services for detecting, preventing and resolving advanced cybersecurity threats across multiple attack vectors.

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 network infrastructures, the breadth of our services and solution offerings 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 file patent applications to protect our intellectual property and believe that the duration of our issued patents is sufficient when considering the expected lives of our products. 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.

Business Seasonality

For discussion of seasonal trends, see our quarterly results of operations discussion within "Management's Discussion and Analysis of Financial Condition and Results of Operations" included in Part II, Item 7 of this Annual Report on Form 10-K.

Employees

As of December 31, 2015, we had approximately 3,100 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 223,000 square feet of space for our corporate headquarters in Milpitas, California under lease agreements that expire during the year ended December 31, 2018. We maintain additional offices throughout the United States and various international locations including, Australia, Dubai, Germany, India, Ireland, Japan, Singapore 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

The information set forth under "Litigation" in Note 9 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 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.

Our future success depends on market adoption of our unique approach to IT security. 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, 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, especially if competitor offerings are free or available at a lower cost.

In addition, changes in customer requirements could reduce customer demand for our virtual machine-based security solutions. For example, if customers were to reduce their number of web egress points in order to reduce their cyber attack surface, they would not need to purchase as many of our Network Threat Prevention appliances, which currently account for the largest portion of our threat prevention product revenue. Similarly, if one or more governments share, on a free or nearly free basis, threat intelligence with other governmental agencies or organizations, such as critical infrastructure companies, then those agencies or organizations might have less demand for additional threat intelligence and may purchase less of our threat intelligence offerings.

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

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

Our headcount increased from approximately 2,500 employees as of December 31, 2014 to approximately 3,100 employees as of December 31, 2015. We expect our headcount to continue to grow rapidly. In addition, our number of end-customers increased from approximately 3,100 to over 4,400 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 continue to enhance our enterprise resource planning system, including revenue recognition and management software, and implement and enhance additional systems and controls. There

is no assurance that we will be able to successfully scale improvements to our enterprise resource planning system or implement or scale improvements to our other systems, processes and controls in a manner that keeps pace with our growth or that such systems, processes and controls 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.

Many of our expenses are relatively fixed, at least in the short term. If our projections or assumptions on which we base our projections are incorrect, we may not be able to adjust our expenses rapidly enough to avoid an adverse impact on our profitability or cash flows.

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;
- continuing to refine our ability to forecast our bookings, billings, revenues, expenses and cash flows;
- 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 and testing 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.

Real or perceived defects, errors or vulnerabilities in our products or services, the misconfiguration of our products, the failure of our products or services to block malware or prevent a security breach, or the failure of customers to take action on attacks identified by our products could harm our reputation and adversely impact our business, financial position and results of operations.

Because our products and services are complex, they have contained and may contain design or manufacturing defects or errors that are not detected until after their deployment. Our products also provide our customers with the ability to customize a multitude of settings, and it is possible that a customer could misconfigure our products or otherwise fail to configure our products in an optimal manner. Such defects and misconfigurations of our products could cause our products or services to be vulnerable to security attacks, cause them to fail to secure networks and detect and block threats, 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 products and services are unable to detect or prevent. Moreover, as our products and services are 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 products and services. If this happens, our networks, products, services and subscriptions could be targeted by attacks specifically designed to disrupt our business and undermine the perception that our products and services are 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. Any breach or perceived security

breaches of our network could materially and adversely affect our business, financial condition and results of operations.

If any of our customers becomes infected with malware after using our products or services, such customer could be disappointed with our products and services, regardless of whether our products or services blocked the theft of any of such customer's data or would have blocked such theft if configured properly. Similarly, if our products detect attacks against a customer but the customer has not permitted our products to block the theft of customer data, customers and the public may erroneously believe that our products were not effective. For any security breaches against customers that use our services, such as customers that have hired us to monitor their networks and endpoints through our own or our co-branded security operation centers, breaches against those customers may result in customers and the public believing that our products and services failed. Furthermore, if any enterprises or governments that are publicly known to use our products or services 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 products and services. 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 products and services 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 products and services 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. In addition, from time to time, firms test our products against other security products. Our products may fail to detect or prevent threats in any particular test for a number of reasons, including misconfiguration. To the extent potential customers, industry analysts or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our products or services 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. In addition, in the event that a customer suffers a cyber attack, we could be subject to claims based on a misunderstanding of the scope of our contractual warranties or the protection afforded by the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, or the SAFETY Act.

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

- a loss of existing or potential customers or channel partners;
- delayed or lost revenue and harm to our financial condition and results of operations;
- a 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.

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, including, but not limited to our GAAP and non-GAAP measures, 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 new and retain existing customers;
- changes in our mix of products, subscriptions and services sold;
- 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;

18

- 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 relationships with channel partners;
- 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, including, without limitation, the purported stockholder lawsuits described under the "Litigation" subheading in Note 9 Commitments and Contingencies contained in the "Notes to Consolidated Financial Statements" in Item 8 of Part II of this Annual Report on Form 10-K;
- seasonality in our business;
- general economic conditions, both domestic and in our foreign markets;
- future accounting pronouncements or changes in our accounting policies or practices;
- the amount and timing of operating costs and capital expenditures related to the expansion of our business; and
- increases or decreases in our revenues and 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. For example, as we offer more and more solutions through subscriptions and services, it becomes increasingly difficult for us to predict whether customers will purchase our solutions as a product, a subscription or a service. If customers purchase our solutions through subscriptions and services that have less profit associated with them than our products, our operating results could be harmed. Changes in the mix of offerings sold impacts the timing of recognition of revenue for our sales. Consequently, given the different revenue recognition policies associated with sales of our products, subscriptions and services, customers purchasing more of our subscription and services offerings and less of our product offerings than we anticipated could result in our actual revenue falling below our publicly announced guidance or the expectations of securities analysts and investors, resulting in a decline in our stock price.

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.

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 acquisition of Mandiant Corporation, or Mandiant, our acquisition of nPulse Technologies, or nPulse, our acquisition of iSIGHT Security, Inc. (d/b/a iSIGHT Partners, Inc.), or iSIGHT, and our acquisition of Invotas International Corporation, or Invotas. 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 acquisitions of Mandiant, nPulse, iSIGHT and Invotas, include:

- diversion of management time and focus from operating our business to addressing acquisition integration challenges;
- coordination of research and development and sales and marketing functions;
- integration of product and service offerings;
- retention of key employees from the acquired company;
- changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisition;

- cultural challenges associated with integrating employees from the acquired company into our organization;
- integration of the acquired company's accounting, management information, human resources and other administrative systems;

- the need to implement or improve controls, procedures, and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;
- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we don't adequately address and that cause our reported results to be incorrect;
- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities;
- unanticipated write-offs or charges; and
- litigation or other claims in connection with the acquired company, including claims from terminated employees, customers, former stockholders or other third parties.

Our failure to address these risks or other problems encountered in connection with our past or future acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally. Future acquisitions could also result in dilutive issuances of equity securities. For example, in December 2013, we 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. In May 2014, we issued 295,681 shares of common stock and assumed options to purchase 63,490 shares of common stock in connection with our acquisition of nPulse. In January 2016, we issued 1,793,305 shares of common stock in connection with our acquisition of iSIGHT, to be distributed to certain former stockholders of iSIGHT upon the achievement of a threat intelligence bookings target. In February 2016, we issued 742,026 shares of common stock in connection with our acquisition of Invotas. 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.

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 $539.2 million, $443.8 million and $120.6 million during the years ended December 31, 2015, 2014 and 2013, respectively. We expect our operating expenses to increase in the future as we expand our sales and marketing efforts and continue to invest in research and development of our technologies. These efforts may be more costly than we expect, and we may not be able to increase our revenue to offset our increased operating expenses. Our revenue growth may slow or our revenue may decline for a number of other reasons, including reduced demand for our platform, increased competition, a decrease in the growth or size of the IT security market, particularly the market for solutions that target the next generation of advanced cyber attacks, or any failure to capitalize on growth opportunities. Any failure to increase our revenue as we grow our business could prevent us from achieving or, if achieved, 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.

In addition, we may have difficulty achieving profitability under U.S. GAAP, due to stock-based compensation, intangible amortization and other non-cash charges.

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 inventory purchases, contract manufacturer relationships and other costs and 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. 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, or EU, 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.

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 HPE 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 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 and compromise assessment 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.

Some of our competitors have made or could make acquisitions of businesses that allow them to offer more competitive and comprehensive solutions. As a result of such acquisitions, our current or potential competitors may be able to accelerate the adoption of new technologies that better address end-customer needs, devote greater resources to bring these products and services to market, initiate or withstand substantial price competition, or develop and expand their product and service offerings more quickly than we do. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, and loss of market share.

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.

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, including members for our board of directors, 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 acquisition of Mandiant, and recent additions to our Worldwide Sales management team. 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 or retaining qualified personnel to fulfill our current or future needs. We are also substantially dependent on the continued service of our existing engineering personnel because of the complexity of our platform. Our competitors

may be successful in recruiting and hiring members of our management team or other key employees, including key employees obtained through our acquisition of Mandiant or iSIGHT, 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 President, our Chief Financial Officer, our Senior Vice President of Worldwide Sales, our Senior Vice President of Engineering 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.

We expect our revenue growth rate to decline.

From the year ended December 31, 2010 to the year ended December 31, 2015, our revenue grew from $11.8 million to $623.0 million, which represents a compounded annual growth rate of approximately 121%. We expect that, to the extent our revenue increases to higher levels, our revenue growth rate will continue to decline. 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; and
- expansion of our professional services organization.

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.

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 shipped in 2008. Since then, we have continued to expand our platform, both organically and through acquisitions, including 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 makes 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.

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 (i) 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, and (ii) our sales compensation plans, which are typically structured around annual quotas and stair step commission rates. 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. 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.

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

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

If 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, for example, as a result of the recent cybersecurity agreement between China and the U.S., may reduce the demand from customers or prospects for our solutions, and therefore could increase our sales cycles and harm our business, results of operations and financial condition.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. As a result, our sales, billings 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 or in advance of those we anticipated, or have not

occurred at all. We are billing an increasing number of large deals and the loss or delay of one or more of these 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. Furthermore, some sales (such as product sales) generally result in immediate recognition of revenue, while other sales, such as product subscription sales, require the recognition of revenue over periods of one year or longer typically. As a result of these factors, it is difficult for us to forecast our revenue accurately in any quarter based on our internal forecasts of billings. 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.

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, general economic conditions, and our customers' satisfaction with our existing solutions they have previously purchased. 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, not grow at all, or even decline.

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 grow more slowly than expected, not grow at all, or even 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 and days 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, or our supply chain 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.

The IT security market has grown quickly and is expected to continue to evolve rapidly. Moreover, 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, the trend of "bring your own device" in enterprises, and the rapidly evolving Internet of Things ("IOT"), 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. 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 or other cloud-based products and services we offer or may offer 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. We also offer additional cloud-based platforms such as our Email Threat Prevention, Mobile Threat Prevention and Threat Analytics Platforms and provide security solutions through our own and our co-branded security operation centers.

Our customers depend on the continuous availability of our DTI and other cloud-based products and services. Our cloud-based products and services are 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. Our data centers 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 or, in the case of technical failures and downtime of security operation centers, all security threats.

In addition, 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 or other cloud-based products and services are unreliable.

In addition, we provide our cloud-based products and services through third-party data center hosting facilities located in the United States and other countries. While we control and have access to our servers and all of the components of our network that are located in our data centers, we do not control the operation of these facilities. The owners of the data center facilities have no obligation to renew their agreements with us on commercially reasonable terms, or at all. If we are unable to renew these agreements on commercially reasonable terms, or if one of our data center operators is acquired, we may be required to transfer our servers and other infrastructure to new data center facilities, and we may incur significant costs and possible service interruption in connection with doing so.

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, subscriptions and services through, or with the assistance of, 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 in training 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.

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.

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.

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 65%, 58% and 45% for the years ended December 31, 2015, 2014 and 2013, respectively. Sales of new or renewal subscription and service contracts may decline or fluctuate as a result of a number of factors, including customers' level of satisfaction with our products and subscriptions, the actual or perceived efficacy of our security solutions, 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 rate 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 decreases in the market acceptance of, or demand for, our subscriptions or services may not be immediately apparent from 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.

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 third-party manufacturers reduces our control over the manufacturing process and exposes us to risks, including reduced control over quality assurance, product costs, 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, our reliance on third-party manufacturers exposes us to the risk that certain minerals, known as “conflict minerals,” that are contained in our products have originated in the Democratic Republic of the Congo or an adjoining country. As a result of the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the SEC adopted disclosure requirements for public companies whose products contain conflict minerals that are necessary to the functionality or production of such products. We have incurred and expect to incur additional costs to comply with the disclosure requirements, including costs related to determining the source of the conflict minerals used in our products. Moreover, the implementation of these new requirements could adversely affect the sourcing, availability and pricing of materials used in the manufacture of our products to the extent that there may be only a limited number of suppliers offering “conflict free” minerals that can be used in our products. There can be no assurance that we will be able to obtain such minerals in sufficient quantities or at competitive prices. We may also encounter customers who require that all of the components of our products be certified as conflict free. If we are not able to meet customer requirements, such customers may choose to not purchase our products, which could impact our sales.

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 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 a suit by a non-practicing entity alleging, among other things, patent infringement, which is 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.

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 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 were to uncover improper or illegal activities; and
- governments may require certain products purchased by it 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, subscriptions and services, anticipation of the introduction of new products, subscriptions or services, 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, or the effective prices we realize in our reporting currency. 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, terrorist act, 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, inhibit adoption of our products by current and future customers, or adversely impact our ability to attract and retain workforce talent.

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 our publicly announced guidance or 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 our publicly announced guidance or 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, resellers and customers 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 additional 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. U.S. regulations surrounding our operating activities in foreign jurisdictions are not always consistent with, and at times are in contravention to, the local regulations or laws in such jurisdictions. Enforcement actions and sanctions could harm our business, reputation, 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, or market penetration of, 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 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 or tax regulations 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.

Further, the interpretation and application of foreign laws and regulations in many cases is uncertain, and our legal and regulatory obligations in foreign jurisdictions are subject to frequent and unexpected changes, including the potential for various regulatory or other governmental bodies to enact new or additional laws or regulations or to issue rulings that invalidate prior laws or regulations.

For example, with regard to transfers of personal data from our European customers and employees to the U.S., we have historically relied on compliance with the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks as agreed to by the U.S. Department of Commerce, and the EU and Switzerland, which established means for legitimizing the transfer of personal data by U.S. companies from the European Economic Area, or EEA, to the U.S. In a recent ruling by the EU Court of Justice in Case C-362/14 (Schrems v. Data Protection Commissioner), or the ECJ Ruling, the U.S.-EU Safe Harbor Framework was deemed an invalid method of compliance with restrictions under EU law regarding the transfer of personal data outside of the EEA. In light of the ECJ Ruling, we anticipate engaging in measures to legitimize our transfers of personal data from the EEA to the United States, and may find it necessary or desirable to make other changes to our personal data handling. We may be unsuccessful in establishing legitimate means for us to transfer such personal data from the EEA or otherwise responding to the ECJ Ruling, and we may experience reluctance or refusal by European customers to use our solutions due to potential risk exposure as a result of the ECJ Ruling. We and our customers may face a risk of enforcement actions taken by EU data protection authorities until the time, if any, that personal data transfers to us and by us from the EEA are legitimized under applicable EU data protection law.

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, strengthening of the U.S. dollar increases the real cost of our products, subscriptions and services to our customers outside of the United States, which could lead to delays in the purchase of our products and services and the lengthening of our sales cycle. If the U.S. dollar continues to strengthen, this 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 to or sell our products in international markets 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 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 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. In 2013, we completed the reorganization of our corporate structure and intercompany relationships to more closely align our corporate organization with the expansion of our

international business activities. Although we anticipate achieving a reduction in our overall effective tax rate in the future as a result of this reorganized 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 reorganized 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 reorganized 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 Our Convertible Senior Notes

We are leveraged financially, which could adversely affect our ability to adjust our business to respond to competitive pressures and to obtain sufficient funds to satisfy our future growth, business needs and development plans.

We have substantial existing indebtedness. In June 2015, we issued $920.0 million aggregate principal amount of convertible senior notes (the “convertible notes”).

The degree to which we are leveraged could have negative consequences, including, but not limited to, the following:

- we may be more vulnerable to economic downturns, less able to withstand competitive pressures and less flexible in responding to changing business and economic conditions;
- our ability to obtain additional financing in the future for working capital, capital expenditures, acquisitions, general corporate or other purposes may be limited
- a substantial portion of our cash flows from operations in the future may be required for the payment of the principal amount of our existing indebtedness when it becomes due; and
- we may elect to make cash payments upon any conversion of the convertible notes, which would reduce our cash on hand.

Our ability to meet our payment obligations under our convertible notes depends on our ability to generate significant cash flow in the future. This, to some extent, is subject to general economic, financial, competitive, legislative, and regulatory factors as well as other factors that are beyond our control. There can be no assurance that our business will generate cash flow from operations, or that additional capital will be available to us, in an amount sufficient to enable us to meet our debt payment obligations and to fund other liquidity needs. If we are unable to generate sufficient cash flow to service our debt obligations, we may need to refinance or restructure our debt, sell assets, reduce or delay capital investments, or seek to raise additional capital. If we were unable to implement

one or more of these alternatives, we may be unable to meet our debt payment obligations, which could have a material adverse effect on our business, results of operations, or financial condition.

The conditional conversion feature of the convertible notes, if triggered, may adversely affect our financial condition and operating results.

In the event the conditional conversion feature of the convertible notes is triggered, holders of such convertible notes will be entitled to convert their convertible notes at any time during specified periods at their option. If one or more holders elect to convert their convertible notes, unless we elect to satisfy our conversion obligation by delivering solely shares of our common stock (other than paying cash in lieu of delivering any fractional share), we would be required to settle a portion or all of our conversion obligation through the payment of cash, which could adversely affect our liquidity. In addition, even if holders do not elect to convert their convertible notes, we could be required under applicable accounting rules to reclassify all or a portion of the outstanding principal of the convertible notes as a current rather than long-term liability, which would result in a material reduction of our net working capital.

The accounting method for convertible debt securities that may be settled in cash, such as the convertible notes, is subject to changes that could have a material effect on our reported financial results.

In May 2008, the Financial Accounting Standards Board, which we refer to as FASB, issued FASB Staff Position No. APB 14-1, Accounting for Convertible Debt Instruments That May Be Settled in Cash Upon Conversion (Including Partial Cash Settlement), which has subsequently been codified as Accounting Standards Codification 470-20, Debt with Conversion and Other Options, which we refer to as ASC 470-20. Under ASC 470-20, an entity must separately account for the liability and equity components of the convertible debt instruments (such as the convertible notes) that may be settled entirely or partially in cash upon conversion in a manner that reflects the issuer's economic interest cost. The effect of ASC 470-20 on the accounting for the convertible notes is that the equity component is required to be included in the additional paid-in capital section of stockholders' equity on our consolidated balance sheet and the value of the equity component would be treated as original issue discount for purposes of accounting for the debt component of the convertible notes. As a result, we will be required to record a greater amount of non-cash interest expense in current periods presented as a result of the amortization of the discounted carrying value of the convertible notes to their face amount over the term of the convertible notes. We will report lower net income in our financial results because ASC 470-20 will require interest to include both the current period's amortization of the debt discount and the instrument's non-convertible coupon interest for the convertible notes, which could adversely affect our reported or future financial results and the trading price of our common stock.

In addition, under certain circumstances, convertible debt instruments (such as the convertible notes) that may be settled entirely or partly in cash are currently accounted for utilizing the treasury stock method, the effect of which is that any shares issuable upon conversion of the convertible notes are not included in the calculation of diluted earnings per share except to the extent that the conversion value of the convertible notes exceeds their principal amount. Under the treasury stock method, for diluted earnings per share purposes, the transaction is accounted for as if the number of shares of common stock that would be necessary to settle such excess, if we elected to settle such excess in shares, are issued. We cannot be sure that the accounting standards in the future will continue to permit the use of the treasury stock method. If we are unable to use the treasury stock method in accounting for the shares issuable upon conversion of the convertible notes, then our diluted earnings per share would be adversely affected.

Conversion of our convertible notes will dilute the ownership interest of existing stockholders and may depress the price of our common stock.

The conversion of some or all of our convertible notes will dilute the ownership interests of then-existing stockholders to the extent we deliver shares upon conversion of any of the convertible notes. Any sales in the public market of the common stock issuable upon such conversion could adversely affect prevailing market prices of our common stock. In addition, the existence of the convertible notes may encourage short selling by market participants because the conversion of the convertible notes could be used to satisfy short positions, or anticipated conversion of the convertible notes into shares of our common stock could depress the price of our common stock.

Risks Related to Ownership of Our Common Stock

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.

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. Furthermore, analysts and investors may develop and publish their own projections of our business, which may form a consensus about our future performance. Our business results may vary significantly from such guidance or that consensus 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 we make downward revisions of our previously announced guidance, or 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 price of our common stock has ranged from $11.35 to $97.35 through February 25, 2016, and the last reported sale price on February 25, 2016 was $15.78. 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 and/or growth 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 expectation 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; and
- 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. The price of our common stock has been highly volatile since our IPO in September 2013, and beginning in June 2014, several lawsuits alleging violations of securities laws were filed against us and

certain of our current and former directors and executive officers. This and any future 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 sales of our common stock by our executive officers and directors under Rule 10b5-1 plans, could adversely affect the market price of our common stock.

Sales of a substantial number of shares of our common stock in the public market, or the perception that such sales could occur, could adversely affect the market price of our common stock and may make it more difficult for you to sell your common stock at a time and price that you deem appropriate. In addition, certain of our executive officers and directors have adopted, and other executive officers and 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 made by our executive officers and directors pursuant to Rule 10b5-1, regardless of the amount of such sales, could adversely affect the market price of our common stock.

The issuance of additional stock in connection with financings, acquisitions, investments, our stock incentive plans, conversion of our convertible notes 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, the conversion of our convertible notes or otherwise. For example, in December 2013, we 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; in May 2014, we issued 295,681 shares of common stock and assumed options to purchase 63,490 shares of our common stock in connection with our acquisition of nPulse Technologies; in January 2016, we issued 1,793,305 shares of common stock in connection with our acquisition of iSIGHT, to be distributed to certain former stockholders of iSIGHT upon the achievement of a threat intelligence bookings target; and in February 2016, we issued 742,026 shares of common stock in connection with our acquisition of Invotas. In addition, in June 2015, we issued $920.0 million aggregate principal amount of convertible senior notes. Any future issuances could result in substantial dilution to our existing stockholders and cause the trading price of our common stock to decline.

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.

We are subject to the independent auditor attestation requirements of Section 404 of the Sarbanes-Oxley Act ("Section 404"), enhanced disclosure obligations regarding executive compensation in our periodic reports and proxy statements, and the requirements of holding a nonbinding advisory vote on executive compensation and stockholder approval of any golden parachute payments not previously approved. While we were able to determine in our management's report for fiscal 2015 that our internal control over financial reporting is effective, as well as provide an unqualified attestation report from our independent registered public accounting firm to that effect, we have and will continue to consume management resources and incur significant expenses for Section 404 compliance on an ongoing basis. In the event that our Chief Executive Officer, Chief Financial Officer, or independent registered public accounting firm determines in the future that our internal control over financial reporting is not effective as defined under Section 404, we could be subject to one or more investigations or enforcement actions by state or federal regulatory agencies, stockholder lawsuits or other adverse actions requiring us to incur defense costs, pay fines, settlements or judgments and causing investor perceptions to be adversely affected and potentially resulting in a decline in the market price of our stock.

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 obligated to 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 this internal control 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.

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. This assessment will need to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting, as well as a statement that our auditors have issued an attestation report on our internal controls.

While we were able to determine in our management's report for fiscal 2014 that our internal control over financial reporting is effective, as well as provide an unqualified attestation report from our independent registered public accounting firm to that effect, we may not be able to complete our evaluation, testing, and any required remediation in a timely fashion or our independent registered public accounting firm may not be able to formally attest to the effectiveness of our internal control over financial reporting in the future. 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 independent registered public accounting firm is unable to attest to the effectiveness of our internal controls or determine we have a material weakness in 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.

Our charter documents and Delaware law, as well as certain provisions of our convertible notes, could discourage takeover attempts and lead to management entrenchment, which could also reduce the market price of our common stock.

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 $^{2}/_{3}$% of the voting power of all of the then outstanding shares of the voting stock, voting together as a single class, to amend the provisions of our amended and restated certificate of incorporation relating to the management of our business (including our classified board structure) or certain provisions of our amended and restated bylaws, which may inhibit the ability of an acquiror to effect such amendments to facilitate an unsolicited takeover attempt;
- the ability of our board of directors to amend the bylaws, which may allow our board of directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquiror to amend the bylaws to facilitate an unsolicited takeover attempt; and
- advance notice procedures with which stockholders must comply to nominate candidates to our board of directors or to propose matters to be acted upon at a stockholders' meeting, which may discourage or deter a potential acquiror from conducting a solicitation of proxies to elect the acquiror's own slate of directors or otherwise attempting to obtain control of us.

In addition, as a Delaware corporation, we are subject to Section 203 of the Delaware General Corporation Law, which may prohibit large stockholders, in particular those owning 15% or more of our outstanding voting stock, from merging or combining with us for a specified period of time. Additionally, certain provisions of our convertible notes could make it more difficult or more expensive for a third party to acquire us. The application of Section 203 or certain provisions of our convertible notes also could have the effect of discouraging, delaying or preventing a transaction involving a change in control of us. Any of these provisions could, under certain circumstances, depress the market price of our common stock.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

Our corporate headquarters is located in Milpitas, California where we currently lease approximately 223,000 square feet of space under lease agreements that expire during the year ended December 31, 2018. We maintain additional offices throughout the United States and various international locations, including Australia, Dubai, Germany, India, Ireland, Japan, Singapore 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 9 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, 2015, there were 114 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, 2015:	High	Low
First Quarter	$46.44	$29.25
Second Quarter	$55.33	$37.66
Third Quarter	$50.94	$30.15
Fourth Quarter	$33.15	$19.76

Year Ended December 31, 2014:	High	Low
First Quarter	$97.35	$40.41
Second Quarter	$65.65	$25.58
Third Quarter	$41.82	$27.06
Fourth Quarter	$34.55	$24.81

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, 2015. 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.

	9/13	9/13	10/13	12/13	2/14	4/14	6/14	8/14	10/14	12/14	2/15	4/15	6/15	8/1
FireEye, Inc.	$100.00	$115.36	$105.28	$121.14	$237.89	$109.06	$112.64	$86.50	$94.42	$87.72	$122.97	$114.72	$135.86	$1
S&P 500	$100.00	$103.14	$107.88	$113.98	$115.07	$116.90	$122.11	$125.25	$126.51	$129.58	$132.91	$132.07	$131.18	$1
S&P Information Technology	$100.00	$102.88	$107.61	$116.52	$118.86	$119.52	$126.94	$133.90	$135.27	$139.96	$145.57	$144.05	$141.03	$1

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

There were no sales of unregistered securities during the period covered by this Annual Report, other than those previously reported in a Quarterly Report on Form 10-Q or in a Current Report on Form 8-K.

Issuer Purchases of Equity Securities

The table below provides information with respect to repurchases of unvested shares of our common stock made pursuant to our 2008 Stock Plan during the fourth quarter of 2015.

Period	Total Number of Shares Purchased (1)	Average Price Paid Per Share	Total Number of Shares Purchased as Part of Publicly Announced Plans or Programs	Maximum Number of Shares that May Yet be Purchased Under the Plans or Programs
October 1 - October 31, 2015	—	$—	—	—
November 1 - November 30, 2015	—	—	—	—
December 1 - December 31, 2015	1,250	1.65	—	—
Total	1,250	$1.65	—	—

(1) Under our 2008 Stock Plan, certain participants may exercise options prior to vesting, subject to a right of a repurchase by us. All shares in the above table were shares repurchased as a result of us exercising this right and not pursuant to a publicly announced plan or program.

Securities Authorized for Issuance Under Equity Compensation Plans

See Item 12 of Part III of this Annual Report on Form 10-K regarding information about securities authorized for issuance under our equity compensation plans.

Item 6. Selected Consolidated Financial Data

The following selected historical financial data should be read in conjunction with Item 7, “Management’s Discussion and Analysis of Financial Condition and Results of Operations,” and 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 the factors that may affect the comparability of the information presented below.

The statements of operations data for the years ended December 31, 2015, 2014 and 2013 and the balance sheet data as of December 31, 2015 and 2014 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, 2012 and 2011 and the balance sheet data as of December 31, 2013, 2012 and 2011 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.

	Year Ended December 31,				
	2015	2014	2013	2012	2011
	(In thousands, except per share data)				
Consolidated Statements of Operations Data:					
Revenue:					
Product	$216,632	$178,246	$88,253	$52,265	$24,888
Subscription and services	406,335	247,416	73,299	31,051	8,770
Total revenue	622,967	425,662	161,552	83,316	33,658
Cost of revenue:					
Product[(1)]	74,481	58,980	28,912	14,467	5,690
Subscription and services	158,723	116,113	18,853	3,163	1,590
Total cost of revenue	233,204	175,093	47,765	17,630	7,280
Total gross profit	389,763	250,569	113,787	65,686	26,378
Operating expenses:					
Research and development[(1)]	279,467	203,187	66,036	16,522	7,275
Sales and marketing[(1)]	476,166	401,151	167,466	67,562	30,389
General and administrative[(1)]	141,790	121,099	52,503	15,221	4,428
Restructuring charges	—	4,327	—	—	—
Total operating expenses	897,423	729,764	286,005	99,305	42,092
Operating loss	(507,660)	(479,195)	(172,218)	(33,619)	(15,714)
Interest income	2,935	713	68	7	3
Interest expense	(27,116)	(26)	(525)	(537)	(194)
Other income (expense), net	(3,284)	(1,936)	(7,257)	(2,572)	(806)
Loss before income taxes	(535,125)	(480,444)	(179,932)	(36,721)	(16,711)
Provision for (benefit from) income taxes	4,090	(36,654)	(59,297)	(965)	71
Net loss attributable to common stockholders	$(539,215)	$(443,790)	$(120,635)	$(35,756)	$(16,782)
Net loss per share attributable to common stockholders, basic and diluted	$(3.50)	$(3.12)	$(2.66)	$(3.28)	$(1.99)
Weighted-average shares used to compute net loss per share attributable to common stockholders	154,120	142,176	45,271	10,917	8,447

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

	Year Ended December 31,				
	2015	2014	2013	2012	2011
	(In thousands)				
Stock-Based Compensation Expense:					
Cost of product revenue	$1,588	$888	$469	$115	$31
Cost of subscription and services revenue	29,435	17,037	2,341	55	8
Research and development	68,329	28,968	6,958	1,465	148
Sales and marketing	73,286	66,773	10,748	1,672	360
General and administrative	49,793	38,186	8,342	3,536	168
Total stock-based compensation expense	$222,431	$151,852	$28,858	$6,843	$715

	As of December 31,				
	2015	2014	2013	2012	2011
Consolidated Balance Sheet Data:	(In thousands)				
Cash and cash equivalents	$402,102	$146,363	$173,918	$60,200	$10,676
Total assets	2,441,473	1,758,881	1,376,313	125,273	35,646
Total deferred revenue	526,998	352,543	187,514	76,406	30,102
Total long-term debt, current portion	—	—	—	1,231	1,400
Total long-term debt, non-current portion	706,198	—	—	10,916	4,528
Total stockholders' equity (deficit)	$1,044,372	$1,250,828	$1,048,102	$5,390	$(14,651)

44

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 Annual Report on Form 10-K.

Overview

We provide a comprehensive cybersecurity solution for detecting, preventing, analyzing and resolving today's advanced cyber-attacks that evade legacy signature-based security products. To address the shortcomings of signature-based security solutions, we developed a new threat prevention platform based on our purpose-built, virtual machine-based detection engine, MVX. Our comprehensive platform combines our MVX virtual execution engine and our cloud-based threat intelligence network to identify previously unknown threats and protect organizations at all stages of the attack lifecycle. Our cybersecurity platform includes a family of software-based appliances, endpoint agents, cloud-based subscription services, support and maintenance and professional consulting services. Our principal threat prevention appliance families address critical vectors of attack: Web, email, file, endpoint and mobile. Our products initially require a mandatory subscription agreement that provides access to our DTI cloud which distributes updated intelligence throughout the network to provide real-time detection of advanced attacks, and we offer optional subscription services that provide additional support and functionality. We also offer a cloud-based threat analysis platform that allows IT security analysts to analyze and prioritize attack alerts from security devices utilizing our repository of dynamic and contextual threat intelligence. Additionally, we provide a family of forensic and analysis appliances and agents to enable investigation and remediation of breaches. Due to our team of highly skilled professional services experts, we provide incident response, security program assessment and other consulting services, as well as our FireEye-as-a-Service subscription services for management of our devices and comprehensive monitoring of attacks based on our threat intelligence and security expertise. Our adaptive approach to cybersecurity represents a paradigm shift in how IT security has been conducted since the earliest days of the information technology industry, and we believe it is imperative for organizations to invest in this new approach to protect their critical assets from the global pandemic of cybercrime, hacktivism, cyber-espionage and cyber-warfare.

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 platform of vector-specific appliances and cloud-based security solutions, consisting of Network Threat Prevention, Email Threat Prevention, Endpoint Threat Prevention, File Content Security and Mobile Threat Prevention. We also offer security management and analysis products including our Central Management System, Threat Analytics Platform and Malware Analysis System, and security forensics products including our Network Forensics Platform, Investigation Analysis System and Mandiant Intelligent Response. We offer this portfolio as a complete solution to protect customers from the next generation of cyber-attacks at all stages of the attack lifecycle and across all primary threat vectors, including web, email, file, endpoint and mobile. Because the typical customer has more web entry points to protect than email and file entry points, customers that purchase our threat prevention portfolio generally purchase more Network Threat Prevention appliances than any other appliance. As a result, Network 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 Network Threat Prevention. Prior to June 2014, revenue associated with Email Threat Prevention was recognized ratably over the longer of the contractual term or the estimated period the customer was expected to benefit from the product. Beginning in June 2014, we started shipping all Email Threat Prevention appliances with software that allows customers to benefit from the product without the associated subscription services. As a result, revenue from sales of Email Threat Prevention appliances is now being recognized at the time of shipment, consistent with our other product offerings. We have also experienced steady growth in sales of our Endpoint Threat Prevention and Network Forensics Platform appliances which we began offering early in 2014. We introduced our File Content Security appliance in the second quarter of 2012.

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. 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 have increased our deferred revenue. As of December 31, 2015 and 2014, our total deferred revenue was $527.0 million and $352.5 million, respectively. Amortization of this growing deferred revenue has contributed to the increase in our subscription and services revenue as a percentage of total revenue. For the years ended December 31, 2015, 2014 and 2013, subscription and services revenue as a percentage of total revenue was 65%, 58%, and 45%, respectively. While most of the growth in our subscription and services revenue during such years relates to the amortization of the initial subscription and services agreements, renewals of such agreements have also contributed to this growth. Our renewal rate for subscriptions expiring in 2015 and 2014 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.

We also offer FireEye-as-a-Service, which may include our Network Platform, Endpoint Security Platform and Network Forensics Platform solutions, managed by our security experts through our security operations centers around the world. Revenue from this service

is recognized ratably over the period the service is provided; typically one to three years. In addition to our product and subscription services, we offer professional services, including incident response and related consulting services for our customers who have experienced a cybersecurity breach or require assistance assessing the vulnerability of their networks. Revenue from these services is recognized as delivered.

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,		
	2015	2014	2013
	(Dollars in thousands)		
Product revenue	$216,632	$178,246	$88,253
Subscription and services revenue	406,335	247,416	73,299
Total revenue	$622,967	$425,662	$161,552
Year-over-year percentage increase	46 %	163 %	94 %
Gross margin percentage	63 %	59 %	70 %
Deferred revenue, current	$305,169	$203,877	$110,535
Deferred revenue, non-current	$221,829	$148,666	$76,979
Billings (non-GAAP)	$797,422	$590,691	$256,561
Net cash provided by (used in) operating activities	$37,015	$(131,270)	$(69,762)
Free cash flow (non-GAAP)	$(17,534)	$(198,985)	$(127,322)

Deferred revenue. Our deferred revenue consists of amounts that have been invoiced but have not yet been recognized as revenue as of the period end. The majority of our deferred revenue consists of the unamortized balance of revenue from subscriptions to our DTI cloud, FireEye-as-a-Service offerings and support and maintenance contracts. Because invoiced amounts for subscriptions and services can be for multiple years, we classify our deferred revenue as current or non-current depending on when we expect to recognize the related revenue. If the deferred revenue is expected to be recognized within 12 months it is classified as current, otherwise, the deferred revenue is classified as non-current. We monitor our deferred revenue balance because it represents a significant portion of revenue to be recognized in future periods. 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.

Billings. Billings are 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. 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 future 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. 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. 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,		
	2015	2014	2013
	(in thousands)		
Revenue	$622,967	$425,662	$161,552
Deferred revenue, end of period	526,998	352,543	187,514
Less: deferred revenue, beginning of period	352,543	187,514	76,406
Less: Mandiant deferred revenue assumed	—	—	16,099
Billings (non-GAAP)	$797,422	$590,691	$256,561

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, the most directly comparable GAAP financial measure, 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 is provided below:

	Year Ended December 31,		
	2015	2014	2013
	(In thousands)		
Cash flow provided by (used in) operating activities	$37,015	$(131,270)	$(69,762)
Less: purchase of property and equipment and demonstration units	(54,549)	(67,715)	(57,560)
Free cash flow (non-GAAP)	$(17,534)	$(198,985)	$(127,322)
Net cash used in investing activities	$(576,749)	$(382,511)	$(148,469)
Net cash provided by financing activities	$795,473	$486,226	$331,949

Factors Affecting our Performance

Market Adoption. We rely on market education to raise awareness of today’s next-generation cyber attacks and 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 nine months, but can be more than a year. 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 certain international markets 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 the 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 support and maintenance services. New or existing customers that purchase one of our Security Forensic Products 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, 2015 and 2014 was in excess of 90%. These high renewal rates are primarily attributable to the incremental value added to our appliances by our cloud subscriptions, support and maintenance and services. As cloud subscriptions, support and maintenance and services represented 65%, 58% and 45% of our total revenue during the years ended December 31, 2015, 2014 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 products, subscriptions and services. 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, add new services, 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 which we generally recognize at the time of shipment, provided that all other revenue recognition criteria have been met.
- Subscription and services revenue. Subscription and services revenue is generated primarily from our cloud subscriptions, FireEye-as-a-Service, support and maintenance services and other professional services. We recognize revenue from subscriptions and support and maintenance services over the one or three year contract term, as applicable. Professional services revenue, which includes incident response and compromise assessments, is offered on a time-and-material basis or through a fixed fee arrangement and is recognized as the services are delivered.

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 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, shipping costs and allocated overhead 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 and services organization and allocated overhead costs. We expect our cost of subscription and services revenue to increase as our customer base grows and as we hire additional support and 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 these factors.

Operating Expenses

Our operating expenses consist of research and development, sales and marketing and general and administrative expenses, as well as restructuring charges. 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 allocated overhead costs consisting of certain facilities, depreciation and information technology costs.

- 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, primarily due to the full year impact of past investments, as well as recent acquisitions in our research and product development efforts to introduce new products, enhance our current 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, primarily

due to the full year impact of past investments, as well as recent acquisitions, in our sales and marketing organizations to 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, primarily due to the full year impact of past investments, as well as recent acquisitions which grew our operations.
- Restructuring charges. Beginning in August 2014, we initiated a series of business restructuring plans to reduce our cost structure and improve efficiency. The expenses incurred primarily consisted of employee severance charges related to workforce reductions, and real estate and related fixed asset charges for the consolidation of certain leased facilities. We did not initiate any plans related to restructuring activities during the year ended December 31, 2015.

Interest Income

Interest income consists of interest earned on our cash and cash equivalent and investment balances. We have historically invested our cash in money-market funds and other short-term, high quality securities. 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 is primarily a result of our convertible senior notes, consisting of interest at the stated rate (coupon) and amortization of discounts and issuance costs.

Other Expense, Net

Other expense, net includes gains or losses on the disposal of fixed assets, foreign currency re-measurement gains and losses and foreign currency transaction gains and losses. We expect other expense, net to fluctuate depending primarily on foreign exchange rate movements.

Provision for (Benefit from) Income Taxes

Provision for (benefit from) income taxes consists primarily of federal and state income taxes in the United States and income taxes in certain foreign jurisdictions in which we conduct business. Income in certain countries may be taxed at statutory tax rates that are lower than the U.S. statutory tax rate. As a result, our overall effective tax rate over the long term may be lower than the U.S. federal statutory tax rate due to a larger proportion of net income which was subject to foreign income tax rates that are lower than the U.S. federal statutory rate.

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,		
	2015	2014	2013
	(In thousands)		
Revenue:			
Product	$216,632	$178,246	$88,253
Subscription and services	406,335	247,416	73,299
Total revenue	622,967	425,662	161,552
Cost of revenue:			
Product	74,481	58,980	28,912
Subscription and services	158,723	116,113	18,853
Total cost of revenue	233,204	175,093	47,765
Total gross profit	389,763	250,569	113,787
Operating expenses:			
Research and development	279,467	203,187	66,036
Sales and marketing	476,166	401,151	167,466
General and administrative	141,790	121,099	52,503
Restructuring charges	—	4,327	—
Total operating expenses	897,423	729,764	286,005
Operating loss	(507,660)	(479,195)	(172,218)
Interest income	2,935	713	68
Interest expense	(27,116)	(26)	(525)
Other expense, net	(3,284)	(1,936)	(7,257)
Loss before income taxes	(535,125)	(480,444)	(179,932)
Provision for (benefit from) income taxes	4,090	(36,654)	(59,297)
Net loss attributable to common stockholders	$(539,215)	$(443,790)	$(120,635)

	Year Ended December 31,		
	2015	2014	2013
	(As a percentage of total revenue)		
Revenue:			
Product	35 %	42 %	55 %
Subscription and services	65	58	45
Total revenue	100	100	100
Cost of revenue:			
Product	12	14	18
Subscription and services	25	27	12
Total cost of revenue	37	41	30
Total gross profit	63	59	70
Operating expenses:			
Research and development	45	48	41
Sales and marketing	76	94	104
General and administrative	23	28	32
Restructuring charges	—	1	—
Total operating expenses	144	171	177
Operating loss	(81)	(112)	(107)
Interest income	—	—	—
Interest expense	(4)	—	—
Other expense, net	(1)	(1)	(4)
Loss before income taxes	(86)	(113)	(111)
Provision for (benefit from) income taxes	1	(9)	(36)
Net loss attributable to common stockholders	(87)%	(104)%	(75)%

Comparison of the Years Ended December 31, 2015 and 2014

Revenue

	Year Ended December 31,							
	2015		2014		Change			
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%		
	(Dollars in thousands)							
Revenue:								
Product	$216,632	35 %	$178,246	42 %	$38,386	22	%	
Subscription and services	406,335	65	247,416	58	158,919	64		
Total revenue	$622,967	100 %	$425,662	100 %	$197,305	46	%	
Subscription and services by type:								
Product subscription	$205,303	33 %	$121,907	29 %	$83,396	68	%	
Support and maintenance	89,800	14	53,406	12	36,394	68		
Professional services	111,232	18	72,103	17	39,129	54		
Total Subscription and services revenue	$406,335	65 %	$247,416	58 %	$158,919	64	%	
Revenue by geographic region:								
United States	$439,206	70 %	$319,144	75 %	$120,062	38	%	
EMEA	80,960	13	57,721	14	23,239	40		
APAC	73,009	12	34,284	8	38,725	113		
Other	29,792	5	14,513	3	15,279	105		
Total revenue	$622,967	100 %	$425,662	100 %	$197,305	46	%	

Product revenue increased by $38.4 million, or 22%, during the year ended December 31, 2015 compared to the year ended December 31, 2014. The increase in product revenue was primarily driven by growth in our installed base of

customers, which grew

from approximately 3,100 as of December 31, 2014 to over 4,400 as of December 31, 2015, as well as follow-on purchases from customers expanding their initial deployments of our product portfolio. Our Network Threat Prevention and Email Threat Prevention products have historically accounted for the largest portion of our product revenue as customers initially focused on protecting Web and email entry points when building our their security infrastructure. Our product revenue growth rates have declined as new customers began adopting our cloud subscriptions, including FireEye-as-a-Service and ETP. We expect product revenue growth rates to continue to decline as part of this ongoing transition.

Subscription and service revenue increased by $158.9 million, or 64%, during the year ended December 31, 2015 compared to the year ended December 31, 2014. This increase is comprised of an increase in subscription revenue of $83.4 million, an increase in professional services revenue of $39.1 million and an increase in support and maintenance revenue of $36.4 million. The increase in subscription revenue of $83.4 million and the increase in support and maintenance revenue of $36.4 million is primarily due to an increase in initial customer purchases of $87.6 million and an increase in the amortization of deferred subscription and support and maintenance revenue related to renewals of $32.2 million for the year ended December 31, 2015 compared to the year ended December 31, 2014. We expect a continued transition of customers from product sales to our cloud subscriptions. 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, 2015 was in excess of 90%.

International revenue increased $77.2 million, or 73%, during the year ended December 31, 2015 compared to the year ended December 31, 2014, which reflects our increasing international market presence.

Cost of Revenue and Gross Margin

	Year Ended December 31,					
	2015		2014		Change	
	Amount	Gross Margin	Amount	Gross Margin	Amount	%
	(Dollars in thousands)					
Cost of revenue:						
Product	$74,481		$58,980		$15,501	26 %
Subscription and services	158,723		116,113		42,610	37
Total cost of revenue	$233,204		$175,093		$58,111	33 %
Gross margin:						
Product		66 %		67 %		
Subscription and services		61 %		53 %		
Total gross margin		63 %		59 %		

The cost of product revenue increased $15.5 million, or 26%, during the year ended December 31, 2015 compared to the year ended December 31, 2014. The increase in cost of product revenue was driven primarily by an increase in product revenue.

The cost of subscription and services revenue increased $42.6 million, or 37%, during the year ended December 31, 2015 compared to the year ended December 31, 2014. The increase in cost of subscription and services revenue was driven by a $16.4 million increase in facility and IT costs to support departmental expansion, a $12.4 million increase in stock-based compensation charges, a $6.8 million increase due to higher data hosting services and a $5.4 million increase in depreciation, of which $1.1 million related to accelerated depreciation as a result of changes in the estimated useful life of certain assets to be replaced in the first quarter of 2016.

Gross margin increased for the year ended December 31, 2015 compared to the year ended December 31, 2014, due to the increase in subscription and services margins. The increase in subscription and services margins is primarily due to the proportion of revenues attributable to subscriptions, which have higher gross margins compared to incident response, compromise assessments and other professional services.

Operating Expenses

	Year Ended December 31,							
	2015		2014		Change			
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%		
	(Dollars in thousands)							
Operating expenses:								
Research and development	$279,467	45 %	$203,187	48 %	$76,280	38	%	
Sales and marketing	476,166	76	401,151	94	75,015	19		
General and administrative	141,790	23	121,099	28	20,691	17		
Restructuring charges	—	—	4,327	1	(4,327)	(100)		
Total operating expenses	$897,423	144 %	$729,764	171 %	$167,659	23	%	
Includes stock-based compensation expense of:								
Research and development	$68,329		$28,968					
Sales and marketing	73,286		66,773					
General and administrative	49,793		38,186					
Total	$191,408		$133,927					

Research and Development

Research and development expense increased $76.3 million, or 38%, during the year ended December 31, 2015 compared to the year ended December 31, 2014. The increase was primarily driven by a $62.2 million increase in personnel costs, primarily due to a $39.4 million increase in stock-based compensation charges, as well as a 24% increase in headcount. Additionally, $8.8 million of the increase was driven by higher facility and IT costs to support departmental expansion and continued investment in our future product and service offerings.

Sales and Marketing

Sales and marketing expense increased $75.0 million, or 19%, during the year ended December 31, 2015 compared to the year ended December 31, 2014. The increase was primarily driven by a $38.7 million increase in personnel costs, of which $6.5 million was related to stock-based compensation charges, largely as a result of a 28% increase in headcount, as well as a $23.4 million increase in commissions associated with higher sales. Additionally, $7.5 million of the increase was driven by higher facility and IT costs to support departmental expansion.

General and Administrative

General and administrative expense increased $20.7 million, or 17%, during the year ended December 31, 2015 compared to the year ended December 31, 2014. The increase was primarily driven by a $21.2 million increase in personnel costs, of which $11.6 million was related to stock-based compensation charges, largely as a result of a 32% increase in headcount.

Restructuring Charges

During the year ended December 31, 2014, we incurred restructuring charges of $4.3 million, of which $1.6 million related to workforce reductions and $2.7 million related to facility consolidations, as part of our plans initiated in August 2014 to reduce our cost structure and improve efficiency. We incurred no restructuring charges during the year ended December 31, 2015.

Interest Income

	Year Ended December 31,		Change		
	2015	2014	Amount	%	
	(Dollars in thousands)				
Interest income	$2,935	$713	$2,222	312	%

Interest income increased during the year ended December 31, 2015 compared to the year ended December 31, 2014 due to higher average balances in our cash and cash equivalents and investments.

Interest Expense

	Year Ended December 31,		Change	
	2015	2014	Amount	%
	(Dollars in thousands)			
Interest expense	$(27,116)	$(26)	$27,090	104,192 %

Interest expense increased during the year ended December 31, 2015 compared to the year ended December 31, 2014 due to cash interest expense of $7.0 million and amortization of discount and issuance costs of $20.1 million from the Convertible Senior Notes issued in June 2015.

Other Expense, Net

	Year Ended December 31,		Change	
	2015	2014	Amount	%
	(Dollars in thousands)			
Other expense, net	$(3,284)	$(1,936)	$1,348	70 %

The increase in other expense, net during the year ended December 31, 2015 compared to the year ended December 31, 2014 was primarily due to foreign currency transaction losses caused by unfavorable changes in foreign currency exchange rates.

Provision for (Benefit from) Income Taxes

	Year Ended December 31,	
	2015	2014
	(Dollars in thousands)	
Provision for (benefit from) income taxes	$4,090	$(36,654)
Effective tax rate	(0.8)%	7.6 %

The change from a benefit from income taxes to a provision for income taxes during the year ended December 31, 2015 compared to the year ended December 31, 2014 is primarily due to the fact that we no longer have deferred tax liabilities in excess of our deferred tax assets which would be available as a source of income for purposes of determining our valuation allowance. We continue to maintain a full valuation allowance on all of our U.S. and Singapore-based deferred tax assets to the extent that deferred tax liabilities are not available as a source of income as of December 31, 2015. The tax expense for the year ended December 31, 2015 is primarily due to foreign taxes.

Comparison of the Years Ended December 31, 2014 and 2013

Revenue

	Year Ended December 31,								
	2014			2013			Change		
	Amount	% of Total Revenue		Amount	% of Total Revenue		Amount	%	
	(Dollars in thousands)								
Revenue:									
Product	$178,246	42	%	$88,253	55	%	$89,993	102	%
Subscription and services	247,416	58		73,299	45		174,117	238	
Total revenue	$425,662	100	%	$161,552	100	%	$264,110	163	%
Revenue by geographic region:									
United States	$319,144	75	%	$116,730	72	%	$202,414	173	%
EMEA	57,721	14		22,845	14		34,876	153	
APAC	34,284	8		16,004	10		18,280	114	
Other	14,513	3		5,973	4		8,540	143	
Total revenue	$425,662	100	%	$161,552	100	%	$264,110	163	%

Product revenue increased by $90.0 million, or 102%, during the year ended December 31, 2014 compared to the year ended December 31, 2013. The increase in product revenue was primarily driven by growth in our installed base of customers, which grew from approximately 2,000 as of December 31, 2013 to approximately 3,100 as of December 31, 2014, as well as follow-on purchases from customers expanding their initial deployments of our product portfolio. Our Network Threat Prevention product accounted for the largest portion of our product revenue as customers that purchase our product portfolio generally purchase more Network Threat Prevention appliances than our other appliances, reflecting the fact that their networks typically have more Web entry points than email, file, endpoint or mobile entry points to protect.

Subscription and service revenue increased by $174.1 million, or 238%, during the year ended December 31, 2014 compared to the year ended December 31, 2013. This increase is comprised of an increase in subscription revenue of $78.9 million, an increase in professional services revenue of $68.7 million and an increase in support and maintenance revenue of $26.5 million. The increase in subscription revenue of $78.9 million and the increase in support and maintenance revenue of $26.5 million is primarily due to initial customer purchases of $117.9 million and subscription revenue resulting from our acquisition of Mandiant. Additionally, there was an increase of $57.4 million in the amortization of deferred subscription and support and maintenance revenue related to renewals for the year ended December 31, 2014. 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 ending December 31, 2014 was in excess of 90%.

International revenue increased $61.7 million, or 138%, during the year ended December 31, 2014 compared to the year ended December 31, 2013, which reflects our increasing international market presence.

Cost of Revenue and Gross Margin

	Year Ended December 31,					
	2014		2013		Change	
	Amount	Gross Margin	Amount	Gross Margin	Amount	%
	(Dollars in thousands)					
Cost of revenue:						