

PROOFPOINT INC
Form 10-K
February 23, 2017
Table of Contents

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

FORM 10-K

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the Fiscal Year Ended December 31, 2016

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 001-35506

PROOFPOINT, INC.

(Exact name of Registrant as specified in its charter)

Delaware 51-0414846

(State or other jurisdiction of (I.R.S. employer
incorporation or organization) identification no.)

892 Ross Drive 94089
Sunnyvale, California (Zip Code)
(Address of principal executive offices)

(408) 517-4710
(Registrant's telephone number, including area code)

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

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

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

None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. YES NO

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. YES NO

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. YES NO

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

Indicate by 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.

o

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.

Large accelerated filer	Accelerated filer	Non-accelerated filer	Smaller reporting company
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> (Do not check if a smaller reporting company)	<input type="checkbox"/>

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

The aggregate market value of the voting and non-voting common equity held by non-affiliates of the registrant, based upon the closing price of a share of the registrant’s common stock on June 30, 2016 as reported by the NASDAQ Global Select Market on that date, was approximately \$2,571,000,000. This calculation does not reflect a determination that certain persons are affiliates of the registrant for any other purpose.

The number of shares outstanding of the registrant’s common stock as of February 3, 2017 was 43,296,403 shares.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant’s Proxy Statement for its 2017 Annual Meeting of Stockholders (the “Proxy Statement”), to be filed with the Securities and Exchange Commission, are incorporated by reference into Part III of this Annual Report on Form 10-K where indicated. The Proxy Statement will be filed with the Securities and Exchange Commission within 120 days of the registrant's fiscal year ended December 31, 2016.

Table of Contents

PROOFPOINT, INC.

FORM 10-K

For the Fiscal Year Ended December 31, 2016

TABLE OF CONTENTS

	Page
PART I.	
Item 1. <u>Business</u>	<u>3</u>
Item 1A. <u>Risk Factors</u>	<u>15</u>
Item 1B. <u>Unresolved Staff Comments</u>	<u>31</u>
Item 2. <u>Properties</u>	<u>31</u>
Item 3. <u>Legal Proceedings</u>	<u>32</u>
Item 4. <u>Mine Safety Disclosures</u>	<u>32</u>
PART II.	
Item 5. <u>Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities</u>	<u>33</u>
Item 6. <u>Selected Financial Data</u>	<u>34</u>
Item 7. <u>Management’s Discussion and Analysis of Financial Condition and Results of Operations</u>	<u>36</u>
Item 7A. <u>Quantitative and Qualitative Disclosures About Market Risk</u>	<u>57</u>
Item 8. <u>Financial Statements and Supplementary Data</u>	<u>58</u>
Item 9. <u>Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</u>	<u>58</u>
Item 9A. <u>Controls and Procedures</u>	<u>58</u>
Item 9B. <u>Other Information</u>	<u>59</u>
PART III.	
Item 10. <u>Directors, Executive Officers and Corporate Governance</u>	<u>60</u>
Item 11. <u>Executive Compensation</u>	<u>60</u>
Item 12. <u>Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</u>	<u>60</u>
Item 13. <u>Certain Relationships and Related Transactions, and Director Independence</u>	<u>60</u>
Item 14. <u>Principal Accountant Fees and Services</u>	<u>60</u>
PART IV.	
Item 15. <u>Exhibits and Financial Statement Schedules</u>	<u>61</u>
<u>Index to Consolidated Financial Statements</u>	<u>62</u>
Signatures	<u>102</u>

Table of Contents

CAUTIONARY STATEMENT REGARDING FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements contained in this Annual Report on Form 10-K other than statements of historical fact, including statements regarding our future results of operations and financial position, our business strategy and plans, and our objectives for future operations, are forward-looking statements. The words "believe," "may," "will," "estimate," "continue," "anticipate," "intend," "expect," and similar expressions are intended to identify forward-looking statements. We have based these forward-looking statements largely on our current expectations and projections about future events and trends that we believe may affect our financial condition, results of operations, business strategy, short-term and long-term business operations and objectives, and financial needs. These forward-looking statements are subject to a number of risks, uncertainties and assumptions, including those described in Part I, Item 1A, "Risk Factors" in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment. 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 future events and trends discussed in this Annual Report on Form 10-K may not occur and actual results could differ materially and adversely from those anticipated or implied in the forward-looking statements. We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements. Unless expressly indicated or the context requires otherwise, the terms "Proofpoint," "Company," "Registrant," "we," "us," and "our" mean Proofpoint, Inc. and its subsidiaries unless the context indicates otherwise.

Table of Contents

PART I

ITEM 1. BUSINESS

Overview

Proofpoint is a leading security-as-a-service provider that enables large and mid-sized organizations worldwide to defend, protect, archive and govern their most sensitive data. Our security-as-a-service platform is comprised of an integrated suite of on-demand data protection solutions, including threat protection, incident response, regulatory compliance, archiving, governance, eDiscovery, and secure communication. Our solutions are built on a flexible, cloud-based platform and leverage a number of proprietary technologies - including big data analytics, machine learning, deep content inspection, secure storage, advanced encryption, intelligent message routing, dynamic malware analysis, threat correlation, and virtual execution environments - to address today's rapidly changing threat landscape.

A fundamental shift in the sources of cyber crime, from hackers to organized crime and governments, combined with the emergence of international data trafficking and sophisticated advanced persistent threats ("APTs"), polymorphic threats, zero-day exploits, and user-transplant "drive-by" downloads, is driving an unprecedented wave of both targeted and broad-based malicious attack campaigns designed to steal valuable information. At the same time, the growth of business-to-business collaboration and the use of social media for mass communication, as well as the consumerization of IT and the associated adoption of mobile devices and unmanaged Internet-based applications, has increased organizations' attack surface through the proliferation of sensitive data, reducing the effectiveness of many existing security products. These factors have contributed to an increasing number of severe data breaches and expanding regulatory mandates, all of which have accelerated demand for effective data protection and governance solutions.

Our platform addresses this growing challenge by not only protecting data as it flows into and out of the enterprise via on-premises and cloud-based email, social media and mobile apps, but also by keeping track of this information as it is modified and distributed throughout the enterprise for compliance and data loss prevention, and securely archiving these communications for compliance and discovery. We address four important problems for the enterprise:

- Protecting users from the advanced attacks that target them via email, social media, and mobile apps;
- Preventing the theft or inadvertent loss of sensitive information and, in turn, ensuring compliance with regulatory data protection mandates;
- Collecting, retaining, supervising and discovering sensitive data for compliance and litigation support; and
- Enabling organizations to respond quickly to security issues, providing both the intelligence and the context to prioritize incidents and orchestrate remediation actions.

Our platform and its associated solutions are sold to customers on a subscription basis and can be deployed through our unique cloud-based architecture that leverages both our global data centers as well as optional points-of-presence behind our customers' firewalls. Our flexible deployment model enables us to deliver superior security and compliance while maintaining the favorable economics afforded by cloud computing, creating a competitive advantage for us over legacy on-premises and cloud-only offerings.

We were founded in 2002 to provide a unified solution to help enterprises address their growing data security requirements. Our first solution was commercially released in 2003 to combat the burgeoning problem of spam and viruses and their impact on corporate email systems. To address the evolving threat landscape and the adoption of

communication and collaboration systems beyond corporate email and networks, we have broadened our solutions to defend against a wide range of threats, including email, mobile apps and social media, to protect the information people create from both compromise and compliance risks, and to archive and govern corporate information. Today, our solutions are used worldwide to protect well over 100 million end-users. We market and sell our solutions worldwide both directly through our sales teams and indirectly through a hybrid model where our sales organization actively assists our network of distributors and resellers. We also distribute our solutions through strategic partners.

Proofpoint Solutions

Our integrated suite of on-demand security-as-a-service solutions enables large and mid-sized organizations to protect people throughout the enterprise from advanced attacks and compliance risks. Our comprehensive platform provides a secure

3

Table of Contents

email gateway, advanced threat protection, threat intelligence, email encryption, data loss prevention, digital risk, archiving, eDiscovery, and threat response capabilities. These solutions are built on a cloud-based architecture, protecting enterprises and their customers from inbound threats via email, social media, and mobile apps, while identifying and protecting enterprise data not only where it is stored within the enterprise but also as it transits beyond the organization's borders such as via email or social media. We have pioneered the use of innovative technologies to deliver better ease-of-use, greater protection against the latest advanced threats, and lower total cost of ownership than traditional alternatives. The key elements of our solution include:

Superior protection against both advanced and targeted threats. We use a combination of proprietary technologies for big data analytics, machine learning, deep content inspection, dynamic malware analysis, threat correlation, threat intelligence extraction, and virtual execution environments to predictively and actively detect and stop targeted "spear phishing" and other sophisticated advanced and next-generation threat attacks, including APTs, that employ malicious attachments, polymorphic threats, zero-day exploits, user-transparent "drive-by" downloads and other penetration tactics. By processing, analyzing and correlating billions of data points on a daily basis, we can recognize anomalies in order to predictively detect targeted attacks before users are exposed. Our deep content inspection technology enables us to identify malicious message attachments and distinguish between valid messages and "phishing" messages designed to look authentic and trick the end-user into divulging sensitive data or clicking on a malicious web link. Our machine learning technology enables us to detect targeted "zero-hour" attacks in real-time, even if they have not been seen previously at other locations, and quarantine them appropriately. Our dynamic malware analysis and virtual execution environment technologies enable us to examine web site destinations and downloadable files to identify and block potentially hostile code that would otherwise compromise end-user computers, even in cases where the web sites are considered reputable or the attachment's malicious payload is obfuscated or otherwise disguised. Our threat correlation technologies enable us to rapidly confirm and contain threats, providing rapid, automated protection. In addition, our threat intelligence and response capabilities enable our customers to both prioritize threats that may have compromised them via our Emerging Threat Intelligence and orchestrate or automate protective countermeasures via Proofpoint Threat Response.

Comprehensive, integrated email security, advanced threat, information protection and archiving, and digital risk protection product families. We offer a comprehensive solution for email security, composed of our Enterprise Protection, Email Fraud Defense, and Email Continuity offerings. Our advanced threat product family includes solutions to protect organizations across the predominant threat vectors, including email, social media, mobile apps, and SaaS applications. To protect enterprise data from security and compliance risks, our Information Protection product family includes a suite of security solutions (Data Loss Prevention, Encryption, and Data Discover for data at rest) and compliance (Enterprise Archive, eDiscovery Analytics, and Supervision). Finally, our digital risk protection suite enables organizations to look beyond their borders for threats targeting their customers across email phishing, malicious web domains, fraudulent mobile apps, and fraudulent social media accounts.

Designed to empower end-users. Unlike legacy offerings that simply block communication or report audit violations, our solutions actively enable secure business-to-business and business-to-consumer communications. Our easy-to-use policy-based email encryption service automatically encrypts sensitive emails and delivers them to any PC or mobile device. In addition, our secure file-transfer solution makes it easy for end-users to securely share various forms of documents and other content that are typically too large to send through traditional e-mail systems. All of our solutions provide mobile-optimized capabilities to empower the growing number of people who use mobile devices as their primary computing platform.

Security optimized cloud architecture. Our multi-tenant security-as-a-service solution leverages a distributed, scalable architecture deployed in our global data centers for deep content inspection, global threat correlation and analytics, high-speed search, secure storage, encryption key management, software updates, intelligent message routing, and other core functions. Our architecture also enables us to look across hundreds of billions of data points gathered from

across our product portfolio and intelligence feeds to better correlate and analyze both targeted and broad-based threat campaigns. Customers can choose to deploy optional physical or virtual points-of-presence behind their firewalls for those who prefer to deploy certain functionality inside their security perimeter. This architecture enables us to leverage the benefits of the cloud to cost-effectively deliver superior security and compliance, while optimizing each deployment for the customer's unique threat environment.

• Extensible security-as-a-service platform. The key components of our security-as-a-service platform, including services for secure storage, content inspection, reputation, big data analytics, encryption, key management, and

Table of Contents

identity and policy, can be exposed through application programming interfaces, or APIs, to integrate with internally developed applications as well as with those developed by third-parties. In addition, these APIs provide a means to integrate with the other security and compliance components deployed in our customers' infrastructures, including Proofpoint's ecosystem partners.

Our Security-as-a-Service Platform

We provide a multi-tiered security-as-a-service platform consisting of solutions, platform technologies and infrastructure. Our platform currently includes product families and related bundles for the convenience of our customers, distributors and resellers. Each of these solutions is built as an aspect of our security-as-a-service platform, which includes both platform services and enabling technologies for both security and compliance. Our platform services provide the key functionality to enable our various solutions while our enabling technologies work in conjunction with our platform services to enable the efficient construction, scaling and maintenance of our customer-facing solutions.

Our suite is delivered by a cloud infrastructure and can be deployed as a secure cloud-only solution, or as a hybrid solution with optional physical or virtual points-of-presence behind our customers' firewalls for those who prefer to deploy certain functionality inside their security perimeter. In all deployment scenarios, our cloud-based architecture enables us to leverage the benefits of the cloud to cost-effectively deliver superior security and compliance while maintaining the flexibility to optimize deployments for customers' unique environments. The modularity of our solutions enables our existing customers to implement additional modules in a simple and efficient manner.

Product Families

Email Security

Proofpoint's Email Security Product family includes the Enterprise Protection secure email gateway, Email Fraud Defense, Email Continuity, and Proofpoint Essentials. This suite of enterprise products is designed to protect customers' mission-critical messaging infrastructure from outside threats, enable enterprises to authenticate their email to reduce consumer phishing and fight business email compromise ("BEC") attacks, and keep email operational in the event of a service provider outage. Proofpoint Essentials provides a version of these capabilities tailored to small- and medium-sized businesses. Key capabilities within the email security products include:

Enterprise Protection. Uses our Proofpoint MLX machine learning technology and reputation data to examine millions of possible attributes in every message to block phishing and spear phishing attacks, spam, viruses, impostor email/business email compromise attacks, and other forms of malicious or objectionable content. This solution also includes sophisticated policy and routing controls designed to ensure security and the effective

Table of Contents

handling of all classifications of content, and includes the Smart Search tool to provide real-time visibility into message flows across an organization's messaging infrastructure, using built-in logging and reporting capabilities with advanced message tracing, forensics and log analysis capabilities.

• **Email Fraud Defense.** Enables organizations to understand who is sending email from their domains, and create a policy to both authenticate legitimate email and block fraudulent email.

• **Email Continuity.** Allows organizations to maintain email communications if their on-premises or cloud-based email servers experience an outage.

• **Proofpoint Essentials.** Our suite of security-as-a-service and compliance solutions specifically designed for distribution across managed service providers and dedicated security resellers. Key capabilities include inbound email filtering to block spam and malware, outbound filtering for compliance with company policies, email continuity to enable email service availability, targeted attack protection, and email archiving.

Key benefits of the email security products include:

• **Superior protection from advanced threats, spam and viruses.** Protects against advanced threats, spam and other malware such as viruses, worms and spyware.

• **Comprehensive outbound threat protection.** Analyzes all outbound email traffic to block spam, viruses and other malicious content from leaving the corporate network, and pinpoint the responsible compromised systems.

• **Effective, flexible policy management and administration.** Provides a user-friendly, web-based administration interface and robust reporting capabilities that make it easy to define, enforce and manage an enterprise's messaging policies.

• **Easy-to-use end-user controls.** Gives email users easy, self-service control over their individual email preferences within the parameters of corporate-defined messaging policies.

• **Superior protection from business email compromise.** Combining a dynamic classifier on the email gateway with a proactive authentication solution delivers superior protection from these attacks.

• **Business continuity.** Provides an always-on insurance policy for crucial business communications via email.

Proofpoint Advanced Threat Protection

Proofpoint's advanced threat protection products leverage a broad set of detection techniques that are constantly refined as the threat landscape evolves. The products are capable of detecting and preventing threats across email, social media, mobile apps, and SaaS applications, and deliver rich intelligence to enable enterprises to understand as much as possible about the attacks they are seeing and the adversaries behind them. Key capabilities of the advanced threat products include:

• **Targeted attack protection.** Enterprises are protected against both commodity and advanced threats such as phishing and other targeted email attacks by the use of big data analysis, predictive, virtual execution and dynamic malware analysis techniques to identify and apply additional security controls against suspicious messages and any associated links to the web. The same detection techniques are extended to look for malicious content in enterprise social media accounts, malicious links and file sent to users via SaaS applications, and malicious mobile apps that siphon off data or function as remote access Trojans.

Threat response. Provides threat information and indicators of compromise ("IoCs") correlation, aggregating across Proofpoint and other third-party security products, to confirm and contain system compromises. By taking advantage of this automated incident response, enterprises can minimize exfiltration windows and leverage staff for breach prevention and mitigation. In addition, it can be leveraged to automatically remove malicious emails that have been delivered to users' email boxes, reducing the potential risk exposure.

Key benefits of Proofpoint Advanced Threat Protection include:

6

Table of Contents

Superior effectiveness. Proofpoint's agility in deploying new detection measures and adjusting defenses in response to changes in the threat landscape results in highly effective in stopping threats before they reach enterprise users.

Curated threat intelligence. Proofpoint's threat research team tracks campaigns and actors, providing detailed research in addition to curated IoCs. The high quality of this threat intelligence enables customers to better prioritize their responses to alerts generated by Proofpoint products, as well as leverage the intelligence to hunt for threats that may have compromised their enterprises via other channels.

Proofpoint Information Protection and Archiving

A comprehensive data protection strategy must address both security and compliance risks. Our data loss prevention, encryption and compliance solution defends against leaks of confidential information, and helps ensure compliance with common U.S., international and industry-specific data protection regulations - including the Health Care Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Gramm-Leach-Bliley Act, Canada's Personal Information Protection and Electronic Documents Act, as well as acts such as CA SB 24, MA 201 CMR 17.00, ITAR, NERC-CIP, CFTC red flag rules, Basel II, EuroSOX (Directive 84/253/EEC), European Union Data Privacy Directive, and the Payment Card Industry Data Security Standard (PCI-DSS).

Proofpoint Information Protection and Archiving is designed to ensure accurate enforcement of data governance, data retention and supervision policies and mandates; cost-effective litigation support through efficient discovery; and active legal-hold management. It can store, govern and discover a wide range of data including email, instant message conversations, social media interactions, and other files throughout the enterprise.

Key capabilities within Proofpoint Information Protection and Archiving include:

Advanced data loss prevention. Our advanced data loss prevention solution identifies regulated private content, valuable corporate assets and confidential information before it leaves the organization via email, web-based applications, or our Secure Share solution. Pre-packaged smart identifiers and dictionaries automatically and accurately detect a wide range of regulated content such as social security numbers, health records, credit card numbers, and driver's license numbers. In addition to regulated content, our machine learning technology can identify confidential, organization-specific content and assets. Once identified and classified, sensitive data can be blocked, encrypted and transmitted or re-routed internally based on content and identity-aware policies.

Flexible remediation and supervision. Content, identity and destination-aware policies enable effective remediation of potential data breaches or regulatory violations. Remediation options include stopping the transfer completely, automatically forcing data-encryption, or routing to a compliance supervisor or the end-user for disposition. The solution also provides comprehensive reporting on potential violations and remediation using our analytics capabilities.

Policy-based encryption. Automatically encrypts regulated and other sensitive data before it leaves an organization's security perimeter without requiring cumbersome end-user key management. This enables authorized external recipients, whether or not they are our customers, to quickly and easily decrypt and view content from most devices.

Secure share. Cloud-based security-focused solution designed to enable enterprise users to securely exchange large files with ease while staying compliant with enterprise data policies.

- Data Discover. Automated discovery and remediation solution that identifies sensitive content across the enterprise and enables corrective action, while reducing risk of data breaches and compliance violations.

Secure cloud storage. With our proprietary double blind encryption technology and the associated data storage architecture, all email messages, files and other content are encrypted with keys controlled by the customer before the data enters the Proofpoint Enterprise Archive. This ensures that even our employees and law-enforcement agencies cannot access a readable form of the customer data without authorized access by the customer to the encryption keys stored behind the customer's firewall.

7

Table of Contents

Search performance. By employing parallel, big data search techniques, we are able to deliver search performance measured in seconds, even when searching hundreds of terabytes of archived data. Traditional on-premises solutions can take hours or even days to return search results to a complex query.

Flexible policy enforcement. Enables organizations to easily define and automatically enforce data retention and destruction policies necessary to comply with regulatory mandates or internal policies that can vary by user, group, geography or domain.

Active legal-hold management. Enables administrators or legal professionals to easily designate specific individuals or content as subject to legal-hold. Proofpoint Enterprise Archive then provides active management of these holds by suspending normal deletion policies and automatically archiving subsequent messages and files related to the designated matter.

End-user supervision. Leveraging our flexible workflow capabilities, Proofpoint Enterprise Archive analyzes all electronic communications, including email and communications from leading instant messaging and social networking sites, for potential violations of regulations, such as those imposed by Financial Industry Regulatory Authority ("FINRA") and the SEC in the financial services industry.

Key benefits of Proofpoint Information Protection and Archiving include:

Regulatory compliance. Data Loss Prevention and Encryption enable outbound messages to comply with national and state government and industry-specific privacy regulations, while Enterprise Archive helps organizations meet regulatory requirements by archiving all messages and content according to compliance retention policies and enabling staff to systematically review messages for compliance supervision.

Superior malicious and accidental data loss protection. Protects against the loss of sensitive data, whether from a cybercriminal attempting to exfiltrate valuable data from a compromised system, or from an employee accidentally distributing a file to the wrong party through email, webmail, social media, file sharing, or other Internet-based mechanisms for publishing content.

Easy-to-use secure communication. Allows corporate end-users to easily share sensitive data without compromising security and privacy, and enables authorized external recipients to transparently decrypt and read the communications from any device. Our mobile-optimized interfaces provide an easy experience for the rapidly growing number of recipients on smartphones and tablets.

Reduction in "attack surface". Enables the automated protection of sensitive data, reducing the amount of critical information potentially exposed to an attacker in a breach scenario.

Proactive data governance. Allows organizations to create, maintain and consistently enforce a clear corporate data retention policy, reducing the risk of data loss and the cost of eDiscovery.

Efficient litigation support. Provides advanced search features that reduce the cost of eDiscovery and allow organizations to more effectively manage the litigation hold process.

Reduced storage and management costs. Helps to simplify mailbox and file system management by automatically moving storage-intensive attachments and files into cost-effective cloud storage.

Proofpoint Digital Risk Protection

Proofpoint Digital Risk Protection looks beyond the enterprise perimeter to deliver real-time, omnichannel digital risk discovery and protection from brand fraud, data loss, physical threats, and cyber threats. With this solution, enterprises can engage with their customers across web, email, mobile, and social media with the confidence that their brands and customers are safe from all forms of digital risk.

The key features of the Digital Risk product family include:

8

Table of Contents

Detecting Brand Fraud. Fraudsters imitate companies' brands across digital channels to target customers with phishing scams, malware, phishing, and counterfeit products. Using a native cloud-based platform, customers can quickly find fraudulent social media accounts, web domains, and mobile apps that are affiliated with their brands.

Detecting External Threats. External threat management tools enable organizations to quickly identify leaked intellectual property, credentials, and customer data on the web or dark web. Additionally, detection measures can identify cyber criminals using digital tools to plan and execute cyber-attacks that target company's digital presence and/or physical attacks on its executives, employees, and physical locations.

Compliance Monitoring and Protection. Leveraging social media APIs, the platform can monitor and apply content policies to the brand's owned social media accounts for security, compliance and acceptable use. Using proprietary Deep Social Linguistic Analysis technology, social media and brand managers can aggregate content from across their enterprise and review it for security, risk and compliance violations (including FINRA, Federal Financial Institutions Examination Council, Food and Drug Administration, SEC, Financial Conduct Authority violations), allowing them to safely syndicate content distribution across their social media marketing platforms.

Key benefits of Proofpoint Digital Risk Protection include:

Reduction of fraud. Enterprises can reduce both the direct and indirect costs relating to fraud by rapidly and proactively identifying fraudulent web domains, mobile apps, and social media accounts leveraged by cyber criminals in phishing and other forms of attacks.

Visibility into external threats. Organizations benefit from early warnings of potentially harmful threats to physical sites, digital presences, and key executives, as well as well as unauthorized posting or resale of their private data.

Enhanced compliance. Reduces potential liability from inadvertent posting of sensitive data and demonstrates compliance with more than 35 standards and industry regulations. Automates compliance review processes and social advocate programs through seamless integration with leading social media management suites.

Platform Services

Our platform services provide the key functionality to implement our various solutions, using our enabling technologies. Our platform services primarily consist of:

Threat detection. Proofpoint deploys an ensemble approach to detect both malware and malware-free attacks. The approach combines multiple forms of detection, including composite reputation correlation, sandboxing for malicious attachments, URLs, and credential phishing, code analysis, network detection, and classifiers for phishing and impostor/BEC attacks.

Threat intel extraction. Proofpoint leverages a dedicated environment to learn as much as possible about threats that are detected by any part of the ensemble approach. The extraction environment leverages virtual sandboxes, physical hardware, and human analysts to induce malware to detonate and gather as much forensic detail about it as possible.

Nexus threat graph. Proofpoint synthesizes threat intelligence gathered from the vectors and threat feeds in a graph database known as Proofpoint Nexus, which is leveraged by threat researchers to correlate threats into campaigns, analyze new threats for links to known actors, and lend context (e.g. what vertical industries are seeing a given campaign) to all detected threats.

•

Real-time detection. Proofpoint leverages platform services to be in the flow of the movement of potentially sensitive data, including our email gateways, API-based social media integrations, mobile applications store scanning tools, and SaaS application API/proxy connectivity.

Information classification. For regulated or otherwise sensitive data, Proofpoint leverages smart identifiers to accurately recognize data types that are relevant from either a security or compliance perspective.

Table of Contents

Intelligent policy. Proofpoint's information protection and archive products leverage an intelligent policy framework that spans retention, legal hold, smart identifiers, and compliance frameworks, regardless of where the data may be stored or by which channel it is being sent.

Enabling Technologies

Our enabling technologies are a proprietary set of building blocks that work in conjunction with our application services to enable the efficient construction, scaling and maintenance of our customer-facing solutions. These technologies primarily consist of:

• **Big data analytics.** Indexes and analyzes petabytes of information in real-time to discover threats, detect data leaks and enable end-users to quickly and efficiently access information distributed across their organizations.

• **Machine learning.** Builds predictive data models using our proprietary Proofpoint MLX machine learning techniques to rapidly identify and classify threats and sensitive content in real-time.

• **Identity and policy.** Enables the definition and enforcement of sophisticated data protection policies based on a wide set of variables, including type of content, sender, recipient, pending legal matters, time and date, regulatory status and more.

• **Secure storage.** Stores petabytes of data in the cloud cost-effectively using proprietary encryption methods, keeping sensitive data tamper-proof and private, yet fully searchable in real-time.

• **Virtual execution environments.** Exposes suspected malware to a permuted set of instrumented virtual system environments, to assess maliciousness, exploit activity and compromise processes.

• **Intelligent message routing.** Policies can be established by administrators to automatically direct email communications differently through the email network, based on aspects of the messages, for security, compliance, supervisory, system performance, or other reasons.

• **Threat intelligence correlation.** Utilizes inputs from Proofpoint, cloud, and other third-party products to assess IoCs and confirm successful system compromises by malicious actors in near-real-time, then administers network controls to effectively contain the compromised systems.

Infrastructure

We deliver our security-as-a-service solutions through our cloud architecture and international data center infrastructure. We operate thousands of physical and virtual servers across eleven data centers located in the United States, Canada, the Netherlands and Germany.

Our cloud architecture is optimized to meet the unique demands of delivering real-time security-as-a-service to global enterprises. Key design elements include:

• **Security.** Security is central to our cloud architecture and is designed into all levels of the system, including physical security, network security, application security, and security at our third-party data centers. Our security measures have met the rigorous standards of SSAE 16 certification. In addition to this commercial certification program, we have also successfully completed the FISMA certification for our cloud-based information protection and archiving solution, enabling us to serve the rigorous security requirements of U.S. federal agencies.

Scalability and performance. By leveraging a distributed, scalable architecture we process billions of requests against our reputation systems and hundreds of millions of messages per day, all in near real-time. Massively-parallel query processing technology is designed to ensure rapid search results over this vast data volume. In addition to this aggregate scalability across all customers, our architecture also scales to effectively meet the needs of several of our largest individual customers, each of which has millions of users and processes tens of millions of messages per day.

Table of Contents

Hybrid Deployment. Our cloud architecture enables individual customers to deploy entirely in Proofpoint's global data centers or in hybrid configurations with optional points of presence located behind the customer's firewall. This deployment flexibility enables us to deliver security, compliance and performance tailored to the unique threat profile and operating environment of each customer.

High availability. Our services employ a wide range of technologies including redundancy, geographic distribution, real-time data replication and end-to-end service monitoring to provide 24x7 system availability.

Network operations control. We employ a team of skilled professionals who monitor, manage and maintain our global data center infrastructure and its interoperability with the distributed points of presence located behind our customers' firewalls to ensure 24x7 operations.

Customers

As of December 31, 2016, we had customers of all sizes across a wide variety of industries. A number of our largest customers use our platform to protect more than a million users and handle over a billion messages per day. We have a highly diversified customer base, with one customer, a strategic partner serving a number of end customers with our platform, who accounted for 12% of total revenue in 2014. There were no single partners or customers that accounted for more than 10% of our total revenue in 2016 and 2015. In each year since the launch of our first solution in 2003, we have maintained a renewal rate with our existing customers of over 90%.

We target large and mid-sized organizations across all major verticals including aerospace and defense, education, financial services, government, healthcare, manufacturing and retail. We have been particularly successful selling to the largest enterprises in the United States as ranked by Fortune Magazine are our customers. We have also had success penetrating the market leaders in a number of significant verticals including:

4 of the 5 largest U.S. retailers

3 of the 5 largest U.S. aerospace and defense contractors

5 of the 5 largest U.S. banks

3 of the 5 largest global pharmaceutical companies

3 of the 5 largest U.S. petroleum refining companies

Sales and Marketing

Sales

We primarily target large and mid-sized organizations across all industries. Our sales and marketing programs are organized by geographic regions, including Asia-Pacific, EMEA, Japan, North America, and South America, and we further segment and organize our sales force into teams that focus on large enterprises (4,000 employees and above), mid-sized organizations (1,000 - 4,000 employees) and existing customers. In addition, we create integrated sales and marketing programs targeting specific vertical-markets. This vertical-market approach enables us to provide a higher level of service and understanding of our customers' unique needs, including the industry-specific business and regulatory requirements in industries such as healthcare, financial services, retail and education.

We sell through both direct and indirect channels, including technology and channel partners:

Direct sales and reseller channel. We market and sell our solutions to large and mid-sized customers directly through our field and inside sales teams as well as indirectly through a hybrid model, where our sales organization actively assists our network of distributors and resellers. Our sales personnel are primarily located in North America, with additional personnel located in Asia-Pacific, EMEA, Japan and South America. Our reseller partners maintain relationships with their customers throughout the territories in which they operate, providing them with services and third-party solutions to help meet their evolving security requirements. As such, these partners act as a direct conduit through which we can connect with these prospective customers to offer our solutions. Our channel partners include security centric resellers such as

Table of Contents

Adaptive Solutions, CDW, Forsythe Technology, Optiv, and SHI International, as well as distributors such as Ingram Micro and Exclusive Networks.

Strategic relationships. We also sell our solutions indirectly through key technology companies that offer our solutions in conjunction with one or more of their own products or services. These companies each have their own base of customers, and they distribute our products to augment their own branded products and solutions, sometimes under their own brand and sometimes under the Proofpoint brand.

For sales involving a partner such as a distributor, reseller or strategic partner, the partner engages with the prospective customer directly and involves our sales team as needed to assist in developing and closing an order. At the conclusion of a successful sales cycle, we sell the associated subscription, hardware and services to the partner who in turn resells these items to the customer, with the partner earning a margin based on the amount paid to Proofpoint as compared to the amount charged to the customer. With the order completed, we provide these customers with direct access to our security-as-a-service platform and other associated services, enabling us to establish a direct relationship and provide them with support as part of ensuring that the customer has a good experience with our platform. At the end of the contract term, the partner engages with the customer to execute a renewal order, with our team providing assistance as required.

Marketing

We have a number of marketing initiatives to build awareness about our solutions and encourage customer adoption of our solutions. Our marketing programs include a variety of digital marketing, advertising, conferences, events, white-papers, public relations activities and web-based seminar campaigns targeted at key decision makers within our prospective customers.

We offer free trials, competitive evaluations and free security and compliance risk assessments to allow prospective customers to experience the quality of our solutions, to learn in detail about the features and functionality of our suite, and to quantify the potential benefits of our solutions.

Customer Service and Support

We believe that our customer service and support provide a competitive advantage and are critical to retaining and expanding our customer base. We conduct regular third-party surveys to measure customer loyalty and satisfaction with our solutions.

Proofpoint Support Services

We deliver 24x7x365 customer support from support centers located in EMEA, North America and Asia-Pacific regions. We offer a wide range of support offerings with varying levels of access to our support resources.

Proofpoint Professional Services and Training

With our security-as-a-service model, our solutions are designed to be implemented, configured, and operated without the need for any training or professional services. For those customers that would like to develop deeper expertise in the use of our solutions or would like some assistance with complex configurations or the importing of data, we offer various training and professional services. Many implementation services can be completed in one day and are primarily provided remotely using web-based conferencing tools. If requested, our professional services organization also provides additional assistance with data importing, design, implementation, customization, or advanced reporting. We also offer a learning center for both in-person and online training and certification.

Research and Development

We devote significant resources to improve and enhance our existing security solutions and maintain the effectiveness of our platform. We also work closely with our customers to gain valuable insights into their threat environments and security management practices to assist us in designing new solutions and features that extend the data protection, archiving and governance capabilities of our platform. Our technical staff monitors and tests our software on a regular basis, and we maintain a regular release process to update and enhance our existing solutions. Leveraging our on-demand platform model, we can deploy real-time upgrades with no downtime.

Research and development expenses were \$98.5 million, \$74.5 million and \$51.9 million for 2016, 2015 and 2014, respectively.

Table of Contents

Competition

Our markets are highly competitive, fragmented and subject to rapid changes in technology. We compete primarily with companies that offer a broad array of data protection and governance solutions. Providers of data protection solutions generally have product offerings that include threat protection, virus protection, data loss prevention, flexible remediation, data encryption, and in some cases secure file transfer. Providers of archive solutions generally have product offerings that provide data storage, search, policy enforcement, legal-hold management, and in some cases supervision.

Key competitors include:

Email and Advanced Threat Protection: Cisco Systems, Inc. (through its acquisitions of IronPort, SourceFire, and ThreatGRID), Microsoft Corporation (through its acquisition of Frontbridge), FireEye, Inc., and Symantec Corporation (through its acquisitions of Brightmail and MessageLabs).

Archiving: Micro Focus International plc and Veritas Technologies LLC (through its acquisitions of KVS and LiveOffice while under the ownership of Symantec Corporation).

We believe we compete favorably based on the following factors:

- effectiveness of our protection against advanced threats;
- comprehensiveness and integration of the solution;
- flexibility of delivery models;
- total cost of ownership;
- scalability and performance;
- customer support; and
- extensibility of platform.

Certain of our competitors have greater sales, marketing and financial resources, more extensive geographic presence and greater name recognition than we do. We may face future competition in our markets from other large, established companies, as well as from emerging companies. In addition, we expect that there is likely to be continued consolidation in our industry that could lead to increased price competition and other forms of competition.

Intellectual Property

We rely on a combination of trade secrets, patents, copyrights and trademarks, as well as contractual protections, to establish and protect our intellectual property rights and protect our proprietary technology. As of December 31, 2016, we had 65 patents and 39 patent applications. We have a number of registered and unregistered trademarks. We require our employees, consultants and other third parties to enter into confidentiality and proprietary rights agreements and control access to software, documentation and other proprietary information. Although we rely on intellectual property rights, including trade secrets, patents, copyrights and trademarks, as well as contractual protections to establish and protect our proprietary rights, we believe that factors such as the technological and

creative skills of our personnel, creation of new modules, features and functionality, and frequent enhancements to our solutions are more essential to establishing and maintaining our technology leadership position.

Despite our efforts to protect our proprietary technology and our intellectual property rights, unauthorized parties may attempt to copy or obtain and use our technology to develop products with the same functionality as our solution. Policing unauthorized use of our technology and intellectual property rights is difficult.

We expect that software and other solutions in our industry may be subject to third-party infringement claims as the number of competitors grows and the functionality of products in different industry segments overlaps. Any of these third parties might make a claim of infringement against us at any time.

Table of Contents

Employees

As of December 31, 2016, we had 1,573 employees. We also engage a number of temporary employees and consultants. None of our employees is represented by a labor union with respect to his or her employment with us. We have not experienced any work stoppages and we consider our relations with our employees to be good. Our future success will depend upon our ability to attract and retain qualified personnel. Competition for qualified personnel remains intense and we may not be successful in retaining our key employees or attracting skilled personnel.

Corporate Information

We were incorporated in Delaware in 2002. Our principal executive offices are located at 892 Ross Drive, Sunnyvale, California 94089, and our telephone number is +1 (408) 517-4710. Our website is www.proofpoint.com.

Proofpoint, the Proofpoint logo, all of our product names and our other registered or common law trademarks, service marks, or trade names appearing in this Annual Report on Form 10-K are our property. Other trademarks appearing in this prospectus are the property of their respective holders.

Geographic Information

For financial reporting purposes, net revenue and long-lived assets attributable to significant geographic areas are presented in Note 11, "Segment Reporting", to the consolidated financial statements, which is incorporated herein by reference.

Available Information

We file annual reports on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, proxy and information statements and amendments to reports filed or furnished pursuant to Sections 13(a), 14 and 15(d) of the Securities Exchange Act of 1934, as amended. The SEC also maintains a website at <http://www.sec.gov> that contains reports, proxy and information statements and other information regarding Proofpoint and other companies that file materials with the SEC electronically. The public may also obtain these filings at the Securities and Exchange Commission ("SEC")'s Public Reference Room at 100 F Street, NE, Washington, DC 20549 or by calling the SEC at 1-800-SEC-0330. Copies of Proofpoint's reports on Form 10-K, definitive Proxy Statements, Forms 10-Q and Forms 8-K, may be obtained, free of charge, electronically through our Internet website, <http://investors.proofpoint.com/financials.cfm>, or by sending an electronic message by visiting the Contact Us section within the investor relations portion of our website.

Table of Contents

ITEM 1A. RISK FACTORS

Investing in our common stock involves a high degree of risk. You should carefully consider the following risk factors, as well as the other information in this Annual Report on Form 10-K, before deciding whether to invest in shares of our common stock. The occurrence of any of the events described below could harm our business, financial condition, results of operation and growth prospects. In such an event, the trading price of our common stock may decline and you may lose all or part of your investment.

Risks Related to Our Business and Industry

We have a history of losses, and we are unable to predict the extent of any future losses or when, if ever, we will achieve profitability in the future.

We have incurred net losses in every year since our inception, including net losses of \$111.2 million, \$98.7 million and \$60.1 million in 2016, 2015 and 2014, respectively. As a result, we had an accumulated deficit of \$469.1 million as of December 31, 2016. Achieving profitability will require us to increase revenue, manage our cost structure, and avoid unanticipated liabilities. We do not expect to be profitable in the near term. Revenue growth may slow or revenue may decline for a number of possible reasons, including slowing demand for our solutions, increasing competition, a decrease in the growth of our overall market, or if we fail for any reason to continue to capitalize on growth opportunities. Any failure by us to obtain and sustain profitability, or to continue our revenue growth, could cause the price of our common stock to decline significantly.

Our quarterly operating results are likely to vary significantly and be unpredictable, which could cause the trading price of our stock to decline.

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

- the level of demand for our solutions, including our newly-introduced solutions, and the level of perceived urgency regarding security threats and compliance requirements;
- the timing of new subscriptions and renewals of existing subscriptions;
- the mix of solutions sold;
- the extent to which customers subscribe for additional solutions or increase the number of users;
- customer budgeting cycles and seasonal buying patterns;
- the extent to which we bring on new distributors;
- any changes in the competitive landscape of our industry, including consolidation among our competitors, customers, partners or resellers;
- timing of costs and expenses during a quarter;
- deferral of orders in anticipation of new solutions or enhancements announced by us;
- price competition;

- changes in renewal rates and terms in any quarter;
- the impact of acquisitions;
- litigation costs;
- any disruption in our sales channels or termination of our relationship with strategic channel partners;
- general economic conditions, both domestically and in our foreign markets, and related changes to currency exchange rates;

15

Table of Contents

- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions; or
- future accounting pronouncements or changes in our accounting policies.

Any one of the factors above or the cumulative effect of some of the factors referred to above may result in significant fluctuations in our financial and other operating results, including fluctuations in our key metrics. This variability and unpredictability could result in our failing to meet the expectations of securities analysts or investors for any period. If we fail to meet or exceed such expectations for these or any other reasons, the market price of our shares could fall substantially and we could face costly lawsuits, including securities class action suits. In addition, a significant percentage of our operating expenses are fixed in nature and based on forecasted revenue and cash flow trends. Accordingly, in the event of revenue shortfalls, we are generally unable to mitigate the negative impact on margins or other operating results in the short term.

We may fail to meet or exceed the expectations of securities analysts and investors, and the market price for our common stock could decline. If one or more of the securities analysts who cover us change their recommendation regarding our stock adversely, the market price for our common stock could decline. Additionally, our stock price may be based on expectations, estimates or forecasts of our future performance that may be unrealistic or may not be achieved. Further, our stock price may be affected by financial media, including press reports and blogs.

If we are unable to maintain high subscription renewal rates, our future revenue and operating results will be harmed. Our customers have no obligation to renew their subscriptions for our solutions after the expiration of their initial subscription period, which typically ranges from one to three years. In addition, our customers may renew for fewer subscription services or users, renew for shorter contract lengths or renew at lower prices due to competitive or other pressures. We cannot accurately predict renewal rates and our renewal rates may decline or fluctuate as a result of a number of factors, including competition, customers' IT budgeting and spending priorities, and deteriorating general economic conditions. If our customers do not renew their subscriptions for our solutions, our revenue would decline and our business would suffer.

If we are unable to sell additional solutions to our customers, our future revenue and operating results will be harmed. Our future success depends on our ability to sell additional solutions to our customers. 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 solutions depends on a number of factors, including the perceived need for additional solutions, growth in the number of end-users, and general economic conditions. If our efforts to sell additional solutions to our customers are not successful, our business may suffer.

If our solutions fail to protect our customers from security breaches, our brand and reputation could be harmed, which could have a material adverse effect on our business and results of operations.

The threats facing our customers are constantly evolving and the techniques used by attackers to access or sabotage data change frequently. As a result, we must constantly update our solutions to respond to these threats. If we fail to update our solutions in a timely or effective manner to respond to these threats, our customers could experience security breaches. Many federal, state and foreign governments have enacted laws requiring companies to notify individuals of data security breaches involving their personal data. These mandatory disclosures regarding a security breach often lead to widespread negative publicity, and any association of us with such publicity may cause our customers to lose confidence in the effectiveness of our data security measures. Any security breach at one of our customers or even an unproven allegation of a security breach at one of our customers, could harm our reputation as a secure and trusted company and could cause the loss of customers. Similarly, if a well-publicized breach of data security at a customer of any other cloud based data protection or archiving service provider or other major enterprise

cloud services provider were to occur, there could be a loss of confidence in the cloud based storage of sensitive data and information generally.

In addition, our solutions work in conjunction with a variety of other elements in customers' IT and security infrastructure, and we may receive blame and negative publicity for a security breach that may have been the result of the failure of one of the other elements not provided by us. The occurrence of a breach, whether or not caused by our solutions, or allegations of a breach, even if such allegations turn out to be untrue, could delay or reduce market acceptance of our solutions and have an adverse effect on our business and financial performance. In addition, any revisions to our solutions that we believe may be necessary or appropriate in connection with any such breach may cause us to incur significant expenses. Any of

Table of Contents

these events could have material adverse effects on our brand and reputation, which could harm our business, financial condition, and operating results.

If our customers experience data losses, our brand, reputation and business could be harmed.

Our customers rely on our archive solutions to store their corporate data, which may include financial records, credit card information, business information, health information, other personally identifiable information or other sensitive personal information. A breach of our network security and systems or other events that cause the loss or public disclosure of, or access by third parties to, our customers' stored files or data could have serious negative consequences for our business, including possible fines, penalties and damages, reduced demand for our solutions, an unwillingness of our customers to use our solutions, harm to our brand and reputation, and time-consuming and expensive litigation. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently, often are not recognized until launched against a target, and may originate from less regulated or remote areas around the world. As a result, we may be unable to proactively prevent these techniques, implement adequate preventative or reactionary measures, or enforce the laws and regulations that govern such activities. In addition, because of the large amount of data that we collect and manage, it is possible that hardware failures, human errors or errors in our systems could result in data loss or corruption, or cause the information that we collect to be incomplete or contain inaccuracies that our customers regard as significant. If our customers experience any data loss, or any data corruption or inaccuracies, whether caused by security breaches or otherwise, our brand, reputation and business would be harmed.

Our errors and omissions insurance may be inadequate or may not be available in the future on acceptable terms, or at all. In addition, our policy may not cover any claim against us for loss of data or other indirect or consequential damages. Defending a suit based on any data loss or system disruption, regardless of its merit, could be costly and divert management's attention.

Defects or vulnerabilities in our solutions could harm our reputation, reduce the sales of our solutions and expose us to liability for losses.

Because our solutions are complex, undetected errors, failures or bugs may occur, especially when solutions are first introduced or when new versions or updates are released, or when we introduce an acquired company's products or services, despite our efforts to test those solutions and enhancements prior to release. We may not be able to correct defects, errors, vulnerabilities or failures promptly, or at all.

Any defects, errors, vulnerabilities or failures in our solutions could result in:

- expenditure of significant financial and development resources in efforts to analyze, correct, eliminate or work around errors or defects or to address and eliminate vulnerabilities;
- loss of existing or potential partners or customers;
- loss or disclosure of our customers' confidential information, or the inability to access such information;
- loss of our proprietary technology;
- our solutions being susceptible to hacking or electronic break-ins or otherwise failing to secure data;
- delayed or lost revenue;
- delay or failure to attain market acceptance;
- lost market share;
- negative publicity, which could harm our reputation; or
- litigation, regulatory inquiries or investigations that would be costly and harm our reputation.

Limitation of liability provisions in our standard terms and conditions and our other agreements may not adequately or effectively protect us from any claims related to defects, errors, vulnerabilities or failures in our solutions, including as a result of federal, state or local laws or ordinances or unfavorable judicial decisions in the United States or other countries.

Table of Contents

Because we provide security solutions, our software, website and internal systems may be subject to intentional disruption that could adversely impact our reputation and future sales.

We could be a target of attacks specifically designed to impede the performance of our solutions and harm our reputation. Similarly, experienced computer hackers may attempt to penetrate our network security or the security of our website and misappropriate proprietary information and/or cause interruptions of our services. Because the techniques used by such computer hackers to access or sabotage networks change frequently and may not be recognized until launched against a target, we may be unable to anticipate these techniques. If an actual or perceived breach of network security occurs, it could adversely affect the market perception of our solutions, and may expose us to the loss of information, litigation and possible liability. In addition, such a security breach could impair our ability to operate our business, including our ability to provide support services to our customers.

Our solutions collect, filter and archive customer data which may contain personal information, which raises privacy concerns and could result in us having liability or inhibit sales of our solutions.

Many federal, state and foreign government bodies and agencies have adopted or are considering adopting laws and regulations regarding the collection, use, and disclosure of personal information. Because many of the features of our solutions use, store, and report on customer data which may contain personal information from our customers, any inability to adequately address privacy concerns, or comply with applicable privacy laws, regulations and policies could, even if unfounded, result in liability to us, damage to our reputation, loss of sales, and harm to our business. Furthermore, the costs of compliance with, and other burdens imposed by, such laws, regulations and policies that are applicable to the businesses of our customers may limit the use and adoption of our solutions and reduce overall demand for them. Privacy concerns, whether or not valid, may inhibit market adoption of our solutions. For example, in the United States regulations such as the Gramm Leach Bliley Act, which protects and restricts the use of consumer credit and financial information, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which regulates the use and disclosure of personal health information, impose significant security and data protection requirements and obligations on businesses that may affect the use and adoption of our solutions. The European Union's Data Protection Directive requires member states to impose restrictions on the collection and use of personal data that, in some respects, are more stringent, and impose more significant burdens on subject businesses, than current privacy standards in the United States.

In the past we have relied on the U.S.-European Union Frameworks, as agreed to by the U.S. Department of Commerce and the European Union ("EU") as one of the means to legally transfer European personal information from Europe to the United States. However, on October 6, 2015, the European Court of Justice invalidated the U.S.-EU Safe Harbor framework. On February 2, 2016, the U.S. and E.U. announced agreement on a new framework for transatlantic data flows entitled the EU-US Privacy Shield and Proofpoint self certified under the EU-US Privacy Shield framework on October 5, 2016. However, it is possible that Privacy Shield may be challenged in EU courts, so there is some uncertainty regarding its future validity and our ability to rely on it for EU to US data transfers. The uncertainty and changes in the requirements of these jurisdictions may increase the cost of compliance to provide services to EU based customers, reduce demand for our services from such customers, restrict our ability to offer services in certain locations, impact our customers' ability to deploy our solutions in Europe, or subject us to sanctions, including fines and a prohibition on data transfers, by EU data protection regulators. Furthermore, future decisions may result in different European data protection regulators applying differing standards for the transfer of personal data, which could result in increased regulation, cost of compliance and limitations on data transfer for us and our customers. These developments could harm our business, financial condition and results of operations.

The regulatory framework for privacy issues is evolving worldwide, and various government and consumer agencies and public advocacy groups have called for new regulation and changes in industry practices. It is possible that new laws and regulations will be adopted in the United States and internationally, or existing laws and regulations may be interpreted in new ways, that would affect our business. Complying with any new regulatory requirements could force

us to incur substantial costs or require us to change our business practices in a manner that could reduce our revenue or compromise our ability to effectively pursue our growth strategy.

Any failure or perceived failure to comply with laws and regulations may result in proceedings or actions against us by government entities or others, or could cause us to lose users and customers, which could potentially have an adverse effect on our business.

We operate in a highly competitive environment with large, established competitors, and our competitors may gain market share in the markets for our solutions that could adversely affect our business and cause our revenue to decline.

Table of Contents

Our traditional competitors include security focused software vendors, such as Symantec Corporation and Cisco Systems, Inc. ("Cisco"), which offer software products that directly compete with our solutions. In addition to competing with these vendors directly for sales to customers, we compete with them for the opportunity to have our solutions bundled with the product offerings of our strategic partners. Our competitors could gain market share from us if any of these partners replace our solutions with the products of our competitors or if these partners more actively promote our competitors' products over our solutions. In addition, software vendors who have bundled our solutions with theirs may choose to bundle their software with their own or other vendors' software, or may limit our access to standard product interfaces and inhibit our ability to develop solutions for their platform.

We also face competition from large technology companies, such as Google Inc., Micro Focus International plc and Microsoft Corporation. These companies are increasingly developing and incorporating into their products data protection and storage software that compete on various levels with our solutions. Our competitive position could be adversely affected to the extent that our customers perceive that the functionality incorporated into these products would replace the need for our solutions or that buying from one vendor would provide them with increased leverage and purchasing power and a better customer experience. We also face competition from independent security vendors such as FireEye, Inc. that offer network security products and many smaller companies that specialize in particular segments of the markets in which we compete.

Many of our competitors have greater financial, technical, sales, marketing or other resources than we do and consequently may have the ability to influence our customers to purchase their products instead of ours. Further consolidation within our industry or other changes in the competitive environment could also result in larger competitors that compete with us on several levels. In addition, acquisitions of smaller companies by large technology companies that specialize in particular segments of the markets in which we compete would result in increased competition from these large technology companies. If we are unsuccessful in responding to our competitors or to changing technological and customer demands, our competitive position and financial results could be adversely affected.

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

We continue to be substantially dependent on our sales force to obtain new customers and to sell additional solutions to our existing customers. We believe that 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. New hires require significant training and may take significant time before they achieve full productivity. Our recent hires and planned hires may not become as productive 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. If we are unable to hire and train sufficient numbers of effective sales personnel, or the sales personnel are not successful in obtaining new customers or increasing sales to our existing customer base, our business will be harmed.

Our sales cycle is long and unpredictable, and our sales efforts require considerable time and expense. As a result, our results are difficult to predict and may vary substantially from quarter to quarter, which may cause our operating results to fluctuate.

We sell our security and compliance offerings primarily to enterprise IT departments that are managing a growing set of user and compliance demands, which has increased the complexity of customer requirements to be met and confirmed in the sales cycle. Increasingly, we have found that increasingly security, legal and compliance departments are involved in testing, evaluating and finally approving purchases, which has also made the sales cycle longer and less predictable. We may not be able to accurately predict or forecast the timing of sales, which makes our future

revenue difficult to predict and could cause our results to vary significantly. In addition, we might devote substantial time and effort to a particular unsuccessful sales effort, and as a result we could lose other sales opportunities or incur expenses that are not offset by an increase in revenue, which could harm our business.

Our cash flow is dependent in part upon our average contract durations, so significant shortening of our average contract durations may cause significant negative impact to our operating results.

With the majority of our business, we invoice our customers for the entire contract amount at the start of the term and these amounts are recorded as deferred revenue on our balance sheet, with the dollar weighted average duration of these contracts for any given period over the past three years typically ranging from 14 to 20 months. As a result, while our practice of invoicing customers for the entire amount of the contract at the start of the term provides us with a relatively immediate

Table of Contents

contribution to cash flow, the revenue is recognized ratably over the term of the contract, and hence contributions toward operating income are realized over an extended period. If these average contract durations were to shorten significantly from their current range, it may cause us to experience less favorable cash flows as compared to our current operating condition, requiring us to seek additional sources of capital to fund our operations.

Because our long-term success depends, in part, on our ability to expand the sales of our platform to our customers located outside of the United States, our business will be increasingly susceptible to risks associated with international operations.

One key element of our growth strategy is to develop a worldwide customer base and expand our operations worldwide. Our international revenue keeps growing as we add employees, offices and customers internationally, particularly in Europe and Asia.

Operating in international markets requires significant resources and management attention and will subject us to regulatory, economic, political and competitive risks and competition that are different from those in the United States. Because of our limited experience with international operations, we cannot assure you that our international expansion efforts will be successful or that expected returns on such investments will be achieved in the future.

In addition, our international operations may fail to succeed due to other risks inherent in operating businesses internationally, including:

- fluctuations in currency exchange rates, which may cause our revenues and operating results to differ materially from expectations;
- our lack of familiarity with commercial and social norms and customs in other countries which may adversely affect our ability to recruit, retain and manage employees in these countries;
- difficulties and costs associated with staffing and managing foreign operations;
- the potential diversion of management's attention to oversee and direct operations that are geographically distant from our U.S. headquarters;
- compliance with multiple, conflicting and changing governmental laws and regulations, including employment, tax, privacy and data protection laws and regulations;
- legal systems in which our ability to enforce and protect our rights may be different or less effective than in the United States, including more limited protection for intellectual property rights in some countries;
- immaturity of compliance regulations in other jurisdictions, which may lower demand for our solutions;
- greater difficulty with payment collections and longer payment cycles;
- higher employee costs and difficulty terminating non-performing employees;
- differences in work place cultures;
- the need to adapt our solutions for specific countries;
- our ability to comply with differing technical and certification requirements outside the United States;
- tariffs, export controls and other non-tariff barriers such as quotas and local content rules;
- uncertainties related to the United Kingdom's withdrawal from the European Union;
- adverse tax consequences;
- restrictions on the transfer of funds;
- anti-bribery compliance by us or our partners, including under the Foreign Corrupt Practices Act and similar laws of other jurisdictions; and
- new and different sources of competition.

Table of Contents

Our failure to manage any of these risks successfully could harm our existing and future international operations and seriously impair our overall business.

If we are unable to enhance our existing solutions and develop new solutions, our growth will be harmed and we may not be able to achieve profitability.

Our ability to attract new customers and increase revenue from existing customers will depend in large part on our ability to enhance and improve our existing solutions and to introduce new solutions. The success of any enhancement or new solution depends on several factors, including the timely completion, introduction and market acceptance of the enhancement or solution. Any new enhancement or solution we develop or acquire may not be introduced in a timely or cost-effective manner and may not achieve the broad market acceptance necessary to generate significant revenue. If we are unable to successfully develop or acquire new solutions or enhance our existing solutions to meet customer requirements, we may not grow as expected and we may not achieve profitability.

We cannot be certain that our development activities will be successful or that we will not incur delays or cost overruns. Furthermore, we may not have sufficient financial resources to identify and develop new technologies and bring enhancements or new solutions to market in a timely and cost-effective manner. New technologies and enhancements could be delayed or cost more than we expect, and we cannot ensure that any of these solutions will be commercially successful if and when they are introduced.

If we are unable to cost-effectively scale or adapt our existing architecture to accommodate increased traffic, technological advances or changing customer requirements, our operating results could be harmed.

As our customer base grows, the number of users accessing our solutions over the Internet will correspondingly increase. Increased traffic could result in slow access speeds and response times. Since our customer agreements often include service availability commitments, slow speeds or our failure to accommodate increased traffic could result in breaches of our service level agreements or obligate us to issue service credits. In addition, the market for our solutions is characterized by rapid technological advances and changes in customer requirements. In order to accommodate increased traffic and respond to technological advances and evolving customer requirements, we expect that we will be required to make future investments in our network architecture. If we do not implement future upgrades to our network architecture cost-effectively, or if we experience prolonged delays or unforeseen difficulties in connection with upgrading our network architecture, our service quality may suffer and our operating results could be harmed.

If we fail to manage our sales and distribution channels effectively or if our partners choose not to market and sell our solutions to their customers, our operating results could be adversely affected.

We have derived and anticipate that in the future we will continue to derive a substantial portion of the sales of our solutions through channel partners. In order to scale our channel program to support growth in our business, it is important that we continue to help our partners enhance their ability to independently sell and deploy our solutions. We may be unable to continue to successfully expand and improve the effectiveness of our channel sales program.

Our agreements with our channel partners are generally non-exclusive and some of our channel partners have entered, and may continue to enter, into strategic relationships with our competitors or are competitors themselves. Further, many of our channel partners have multiple strategic relationships and they may not regard us as significant for their businesses. Our channel partners may terminate their respective relationships with us with limited or no notice and with limited or no penalty, pursue other partnerships or relationships, or attempt to develop or acquire products or services that compete with our solutions. Our partners also may impair our ability to enter into other desirable strategic relationships. If our channel partners do not effectively market and sell our solutions, if they choose to place greater emphasis on products of their own or those offered by our competitors, or if they fail to meet the needs of our customers, our ability to grow our business and sell our solutions may be adversely affected. Similarly, the loss of a substantial number of our channel partners, and our possible inability to replace them, the failure to recruit additional

channel partners, any reduction or delay in their sales of our solutions, or any conflicts between channel sales and our direct sales and marketing activities could materially and adversely affect our results of operations.

Because we recognize revenue from subscriptions over the term of the relevant service period, decreases or increases in sales are not immediately reflected in full in our operating results.

21

Table of Contents

We recognize revenue from subscriptions over the term of the relevant service period, which typically range from one to three years, with some up to five years. As a result, most of our quarterly revenue from subscriptions results from agreements entered into during previous quarters. Consequently, a shortfall in demand for our solutions in any quarter may not significantly reduce our subscription revenue for that quarter, but could negatively affect subscription revenue in future quarters. We may be unable to adjust our cost structure to compensate for this potential shortfall in subscription revenue. Accordingly, the effect of significant downturns in sales of subscriptions may not be fully reflected in our results of operations until future periods. Our subscription model also makes it difficult for us to rapidly increase our subscription revenue through additional sales in any period, as subscription revenue must be recognized over the term of the contract.

Interruptions or delays in services provided by third parties could impair the delivery of our service and harm our business.

We currently serve our customers from third party data center facilities and resources located in the United States, Canada and Europe. We also rely on bandwidth providers, Internet service providers, and mobile networks to deliver our solutions. Any damage to, or failure of, the systems of our third party providers could result in interruptions to our service. If for any reason our arrangement with one or more of our data centers is terminated we could experience additional expense in arranging for new facilities and support. Our data center facilities providers have no obligations to renew their agreements with us on commercially reasonable terms, or at all. If we are unable to renew our agreements with the facilities providers on commercially reasonable terms or if in the future we add additional data center facility providers, we may experience costs or downtime in connection with the transfer to, or the addition of, new data center facilities. In addition, the failure of our data centers to meet our capacity requirements could result in interruptions in the availability of our solutions, impair the functionality of our solutions or impede our ability to scale our operations. As we continue to add data centers, restructure our data management plans, and increase capacity in existing and future data centers, we may move or transfer our data and our customers' data. Despite precautions taken during such processes and procedures, any unsuccessful data transfers may impair the delivery of our service, and we may experience costs or downtime in connection with the transfer of data to other facilities.

We also depend on access to the Internet through third party bandwidth providers to operate our business. If we lose the services of one or more of our bandwidth providers, or if these providers experience outages, for any reason, we could experience disruption in delivering our solutions or we could be required to retain the services of a replacement bandwidth provider. Our business also depends on our customers having high-speed access to the Internet. Any Internet outages or delays could adversely affect our ability to provide our solutions to our customers.

The occurrence of an extended interruption of our or third party services for any reason could result in lengthy interruptions in our services or in the delivery of customers' email and require us to provide service credits, refunds, indemnification payments or other payments to our customers, and could also result in the loss of customers.

Any failure to offer high-quality technical support services may adversely affect our relationships with our customers and harm our financial results.

Once our solutions are deployed, our customers depend on our support organization to resolve any technical issues relating to our solutions. In addition, our sales process is highly dependent on our solutions and business reputation and on strong recommendations from our existing customers. Any failure to maintain high-quality technical support, or a market perception that we do not maintain high-quality support, could harm our reputation, adversely affect our ability to sell our solutions to existing and prospective customers, and harm our business, operating results and financial condition.

We offer technical support services with many of our solutions. We may be unable to respond quickly enough to accommodate short-term increases in customer demand for support services. We also may be unable to modify the format of our support services to compete with changes in support services provided by competitors. Increased customer demand for these services, without corresponding revenue, could increase costs and adversely affect our

operating results.

We have outsourced a substantial portion of our worldwide customer support functions to third party service providers. If these companies experience financial difficulties, do not maintain sufficiently skilled workers and resources to satisfy our contracts, or otherwise fail to perform at a sufficient level, the level of support services to our customers may be significantly disrupted, which could materially harm our reputation and our relationships with these customers.

If we fail to develop or protect our brand, our business may be harmed.

22

Table of Contents

We believe that developing and maintaining awareness and integrity of our company and our brand are important to achieving widespread acceptance of our existing and future offerings and are important elements in attracting new customers. We believe that the importance of brand recognition will increase as competition in our market further intensifies. Successful promotion of our brand will depend on the effectiveness of our marketing efforts and on our ability to provide reliable and useful solutions at competitive prices. We plan to continue investing substantial resources to promote our brand, both domestically and internationally, but there is no guarantee that our brand development strategies will enhance the recognition of our brand. Some of our existing and potential competitors have well-established brands with greater recognition than we have. If our efforts to promote and maintain our brand are not successful, our operating results and our ability to attract and retain customers may be adversely affected. In addition, even if our brand recognition and loyalty increases, this may not result in increased use of our solutions or higher revenue.

In addition, independent industry analysts often provide reviews of our solutions, as well as those of our competitors, and perception of our solutions in the marketplace may be significantly influenced by these reviews. We have no control over what these industry analysts report, and because industry analysts may influence current and potential customers, our brand could be harmed if they do not provide a positive review of our solutions or view us as a market leader.

The steps we have taken to protect our intellectual property rights may not be adequate.

We rely on a combination of contractual rights, trademarks, trade secrets, patents and copyrights to establish and protect our intellectual property rights. These offer only limited protection, however, and the steps we have taken to protect our proprietary technology may not deter its misuse, theft or misappropriation. Any of our patents, copyrights, trademarks or other intellectual property rights may be challenged by others or invalidated through administrative process or litigation. Competitors may independently develop technologies or products that are substantially equivalent or superior to our solutions or that inappropriately incorporate our proprietary technology into their products. Competitors may hire our former employees who may misappropriate our proprietary technology or misuse our confidential information. Although we rely in part upon confidentiality agreements with our employees, consultants and other third parties to protect our trade secrets and other confidential information, those agreements may not effectively prevent disclosure of trade secrets and other confidential information and may not provide an adequate remedy in the event of misappropriation of trade secrets or unauthorized disclosure of confidential information. In addition, others may independently discover our trade secrets and confidential information, and in such cases we could not assert any trade secret rights against such parties.

We might be required to spend significant resources to monitor and protect our intellectual property rights. We may initiate claims or litigation against third parties for infringement of our intellectual property rights or misappropriation of our trade secrets, or to establish the validity of our intellectual property rights. Any litigation, whether or not it is resolved in our favor, could result in significant expense to us and divert the efforts of our technical and management personnel, which may adversely affect our business, operating results and financial condition. Certain jurisdictions may not provide adequate legal infrastructure for effective protection of our intellectual property rights. Changing legal interpretations of liability for unauthorized use of our solutions or lessened sensitivity by corporate, government or institutional users to refraining from intellectual property piracy or other infringements of intellectual property could also harm our business.

Our issued patents may not provide us with any competitive advantages or may be challenged by third parties, and our patent applications may never be granted at all. It is possible that innovations for which we seek patent protection may not be protectable. Additionally, the process of obtaining patent protection is expensive and time consuming, and we may not be able to prosecute all necessary or desirable patent applications at a reasonable cost or in a timely manner. Given the cost, effort, risks and downside of obtaining patent protection, including the requirement to ultimately disclose the invention to the public, we may not choose to seek patent protection for certain innovations. However, such patent protection could later prove to be important to our business. Even if issued, there can be no assurance that any patents will have the coverage originally sought or adequately protect our intellectual property, as the legal standards relating to the validity, enforceability and scope of protection of patent and other intellectual property rights

are uncertain. Any patents that are issued may be invalidated or otherwise limited, or may lapse or may be abandoned, enabling other companies to better develop products that compete with our solutions, which could adversely affect our competitive business position, business prospects and financial condition.

We cannot assure you that the measures we have taken to protect our intellectual property will adequately protect us, and any failure to protect our intellectual property could harm our business.

Third parties claiming that we infringe their intellectual property rights could cause us to incur significant legal expenses and prevent us from selling our solutions.

Table of Contents

Companies in the software and technology industries, including some of our current and potential competitors, own large numbers of patents, copyrights, trademarks and trade secrets and frequently enter into litigation based on allegations of infringement, misappropriation or other violations of intellectual property rights. In addition, many of these companies have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them. The litigation may involve patent holding companies or other adverse patent owners who have no relevant product revenue and against whom our potential patents may provide little or no deterrence. We have received, and may in the future receive, notices that claim we have infringed, misappropriated or otherwise violated other parties' intellectual property rights. In the past we have been involved in litigation involving such allegations of infringement. To the extent we gain greater visibility, we could face a higher risk of being the subject of intellectual property infringement claims, which is not uncommon with respect to software technologies in general and information security technology in particular. There may be third party intellectual property rights, including issued or pending patents that cover significant aspects of our technologies or business methods. Any intellectual property claims, with or without merit, could be very time consuming, could be expensive to settle or litigate and could divert our management's attention and other resources. These claims could also subject us to significant liability for damages, potentially including treble damages if we are found to have willfully infringed patents or copyrights. These claims could also result in our having to stop using technology found to be in violation of a third-party's rights. We might be required to seek a license for the intellectual property, which may not be available on reasonable terms or at all. Even if a license were available, we could be required to pay significant royalties, which would increase our operating expenses. As a result, we may be required to develop alternative non-infringing technology, which could require significant effort and expense. If we cannot license or develop technology for any infringing aspect of our business, we would be forced to limit or stop sales of one or more of our solutions or features of our solutions and may be unable to compete effectively. Any of these results would harm our business, operating results and financial condition.

In addition, most of our agreements with customers and channel partners include indemnification provisions under which we agree to indemnify them for losses suffered or incurred as a result of claims of intellectual property infringement and, in some cases, for damages caused by us to property or persons. Large indemnity payments could harm our business, operating results and financial condition.

We rely on technology and intellectual property licensed from other parties, the failure or loss of which could increase our costs and delay or prevent the delivery of our solutions.

We utilize various types of software and other technology, as well as intellectual property rights, licensed from unaffiliated third parties in order to provide certain elements of our solutions. Any errors or defects in any third party technology could result in errors in our solutions that could harm our business. In addition, licensed technology and intellectual property rights may not continue to be available on commercially reasonable terms, or at all. While we believe that there are currently adequate replacements for the third party technology we use, any loss of the right to use any of this technology on commercially reasonable terms, or at all, could result in delays in producing or delivering our solutions until equivalent technology is identified and integrated, which delays could harm our business. In this situation we would be required to either redesign our solutions to function with software available from other parties or to develop these components ourselves, which would result in increased costs. Furthermore, we might be forced to limit the features available in our current or future solutions. If we fail to maintain or renegotiate any of these technology or intellectual property licenses, we could face significant delays and diversion of resources in attempting to develop similar or replacement technology, or to license and integrate a functional equivalent of the technology.

Some of our solutions contain "open source" software, and any failure to comply with the terms of one or more of these open source licenses could negatively affect our business.

Some of our solutions are distributed with software licensed by its authors or other third parties under so-called “open source” licenses, which may include, by way of example, the GNU General Public License, or GPL, and the Apache License. Some of these licenses contain requirements that we make available source code for modifications or derivative works we create based upon the open source software, and that we license such modifications or derivative works under the terms of a particular open source license or other license granting third parties certain rights of further use. By the terms of certain open source licenses, we could be required to release the source code of our proprietary software, and to make our proprietary software available under open source licenses, if we combine our proprietary software with open source software in a certain manner. In the event that portions of our proprietary software are determined to be subject to an open source license, we could be required to publicly release the affected portions of our source code, re-engineer all or a portion of our technologies, or otherwise be limited in the licensing of our technologies, each of which could reduce or eliminate the value of our technologies and solutions. In addition to risks related to license requirements, usage of open source software can lead to greater risks than use of third-party commercial software, as open source licensors generally do not provide warranties or controls on the origin

Table of Contents

of the software. We have established processes to help alleviate these risks, including a review process for screening requests from our development organizations for the use of open source software, but we cannot be sure that all open source software is submitted for approval prior to use in our solutions, that our programmers have not incorporated open source software into our proprietary solutions and technologies or that they will not do so in the future. In addition, many of the risks associated with usage of open source software cannot be eliminated, and could, if not properly addressed, negatively affect our business.

Governmental regulations affecting the export of certain of our solutions could negatively affect our business. Some of our products are subject to U.S. export controls, and we incorporate encryption technology into certain of our products. These encryption products and the underlying technology may be exported outside the United States only with the required export authorizations, including by license, a license exception or other appropriate government authorizations, including the filing of an encryption registration. Governmental regulation of encryption technology and regulation of imports or exports, or our failure to obtain required import or export approval for our products, could harm our international sales and adversely affect our revenue.

Failure to comply with such regulations, whether by us or companies that we have acquired, in the future could result in penalties, costs, and restrictions on export privileges, which could also harm our operating results.

We have and may further expand through acquisitions of, or investments in, other companies, which may divert our management's attention, dilute our stockholders and consume corporate resources that otherwise would be necessary to sustain and grow our business.

We have made multiple acquisitions in the past, and our business strategy may, from time to time, continue to include acquiring complementary products, technologies or businesses. We also may enter into relationships with other businesses in order to expand our solutions, which could involve preferred or exclusive licenses, additional channels of distribution, or investments by or between the two parties. Negotiating these transactions can be time consuming, difficult and expensive, and our ability to close these transactions may be subject to third party approvals, such as government regulation, which are beyond our control. Consequently, we can make no assurance that these transactions, once undertaken and announced, will close.

These transactions may result in unforeseen operating difficulties and expenditures. In particular, we may encounter difficulties assimilating or integrating the businesses, technologies, products, personnel or operations of acquired companies, particularly if the key personnel of the acquired business choose not to work for us, and we may have difficulty retaining the customers of any acquired business. Acquisitions may also disrupt our ongoing business, divert our resources and require significant management attention that would otherwise be available for development of our business. Any acquisition or investment could expose us to unknown liabilities.

In addition, as of December 31, 2016, we had \$229.0 million of goodwill and intangible assets, net of accumulated amortization, recorded on our consolidated balance sheet. We will incur expenses related to the amortization of intangible assets and we may in the future need to incur charges with respect to the impairment of goodwill or intangible assets, which could adversely affect our operating results. Moreover, we cannot assure you that the anticipated benefits of any acquisition or investment would be realized or that we would not be exposed to unknown liabilities. In connection with these types of transactions, we may issue additional equity securities that would dilute our stockholders' ownership interests, use cash that we may need in the future to operate our business, incur debt on terms unfavorable to us or that we are unable to repay, incur large charges or substantial liabilities, encounter difficulties integrating diverse business cultures, and become subject to adverse tax consequences, substantial depreciation or deferred compensation charges. These challenges related to acquisitions or investments could adversely affect our business, operating results and financial condition.

If we are unable to attract and retain qualified employees, lose key personnel, fail to integrate replacement personnel successfully, or fail to manage our employee base effectively, we may be unable to develop new and enhanced solutions, effectively manage or expand our business, or increase our revenue.

Our future success depends upon our ability to recruit and retain key management, technical, sales, marketing, finance, and other critical personnel. Competition for qualified management, technical and other personnel is intense,

and we may not be successful in attracting and retaining such personnel. If we fail to attract and retain qualified employees, our ability to grow our business could be harmed. Our officers and other key personnel are employees-at-will, and we cannot assure you that we

25

Table of Contents

will be able to retain them. Competition for people with the specific skills that we require is significant. In order to attract and retain personnel in a competitive marketplace, we believe that we must provide a competitive compensation package, including cash and equity based compensation. Volatility in our stock price may from time to time adversely affect our ability to recruit or retain employees. If we are unable to hire and retain qualified employees, or conversely, if we fail to manage employee performance or reduce staffing levels when required by market conditions, our business and operating results could be adversely affected.

In addition, hiring, training, and successfully integrating replacement personnel could be time consuming, may cause additional disruptions to our operations, and may be unsuccessful, which could negatively impact future revenue.

Changes in laws and/or regulations related to the Internet or changes in the Internet infrastructure itself may diminish the demand for our solutions, and could have a negative impact on our business.

The future success of our business depends upon the continued use of the Internet as a primary medium for commerce, communication and business applications. Federal, state or foreign government bodies or agencies have in the past adopted, and may in the future adopt, laws or regulations affecting data privacy and the use of the Internet as a commercial medium. Changes in these laws or regulations could require us to modify our solutions in order to comply with these changes. In addition, government agencies or private organizations may begin to impose taxes, fees or other charges for accessing the Internet or commerce conducted via the Internet. These laws or charges could limit the growth of Internet related commerce or communications generally, result in a decline in the use of the Internet and the viability of Internet based applications such as ours and reduce the demand for our solutions.

The legal and regulatory framework also drives demand for our solutions. Our customers are subject to laws, regulations and internal policies that mandate how they process, handle, store, use and transmit a variety of sensitive data and communications. These laws and regulations are subject to revision, change and interpretation at any time, and any such change could either help or hurt the demand for our solutions. We cannot be sure that the legal and regulatory framework in any given jurisdiction will be favorable to our business or that we will be able to sustain or grow our business if there are any adverse changes to these laws and regulations.

If we are required to collect sales and use taxes on the solutions we sell, we may be subject to liability for past sales and our future sales may decrease.

State and local taxing jurisdictions have differing rules and regulations governing sales and use taxes, and these rules and regulations are subject to varying interpretations that may change over time. In particular, the applicability of sales taxes to our subscription services in various jurisdictions is unclear. It is possible that we could face sales tax audits and that our liability for these taxes could exceed our estimates as state tax authorities could still assert that we are obligated to collect additional amounts as taxes from our customers and remit those taxes to those authorities. We could also be subject to audits with respect to state and international jurisdictions for which we have not accrued tax liabilities. A successful assertion that we should be collecting additional sales or other taxes on our services in jurisdictions where we have not historically done so and do not accrue for sales taxes could result in substantial tax liabilities for past sales, discourage customers from purchasing our application or otherwise harm our business and operating results.

Adverse conditions in the national and global economies and financial markets may adversely affect our business and financial results.

Our financial performance depends, in part, on the state of the economy, which deteriorated in the recent broad recession, and which may deteriorate in the future. Challenging economic conditions worldwide have from time to time contributed, and may continue to contribute, to slowdowns in the information technology industry, resulting in reduced demand for our solutions as a result of continued constraints on IT-related capital spending by our customers and increased price competition for our solutions. Moreover, we target some of our solutions to the financial services

industry and therefore if there is consolidation in that industry, or layoffs, or lack of funding for IT purchases, our business may suffer. If unfavorable economic conditions continue or worsen, our business, financial condition and operating results could be materially and adversely affected.

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

Table of Contents

Natural disasters or other catastrophic events may cause damage or disruption to our operations, international commerce and the global economy, and thus could have a strong negative effect on us. We have significant operations in the Silicon Valley area of Northern California, a region known for seismic activity. A major earthquake or other natural disaster, fire, act of terrorism or other catastrophic event that results in the destruction or disruption of any of our critical business operations or information technology systems could severely affect our ability to conduct normal business operations and, as a result, our future operating results could be harmed. These negative events could make it difficult or impossible for us to deliver our services to our customers, and could decrease demand for our services. Because we do not carry earthquake insurance for direct quake related losses, and significant recovery time could be required to resume operations, our financial condition and operating results could be materially adversely affected in the event of a major earthquake or catastrophic event.

A portion of our revenue is generated by sales to government entities, which are subject to a number of challenges and risks.

Sales to U.S. and foreign federal, state and local governmental agency customers have accounted for a portion of our revenue in past periods, and we may in the future increase sales to government entities. Sales into government entities are subject to a number of risks. Selling to government entities can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that we will win a sale. We have invested in the creation of a cloud offering that has been certified under both the Federal Information Security Management Act and the Federal Risk and Authorization Management Program for government usage but we cannot be sure that we will continue to sustain or renew this certification, that the government will continue to mandate such certification or that other government agencies or entities will use this cloud offering. Government demand and payment for our solutions may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our solutions. Government entities may have 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. For example, if the distributor receives a significant portion of its revenue from sales to such governmental entity, the financial health of the distributor could be substantially harmed, which could negatively affect our future sales to such distributor. Governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our solutions, a reduction of revenue or fines or civil or criminal liability if the audit uncovers improper or illegal activities. Any such penalties could adversely impact our results of operations in a material way.

If we fail to maintain an effective system of internal controls, our ability to produce timely and accurate financial statements or comply with applicable regulations could be impaired.

As a public company, we are subject to the reporting requirements of the Exchange Act, the Sarbanes Oxley Act of 2002 (the "Sarbanes-Oxley Act"), and the rules and regulations of the NASDAQ Global Market. We expect that the requirements of these rules and regulations will continue to increase our legal, accounting and financial compliance costs, make some activities more difficult, time consuming and costly, and place significant strain on our personnel, systems and resources.

The Sarbanes-Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We are continuing to develop and refine our disclosure controls and other procedures that are designed to ensure that information required to be disclosed by us in the reports that we file with the SEC, is recorded, processed, summarized and reported within the time periods specified in SEC rules and forms, and that information required to be disclosed in reports under the Exchange Act is accumulated and communicated to our principal executive and financial officers.

Our current controls and any new controls that we develop may become inadequate because of changes in conditions in our business. In addition, because we have acquired companies in the past and may continue to do so in the future, we will also need to expend resources to integrate the controls of these acquired entities with ours. Further, weaknesses in our internal controls may be discovered in the future. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our operating results or cause us to fail to meet our reporting obligations and may result in a restatement of our financial statements for prior periods. Any failure to implement and maintain effective internal controls also could adversely affect the results of periodic management evaluations and annual independent registered public accounting firm report regarding the effectiveness of our internal control over financial reporting that we are required to include in our Annual Report on Form 10-K under Section 404 of the Sarbanes Oxley Act. Ineffective disclosure controls and procedures and internal control over financial reporting could also cause investors to lose confidence in our reported financial and other information, which would likely have a negative effect on the trading price of our common stock.

In order to maintain and improve the effectiveness of our disclosure controls and procedures and internal control over financial reporting, we have expended, and anticipate that we will continue to expend, significant resources, including

Table of Contents

accounting related costs, and provide significant management oversight. Any failure to maintain the adequacy of our internal controls, or consequent inability to produce accurate financial statements on a timely basis, could increase our operating costs and could materially impair our ability to operate our business. In the event that we or our independent registered public accounting firm are not able to complete the work required under Section 404 of the Sarbanes-Oxley Act on a timely basis, or we are not able to demonstrate compliance with Section 404, we could be subject to late filings of our annual and quarterly reports, restatements of consolidated financial statements or other corrective disclosure, and, investors may lose confidence in our operating results and our stock price could decline. In addition, if we are unable to continue to meet these requirements, we may not be able to remain listed on the NASDAQ Global Market.

We may not be able to utilize a significant portion of our net operating loss or research tax credit carryforwards, which could adversely affect our profitability.

As of December 31, 2016, we had federal and state net operating loss carryforwards due to prior period losses, which if not utilized will begin or continue to expire in 2018 and 2017 for federal and state purposes, respectively. We also have federal research tax credit carryforwards, which if not utilized will begin to expire in 2022. These net operating loss and research tax credit carryforwards could expire unused and be unavailable to offset future income tax liabilities, which could adversely affect our profitability.

In addition, under Sections 382 and 383 of the Internal Revenue Code of 1986, as amended, our ability to utilize net operating loss carryforwards or other tax attributes, such as research tax credits, in any taxable year may be limited if we experience an “ownership change.” An “ownership change” generally occurs if one or more stockholders or groups of stockholders who own at least 5% of our stock increase their ownership by more than 50 percentage points over their lowest ownership percentage within a rolling three-year period. Similar rules may apply under state tax laws.

Future issuances of our stock could cause an “ownership change.” It is possible that any future ownership change could have a material effect on the use of our net operating loss carryforwards or other tax attributes, which could adversely affect our profitability.

We have been incurring significantly increased costs and devoting substantial management time as a result of operating as a public company.

As a public company, we incur significant legal, accounting and other expenses. For example, we are required to comply with certain of the requirements of the Sarbanes Oxley Act and the Dodd Frank Wall Street Reform and Consumer Protection Act, as well as rules and regulations subsequently implemented by the SEC, and the NASDAQ Global Market, our stock exchange, including the establishment and maintenance of effective disclosure and financial controls and changes in corporate governance practices. We expect that compliance with these requirements will continue to increase our legal and financial compliance costs and will make some activities more time consuming and costly. In addition, we expect that our management and other personnel will need to divert attention from operational and other business matters to devote substantial time to these public company requirements.

We have incurred and expect to continue to incur significant expenses and devote substantial management effort toward ensuring compliance with the requirements of Section 404 of the Sarbanes Oxley Act. We will need to hire additional accounting and financial staff with appropriate public company experience and technical accounting knowledge. We cannot predict or estimate the amount of additional costs we may incur as a public company or the timing of such costs.

Risks Related to the Ownership of Our Common Stock

Our stock price has been volatile in the past and may be subject to volatility in the future.

The trading prices of our common stock has been volatile historically, and is likely to continue to be subject to wide fluctuations in response to various factors described below. These factors, as well as the volatility of our common

stock, could also impact the price of our convertible notes. Factors affecting the market price of our securities include: variations in our revenue, billings, gross margin, operating results, free cash flow, loss per share and how these results compare to analyst expectations;

28

Table of Contents

• forward looking guidance that we may provide regarding financial metrics such as billings, revenue, gross margin, operating results, free cash flow, and loss per share;
• announcements of technological innovations, new products or services, strategic alliances, acquisitions or significant agreements by us or by our competitors;
• disruptions in our cloud-based operations or services or disruptions of other prominent cloud-based operations or services;
• the economy as a whole, market conditions in our industry, and the industries of our customers;
• trading activity by directors, executive officers and significant stockholders, or the perception in the market that the holders of a large number of shares intend to sell their shares;
• the size of our market float and significant option exercises;

• any future issuances of securities;

• sales and purchases of any common stock issued upon conversion of our convertible notes; and

• any other factors discussed herein.

In addition, the stock markets in general and the NASDAQ Global Market in particular, have experienced substantial price and volume volatility that is often seemingly unrelated to the operating results of any particular companies. Moreover, if the market for technology stocks, especially security and cloud computing-related stocks, or the stock market in general experiences uneven investor confidence, the market price of our common stock could decline for reasons unrelated to our business, operating results or financial condition. The market price for our stock might also decline in reaction to events that affect other companies within, or outside, our industry, even if these events do not directly affect us. Some companies that have experienced volatility in the trading price of their stock have been subject of securities litigation. If we are the subject of such litigation, it could result in substantial costs and a diversion of management's attention and resources.

We have indebtedness in the form of convertible senior notes.

In December 2013, we completed an offering of \$201.3 million aggregate principal amount of 1.25% convertible senior notes due 2018 and in June 2015, we completed an offering of \$230.0 million aggregate principal amount of 0.75% convertible senior notes due 2020. As a result of these convertible notes offerings, we incurred \$431.3 million principal amount of indebtedness, the principal amounts of which we may be required to pay at maturity in 2018 and 2020, or, upon the occurrence of a make-whole fundamental change (as defined in the indentures). There can be no assurance that we will be able to repay this indebtedness when due, or that we will be able to refinance this indebtedness on acceptable terms or at all. In addition, this indebtedness could, among other things:

• make it difficult for us to pay other obligations;

• make it difficult to obtain favorable terms for any necessary future financing for working capital, capital expenditures, debt service requirements or other purposes;

• require us to dedicate a substantial portion of our cash flow from operations to service the indebtedness, reducing the amount of cash flow available for other purposes; and

• limit our flexibility in planning for and reacting to changes in our business.

Conversion of our Notes may affect the price of our common stock and the value of the Notes.

The conversion of some or all of our Notes may dilute the ownership interest of existing stockholders to the extent we deliver shares of common stock upon conversion. Holders of the Notes will be able to convert them only upon the satisfaction of certain conditions prior to June 15, 2018 and December 15, 2019, as applicable. The notes due June 15, 2018 are now convertible upon the election on holders. Upon conversion, holders of the Notes will receive cash,

shares of common stock or a combination of cash and shares of common stock, at our election. Any sales in the public market of shares of common stock issued upon conversion of such Notes could adversely affect the trading price of our common stock and the value of the Notes.

Table of Contents

Anti-takeover provisions contained in our certificate of incorporation and bylaws, as well as provisions of Delaware law, could impair a takeover attempt.

Our certificate of incorporation and bylaws contain provisions that could have the effect of rendering more difficult, delaying or preventing an acquisition of our company deemed undesirable by our board of directors. These provisions could also reduce the price that investors might be willing to pay in the future for shares of our common stock and result in the market price of our common stock being lower than it would be without these provisions. Our corporate governance documents include provisions:

- creating a classified board of directors whose members serve staggered three-year terms;
- authorizing “blank check” preferred stock, which could be issued by our board without stockholder approval which may contain voting, liquidation, dividend and other rights which are superior to our common stock;
- limiting the liability of, and providing indemnification to, our directors and officers;
- limiting the ability of our stockholders to call and bring business before special meetings by providing that any stockholder action must be effected at a duly called meeting of the stockholders and not by a consent in writing, and providing that only our board of directors, the chairman of our board of directors, our Chief Executive Officer or President may call a special meeting of the stockholders; and
- requiring advance notice of stockholder proposals for business to be conducted at meetings of our stockholders and for nominations of candidates for election to our board of directors.

These provisions, alone or together, could frustrate, delay or prevent hostile takeovers and changes in control or changes in our management.

In addition, the fundamental changes provisions of our Notes may delay or prevent a change in control of our company, because those provisions allow note holders to require us to repurchase such Notes upon the occurrence of a fundamental change (as defined in the indenture for the Notes). Furthermore, the indenture for the Notes prohibits us from engaging in certain mergers or acquisitions unless, among other things, the surviving entity assumes our obligations under the Notes.

As a Delaware corporation, we are also subject to provisions of Delaware law, including Section 203 of the Delaware General Corporation law, which prevents some stockholders holding more than 15% of our outstanding common stock from engaging in certain business combinations merging or combining with us without approval of the holders of a substantial majority of all of our outstanding common stock.

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

We may need to raise additional funds, and we may not be able to obtain additional debt or equity financing on favorable terms, if at all. 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. If we issue equity securities in any additional financing, the new securities may have rights and preferences senior to our common stock. If we engage in debt financing, we may be required to accept terms that restrict our ability to incur additional indebtedness and force us to maintain specified liquidity or other ratios. 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 application and services;
- continue to expand our product development, sales and marketing organizations;
- acquire complementary technologies, products or businesses;
- expand operations, in the United States or internationally;
- hire, train and retain employees; or

Table of Contents

respond to competitive pressures or unanticipated working capital requirements.

Future sales of our common stock in the public market could lower the market price for our common stock and adversely impact the trading price of the notes.

In the future, we may sell additional shares of our common stock to raise capital. In addition, a substantial number of shares of our common stock is reserved for issuance upon the exercise of stock options, the vesting of restricted stock units and restricted stock pursuant to our employee benefit plans, for purchase by employees under our employee stock purchase plan, and upon conversion of our outstanding convertible notes. We cannot predict the size of future issuances or the effect, if any, that they may have on the market price for our common stock. The issuance and sale of substantial amounts of common stock, or the perception that such issuances and sales may occur, could adversely affect the trading price of the notes and the market price of our common stock and impair our ability to raise capital through the sale of additional equity securities.

We do not anticipate paying cash dividends, and accordingly, stockholders must rely on stock appreciation for any return on their investment.

We do not anticipate paying cash dividends on our common stock in the future. As a result, only appreciation of the price of our common stock will provide a return to our stockholders. Investors seeking cash dividends should not invest in our common stock.

ITEM 1B. UNRESOLVED STAFF COMMENTS

None.

ITEM 2. PROPERTIES

Our corporate headquarters, which includes our operations and research and development facilities, is located in Sunnyvale, California, and currently consists of 95,557 square feet of space under a lease that expires in 2020, with a five-year extension option. In 2016, we leased additional 43,925 square feet building in Sunnyvale, California, which is currently under renovation, and upon completion, will serve as expansion of our corporate headquarters. The 2016 leases expires in 2024, with a five-year extension option.

We lease additional U.S. offices in Utah, Texas, Indiana and Colorado. We also lease offices in Toronto, Canada; Paris, France; Tokyo, Japan; Nurnberg, Germany; London and Reading, United Kingdom; Belfast, Ireland, Sydney, Australia; Taipei, Taiwan and Herzliya, Israel. We believe our facilities are adequate for our current needs and for the foreseeable future.

The following is a list of our locations and the primary functions.

Location	Primary function
Sunnyvale, California, U.S.	Research and development, sales, marketing and administration
Minuteman, Utah, U.S.	Research and development, sales, marketing and administration
Austin, Texas, U.S.	Research and development, marketing
Indianapolis, Indiana, U.S.	Research and development
Denver and Broomfield, Colorado	Research and development, sales and marketing
Herzliya, Israel	Research and development
Toronto, Canada	Research and development, sales, marketing and administration
United Kingdom	Research and development, sales and marketing
Paris, France	Sales
Tokyo, Japan	Sales
Nurnberg, Germany	Sales
Belfast, Ireland	Research and development, sales and marketing
Taipei, Taiwan	Research and development, sales, marketing and administration

Sydney, Australia

Sales and marketing

31

Table of Contents

We operate eleven data centers at third-party facilities throughout the world: six in the United States, two in Canada, one in the Netherlands and two in Germany.

ITEM 3. LEGAL PROCEEDINGS

From time to time, we may be involved in legal proceedings and subject to claims in the ordinary course of business.

Although the results of these proceedings and claims cannot be predicted with certainty, we do not believe the ultimate cost to resolve these matters would individually, or taken together, have a material adverse effect on our business, operating results, cash flows or financial condition. Regardless of the outcome, such proceedings can have an adverse impact on us because of defense and settlement costs, diversion of resources and other factors, and there can be no assurances that favorable outcomes will be obtained.

ITEM 4. MINE SAFETY DISCLOSURES

Not applicable.

Table of Contents

PART II.

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Price of Our Common Stock

Our common stock is traded on the NASDAQ Global Market, under the symbol PFPT. The following table set forth, for the periods, indicated, the highest and lowest intraday sales price of our common shares as reported by the NASDAQ Global Market.

	High	Low
Year Ended December 31, 2016		
First Quarter	\$65.28	\$35.56
Second Quarter	\$65.19	\$46.58
Third Quarter	\$80.68	\$63.01
Fourth Quarter	\$88.00	\$68.04
Year Ended December 31, 2015		
First Quarter	\$60.72	\$45.37
Second Quarter	\$67.87	\$50.53
Third Quarter	\$72.70	\$50.82
Fourth Quarter	\$75.46	\$54.87

Holders of our Common Shares

As of February 3, 2017, there were 45 stockholders of record, although we believe that there are a larger number of beneficial owners as many of our shares of our common stock are held by brokers and other institutions on behalf of stockholders.

Dividend Policy

We have never declared or paid any cash dividends on our common stock. We currently intend to retain any future earnings and do not expect to pay any cash dividends on our common stock for the foreseeable future. Any determination to pay dividends in the future will be at the discretion of our board of directors and will be dependent on a number of factors, including our earnings, capital requirements and overall financial conditions.

Unregistered Sales of Equity Securities

On October 24, 2016, the Company issued 110,782 shares of its common stock to certain stockholders of FireLayers, Ltd. as partial consideration paid by the Company in connection with the consummation of the Company's acquisition of FireLayers, Ltd. The shares were not registered under the Securities Act of 1933, as amended ("Securities Act") in reliance upon the exemption from registration pursuant to Section 4(a)(2) of the Securities Act.

Use of Proceeds from Public Offering of Common Stock

There has been no material change in the use of proceeds from our initial public offering in April 2012.

Stock Performance Graph

The following graph shows a comparison from April 20, 2012 through December 31, 2016, of the cumulative total return for our common stock, the NASDAQ Composite Index, and the NASDAQ Computer Index. The graph assumes an investment of \$100 on April 20, 2012 and reinvestment of any dividends. The comparisons in the graph below are

required by the Securities and Exchange Commission and are not intended to forecast or be indicative of possible future performance of our common shares.

Table of Contents

	April 20, 2012	December 31, 2012	December 31, 2013	December 31, 2014	December 31, 2015	December 31, 2016
Proofpoint, Inc.	100.00	87.43	235.58	342.54	461.72	501.78
NASDAQ Composite - Total Returns	100.00	101.92	142.87	163.50	174.88	190.39
NASDAQ Computer Index	100.00	95.61	128.24	156.01	167.97	188.58

The above stock Performance Graph and related information shall not be deemed "filed" with the SEC and is not to be incorporated by reference into any filing of Proofpoint, Inc. made under the Securities Act of 1933, as amended, or the Securities Exchange Act of 1934, as amended.

ITEM 6. SELECTED CONSOLIDATED FINANCIAL DATA

The following tables present selected historical financial data for our business. You should read this information together with "Management's Discussion and Analysis of Financial Condition and Results of Operations" and the consolidated financial statements, related notes and other financial information included elsewhere in this Annual Report on Form 10-K. The selected consolidated financial data in this section are not intended to replace the consolidated financial statements and are qualified in their entirety by the consolidated financial statements and related notes included elsewhere in this Annual Report on Form 10-K.

We derived the consolidated statements of operations data for the years ended December 31, 2016, 2015 and 2014, and the consolidated balance sheet data as of December 31, 2016 and 2015 from our audited consolidated financial statements included elsewhere in this report. We derived the consolidated statements of operations data for the years ended December 31, 2013 and 2012 and the consolidated balance sheet data as of December 31, 2014, 2013 and 2012 from our consolidated financial statements not included in this report. Effective January 1, 2016, we changed our accounting policy for sales commissions that are incremental and directly related to customer sales contracts in which revenue is deferred. The adoption of this accounting policy change has been applied retrospectively for all periods presented. See Note 1 of the Notes to Consolidated Financial Statements in this annual report for information regarding the change in accounting policy for sales commissions. Our historical results are not necessarily indicative of the results to be expected in the future.

Table of Contents

	Years Ended December 31,				
	2016	2015	2014	2013	2012
	(in thousands, except per share data)				
Consolidated Statements of Operations Data:					
Revenue:					
Subscription	\$365,960	\$257,329	\$187,527	\$132,062	\$101,470
Hardware and services	9,536	8,068	8,080	5,869	4,825
Total revenue	375,496	265,397	195,607	137,931	106,295
Cost of revenue:(1)					
Subscription	94,716	71,746	53,136	35,468	28,246
Hardware and services	13,877	12,312	12,543	6,124	4,867
Total cost of revenue	108,593	84,058	65,679	41,592	33,113
Gross profit	266,903	181,339	129,928	96,339	73,182
Operating expense:(1)					
Research and development	98,506	74,459	51,903	34,449	24,827
Sales and marketing	201,204	148,414	98,333	69,123	53,445
General and administrative	52,774	36,616	26,679	19,622	12,693
Total operating expense	352,484	259,489	176,915	123,194	90,965
Operating loss	(85,581)	(78,150)	(46,987)	(26,855)	(17,783)
Interest expense	(23,538)	(18,000)	(11,213)	(641)	(108)
Other expense, net	(1,103)	(1,927)	(2,230)	(215)	(154)
Loss before (provision for) benefit from income taxes	(110,222)	(98,077)	(60,430)	(27,711)	(18,045)
(Provision for) benefit from income taxes	(986)	(635)	313	2,808	(521)
Net loss	\$(111,208)	\$(98,712)	\$(60,117)	\$(24,903)	\$(18,566)
Net loss per share, basic and diluted	\$(2.66)	\$(2.48)	\$(1.61)	\$(0.71)	\$(0.77)
Weighted average shares outstanding, basic and diluted	41,859	39,787	37,381	34,874	24,056

(1) Includes stock-based compensation and amortization of intangible assets as follows:

	Years Ended December 31,				
	2016	2015	2014	2013	2012
	(in thousands)				
Stock-based compensation:					
Cost of subscription revenue	\$7,427	\$5,028	\$2,404	\$1,007	\$657
Cost of hardware and services revenue	\$1,494	\$1,098	\$604	\$196	\$70
Research and development	\$24,342	\$20,672	\$10,204	\$3,608	\$1,869
Sales and marketing	\$28,607	\$21,511	\$10,795	\$4,270	\$3,103
General and administrative	\$16,826	\$11,785	\$6,997	\$3,002	\$1,622
Amortization of intangible assets:					
Cost of subscription revenue	\$9,423	\$7,079	\$4,157	\$2,220	\$2,785
Research and development	\$60	\$91	\$93	\$47	\$30
Sales and marketing	\$4,938	\$5,074	\$4,494	\$1,743	\$461
General and administrative	\$—	\$12	\$46	\$34	\$—

Table of Contents

	As of December 31,				
	2016	2015	2014	2013	2012
	(in thousands)				
Consolidated Balance Sheet Data:					
Cash, cash equivalents and short-term investments	\$396,751	\$406,237	\$214,986	\$251,801	\$86,517
Deferred commissions, current and long-term	\$25,664	\$22,802	\$15,060	\$10,938	\$8,280
Property and equipment, net	\$52,523	\$34,501	\$18,718	\$11,221	\$8,560
Total assets	\$801,660	\$705,616	\$439,076	\$401,211	\$148,721
Convertible senior notes	\$366,541	\$345,699	\$161,396	\$152,642	\$—
Debt, current and long-term	\$123	\$155	\$695	\$2,350	\$4,012
Deferred revenue, current and long-term	\$312,181	\$223,726	\$162,675	\$123,983	\$86,859
Total stockholders' equity	\$44,923	\$83,185	\$71,533	\$88,098	\$42,088

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 "Selected Consolidated Financial Data" and our consolidated financial statements and related notes included elsewhere in this Annual Report on Form 10-K. This discussion contains forward-looking statements that involve risks and uncertainties. Our actual results could differ materially from those forward-looking statements below. Factors that could cause or contribute to those differences include, but are not limited to, those identified below and those discussed in the section entitled "Risk Factors" included elsewhere in this Annual Report on Form 10-K. This Annual Report on Form 10-K contains "forward-looking statements" within the meaning of Section 21E of the Securities Exchange Act of 1934, as amended (the "Exchange Act"). These statements are often identified by the use of words such as "may," "will," "expect," "believe," "anticipate," "intend," "could," "estimate," or "continue," and similar expressions and variations. Such forward-looking statements are subject to risks, uncertainties and other factors that could cause actual results and the timing of certain events to differ materially from future results expressed or implied by such forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to, those identified herein, and those discussed in the section titled "Risk Factors", set forth in Part I, Item 1A of this Form 10-K. Except as required by law, we disclaim any obligation to update any forward-looking statements to reflect events or circumstances after the date of such statements.

Overview

Proofpoint is a leading security-as-a-service ("SaaS") provider that enables large and mid-sized organizations worldwide to defend, protect, archive and govern their most sensitive data. Our SaaS platform is comprised of an integrated suite of on-demand data protection solutions, including threat protection and incident response, regulatory compliance, archiving, data governance and eDiscovery, and secure communication. Our solutions are built on a flexible, cloud-based platform and leverage a number of proprietary technologies, including big data analytics, machine learning, deep content inspection, secure storage, advanced encryption, intelligent message routing, dynamic malware analysis, threat correlation, and virtual execution environments, to address today's rapidly changing threat landscape.

Our platform addresses this growing challenge by not only protecting data as it flows into and out of the enterprise via on-premises and cloud-based email, instant messaging, social media and other web-based applications, but also by keeping track of this information as it is modified and distributed throughout the enterprise for compliance and data loss prevention, and securely archiving these communications for compliance and discovery. We address four important problems for the enterprise:

protecting users from the advanced attacks that target them via email, social media and mobile applications;
preventing the theft or inadvertent loss of sensitive information and, in turn, ensuring compliance with regulatory data protection mandates;
collecting, retaining, governing and discovering sensitive data for compliance and litigation support; and
enabling organizations to respond quickly to security issues, providing both the intelligence and the context to prioritize incidents and orchestrate remediation actions.

Our platform and its associated solutions are sold to customers on a subscription basis and can be deployed through our unique cloud-based architecture that leverages both our global data centers as well as optional points-of-presence behind

Table of Contents

our customers' firewalls. Our flexible deployment model enables us to deliver superior security and compliance while maintaining the favorable economics afforded by cloud computing, creating a competitive advantage for us over legacy on-premises and cloud-only offerings.

We were founded in 2002 to provide a unified solution to help enterprises address their growing data security requirements. Our first solution was commercially released in 2003 to combat the burgeoning problem of spam and viruses and their impact on corporate email systems. To address the evolving threat landscape and the adoption of communication and collaboration systems beyond corporate email and networks, we have broadened our solutions to defend against a wide range of threats, protect against outbound security risks, and archive and govern corporate information. As the threat environment has continued to evolve, we have dedicated significant resources to meet the ongoing challenges that this highly dynamic environment creates for our customers such as investing significantly to expand the breadth of our data protection platform as these expenditures are primarily in connection with the replacement and upgrade of equipment to lower the cost of deployment as well as to improve the efficiency for our cloud-based architecture.

Our business is based on a recurring revenue model. Our customers pay a subscription fee to license the various components of our SaaS platform for a contract term that is typically one to three years. At the end of the license term, customers may renew their subscription and in each year since the launch of our first solution in 2003, we have maintained a renewal rate with our existing customers of over 90%. We derive this retention rate by calculating the total annually recurring subscription revenue from customers currently using our SaaS platform and dividing it by the total annually recurring subscription revenue from both these current customers as well as all business lost through non-renewal. A growing number of our customers increase their annual subscription fees after their initial purchase by broadening their use of our platform or by adding more users, and these sales have consistently represented greater than 15% of our billings each year since 2008.

We market and sell our solutions worldwide both directly through our sales teams and indirectly through a hybrid model where our sales organization actively assists our network of distributors and resellers. We also derive a lesser portion of our total revenue from the license of our solutions to strategic partners who offer our solutions in conjunction with one or more of their own products or services.

Our solutions are designed to be implemented, configured and operated without the need for any training or professional services. We offer various trainings and professional services for those customers that seek to develop deeper expertise in the use of our solutions or would like assistance with complex configurations or the importing of data. In some cases, we provide a hardware appliance to those customers that elect to host elements of our solution behind their firewall. Increasing adoption of virtualization in the data center has led to a decline in the sales of our hardware appliances and a shift towards our software-based virtual appliances, which are delivered as a download via the Internet. Our hardware and services offerings carry lower margins and are provided as a courtesy to our customers. We expect the overall proportion of revenue derived from the hardware and services offerings to generally remain below 5% of our total revenue.

Historically, the majority of our revenue is derived from our customers in the United States. We believe the markets outside of the United States offer an opportunity for growth and we intend to make additional investments in sales and marketing to expand in these markets. Revenue from customers outside of the United States grew 34% for the year ended December 31, 2016 as compared to prior year. In terms of customer concentration, there were no individual customers or partners that accounted for more than 10% of our total revenue for the years ended December 31, 2016 and 2015.

We have not been profitable to date and will need to grow revenue at a rate faster than our investments in cost of revenue and operating expenses in order to achieve profitability, as discussed in more detail below.

Key Opportunities and Challenges

The total costs associated with the teams tasked with closing business with new customers and additional business with our existing customers have represented more than 90% of our total sales and marketing costs since 2008. Although we expect customers to be profitable over the duration of the customer relationship, the upfront costs typically exceed related revenue during the earlier periods of a contract. As a result, while our practice of invoicing our customers for the entire amount of the contract at the start of the term provides us with a relatively immediate contribution to cash flow, the revenue is recognized ratably over the term of the contract, and hence contributions toward operating income are limited in the period where the sales and marketing costs are incurred. Accordingly, an increase in the mix of new customers as a percentage of total customers would likely negatively impact our near-term operating results. On the other hand, we expect that an increase in the mix of existing customers as a percentage of total customers would positively impact our operating results over time. As we accumulate customers that continue to renew their contracts, we anticipate that our mix of existing customers will increase,

Table of Contents

contributing to a decrease in our sales and marketing costs as a percentage of total revenue and a commensurate improvement in our operating income.

As part of maintaining our SaaS platform, we provide ongoing updates and enhancements to the platform services both in terms of the software as well as the underlying hardware and data center infrastructure. These updates and enhancements are provided to our customers at no additional charge as part of the subscription fees paid for the use of our platform. While more traditional products eventually become obsolete and require replacement, we are constantly updating and maintaining our cloud-based services and as such they operate with a continuous product life cycle. Much of this work is designed to both maintain and enhance the customers' experience over time while also lowering our costs to deliver the service. Our SaaS platform is a shared infrastructure that is used by all of our customers. Accordingly, the costs of the platform are spread in a relatively uniform manner across the entire customer base and no specific infrastructure elements are directly attached to any particular customer. As such, in the event that a customer chooses to not renew its subscription, the underlying resources are reallocated either to new customers or to accommodate the expanding needs of our existing customers and, as a result, we do not believe that the loss of any particular customer has a meaningful impact on our gross profit as long as we continue to grow our customer base.

To date, our customers have primarily used our solutions in conjunction with email messaging content. We have developed solutions to address new and evolving messaging solutions such as social media and file sharing applications, but these solutions are relatively nascent. If customers increase their use of these new messaging solutions in the future, we anticipate that our growth in revenue associated with older email messaging solutions may slow over time. Although revenue associated with our social media and file sharing applications has not been material to date, we believe that our ability to provide security, archiving, governance and discovery for these new solutions will be viewed as valuable by our existing customers, enabling us to derive revenue from these new forms of messaging and communication.

While the majority of our current and prospective customers run their email systems on premise, we believe that there is a trend for large and mid-sized enterprises to migrate these systems to the cloud. While our current revenue derived from customers using cloud-based email systems continues to grow as a percentage of our total revenue, many of these cloud-based email solutions offer some form of threat protection and governance services, potentially mitigating the need for customers to buy these capabilities from third parties such as ourselves. We believe that we can continue to provide security, archiving, governance, and discovery solutions that are differentiated from the services offered by cloud-based email providers, and as such our platform will continue to be viewed as valuable to enterprises once they have migrated their email services to the cloud, enabling us to continue to derive revenue from this new trend toward cloud-based email deployment models.

With the majority of our business, we invoice our customers for the entire contract amount at the start of the term and these amounts are recorded as deferred revenue on our balance sheet, with the dollar weighted average duration of these contracts for any given period over the past three years typically ranging from 14 to 20 months. As a result, while our practice of invoicing customers for the entire amount of the contract at the start of the term provides us with a relatively immediate contribution to cash flow, the revenue is recognized ratably over the term of the contract, and hence contributions toward operating income are realized over an extended period. As such, our efforts to improve our profitability require us to invest far less in operating expenses than the cash flow generated by our business might otherwise allow. As we strive to invest in an effort to continue to increase the size and scale of our business, we expect that the level of investment afforded by our growth in revenue should be sufficient to fund the investments needed to drive revenue growth and broaden our product line.

Considering all of these factors, we do not expect to be profitable on a GAAP basis in the near term and in order to achieve profitability we will need to grow revenue at a rate faster than our investments in operating expenses and cost of revenue.

We intend to grow our revenue through acquiring new customers by investing in our sales and marketing activities. We believe that an increase in new customers in the near term will result in a larger base of renewal customers, which, over time, we expect to be more profitable for us.

Sales and marketing is our largest expense and hence a significant contributing factor to our operating losses. We believe that our opportunity to improve our return on investment on sales and marketing costs relies primarily on our ongoing ability to cost-effectively renew our business with existing customers, thereby lowering our overall sales and marketing costs as a percentage of revenue as the mix of revenue derived from this more profitable renewal activity increases over time. Therefore, we anticipate that our initial significant investments in sales and marketing activities will, over time, generate a larger base of more profitable customers. Cost of subscription revenue is also a significant expense for us, and we expect to continue to build on the improvements over the past years, such as in replacing third-party technology with our proprietary technology and improving the utilization of our fixed investments in equipment and infrastructure, in order to provide the

Table of Contents

opportunity for improved subscription gross margins over time. Although we plan to continue enhancing our solutions, we intend to lower our rate of investment in research and development as a percentage of revenue over time by deriving additional revenue from our existing platform of solutions rather than by adding entirely new categories of solutions. In addition, as personnel costs are one of the primary drivers of the increases in our operating expenses, we plan to reduce our historical rate of headcount growth over time.

Key Metrics

We regularly review a number of metrics, including the following key metrics presented in the table below, to evaluate our business, measure our performance, identify trends in our business, prepare financial projections and make strategic decisions. Many of these key metrics, such as non-GAAP gross margin, billings, adjusted EBITDA and free cash flows, are non-GAAP measures. This non-GAAP information is not necessarily comparable to non-GAAP information of other companies. Users of this financial information should consider the types of events and transactions for which adjustments have been made.

	Year Ended December 31,		
	2016	2015	2014
	(in thousands)		
Total revenue	\$375,496	\$265,397	\$195,607
Growth	41	% 36	% 42
Gross margin percentage	71	% 68	% 66
Non-GAAP gross margin	76	% 73	% 70
Billings (non-GAAP)	\$462,751	\$324,348	\$233,699
Growth	43	% 39	% 46
Adjusted EBITDA (non-GAAP)	\$38,697	\$12,332	\$3,627
Free cash flows (non-GAAP)	\$59,828	\$20,677	\$7,625

Non-GAAP gross margin

We define non-GAAP gross margin as non-GAAP gross profit divided by GAAP revenue. We define non-GAAP gross profit as GAAP gross profit, adjusted to exclude stock-based compensation expense and the amortization of intangible assets associated with acquisitions. We consider this non-GAAP financial measure to be a useful metric for management and investors because it excludes the effect of stock-based compensation expense and the amortization of intangible assets associated with acquisitions so that our management and investors can compare our business operating results over multiple periods, and compare the Company's financial results with other companies in its industry, many of which present similar non-GAAP financial measure. However, there are a number of limitations related to the use of non-GAAP gross margin versus gross margin calculated in accordance with GAAP. For example, stock-based compensation has been and will continue to be for the foreseeable future a significant recurring expense in our business. Stock-based compensation is an important part of our employees' compensation and impacts their performance. In addition, the components of the costs that we exclude in our calculation of non-GAAP gross margin may differ from the components that our peer companies exclude when they report their non-GAAP results. Management compensates for these limitations by providing specific information regarding the GAAP amounts excluded from non-GAAP gross margin and evaluating non-GAAP gross margin together with gross margin calculated in accordance with GAAP.

The following table presents the reconciliation of gross margin to Non-GAAP gross margin for the years ended December 31, 2016, 2015 and 2014:

Table of Contents

	Year Ended December 31,		
	2016	2015	2014
	(in thousands)		
GAAP gross profit	\$266,903	\$181,339	\$129,928
GAAP gross margin	71	% 68	% 66
Plus:			
Stock-based compensation expense	8,921	6,126	3,008
Amortization of intangible assets	9,423	7,079	4,157
Non-GAAP gross profit	\$285,247	\$194,544	\$137,093
Non-GAAP gross margin	76	% 73	% 70

Billings

We have included billings, a non-GAAP financial measure, in this report because it is a key measure used by our management and board of directors to manage our business and monitor our near term cash flows. We define billings as total revenue plus change in deferred revenue during a period, less deferred revenue from acquisitions. We have provided reconciliation between total revenue, the most directly comparable GAAP financial measure, and billings. Accordingly, we believe that billings provides useful information to investors and others in understanding and evaluating our operating results in the same manner as our management and board of directors.

Our use of billings as a non-GAAP measure has limitations as an analytical tool, and you should not consider it in isolation or as a substitute for revenue or an analysis of our results as reported under GAAP. Some of these limitations are:

Billings is not a substitute for revenue, as trends in billings are not directly correlated to trends in revenue; Billings is affected by a combination of factors including the timing of renewals, the sales of our solutions to both new and existing customers, the relative duration of contracts sold, and the relative amount of business derived from strategic partners. As each of these elements has unique characteristics in the relationship between billings and revenue, our billings activity is not closely correlated to revenue except over longer periods of time; and Other companies, including companies in our industry, may not use billings, may calculate billings differently, or may use other financial measures to evaluate their performance all of which reduce the usefulness of billings as a comparative measure.

The following table presents the reconciliation of total revenue to billings for the years ended December 31, 2016, 2015 and 2014:

	Year Ended December 31,		
	2016	2015	2014
	(in thousands)		
Total revenue	\$375,496	\$265,397	\$195,607
Deferred revenue			
Ending	312,181	223,726	162,675
Beginning	223,726	162,675	123,983
Net change	88,455	61,051	38,692
Less: deferred revenue contributed by acquisitions	(1,200)	(2,100)	(600)
Billings	\$462,751	\$324,348	\$233,699

Adjusted EBITDA

Table of Contents

We define adjusted EBITDA as net loss, adjusted to exclude: depreciation, amortization of intangible assets, interest (income) expense, net, provision for (benefit from) income taxes, stock-based compensation, acquisition- and litigation-related (income) expenses, net, and other (income) expense, net. Acquisition related expense, net, include legal, accounting, and other professional fees, as well as changes in the fair value of contingent consideration obligations. We believe that adjusted EBITDA is useful to investors and other users of our financial statements in evaluating our operating performance because it provides them with an additional tool to compare business performance across companies and across periods. We believe that:

Adjusted EBITDA provides investors and other users of our financial information consistency and comparability with our past financial performance, facilitates period-to-period comparisons of operations and facilitates comparisons with our peer companies, many of which use similar non-GAAP financial measures to supplement their GAAP results; and It is useful to exclude certain non-cash charges, such as depreciation, amortization of intangible assets and stock-based compensation, and acquisition- and litigation-related (income) expenses from adjusted EBITDA because the amount of such expenses in any specific period may not be directly correlated to the underlying performance of our business operations and these expenses can vary significantly between periods as a result of new acquisitions, full depreciation of previously acquired tangible and amortization of intangible assets, the timing of new stock based awards or litigation-related (income) expenses, as the case may be.

We use adjusted EBITDA in conjunction with traditional GAAP operating performance measures as part of our overall assessment of our performance, for planning purposes, including the preparation of our annual operating budget, to evaluate the effectiveness of our business strategies and to communicate with our board of directors concerning our financial performance.

We do not place undue reliance on adjusted EBITDA as our only measure of operating performance. Adjusted EBITDA should not be considered as a substitute for other measures of financial performance reported in accordance with GAAP. There are limitations to using non-GAAP financial measures, including that other companies may calculate these measures differently than we do, that they do not reflect our capital expenditures or future requirements for capital expenditures and that they do not reflect changes in, or cash requirements for, our working capital.

The following table presents the reconciliation of net loss to adjusted EBITDA for the years ended December 31, 2016, 2015 and 2014:

	Year Ended December 31,		
	2016	2015	2014
	(in thousands)		
Net loss	\$(111,208)	\$(98,712)	\$(60,117)
Depreciation	17,131	12,644	9,033
Amortization of intangible assets	14,421	12,256	8,790
Interest expense	23,538	18,000	11,213
Provision for (benefit from) income taxes	986	635	(313)
EBITDA	(55,132)	(55,177)	(31,394)
Stock-based compensation expense	78,696	60,094	31,004
Acquisition-related expense	1,080	911	612
Litigation-related expense	12,950	4,577	1,175
Other expense, net	1,103	1,927	2,230
Adjusted EBITDA	\$38,697	\$12,332	\$3,627
Free cash flows			

We define free cash flow as net cash provided by operating activities minus capital expenditures. We consider free cash flow to be a liquidity measure that provides useful information to management and investors about the amount of cash generated by the business that, after the acquisition of property and equipment, can be used for strategic opportunities, including investing in our business, making strategic acquisitions, and strengthening the balance sheet.

Analysis of free cash

41

Table of Contents

flow facilitates management's comparisons of our operating results to competitors' operating results. A limitation of using free cash flow versus the GAAP measure of net cash provided by operating activities as a means for evaluating our company is that free cash flow does not represent the total increase or decrease in the cash balance from operations for the period because it excludes cash used for capital expenditures during the period. Management compensates for this limitation by providing information about our capital expenditures on the face of the cash flow statement and in the "Liquidity and Capital Resources" section below.

	Year Ended December 31,		
	2016	2015	2014
	(in thousands)		
GAAP cash flows provided by operating activities:	\$94,235	\$46,504	\$22,613
Less:			
Purchase of property and equipment	(34,407)	(25,827)	(14,988)
Non-GAAP free cash flows	\$59,828	\$20,677	\$7,625
Components of Our Results of Operations			

Revenue

We derive our revenue primarily through the license of various solutions and services on our security-as-a-service platform on a subscription basis, supplemented by the sales of training, professional services and hardware depending upon our customers' requirements.

Subscription. We license our platform and its associated solutions and services on a subscription basis. The fees are charged on a per user, per year basis. Subscriptions are typically one to three years in duration. We invoice our customers upon signing for the entire term of the contract. The invoiced amounts billed in advance are treated as deferred revenue on the balance sheet and are recognized ratably, in accordance with the appropriate revenue recognition guidelines, over the term of the contract. We also derive a portion of our subscription revenue from the license of our solutions to strategic partners. We bill these strategic partners monthly. We expect our subscription revenue will continue to grow and remain above 95% of our total revenue.

Hardware and services. We provide hardware appliances as a convenience to our customers and as such it represents a small part of our business. Our solutions are designed to be implemented, configured and operated without the need for any training or professional services. For those customers that seek to develop deeper expertise in the use of our solutions or would like assistance with complex configurations or the importing of data, we offer various training and professional services. We typically invoice the customer for hardware at the time of shipment. We typically invoice customers for services at the time the order is placed and recognize this revenue ratably over the term of the contract. On occasion, customers may retain us for special projects such as archiving import and export services; these types of services are recognized upon completion of the project. We expect the overall proportion of revenue derived from hardware and service offerings to generally remain below 5% of our total revenue.

Cost of Revenue

Our cost of revenues consists of cost of subscription revenue and cost of hardware and services revenue. Personnel costs, data center costs and hardware costs are the most significant components of our cost of revenues. We expect personnel costs to continue to increase in absolute dollars as we hire new employees to continue to grow our business.

Cost of Subscription Revenue. Cost of subscription revenue primarily includes personnel costs, consisting of salaries, benefits, bonuses, and stock-based compensation, for employees who provide support services to our customers and operate our data centers. Other costs include fees paid to contractors who supplement our support and data center

personnel; expenses related to the use of third-party data centers in both the United States and internationally; depreciation of data center equipment; amortization of licensing fees and royalties paid for the use of third-party technology; amortization of internally developed intangible assets; and the amortization of intangible assets acquired through business combinations. Growth in subscription revenue generally consumes production resources, requiring us to gradually increase our cost of subscription revenue in absolute dollars as we expand our investment in data center equipment, the third-party data center space required to house this equipment, and the personnel needed to manage this higher level of activity.

Table of Contents

Cost of Hardware and Services Revenue. Cost of hardware and services revenue includes personnel costs for employees who provide training and professional services to our customers as well as the cost of server hardware shipped to our customers that we procure from third parties and configure with our software solutions.

Operating Expenses

Our operating expenses consist of research and development, sales and marketing, and general and administrative expenses. Personnel costs, which consist of salaries, benefits, bonuses, and stock-based compensation, are the most significant component of our operating expenses. We expect personnel costs to continue to increase in absolute dollars as we hire new employees to continue to grow our business. Our headcount has increased from 449 employees as of December 31, 2012 to 1,573 employees as of December 31, 2016. As a result of this growth in headcount, operating expenses have increased significantly over these periods. We expect personnel costs to continue to increase in absolute dollars as we hire new employees to continue to grow our business.

Research and Development. Research and development expenses include personnel costs, consulting services and depreciation. We believe that these investments have played an important role in broadening the capabilities of our platform over the course of our operating history, enhancing the relevance of our solutions in the market in general and helping us to retain our customers over time. We expect to continue to devote substantial resources to research and development in an effort to continuously improve our existing solutions as well as to develop new offerings. We believe that these investments are necessary to maintain and improve our competitive position. However, over the longer term, we intend to monitor these costs so as to decrease this spending as a percentage of total revenue. Our research efforts include both software developed for our internal use on behalf of our customers as well as software elements to be used by our customers in their own facilities. To date, our capitalized costs on software developed for internal use on behalf of our customers have not been material. For the software developed for use on our customers' premises, the costs associated with the development work between technological feasibility and the general availability has not been material and as such we have not capitalized any of these development costs to date.

Sales and Marketing. Sales and marketing expenses include personnel costs, sales commissions, and other costs including travel and entertainment, marketing and promotional events, public relations and marketing activities. These costs also include amortization of intangible assets as a result of our past acquisitions. Due to our continued investment in growing our sales and marketing operations, both domestically and internationally, headcount increases were reflected in higher compensation expense consistent with our revenue growth. Our sales personnel are typically not immediately productive, and therefore the increase in sales and marketing expenses we incur when we add new sales representatives is not immediately offset by increased revenue and may not result in increased revenue over the long-term if these new sales people fail to become productive. The timing of our hiring of new sales personnel and the rate at which they generate incremental revenue will affect our future financial performance. We expect that sales and marketing expenses will continue to increase in absolute dollars and be among the most significant components of our operating expenses.

General and Administrative. General and administrative expenses consist of personnel costs, consulting services, audit fees, tax services, legal expenses and other general corporate items. As a result of our operational growth, we expect our general and administrative expenses to increase in absolute dollars in future periods as we continue to expand our operations and hire additional personnel.

Interest Expense

Interest expense consists of interest income earned on our cash, cash equivalents and short-term investments, the interest expense related to our convertible senior notes and our capital lease payments.

Other Income (Expense), Net

Other income (expense), net, consists primarily of the net effect of foreign currency transaction gains and losses.

(Provision For) Benefit From Income Taxes

For 2013 and prior years, the (provision for) benefit from income taxes was related to state and foreign income taxes. As we have incurred operating losses in all periods to date and recorded a full valuation allowance against our deferred tax assets, we have not historically recorded a provision for federal income taxes. However, in the years ended December 31, 2016 and 2015, we recognized \$0.4 million and \$0.1 million, respectively, of deferred tax expense in the U.S. related to amortization

Table of Contents

of tax goodwill on business acquisitions. We also recognized a \$0.8 million deferred tax benefit in 2014 related to the release of U.S. valuation allowances as a result of business acquisitions. Realization of any of our deferred tax assets depends upon future earnings, the timing and amount of which are uncertain. Utilization of our net operating losses and research and development credits may be subject to substantial annual limitation due to the ownership change limitations provided by the Internal Revenue Code and similar state provisions. Analyses have been conducted to determine whether an ownership change had occurred since inception. The analyses have indicated that although ownership changes have occurred in prior years, the net operating losses and research and development credits would not expire before utilization as a result of the ownership change. In the event we have subsequent changes in ownership, net operating losses and research and development credit carryovers could be limited and may expire unutilized as a result of the subsequent ownership change.

Results of Operations

The following table is a summary of our consolidated statements of operations.

	Year Ended December 31,		
	2016	2015	2014
	(in thousands)		
Revenue:			
Subscription	\$365,960	\$257,329	\$187,527
Hardware and services	9,536	8,068	8,080
Total revenue	375,496	265,397	195,607
Cost of revenue:(1)			
Subscription	94,716	71,746	53,136
Hardware and services	13,877	12,312	12,543
Total cost of revenue	108,593	84,058	65,679
Gross profit	266,903	181,339	129,928
Operating expense:(1)			
Research and development	98,506	74,459	51,903
Sales and marketing	201,204	148,414	98,333
General and administrative	52,774	36,616	26,679
Total operating expense	352,484	259,489	176,915
Operating loss	(85,581)	(78,150)	(46,987)
Interest expense	(23,538)	(18,000)	(11,213)
Other expense, net	(1,103)	(1,927)	(2,230)
Loss before (provision for) benefit from income taxes	(110,222)	(98,077)	(60,430)
(Provision for) benefit from income taxes	(986)	(635)	313
Net loss	\$(111,208)	\$(98,712)	\$(60,117)

The following table sets forth our consolidated results of operations for the specified periods as a percentage of our total revenue for those periods.

Table of Contents

	Year Ended					
	December 31,					
	2016	2015	2014			
Revenue:						
Subscription	97	%	97	%	96	%
Hardware and services	3		3		4	
Total revenue	100		100		100	
Cost of revenue:(1)						
Subscription	25		27		27	
Hardware and services	4		5		7	
Total cost of revenue	29		32		34	
Gross profit	71		68		66	
Operating expense:(1)						
Research and development	26		28		26	
Sales and marketing	54		56		50	
General and administrative	14		14		14	