

PROOFPOINT INC  
Form 10-K  
February 26, 2015  
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, 2014

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

(State or other jurisdiction of  
incorporation or organization)

51-0414846

(I.R.S. employer  
identification no.)

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

94089

(Zip Code)

(408) 517-4710

(Registrant's telephone number, including area code)

---

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

Title of Each Class

Common Stock , \$0.0001 par value per  
share

Name of each exchange on which  
registered

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.

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
<input type="checkbox"/>	<input type="checkbox"/>	(Do not check if a smaller reporting company)	company
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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, 2014 as reported by the NASDAQ Global Select Market on that date, was approximately \$1,291,000,000. 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 13, 2015 was 38,993,942 shares.

---

#### DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement for its 2015 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, 2014.

Table of Contents

PROOFPOINT, INC.

FORM 10-K

For the Fiscal Year Ended December 31, 2014

TABLE OF CONTENTS

	Page
PART I.	
Item 1. Business	<u>3</u>
Item 1A. Risk Factors	<u>16</u>
Item 1B. Unresolved Staff Comments	<u>33</u>
Item 2. Properties	<u>33</u>
Item 3. Legal Proceedings	<u>33</u>
Item 4. Mine Safety Disclosures	<u>33</u>
PART II.	
Item 5. Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities	<u>35</u>
Item 6. Selected Financial Data	<u>36</u>
Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations	<u>38</u>
Item 7A. Quantitative and Qualitative Disclosures About Market Risk	<u>60</u>
Item 8. Financial Statements and Supplementary Data	<u>61</u>
Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure	<u>61</u>
Item 9A. Controls and Procedures	<u>61</u>
Item 9B. Other Information	<u>62</u>
PART III.	
Item 10. Directors, Executive Officers and Corporate Governance	<u>63</u>
Item 11. Executive Compensation	<u>63</u>
Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters	<u>63</u>
Item 13. Certain Relationships and Related Transactions, and Director Independence	<u>63</u>
Item 14. Principal Accountant Fees and Services	<u>63</u>
PART IV.	
Item 15. Exhibits and Financial Statement Schedules	<u>64</u>
Index to Consolidated Financial Statements	<u>65</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 targeted, malicious attacks 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 proliferated sensitive data and reduced 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-premise and cloud-based email, instant messaging, social media and other web-based applications, but also by keeping track of such 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:

• Keeping malicious content out of the extended enterprise;

• 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

• Securely sharing sensitive data with customers, partners and suppliers.

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-premise 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. Today, our solutions are used by approximately 3,300 customers worldwide, including 45 of the Fortune 100, protecting tens of millions of 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.

### The Proofpoint Solution

Our integrated suite of on-demand security-as-a-service solutions enables large and mid-sized organizations to defend, protect, archive and govern their sensitive data. Our comprehensive platform provides threat protection, incident response, regulatory compliance, archiving, governance, eDiscovery, and secure communication. These solutions are built on a cloud-based architecture, protecting data not only as it flows into and out of the enterprise via on-premise and cloud-based email,

3

---

## Table of Contents

instant messaging, social media and other web-based applications, and also keeps 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 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 advanced, targeted threats. We use a combination of proprietary technologies for big data analytics, machine learning, deep content inspection, dynamic malware analysis, threat correlation, 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 polymorphic threats, zero-day exploits, user-transparent "drive-by" downloads and other penetration tactics. By processing and modeling billions of requests per day, we can recognize anomalies in traffic flow 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 if such web sites are otherwise benign and considered reputable. Our threat correlation technologies enable us to rapidly confirm and contain threats, providing rapid automated incident response.

Comprehensive, integrated data protection, compliance, and eDiscovery suite. We offer a comprehensive solution for data protection and governance through an integrated, security-as-a-service platform that is comprised of five main suites: Proofpoint Enterprise Protection, Proofpoint Enterprise Privacy, Proofpoint Enterprise Archive & Governance, Proofpoint Nexgate Social Media Security & Compliance, and Proofpoint Essentials. Together, these solutions can improve an organization's ability to detect and mitigate inbound and outbound threats and securely archive and discover communication across all major communication channels including on-premise and cloud-based email, instant messaging, social media and other web-based applications. In addition, our common policy framework and reporting systems enable organizations to comply with complex regulatory mandates, implement consistent data governance policies and ensure end-to-end incident response across the enterprise.

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. 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

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.

Our Security-as-a-Service Platform

4

---



## Table of Contents

We provide a multi-tiered security-as-a-service platform consisting of solutions, platform technologies and infrastructure. Our platform currently includes five solutions bundled for the convenience of our customers, distributors and resellers: Proofpoint Enterprise Protection, Proofpoint Enterprise Privacy, Proofpoint Enterprise Archive & Governance, Proofpoint Nexgate Social Media Security & Compliance, and Proofpoint Essentials. Each of these solutions is built as an aspect of our security-as-a-service platform, which includes both platform services and enabling technologies. 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.

## Solutions

### Proofpoint Enterprise Protection

Proofpoint Enterprise Protection is our communications and collaboration security suite designed to protect customers' mission-critical messaging infrastructure from outside threats including spam, phishing, unpredictable email volumes, malware and other forms of objectionable or dangerous content before they reach the enterprise. Key capabilities within Proofpoint Enterprise Protection include:

- Threat detection. Uses our Proofpoint MLX machine learning technology and reputation data to examine millions of possible attributes in every message, including envelope headers and structure, embedded web links, images, attachments and sender reputation, as well as unstructured content in the message body, to block phishing and spear phishing attacks, spam and other forms of malicious or objectionable content. This solution also includes sophisticated policy and routing controls designed to ensure security and the effective handling of all classifications of content.

## Table of Contents

Virus protection. Combats email-borne viruses, worms and trojans with a solution that combines efficient message handling, comprehensive reporting, and robust policy management with leading third-party antivirus scanning engines.

Zero-hour threat detection. Protects enterprises against new phishing attacks, viruses and other forms of malicious code during the critical period after new attacks are released and before full information is available to characterize the threat.

Smart search. Offers an easy-to-use interface that provides 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.

Targeted attack protection. Enterprises are protected against advanced persistent 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.

- Threat response. Provides threat information and Indicators of Compromise 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.

Key benefits of Proofpoint Enterprise Protection include:

- Superior protection from advanced threats, spam and viruses. Protects against advanced threats, spam and other malicious code 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.

- Automated Incident Response. Analyzes and correlates incident data to confirm system compromises, then acts to contain systems to help minimize and mitigate exposure.

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.

## Proofpoint Enterprise Privacy

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 Security Standards. Key capabilities within Proofpoint

Enterprise Privacy 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.

6

---

## Table of Contents

**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. Proofpoint Enterprise Privacy 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 file transfer.** Provides secure, large file transfer capabilities that enables end-users to send large files quickly, easily, and securely while eliminating the impact of large attachments on an email infrastructure.

**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.

**Content Control.** Automated discovery and remediation solution identifies and enables corrective action on sensitive content across enterprise; reduces risk of data breaches and compliance violations.

Key benefits of Proofpoint Enterprise Privacy include:

**Regulatory compliance.** Enables outbound messages to comply with national and state government and industry-specific privacy regulations.

**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.

### Proofpoint Enterprise Archive & Governance

Proofpoint Enterprise Archive & Governance 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.

Proofpoint Enterprise Archive can store, govern and discover a wide range of data including email, instant message conversations, social media interactions, and other files throughout the enterprise. The key capabilities within Proofpoint Enterprise Archive include:

**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.

**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-premise 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.

7

---

## Table of Contents

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 Enterprise Archive include:

Regulatory compliance. 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.

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 Enterprise Governance can track, classify, monitor, and apply governance policies to unstructured information across the enterprise. By proactively governing unstructured information "in-place," organizations can effectively manage regulatory compliance, increase control over information and mitigate legal and financial risks. The key capabilities within Proofpoint Enterprise Governance include:

Document tracking—digital thread. Proofpoint Enterprise Governance creates a unique "digital fingerprint" for every document and version. Our solution can monitor most major document stores including share-drives, Microsoft Sharepoint, Microsoft Exchange, Lotus Domino, EMC Documentum and desktops, and track every document, version and location. This enables organizations to track and govern their sensitive documents wherever they travel inside or outside the enterprise.

Cloud-based search and analytics. By employing advanced search techniques, we are able to deliver detailed reporting on all monitored documents and locations. Administrators can quickly locate all copies and versions of a given document or run summary reports detailing types and locations of stored documents throughout the enterprise.

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, project or geography.

Key benefits of Proofpoint Enterprise Governance include:

Regulatory compliance. Helps organizations meet regulatory requirements by systematically retaining required documents and unstructured content according to compliance retention policies and enabling staff to efficiently

review and enforce these policies.

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

Efficient litigation support. Provides advanced search features that locate all copies of documents wherever they live reducing the cost of eDiscovery and allowing organizations to effectively manage the litigation process.

8

---

## Table of Contents

Reduced storage and management costs. Reduces document management and storage costs by automating the reporting and clean-up of unnecessary documents including duplicates, intermediate versions and non-business records.

### Proofpoint Nexgate Social Media & Compliance

Our Nexgate Social Media Security & Compliance solution enables customers to effectively protect their online brand presence and social media communication infrastructure. Nexgate technology automatically identifies and remediates fraudulent social media accounts, account hacks, and content that contains malware, spam and abusive language. In addition, the Nexgate solution enables enterprises to enforce policies on authorized accounts and posts in order to comply with a wide-range of social media regulatory requirements including FTC, FINRA, FFIEC, FDA, HIPAA, PHI, SEC, ABA and more. Key capabilities within Proofpoint Nexgate Social Media & Compliance include:

**Discovery:** Using a native cloud-based platform, customers can quickly find the social media applications, accounts, and properties that are affiliated with their brands, measure the footprint and activity for their accounts, benchmark that against competitors, identify key content and risks and report on aspects of security and compliance.

- **Monitoring:** 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.

**Protection:** Using proprietary Deep Social Linguistic Analysis (DSLA) technology, social media and brand managers can aggregate content from across their enterprise and review it for security, risk and compliance violations (including FINRA, FFIEC, FDA, SEC, FCA violations), allowing them to safely syndicate content distribution across their social media marketing platforms.

Key benefits of Proofpoint Nexgate Social Media Security & Compliance include:

**Abuse prevention:** Scans social networks to discover and track an organization's accounts and detect fraudulent social media accounts. Automatically protects social media channels from malware, spam, hacks, abusive and offensive content. Effectively scales account moderation with automated, accurate identification of bad content.

**Additional security:** Detects unauthorized changes and anomalous behavior on social account profiles. Locks down pages and accounts in the event of vandalism or hack. Catches and logs unauthorized changes to accounts and associated applications.

**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.

### Proofpoint Essentials

Proofpoint Essentials is 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 and email archiving.

### Platform Services



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

9

---

## Table of Contents

**Content inspection.** Applies our Proofpoint MLX machine learning techniques to understand the meaning of email, documents and social networking communications and to identify and classify content as malicious, sensitive or relevant to a litigation matter for threat protection, data loss prevention and discovery.

**Reputation.** Leverages machine learning and big data analytics to analyze and correlate billions of requests per day to create a dynamic reputation profile of hundreds of millions of IP addresses, domains, web links and other Internet content. This database of reputation profiles is used to help identify and block malicious attacks.

**Encryption and key management.** Securely encrypts data and stores and indexes hundreds of thousands of individual encryption keys without requiring cumbersome key-exchange or other end-user set-up. Enables authorized users to quickly and easily decrypt and view content from a wide variety of devices.

**Notification and workflow.** Creates notifications and an enabling workflow to alert administrators and compliance officers of an incident and enable subsequent review, commentary, tracking, escalation and remediation of each event.

**Analytics and search.** Provides an easy-to-use, web-based interface for searching and analyzing information to enable enterprises to rapidly trace inbound and outbound messages, analyze how messages were processed by a Proofpoint Enterprise deployment, report on the disposition and status of any email message, and retrieve in real-time archived communications for litigation support and eDiscovery.

## 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.

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

**Virtual execution environments.** An advanced approach to threat detection wherein suspected malware is exposed to a permuted set of instrumented virtual system environments, to assess maliciousness, exploit activity and compromise

processes.

Infrastructure

10

---

## Table of Contents

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 eight 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 archiving and governance 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.

**Flexibility.** 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.

**Low cost.** We deploy our services on shared, low-cost, commodity computing and storage infrastructure. In addition, we utilize multi-tenancy and hardware virtualization to further reduce hardware and management costs. Because we primarily rely on internally developed and open source technology instead of commercially licensed technology, we are able to offer a cost-effective solution to our customers.

## Customers

As of December 31, 2014, we had approximately 3,300 customers of all sizes across a wide variety of industries, including 45 of the Fortune 100. A number of our largest customers use our platform to protect millions of users and handle tens of millions of 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 and 14% of total revenue in both 2013 and 2012. In each year since the launch of our first solution in 2003, we have retained over 90% of our customers.

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; 25 of the 50 largest companies 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:

3 of the 5 largest U.S. retailers

2 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

11

---

## Table of Contents

2 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 (2,500 employees and above), mid-sized organizations (500 - 2,500 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 reseller channel includes top security organizations including Accuvant, Adaptive Solutions, Inc., Exclusive Networks SAS, FishNet Security, Forsythe Technology Inc., Insight Direct USA, SBS Security, SHI International Corp, Vinitech, Inc. and World Wide Technology Inc.

**Strategic relationships.** We also sell our solutions indirectly through key technology companies such as IBM and Microsoft that offer our solutions in conjunction with one or more of their own products or services. These companies each have a large, established customer base built around a broad platform of products and solutions sold under their own brand, and they promote our products to augment their own branded solutions.

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 fee based on the total value of the order. 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

Our marketing programs include a variety of online marketing, advertising, conferences, events, white-papers, public relations activities and web-based seminar campaigns targeted at key decision makers within our prospective customers.

We have a number of marketing initiatives to build awareness about our solutions and encourage customer adoption of our solutions. We offer free trials, competitive evaluations and free security and compliance risk audits 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.

## Table of Contents

### Proofpoint Support Services

We deliver 24x7x365 customer support from support centers located in the United States, Japan, Malaysia, Singapore, Canada and the United Kingdom. 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 \$51.9 million, \$34.4 million and \$24.8 million for 2014, 2013 and 2012, respectively.

### 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 governance solutions generally have product offerings that provide data storage, search, policy enforcement, legal-hold management, and in some cases supervision.

Key competitors include:

**Data Protection and Privacy:** Cisco (through its acquisition of IronPort), McAfee, an Intel subsidiary (through its acquisitions of Secure Computing and MX Logic), Microsoft (through its acquisition of Frontbridge), and Symantec (through its acquisitions of Brightmail and MessageLabs)

**Archiving and Governance:** Hewlett-Packard (through its acquisition of Autonomy) and Symantec (through its acquisitions of KVS and LiveOffice)

We believe we compete favorably based on the following factors:

• Level of protection against advanced threats;



•comprehensiveness and integration of the solution;

•flexibility of delivery models;

•total cost of ownership;

•scalability and performance;

•customer support; and

13

---

## Table of Contents

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, 2014, we had 42 patents and 24 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.

## Employees

As of December 31, 2014, we had 859 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 (408) 517-4710. Our website is [www.proofpoint.com](http://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 13, "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 public may 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. 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. Copies of Proofpoint's reports on Form 10-K, Forms 10-Q and Forms 8-K, may be obtained, free of charge, electronically through our Internet website, <http://>

Table of Contents

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.

15

---

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 \$64.2 million, \$27.5 million and \$20.4 million in 2014, 2013 and 2012, respectively. As a result, we had an accumulated deficit of \$274.2 million as of December 31, 2014. 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 important channel partners;
- general economic conditions, both domestically and in our foreign markets;

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



## Table of Contents

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 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.

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.

## Table of Contents

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.

We believe that there is a trend for large and mid sized enterprises to migrate their on premise email systems to cloud based offerings. If we fail to successfully develop, market, broaden or enhance our solutions to continue to be attractive to existing customers currently using cloud based email systems or to new prospects, our ability to grow or maintain our revenue could be harmed, and our business could suffer.

We derive a substantial portion of our revenue from our solutions that protect and archive data in our customers' on-premise email systems and expect to continue to do so for the foreseeable future. We currently derive a portion of our revenue from customers using cloud-based email systems such as Google's Google Apps and Microsoft's Office 365, both of which include varying degrees of threat protection and governance services as part of their offering. A significant market shift from on premise email systems toward such cloud based email systems could decrease demand for our solutions because customers who move to cloud based email systems may no longer value our threat and governance solutions and may choose to instead use competing or low cost alternatives from companies such as Google or Microsoft that may offer competing solutions in connection with their cloud-based email systems. If our current or prospective customers who utilize cloud based systems fail to find value in our solutions or migrate to these other threat or governance offerings, our business could be adversely affected.

Historically, our solutions have been used primarily for email, and any decrease in the use of email systems by large and mid sized enterprises over time, or the failure of our newly developed solutions for emerging methods of communication and collaboration to gain acceptance could harm our business.

Historically, our customers have primarily used our solutions to protect and archive data in their corporate email systems. If the use of email decreases, demand for our solutions would decrease and we may fail to diversify our revenue base by increasing demand for our other technology solutions.

In addition, messaging and collaboration technologies are evolving rapidly. For instance, the widespread adoption and use of mobile devices, unmanaged Internet based collaboration and file sharing applications and social networking sites have caused valuable and sensitive data to proliferate well beyond traditional corporate email systems, resulting in new and increasing security risks. We are devoting resources to continue acquiring, developing and marketing our solutions for these emerging methods of communication and collaboration. However, our customers may not perceive the need to deploy our solutions intended to address these emerging areas. If we are unable to successfully develop, market, broaden or enhance our solutions to address the wider range of threats caused by the proliferation of new technologies and methods of communication, demand for our existing solutions would decrease, and our business would be harmed.

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

Table of Contents

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.

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.

Our traditional competitors include security focused software vendors, such as Symantec Corporation and McAfee, Inc., an Intel Corporation subsidiary, 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 Cisco, Google Inc., Hewlett Packard Company, Intel and Microsoft. 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 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. For example, Cisco's acquisition of IronPort, an email and web security service, resulted in Cisco becoming one of our competitors. 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 to support our growth. 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.

## Table of Contents

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. Additionally, 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 17 to 22 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. 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;



Table of Contents

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;  
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  
new and different sources of competition.

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

If the market for our delivery model and cloud computing services develops more slowly than we expect, our business could be harmed.

Our success will depend to a substantial extent on the willingness of enterprises, large and small, to increase their use of cloud computing services. The market for messaging security and data compliance solutions delivered as a service in particular is at an early stage relative to on-premise solutions, and these applications may not achieve and sustain high levels of demand and market acceptance. Many enterprises have invested substantial personnel and financial resources to integrate traditional enterprise software or hardware appliances for these applications into their businesses or may be reluctant or unwilling to use cloud computing services because they have concerns regarding the risks associated with reliability and security, among other things, of this delivery model, or its ability to help them comply with applicable laws and regulations. If enterprises do not perceive the benefits of this delivery model, then the market for our services may develop more slowly than we expect, which would adversely affect our business and operating results.

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



## Table of Contents

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.

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.

Table of Contents

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.

Our operations also rely heavily on the availability of electricity, which also comes from third party providers. If we or the third party data center facilities that we use to deliver our services were to experience a major power outage or if the cost of electricity were to increase significantly, our operations and financial results could be harmed. If we or our third party data centers were to experience a major power outage, we or they would have to rely on back-up generators, which might not work properly or might not provide an adequate supply during a major power outage. Such a power outage could result in a significant disruption of our business.

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.

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.

24

---

Table of Contents

We rely on a combination of contractual rights, trademarks, trad