PROOFPOINT INC
Form 10-K
March 08, 2013
Table of Contents

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

FORM 10-K

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

For the Fiscal Year Ended December 31, 2012

OR

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

For the Transition Period from to

Commission File Number 001-35506

PROOFPOINT, INC.

(Exact name of Registrant as specified in its charter)

Delaware	51-0414846
(State or other jurisdiction of incorporation or organization)	(I.R.S. employer identification no.)
892 Ross Drive Sunnyvale, California	94089
(Address of principal executive offices)	(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	Name of each exchange on which registered
Common Stock , $0.0001 par value per share	NASDAQ Global Select Market

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

None

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

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 o NO þ

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 þ NO o

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 þ NO o

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

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

Large accelerated filer o	Accelerated filer o	Non-accelerated filer þ (Do not check if a smaller reporting company)	Smaller reporting company o

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

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, 2012 as reported by the NASDAQ Global Select Market on that date, was approximately $250,969,000. 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 December 31, 2012 was 33,043,665 shares.

_____

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement for its 2012 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, 2012.

Table of Contents

PROOFPOINT, INC.
FORM 10-K
For the Fiscal Year Ended December 31, 2012
TABLE OF CONTENTS

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 pioneering security-as-a-service vendor 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, regulatory compliance, archiving and governance, 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 and advanced encryption, 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, are driving an unprecedented wave of targeted, malicious attacks designed to steal valuable information. At the same time, the growth of business-to-business collaboration, as well as the consumerization of IT and the associated adoption of mobile devices and unmanaged Internet-based applications, have 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 securely archiving these communications for compliance and discovery. We address four important problems for the enterprise:

- Keeping malicious content out;
- 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 2,700 customers worldwide, including 27 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 including IBM, Microsoft and VMware.

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, regulatory compliance, archiving and governance, 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, instant messaging, social media and other web-based applications, but also 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:

Table of Contents

- Superior protection against advanced, targeted threats. We use a combination of proprietary technologies for big data analytics, machine learning and deep content inspection to detect and stop targeted "spear phishing" and other sophisticated attacks. By processing and modeling billions of requests per day, we can recognize anomalies in traffic flow to detect targeted attacks. 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.

- Comprehensive, integrated data protection suite. We offer a comprehensive solution for data protection and governance through an integrated, security-as-a-service platform that is comprised of four main suites: Proofpoint Enterprise Protection, Proofpoint Enterprise Privacy, Proofpoint Enterprise Archive and Proofpoint Enterprise Governance. 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 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

We provide a multi-tiered security-as-a-service platform consisting of solutions, platform technologies and infrastructure. Our platform currently includes four solutions bundled for the convenience of our customers, distributors and resellers: Proofpoint Enterprise Protection, Proofpoint Enterprise Privacy, Proofpoint Enterprise Archive and Proofpoint Enterprise Governance. Each of these solutions is built on 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.

Table of Contents

Solutions

Our security-as-a-service platform includes four solutions bundled for the convenience of our customers: Proofpoint Enterprise Protection, Proofpoint Enterprise Privacy, Proofpoint Enterprise Archive and Proofpoint Enterprise Governance.

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.

- 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 anti-virus 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.

Table of Contents

- 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. Protects enterprises against advanced persistent threats such as phishing and other targeted email attacks using big data analysis techniques to identify and apply additional security controls against suspicious messages and any associated links to the web.

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.

- 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 (GLBA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the Payment Card Industry Security Standard Council's Data Security Standards (PCI-DSS). 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.

- 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 users, 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 allow 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.

Table of Contents

Key benefits of Proofpoint Enterprise Privacy include:

- Regulatory compliance. Allows 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 accidently 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

Proofpoint Enterprise Archive 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.

- 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.

Table of Contents

- 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

Proofpoint Enterprise Governance provides organizations the ability to 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 clearcorporate 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.

- 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.

Platform Services

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

- 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.

Table of Contents

- 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 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.

Infrastructure

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

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.

Table of Contents

- 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.

During 2012, we had $5.9 million in capital spending in part to support infrastructure expansion. These expenditures are primarily in connection with the replacement and upgrade of equipment to lower the cost of deployment as well as to improve the efficiency for our cloud-based architecture.

Customers

As of December 31, 2012 we had approximately 2,700 customers of all sizes across a wide variety of industries, including 27 of the Fortune 100. Several 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 no single partner or customer accounting for more than 10% of total revenue in 2010 or 2011 and one customer, a strategic partner serving a number of end customers with our platform, who accounted for 14% of total revenue in 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 financial services, retail, manufacturing, aerospace and defense, healthcare, education and government. We have been particularly successful selling to the largest enterprises; 19 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:

- 4 of the 5 largest U.S. retailers