

PROOFPOINT INC
Form 10-K
February 21, 2019
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, 2018

OR

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

For the Transition Period from to

Commission File Number 001-35506

PROOFPOINT, INC.

(Exact name of Registrant as specified in its charter)

Delaware	51-0414846
(State or other jurisdiction of 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

Edgar Filing: PROOFPOINT INC - Form 10-K

Common Stock, \$0.0001 par value per share NASDAQ Global Select Market
Securities registered pursuant to Section 12(g) of the Act:

None

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

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

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

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted 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 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, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer", "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	Accelerated filer
Non-accelerated filer	Smaller reporting company
	Emerging growth company

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

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, 2018 as reported by the NASDAQ Global Select Market on that date, was approximately \$5,798 million. 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 8, 2019 was 55,349,592 shares.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement for its 2018 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, 2018.

PROOFPOINT, INC.

FORM 10-K

For the Fiscal Year Ended December 31, 2018

TABLE OF CONTENTS

	Page
<u>PART I.</u>	
Item 1. <u>Business</u>	4
Item 1A. <u>Risk Factors</u>	16
Item 1B. <u>Unresolved Staff Comments</u>	33
Item 2. <u>Properties</u>	33
Item 3. <u>Legal Proceedings</u>	34
Item 4. <u>Mine Safety Disclosures</u>	34
<u>PART II.</u>	
Item 5. <u>Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities</u>	35
Item 6. <u>Selected Financial Data</u>	36
Item 7. <u>Management's Discussion and Analysis of Financial Condition and Results of Operations</u>	39
Item 7A. <u>Quantitative and Qualitative Disclosures About Market Risk</u>	60
Item 8. <u>Financial Statements and Supplementary Data</u>	61
Item 9. <u>Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</u>	61
Item 9A. <u>Controls and Procedures</u>	61
Item 9B. <u>Other Information</u>	61
<u>PART III.</u>	
Item 10. <u>Directors, Executive Officers and Corporate Governance</u>	62
Item 11. <u>Executive Compensation</u>	62
Item 12.	62

Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters

Item 13. Certain Relationships and Related Transactions, and Director Independence 62

Item 14. Principal Accountant Fees and Services 62

PART IV.

Item 15. Exhibits and Financial Statement Schedules 63

Signatures 106

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.

PART I

ITEM 1. BUSINESS

Overview

Proofpoint is a leading next-generation cybersecurity company that enables large and mid-sized organizations worldwide to protect the way their people work from advanced threats and compliance risks. Our integrated suite of products works together to help organizations build people-centric security and compliance programs. We provide threat protection, information protection, user protection, business ecosystem protection, and compliance solutions to address today's rapidly changing threat and compliance landscape. Our solutions are built on a flexible, cloud-based platform and leverage 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.

Every company's greatest asset and greatest security risk is its people. Cyberattacks have fundamentally shifted from targeting infrastructure to targeting people, relying on tricking users into running code, divulging their passwords, or even sending money or data. This transformation of the threat landscape manifests in nearly every form of cyber threat, from nation state advanced persistent threat (APT) actors relying on phishing, through to cybercriminals launching massive ransomware email campaigns, and more targeted campaigns designed to steal valuable data from both legacy and cloud-based systems. At the same time, the rapid adoption of cloud applications has increased organizations' attack surface by moving both threats and sensitive data away from the traditional network perimeter, reducing the effectiveness of many existing security products. These factors have contributed to an increasing number of severe data breaches and expanding regulatory mandates, notably the European Union's General Data Protection Regulation (GDPR), all of which have accelerated demand for effective threat protection and compliance solutions.

Our platform addresses this growing challenge by not only protecting data as it flows into and out of the enterprise via on-premises and cloud-based email, social media, and other cloud applications, but also by keeping track of this information as it is modified and distributed throughout the enterprise for compliance and data loss prevention, and securely archiving these communications for compliance and discovery. We help organizations reduce their critical risk in five major ways:

- Protecting users from the advanced attacks that target them via email, web, networks, social media, and cloud apps;
- Preventing the theft or inadvertent loss of sensitive information and, in turn, ensuring compliance with regulatory data protection mandates;
- Improving the resilience of end-users to the threats that target them and training them to be better caretakers of their organizations' critical data;
- Collecting, retaining, supervising and discovering communications and sensitive data for compliance and litigation support; and
- Enabling organizations to respond quickly to security issues, providing both the intelligence and the context to prioritize incidents and orchestrate remediation actions.

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

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

defend against a wide range of threats, including email, mobile apps and social media, to protect the

4

information people create from both compromise and compliance risks, and to archive and govern corporate information. Today, our solutions are used worldwide to protect well over 100 million end-users at enterprise customers, and millions more via service providers through our Cloudmark division. We market and sell our solutions worldwide both directly through our sales teams and indirectly through a hybrid model where our sales organization actively assists our network of distributors and resellers. We also distribute our solutions through strategic partners.

Proofpoint Solutions

Our integrated suite of on-demand security-as-a-service solutions enables large and mid-sized organizations to protect people throughout the enterprise from advanced attacks and compliance risks. Our comprehensive platform provides a secure email gateway, advanced threat protection, security awareness training, threat intelligence, email authentication, email encryption, data loss prevention, digital risk protection, cloud application protection, web browser isolation, archiving, e-discovery, and threat response capabilities. These solutions are built on a cloud-based architecture, protecting enterprises and their customers from inbound threats via email, social media, and mobile apps, while identifying and protecting enterprise data not only where it is stored within the enterprise but also as it transits beyond the organization's borders such as via email or social media. We have pioneered the use of innovative technologies to deliver better ease-of-use, greater protection against the latest advanced threats, and lower total cost of ownership than traditional alternatives. The key elements of our solution include:

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

• **Comprehensive, integrated email security, advanced threat, information protection and archiving, and digital risk protection product families.** We offer a comprehensive solution for email security that we believe is unparalleled in the market. Our Threat Protection product family includes solutions to protect organizations across the predominant threat vectors, including email, web, social media, and cloud applications. To protect enterprise data from security and compliance risks, our Information Protection product family includes a suite of security and compliance solutions. Finally, we enable organizations to look beyond their borders for threats targeting their customers across email phishing, malicious web domains, compromised cloud accounts, and fraudulent social media accounts.

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

devices as their primary computing platform. We also provide solutions that train end-users to be the last line of defense against cyber-attacks.

5

• **Security optimized cloud architecture.** Our multi-tenant security-as-a-service solution leverages a distributed, scalable architecture deployed in our global data centers for deep content inspection, global threat correlation and analytics, high-speed search, secure storage, encryption key management, software updates, intelligent message routing, and other core functions. Our architecture also enables us to look across hundreds of billions of data points gathered from across our product portfolio and intelligence feeds to better correlate and analyze both targeted and broad-based threat campaigns. Customers can choose to deploy optional physical or virtual points-of-presence behind their firewalls for those who prefer to deploy certain functionality inside their security perimeter. This architecture enables us to leverage the benefits of the cloud to cost-effectively deliver superior security and compliance, while optimizing each deployment for the customer's unique threat environment.

• **Extensible security-as-a-service platform.** The key components of our security-as-a-service platform, including services for secure storage, content inspection, reputation, big data analytics, encryption, key management, and identity and policy, can be exposed through application programming interfaces, or APIs, to integrate with internally developed applications as well as with those developed by third-parties. In addition, these APIs provide a means to integrate with the other security and compliance components deployed in our customers' infrastructures, including Proofpoint's ecosystem partners.

Our Security-as-a-Service Platform

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

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

Product Families

Proofpoint Threat Protection

Proofpoint Threat Protection products leverage a broad set of detection techniques that are constantly refined as the threat landscape evolves. The products detect and prevent threats across email, web, networks, and cloud applications, and deliver rich intelligence to enable enterprises to understand as much as possible about the attacks they are seeing and the adversaries behind them.

Key capabilities within the Threat Protection products include:

• **Email security and continuity.** Provides protection from unwanted and malicious email, with granular visibility and business continuity for organizations of all sizes. It provides IT and security teams with confidence in securing end-users from email threats and maintain email communications during outages.

•

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

Protection from targeted attacks. Enterprises are protected against both commodity and advanced threats such as phishing and other targeted email attacks using big data analysis, predictive, virtual execution, static analysis, protocol analysis, and dynamic malware analysis techniques to identify and apply additional security controls against suspicious messages, attachments and any associated links to the web. The same detection techniques are extended to look for malicious content in enterprise social media accounts, malicious links and files sent to users via cloud applications. It also detects suspicious login activity that could indicate signs of account compromise.

Detection of compromised cloud accounts and internal email threats. We take a multi-layered approach to protect an organization's internal email by scanning all internal email for spam, malicious attachments, and malicious URLs. We also provide automated protection of account compromise in Office 365. These threats typically start with phishing or other techniques, such as credential-stealing malware and brute-force credential stuffing. Compromised accounts are then used to launch lateral attacks, everything from business email compromise ("BEC") to internal phishing attacks, both inside and outside organizations.

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

Web browser isolation. Allows end-users to access websites and personal webmail from corporate devices while preventing malware or malicious content from impacting the user or device.

Threat intelligence feed and ruleset. Verified threat intelligence from one of the world's largest malware exchanges. Unlike other intelligence sources that report only domains or IP addresses, ET Intelligence includes a five-year history, proof of conviction, more than 40 threat categories and related IPs, domains, and samples. This also comes in the form of a timely and accurate rule set for detecting and blocking threats using existing network security appliances—including next generation firewalls (NGFW) and network IDS/IPS.

Key benefits of Proofpoint Threat Protection include:

Superior protection from advanced threats, spam and viruses. Proofpoint's agility in deploying new detection measures and adjusting defenses in response to changes in the threat landscape results in high effectiveness in stopping threats before they reach enterprise users. Protects against advanced threats, spam and other malware such as remote access Trojans, banking Trojans, ransomware, viruses, 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.

Protection from internal threats, including compromised email or cloud accounts. Security teams gain visibility into cloud accounts that sent malicious emails or exhibited suspicious activity, so they can quickly track down and act upon potentially compromised accounts.

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

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

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

- Superior protection from business email compromise. Combining a dynamic classifier on the email gateway with a proactive authentication solution and a lookalike domain discovery service delivers protection from these attacks.
- Business continuity. Provides an always-on insurance policy for crucial business communications via email.
- Automation of incident response to save time and optimize resources. Automate the threat data enrichment, forensic verification, and response processes after a security alert is received. Automatically confirm malware infections, check for evidence of past infections, and enrich security alerts by automatically adding internal and external context and intelligence.
- Secure, anonymous web browsing for employees. Mitigates security, productivity, and privacy challenges associated with untrusted, high-risk web use by employees.

Proofpoint Information Protection

A comprehensive data protection strategy must address both security and compliance risks. Our data loss prevention, encryption and compliance solutions defend 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), the European Union GDPR, and the Payment Card Industry Data Security Standard (PCI-DSS).

Key capabilities within Proofpoint Information Protection products 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, cloud 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.
- 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.
- Encrypted message portal. Organizations in regulated industries like financial services and healthcare frequently need to share highly confidential messages with outside parties. Proofpoint provides a “pull encryption” portal that enables these organizations to create branded portals that seamlessly integrate with their email systems to securely communicate with their customers, patients, or other third parties.
- Secure file sharing. Cloud-based security-focused solution designed to enable enterprise users to securely exchange large files with ease while staying compliant with enterprise data policies.
- Discovery of sensitive data in on-premises and cloud-based file stores. Automated discovery and remediation solution that identifies sensitive content across the enterprise and enables corrective action, while reducing risk of data breaches and compliance violations.

Key benefits of Proofpoint Information Protection include:

- Regulatory compliance. Data Loss Prevention and Encryption enable outbound messages to comply with national and state government and industry-specific privacy regulations, while Enterprise Archive helps organizations meet regulatory requirements by archiving all messages and content according to compliance retention policies and enabling staff to systematically review messages for compliance supervision. SaaS Protection extends the same compliance functionality to cloud applications like Office 365, Box, Salesforce, and G Suite.

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

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

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

Proofpoint User Protection

Proofpoint User Protection combines simulation, assessments, education, reinforcement, and measurement to provide the ideal foundation for your security awareness and training program, utilizing hundreds of different phishing templates across dozens of languages and categories to simulate attacks and evaluate end-users on various threats, including malicious attachments, embedded links, and requests for personal data. Users who are deceived by simulated attacks receive “just-in-time teaching” and administrators receive real-time reporting to focus awareness efforts and track progress.

Key capabilities within Proofpoint User Protection products include:

• **Simulating phishing attacks.** Create simulated attacks that include attachments, embedded links, and requests for personal data in different languages.

• **End-user reporting of phishing.** End-users can report a suspicious message with a single click using the email reporting button. Automatically analyze reported messages against multiple intelligence and reputation systems. The system can be configured with other Proofpoint solutions to delete or quarantine real threats with a single click.

• **Security awareness training and assessments.** Educate employees to improve awareness, change user behavior, and reduce security risk to the organization. Proofpoint provides a comprehensive and effective library of anti-phishing training.

Key benefits of Proofpoint User Protection include:

• **Understand organization’s security and compliance risk.** Track training, phishing simulation, and threat reporting results to build your security awareness program accordingly.

• **Change end-user behavior to reduce risk to your organization.** Application of our continuous training methodology produces highly effective results for changing user behavior.

Proofpoint Business Ecosystem Protection

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

Key capabilities within Proofpoint Business Ecosystem Protection products include:

• **Preventing email fraud.** Enables organizations to understand who is sending email from their domains and create a policy to both authenticate legitimate email and block fraudulent email.

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

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

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

Key benefits of Proofpoint Business Ecosystem Protection include:

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

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

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

Proofpoint Compliance Solutions

Proofpoint Compliance Solutions are designed to ensure accurate enforcement of data governance, data retention and supervision policies and mandates; cost-effective litigation support through efficient discovery; and active legal-hold management. It can store, govern and discover a wide range of data including email, instant message conversations, social media interactions, and other files throughout the enterprise. With this solution, enterprises can engage with their customers across web, email, mobile, and social media with the confidence that their brands and customers are safe from all forms of digital risk.

The key features of the Compliance Solutions product family 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.

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

• **Search performance.** By employing parallel, big data search techniques, we can 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 FINRA and the SEC in the financial services industry.

Key benefits of Proofpoint Compliance Solutions include:

✦ **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 e-discovery.

✦ **Efficient litigation support.** Provides advanced search features that reduce the cost of e-discovery 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.

Platform Services

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

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

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

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

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

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

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

Enabling Technologies

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

- **Big data analytics.** Indexes and analyzes petabytes of information in real-time to discover threats, detect data leaks and enable end-users to quickly and efficiently access information distributed across their organizations.
- **Machine learning.** Builds predictive data models using our proprietary Proofpoint MLX machine learning techniques to rapidly identify and classify threats and sensitive content in real-time.
- **Identity and policy.** Enables the definition and enforcement of sophisticated data protection policies based on a wide set of variables, including type of content, sender, recipient, pending legal matters, time and date, regulatory status and more.
- **Secure storage.** Stores petabytes of data in the cloud cost-effectively using proprietary encryption methods, keeping sensitive data tamper-proof and private, yet fully searchable in real-time.
- **Virtual execution environments.** Exposes suspected malware to a permuted set of instrumented virtual system environments, to assess maliciousness, exploit activity and compromise processes.
- **Intelligent message routing.** Policies can be established by administrators to automatically direct email communications differently through the email network, based on aspects of the messages, for security, compliance, supervisory, system performance, or other reasons.
- **Threat intelligence correlation.** Utilizes inputs from Proofpoint, cloud, and other third-party products to assess IoCs and confirm successful system compromises by malicious actors in near-real-time, then administers network controls to effectively contain the compromised systems.

Infrastructure

We deliver our security-as-a-service solutions through our cloud architecture and international data center infrastructure. We operate thousands of physical and virtual servers across seventeen data centers located in the United States, Canada, the Netherlands, France, 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 information protection and archiving solution, enabling us to serve the rigorous security requirements of U.S. federal agencies.
- **Scalability and performance.** By leveraging a distributed, scalable architecture we process billions of requests against our reputation systems and hundreds of millions of messages per day, all in near real-time. Massively-parallel query processing technology is designed to ensure rapid search results over this vast data volume. In addition to this aggregate scalability across all customers, our architecture also scales to effectively meet the needs of several of our largest individual customers, each of which has millions of users and processes tens of millions of messages per day.
- **Hybrid Deployment.** Our cloud architecture enables individual customers to deploy entirely in Proofpoint's global data centers or in hybrid configurations with optional points of presence located behind the customer's firewall. This deployment flexibility enables us to deliver security, compliance and performance tailored to the unique threat profile and operating environment of each customer.

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

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

Customers

As of December 31, 2018, we had customers of all sizes across a wide variety of industries. A number of our largest customers use our platform to protect more than a million users and handle over a billion messages per day. During the years ended December 31, 2018 and 2017, one partner accounted for 12% of total revenue, although the partner sold to a number of end-users, none of which accounted for more than 10% of our total revenue in 2018 and 2017. During the year ended December 31, 2016, no individual customer accounted for more than 10% of total revenue. In each year since the launch of our first solution in 2003, we have maintained a renewal rate with our existing customers of over 90%.

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

- 3 of the 5 largest U.S. retailers
- 4 of the 5 largest U.S. aerospace and defense contractors
- 5 of the 5 largest U.S. banks
- 4 of the 5 largest global pharmaceutical companies
- 4 of the 5 largest U.S. petroleum refining companies

Sales and Marketing

Sales

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

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

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

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

under their own brand and sometimes under the Proofpoint brand. In addition, our Cloudmark division delivers email protection to many of the largest global internet service providers.

13

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

Marketing

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

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

Customer Service and Support

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

Proofpoint Support Services

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

Proofpoint Professional Services and Training

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

Research and Development

We devote significant resources to improve and enhance our existing security solutions and maintain the effectiveness of our platform, monitoring the threat landscape in real-time and making constant adjustments to remain effective as the threat landscape shifts. 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.

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

Key competitors include:

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

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

We believe we compete favorably based on the following factors:

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

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

Intellectual Property

We rely on a combination of trade secrets, patents, copyrights and trademarks, as well as contractual protections, to establish and protect our intellectual property rights and protect our proprietary technology. As of December 31, 2018, we had 120 patents and 54 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, 2018, we had 2,613 employees. We also engage a number of temporary employees and consultants. None of our employees is represented by a labor union with respect to his or her employment with us. We have not experienced any work stoppages and we consider our relations with our employees to be good. Our future success will depend upon our ability to attract and retain qualified personnel. Competition for qualified personnel remains intense and we may not be successful in retaining our key employees or attracting skilled personnel.

Corporate Information

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

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

Geographic Information

For financial reporting purposes, net revenue and long-lived assets attributable to significant geographic areas are presented in Note 12, “Segment Reporting”, to the consolidated financial statements, which is incorporated herein by reference.

Available Information

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