

## Spam 2011: Protection Against Evolving Threats



**A Proofpoint White Paper**

The very best anti-spam solutions today deliver 95% effectiveness. Unfortunately, that's not good enough. A border-line attack that gets through a 5% gap in defenses could cost your organization millions of dollars in terms of business lost, exposure to privacy threats, and brand loyalty.

This white paper discusses the ongoing evolution of spam threats and the technology needed to close that remaining 5% gap in defenses. To defeat spam, enterprises need a holistic approach rather than an uncoordinated collection of features and filters. By systematically tying features together through real-time machine learning and analysis, enterprises can increase the effectiveness of their spam defenses to nearly 100%.

## CONTENTS

---

Introduction: The Spam Onslaught Continues	1
Understanding the Evolving Threat	1
Botnets	1
Phishing and Low-Volume Targeted Threats	1
Blended Threats	2
Social Engineering	2
Outbound Spam	2
Requirements for Effective Defenses Against Spam	3
Core Technology Capabilities	3
Enterprise Readiness Capabilities	4
Proofpoint's Anti-spam Solution	5
Anti-phishing Protection	7
Anti-virus and Anti-malware Protection	7
Manageability and End User Controls	7
Flexibility: SaaS Without Compromise	7
Integration with Email Infrastructure and Other Security Solutions	7
Benefits of Proofpoint Enterprise Protection	8
Conclusion	8
About Proofpoint, Inc.	8
Notes	8

## INTRODUCTION: THE SPAM ONSLAUGHT CONTINUES

The very best anti-spam solutions today deliver 95% effectiveness. Unfortunately, that's not good enough. A border-line attack that gets through a 5% gap in defenses could cost your organization millions of dollars in terms of business lost, exposure to privacy threats, and brand loyalty.

Recent attacks show that hackers are determined to find their way through any gap, however slight, in an enterprise's defenses. They're exploiting a variety of tactics—including blended attacks combining email, Web access, and phony Web sites—to infect systems on enterprise networks. Blocking 95% of attacks is impressive but ultimately insufficient if the attacks that do reach your network disrupt business continuity, leak intellectual assets, perpetrate fraud, and tarnish your organization's brand.

Throughout 2010 and into the early months of 2011, spam has accounted for roughly 90% of all email. Spam volumes rise and fall, but declines in spam volumes never last long. The bottom line for enterprises? They can't afford to be complacent. The threats are real, and so are the repercussions.

This white paper discusses the ongoing evolution of spam threats and the technology needed to close that remaining 5% gap in defenses. To defeat spam, enterprises need a holistic approach rather than an uncoordinated collection of features and filters. By systematically tying features together through real-time machine learning and analysis, enterprises can increase the effectiveness of their spam defenses to nearly 100%.

After surveying the requirements for anti-spam defenses, this paper concludes with a summary of the Proofpoint Enterprise Protection solution, which applies machine learning to create a holistic, enterprise-class solution for defending against both inbound and outbound spam threats, viruses, Zero-Day attacks, and other types of malware.

## UNDERSTANDING THE EVOLVING THREAT

What characterizes spam in 2011? And how do new types of spam change the requirements for anti-spam defenses?

### Botnets

Let's begin with botnets, since the vast majority of spam travels through botnets.

A botnet is a network of malware-infected computers that can be controlled remotely by a hacker. A single botnet gives a spammer access to hundreds of thousands—even millions—of systems for copying and sending email. Some spammers have their own botnets; other spammers rent botnets from other hackers or criminal syndicates. In 2010, botnets accounted for over 88% of all spam.

Botnets have two major ramifications for spam defenses. First, spammers can start and stop massive spam attacks quickly. In the course of an hour, a spammer can activate a botnet, transmit millions of spam messages, and then turn the botnet off. Effective spam defenses need to account for the rapid start-up and shut-down times associated with botnet attacks.

Second, because each system in a botnet is responsible for sending only a fraction of the botnet's total volume of spam, the spam attack cannot be traced to a few IP addresses and then blocked. Spam defenses need to be able to detect and block spam attacks coming from a wide range of addresses.

Third, botnets' transformation of legitimate IP addresses into malicious IP addresses confounds many reputation-based spam defense systems. Slow-to-respond reputation-based systems will continue accepting email—now spam—from addresses that were trustworthy until the attack began. Effective spam defenses must rely on more than reputation analysis if they are going to stop spam attacks promptly.

### Phishing and Low-Volume Targeted Attacks

Another new trend in spam attacks is the rising occurrence of low-volume, targeted attacks, including phishing attacks.

Phishing is spam that impersonates an email from a trusted site, such as a bank, brokerage, or social media site, in order to lure recipients into clicking on a link or giving away confidential information. Phishing attacks can be used to steal users' login credentials and other information, or to infect the recipient's computer system with malware.

Because they resemble legitimate messages, many phishing attacks are able to slip through spam defenses. Reputation-based spam detection systems, which typically do well against high-volume attacks, often

fail to identify these low-volume attacks as spam. IT vendors that tout anti-spam effectiveness of 95% or higher might tolerate these low-volume attacks, since they don't represent a high percentage of spam overall. But though small in number, phishing attacks can be harmful and costly, and enterprises must guard against them.

## Blended Threats

Blended threats combine email with other technologies such as Web sites, to create an attack more difficult to detect. For example, a phishing attack that includes a URL to a fake login page that results in downloaded malware is a blended threat. Many spam defense products have difficulty identifying blended threats at attacks, because the email message includes no malware or tell-tale keywords. Defense systems treat the blended threat's email message as legitimate, even though it's part of a complex, carefully orchestrated attack.

Blended threats are often effective at using trusted brands, such as YouTube and Google, to win the trust of users and luring them into clicking on links or downloading software that turns out to be dangerous.

## Social Engineering

Social engineering is the use of knowledge about people or organizations to perpetrate a security attack. A spam message becomes much more credible if it mentions non-public information, such as the names of friends, the name of an internal project, or the name of an event the recipient recently attended. When many users receive information with specific "social" information like this, they don't think twice about clicking on a link, entering login credentials, or transferring confidential files such as financial statements.

The growing popularity of social networks such as Facebook (500 million members and growing), "business card" sites such as Jigsaw, and professional sites such as LinkedIn, makes it easier than ever for spammers to construct "social maps" of users and discover who is acquainted with whom. Spammers can also draw on the wealth of personal information people voluntarily publish—information such as travel schedules (through Twitter and sites like Triplt), current whereabouts (through Twitter and services such as FourSquare), and hobbies and interests (through Facebook profiles).

Using this information, spammers can craft highly believable blended threats that fool recipients into thinking they're responding to a Facebook message or answering a query sent by a colleague. In reality, though, these messages can be part of a devious scheme to give hackers access to user accounts or to other confidential data that can be sold or used for identity theft.

## Outbound Spam

When most people think of security problems associated with spam, they think only about inbound spam. But outbound spam can be a serious problem as well.

Most outbound spam is not the result of internal users deciding to make money or cause havoc. Rather, it's the result of internal systems becoming infected by malware that transforms them into nodes in a botnet. In most cases, the users of the infected systems have no idea that their systems' security has been compromised.

Conventional spam defense products don't monitor outbound traffic at all. They focus only on inbound spam. Even if they did monitor outbound traffic, their detection algorithms would likely fail to detect spam. A reputation-based system, for example, is unlikely to flag messages from its own network as suspicious.

But outbound spam is too dangerous to overlook. Like all spam, it needlessly consumes network and storage resources. Worse, it can damage a company's reputation if recipients discover that the company is sending spam. It can even prevent the enterprise from delivering legitimate messages to any other users, including partners and customers, whose spam defense systems block traffic from any IP address on a spam blacklist. An enterprise might find itself suddenly unable to deliver contracts to partners or promotions to customers. When outbound spam is flowing, business-critical email might not be. Consider a scenario where an employee's account is compromised. The hacker then begins to send spam or phish attacks to the employee's address book. These outbound, low-volume attacks would be difficult to detect without the appropriate technology.

## REQUIREMENTS FOR EFFECTIVE DEFENSES AGAINST SPAM

How should enterprises defend themselves against the ever-evolving threat of spam?

They should deploy anti-spam solutions that feature a baseline set of core technology capabilities implemented in a flexible, manageable solution that integrates easily with enterprise messaging and security infrastructures. The core technology capabilities are proven to stop nearly all spam attacks. When combined with machine-learning and real-time analysis, these core technology capabilities give enterprises the optimal defenses they need.

### Core Technology Capabilities

Good anti-spam solutions have four technology components:

- Verification Techniques
- Reputation Analysis
- Content Scanning
- Behavioral Analysis

If an anti-spam solution is going to provide the highest possible effectiveness, it must include all four of these components (even if the components are given different names by different vendors). The components must not only be present but must work together in order for the solution overall to be able to enforce security policies consistently and to optimize anti-spam defenses. Accordingly, these components belong on any product-evaluation checklist an enterprise might use for evaluating anti-spam solutions.

### Verification Techniques

Verification techniques detect spam and reduce spam volumes by using Internet standards and other enterprise services to verify the identity of email senders. Verification provides a baseline of functionality that addresses a large portion of basic spam attacks, especially phishing attacks and Denial of Service (DoS) attacks. Examples of verification techniques include:

- Recipient verification – ensuring that each recipient address in inbound emails matches a corresponding entry in an organization's Active Directory or LDAP directory.
- Bounce Address Tag Validation (BATV) – a standards-based technique that ensures that Non Delivery Reports bounced back to an organization are legitimate and not spoofs for spam.
- Sender Authentication – ensuring that the sender is who they say they are. Common techniques are SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail).

*Good questions for enterprises to ask: "What verification technologies do you use? Do you use BATV?"*

### Reputation Analysis

This technology tracks the reputation (normally as a numeric score) of a large number of source IP addresses that an enterprise encounters. The key advantage of reputation analysis is efficiency. To determine whether or not a message is spam, the system just needs to vet the message's IP address (merely a few bytes of data) as opposed to scanning the entire message and assessing tens or hundreds of kilobytes of content. The key disadvantage is that this technology is not effective against spam sent outbound from an organization, since the source IP will be that of the organization running the anti-spam defenses. Even for filtering inbound messages, this technology requires a real-time snapshot of IP addresses. This is because the source IP addresses of botnets can shift hour to hour, and the reputation service must be able to track and monitor the state of IP addresses across botnets.

*Good questions for enterprises to ask: "How real-time is your reputation analysis? How do you detect botnets? Can you detect a botnet that launched an attack 15 minutes ago?"*

### Content Scanning

As its name suggests, content scanning is the scanning of email contents for spam and malware. The most sophisticated content scanning solutions examine hundreds of thousands of attributes in email, and within a single message, examine hundreds of message attributes, including HTML and linguistic structures, to detect even subtle indications of the presence of spam. Spammers often use adversarial techniques to fool content filters into accepting spam messages, so the most effective solutions apply advanced statistics-

based classification methods such as machine learning to discover these new techniques and stay one step ahead of spammers. Other content scanning techniques based on heuristics or naïve Bayesian algorithms have proven less effective than machine learning.

For example, a good machine-learning technology can differentiate "I would love to buy a Rolex" (a legitimate message) from "Buy a Rolex online" (a spammy message). Content scanning is becoming increasingly important, because unlike techniques such as reputation analysis, which rely on analyzing the source IP address, it can be used to detect outbound spam.

*Good questions for enterprises to ask: "What techniques do you use to scan content? Do you also scan attachments? Can you detect outbound spam?"*

### **Behavioral Analysis**

This is the newest class of techniques, and its use can mean the difference between 99.5% and 99.99% effectiveness. When all is said and done, behavioral techniques fill in the analytical gaps required to identify the most sophisticated attacks. Behavioral technology looks at attributes of all incoming requests, and establishes insights and patterns into any anomalous behavior. This works well for previously unseen (e.g., Zero Day), low-volume attacks. Behavioral techniques require a large cloud infrastructure to be able to collect the data, baseline the performance, process insights, update the spam models, and push them back to customer sites in real time.

*Good questions for enterprises to ask: "How do you handle unseen spam? What about low volume targeted spam? What cloud-based analytics are used by your technology?"*

### **Machine Learning**

All four components described above require computation. How computation is performed is critical to vetting the right vendor. For example, using basic heuristic techniques for reputation and content scanning can yield false positives, because heuristic rules tend to be overly simplistic in their assessment of spam. It's critical that vendors rely on more advanced statistical technologies such as machine learning to ensure that the final probabilities computed (e.g. determining the probability that a message is spam) are free of false positives and as absolutely accurate as possible.

*Good questions for enterprises to ask: "What statistical techniques – if any – are used in your anti-spam defense? Does your solution automatically improve its accuracy over time?"*

The four components mentioned above, when built around a machine learning engine and operating in concert with one another, provide the most effective email defenses for enterprises. The techniques themselves operate "under the hood" and should be invisible to email administrators and security teams. A good anti-spam solution should "just work", and the true litmus test is whether or not it can deliver the highest effectiveness and lowest false positive possible.

### **Enterprise Readiness Capabilities**

In addition to the Technology Core outlined above, the solution should provide additional capabilities such as reliable spam detection that keeps up with latest spamming techniques, including blended threats and spam masquerading as legitimate messages from social networks. To detect Zero-Day threats, it needs to include algorithms that do not rely on signatures or blacklists, though signatures and blacklists may be used as part of a multi-layered approach to security.

*Good questions for enterprises to ask: "How does your solution detect Zero Day threats? How about attacks from social networks? What techniques does it use besides signatures and blacklists?"*

### **Bi-directional Filtering**

The solution should filter both inbound and outbound traffic to halt the flow of spam and prevent internal data loss. The importance of bi-directional filtering cannot be overlooked. Organizations who fall susceptible to outbound spam can suffer consequences such as having email servers blacklisted by ISPs, who then refuse to forward the organization's email to other users.

Outbound spam protection should not be confused with outbound filtering for data loss prevention. Good email security solutions provide both outbound spam analysis as well as outbound data loss prevention. (For a more in-depth discussion of data loss prevention, see the Proofpoint report, Outbound Email and Data Loss Prevention in Today's Enterprise, 2010. The report is available [here](#).)

*Good questions for enterprises to ask: "Does your solution monitor outbound email? Does it integrate with data loss prevention products?"*

### **Holistic Protection against Email Malware**

Enterprises need protection not just against phishing attacks, bogus pharmaceutical ads, and time-wasting email messages—they also need protection against email-borne viruses and other malware. Holistic protection against malware includes signature-based anti-virus (AV) protection, as well as Zero-Day AV protection capable of detecting new virus, worm, and rootkit attacks whose signatures are not known.

*Good questions for enterprises to ask: "Does your solution detect malware such as viruses and worms? Does AV protection include not only signature-based defenses but also protection against Zero-Day threats?"*

### **Flexible Architecture**

The solution should accommodate various email infrastructures and messaging platforms (such as Microsoft Exchange, Lotus Notes, etc.), as well as on-premise, virtualization, private cloud, and public cloud-based architectures. The solution should not require the enterprise to replace its current messaging infrastructure. Nor should the solution limit its capabilities because particular services are running on premise or in the cloud; it should provide comprehensive protection in any on-premise, cloud, or hybrid deployment.

*Good questions for enterprises to ask: "How does the solution integrate with our email services? Can the solution protect email services running locally as well as in the cloud? Is the anti-spam solution itself available as an on-premise solution as well as a cloud service?"*

### **Manageability**

The solution should impose a minimal workload on IT engineers, security officers, and end users. When possible, it should allow end users to participate in security practices, so that IT review of messages does not become an operational bottleneck.

*Good questions for enterprises to ask: "How do email administrators use the product? Can security and compliance officers audit email activity easily? Will the solution overburden email administrators with work, such as analyzing quarantined messages? Can authorized users contribute their knowledge to the analysis of email?"*

## **PROOFPOINT'S ANTI-SPAM SOLUTION**

Since 2003, Proofpoint, Inc. has been protecting mission-critical email infrastructure from outside threats including spam, phishing, unpredictable email volumes, malware, and other forms of objectionable or dangerous content. The Proofpoint Enterprise Protection™ Suite delivers best-in-class, inbound and outbound email security and management in one cost-effective, easy-to-use, cloud-enabled solution.

The Proofpoint solution incorporates all four key technology capabilities described above, and implements them in a machine-learning platform that meets all the requirements for enterprise readiness. (See Table 1.)

Proofpoint Spam Detection™, included in the Proofpoint Enterprise Protection Suite, delivers the most powerful and accurate approach to detecting and eliminating spam and phishing attacks in any language. Proofpoint combines the most effective spam filtering methods with its Proofpoint MLX™ machine-learning technology to deliver the industry's highest spam effectiveness—greater than 99.8% effective—and the lowest rate of false positives—less than 1 in 350,000 messages.

In addition to spam detection, Proofpoint Enterprise Protection includes a multi-layered antivirus engine (signature and behavior based), enabling protection against viruses and Zero-Day malware attacks.

**Table 1. Anti-Spam Requirements and the Proofpoint Solution**

Category	Requirement	Proofpoint Solution
Core Technology	Verification Techniques	<ul style="list-style-type: none"> <li>• Recipient verification, including LDAP verification</li> <li>• Bounce Address Tag Verification (BATV)</li> <li>• Sender Authentication, including verification with the Sender Policy Framework (SPF) and Domain-Keys Identified Mail (DKIM)</li> </ul>
	Reputation Analysis	<ul style="list-style-type: none"> <li>• Applies Proofpoint Dynamic Reputation™ technology to reduce inbound connection volumes by 80% or more, making intelligent decisions about whether to accept, reject or throttle incoming email connections.</li> <li>• Delivers real-time analysis of sender reputation—fast enough to stop botnet attacks</li> </ul>
	Content Scanning	<ul style="list-style-type: none"> <li>• Sophisticated analysis based on scanning hundreds of thousands of message attributes and applying machine-learning algorithms</li> </ul>
	Behavioral Analysis	<ul style="list-style-type: none"> <li>• Applies behavioral analysis to detect low-volume attacks and Zero Day attacks, increasing anti-spam effectiveness to nearly 99.99%.</li> </ul>
	Machine Learning	<ul style="list-style-type: none"> <li>• Applies Proofpoint MLX™ machine-learning technology to deliver the industry’s highest anti-spam effectiveness.</li> <li>• Minimizes false positives.</li> </ul>
Enterprise Readiness	Comprehensive Defenses	<ul style="list-style-type: none"> <li>• Defends against all types of spam attacks, including Zero Day attacks, blended threats, social media attacks, and more.</li> </ul>
	Bi-directional Filtering	<ul style="list-style-type: none"> <li>• Scans both inbound and outbound email for spam and viruses.</li> </ul>
	Holistic Protection against Email Malware	<ul style="list-style-type: none"> <li>• Detects and blocks email-borne malware, including viruses, worms, and rootkits.</li> <li>• Guards against known and unknown threats using signature-based AV detection, reputation analysis, and real-time behavioral analysis to detect Zero-Day threats.</li> </ul>
	Flexible Architecture	<ul style="list-style-type: none"> <li>• Integrates with enterprise messaging and collaboration infrastructures, including Microsoft Exchange, Lotus Notes, and LDAP.</li> <li>• Integrates with on-premise and cloud-based email services.</li> <li>• Available as an on-premise appliance or as a cloud service.</li> </ul>
	Manageability	<ul style="list-style-type: none"> <li>• Provides easy-to-use dashboards for email administrators and security teams.</li> <li>• Provides audit controls and reporting.</li> <li>• Provides Smart Send capabilities that enable authorized users to assist in the categorization of spam.</li> </ul>

## Anti-Phishing Protection

To block phishing attacks, Proofpoint Spam Detection uses all its anti-spam and anti-virus technologies, including content-filtering, reputation analysis, and real-time analysis of over 1 million message attributes. In addition, it uses Internet standards to verify the authenticity of message senders and to ferret out spoofed addresses. These standards include the verification standards mentioned above—DKIM, SPF, and BATV.

## Anti-virus and Anti-Malware Protection

Proofpoint Enterprise Protection protects enterprises from viruses, worms, spyware and other types of malicious code. It uses both signature-based anti-virus and behavioral-based zero-hour virus detection technologies to protect against all types of malware—including both known and emerging viruses—in the earliest stages of their proliferation.

## Manageability and End User Controls

Proofpoint Enterprise Protection makes it easy to define and enforce an organization's unique acceptable use policies, with an advanced email firewall, deep content inspection and outbound filtering capabilities.

A convenient point-and-click interface simplifies the process of defining complex rules related to file types, message size, and the contents of messages and their attachments. Proofpoint Enterprise Protection can identify and prevent a wide variety of both inbound and outbound policy violations—including offensive language, harassment, file sharing and violations of external regulations. The solution also features alerting and notifications so that email and security teams can respond quickly to changing situations.

Proofpoint Enterprise Protection offers many end user-controls to make spam defenses as manageable as possible. End-user controls are available in a number of ways: email-based, Web-based, and Outlook plug-ins. Proofpoint's end-user controls provide a full range of controls, including safelists, blocklists, spam thresholds, and other features that can all be set at the user, group, or organization level. Proofpoint Smart Send™ enables end users to decide how to remediate outbound messages flagged by Proofpoint and quarantined as spam or as data leaks. By enabling end users to resolve their own security policy violations, Smart Send reduces the need for IT oversight. The process of reviewing email for spam or policy violations also trains users to be more careful about their email contents. Proofpoint Smart Send is especially useful for organizations such as universities that prefer to delegate as much control as possible to end users.

## Flexibility: SaaS without Compromise

Cloud-based solutions such as a Software-as-a-Service (SaaS) are increasingly popular with enterprises. SaaS applications deploy quickly and can typically be run much more cheaply than on-premise alternatives. Hosted in world-class, SAS70-compliant datacenters,<sup>1</sup> Proofpoint's SaaS email security and compliance solutions deliver true enterprise-grade availability, performance, reliability and security. For its SaaS operations, Proofpoint guarantees:

- 99.999% Service Availability
- Sub-minute email latency

Administrative dashboards and policy engines give email administrators, security officers, and other IT personnel the fine-grained controls they would expect from an email security application running in house.

Proofpoint enables enterprises to take advantage of the flexibility and cost savings of SaaS without compromising on control or reliability.

## Integration with Email Infrastructure and Other Security Solutions

The Proofpoint Enterprise Protection Suite can be integrated with other Proofpoint offerings such as Proofpoint Encryption, which offers policy-based email encryption for regulatory compliance. It can also be integrated with other SaaS security and compliance solutions such as Data Leak Protection (DLP) products.

Proofpoint solutions work with all standard enterprise email solutions, including Microsoft Exchange and Lotus Notes.

## Benefits of Proofpoint Enterprise Protection

Proofpoint Enterprise Protection offers enterprises these benefits for spam prevention and email security:

- Inbound and outbound email security features—including anti-spam, anti-virus, email policy enforcement, message tracing and TLS encryption—as a cost-effective, on-demand service.
- 99.8%+ effectiveness against all types of spam, thanks to Proofpoint MLX™ machine learning technology.
- Total control and flexibility for email security preferences, policies, enabled services, end-user controls, alerts and reporting.
- Enterprise-class security, availability and scalability, ensuring continuous service and complete security of data.
- Architectural flexibility, offering anti-spam protection as an on-premises solution or a hybrid solution with cloud-enabled appliances.

## CONCLUSION

Enterprises should expect the onslaught of spam to continue. Botnets aren't going away. Criminal syndicates won't abandon a profitable business. In 2011 and beyond, attacks will likely become more frequent, devious, and malicious.

Enterprises can defend themselves with a comprehensive and adaptive anti-spam solution such as the Proofpoint Protection Suite. To keep up with evolution of spam attacks, enterprises need a defensive technology that stays one step ahead. Combining advanced MLX machine-learning technology, behavioral analysis, Dynamic Reputation analysis, bi-directional filtering, and more, the Proofpoint Protection Suite offers enterprises the comprehensive protection they need to defeat the spam attacks of today and tomorrow.

For more information about Proofpoint Enterprise Protection and Proofpoint Enterprise Privacy, please visit [www.proofpoint.com](http://www.proofpoint.com) or call +1 (408) 517-4710.

## FOR FURTHER READING

Proofpoint offers a variety of free educational whitepapers that further describe the risks associated with outbound email and the policies, processes and technologies that can be used to reduce those risks. Visit our online resource center at <http://www.proofpoint.com/resources> for the latest information.

## ABOUT PROOFPOINT, INC.

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging. Learn more at [www.proofpoint.com](http://www.proofpoint.com).

### Notes

<sup>1</sup> SAS 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants that validates that a service organization has been through an in-depth audit of its control activities, and demonstrates that they have adequate controls and safeguards when they host or process data belonging to their customers. For more information, please see <http://www.aicpa.org/Pages/Default.aspx>.



**US Worldwide  
Headquarters**

Proofpoint, Inc.  
892 Ross Drive  
Sunnyvale, CA 94089  
United States  
Tel +1 408 517 4710

**US Federal Office**

Proofpoint, Inc.  
13800 Coppermine  
Road  
Suite 203  
Herndon, VA 20171  
United States  
Tel +1 703 885 6809

**Asia Pacific**

Proofpoint APAC  
Suntec Tower 2,  
9 Temasek Boulevard,  
31F  
Singapore 038989  
Tel +65 6559 6128

**EMEA**

Proofpoint, Ltd.  
200 Brook Drive  
Green Park  
Reading, UK  
RG2 6UB  
Tel +44 (0) 870 803  
0704

**Japan**

Proofpoint Japan K.K.  
BUREX Kojimachi  
Kojimachi 3-5-2,  
Chiyoda-ku  
Tokyo, 102-0083  
Japan  
Tel +81 3 5210 3611

**Canada**

Proofpoint Canada  
210 King Street East,  
Suite 300  
Toronto, Ontario,  
M5A 1J7  
Canada  
Tel +1 647 436 1036

**Mexico**

Proofpoint Mexico  
Salaverry 1199  
Col. Zacatenco  
CP 07360  
México D.F.  
Tel: +52 55 5905 5306

*Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.*

**proofpoint**<sup>™</sup>  
Control tomorrow's email risks today

[www.proofpoint.com](http://www.proofpoint.com)

