

Proofpoint Spam Detection

Enterprise-Class Detection and Elimination of All Types of Spam

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 has combined the most effective spam filtering methods with its breakthrough Proofpoint MLX™ machine learning technology to deliver the industry's highest spam effectiveness, greater than 99.8%, and lowest rate of false positives.

Proofpoint Enterprise Protection Suite Components

The following comprehensive protection components are offered through the Proofpoint Enterprise Protection Suite:

- **Proofpoint Dynamic Reputation™**
Connection management for powerful spam protection
- **Proofpoint Email Firewall™**
Detects sensitive information in message content and subject line
- **Proofpoint Spam Detection**
Detects and eliminates spam and phishing attacks in any language
- **Proofpoint Zero-Hour Anti-Virus™**
Protects enterprises against new viruses and malicious code moments after their release
- **Proofpoint Virus Protection™**
A wide variety of enterprise-class virus solutions

Technology-powered spam detection

Powered by a machine learning technology, Proofpoint Spam Detection (part of the Proofpoint Enterprise Protection Suite) examines millions of possible attributes in every email—including message envelope headers and structure, images, sender reputation as well as unstructured content in the message body—to block spam, image-based spam and phishing attacks, while automatically adapting to new attacks as they appear. In addition, spam protection is automatically kept up-to-date, ensuring maximum effectiveness at all times. Individually controllable spam and adult content, phishing and bulk scores allow an organization to enforce zero-tolerance policies against pornographic spam. Anti-phishing features (including DKIM and ADSP signing and verification of outbound email and domain-based sender authentication techniques) stop the spread of phishing, and prevent the theft of personal information from employees.

Proofpoint Spam Detection

Feature	Benefit
Proofpoint MLX	Proofpoint MLX automatically evolves with new spamming techniques to accurately stop new attacks, staying highly effective over time. It is superior to simple statistical techniques and doesn't rely on signatures or fingerprinting techniques, allowing Proofpoint to provide the most accurate spam detection.
Proofpoint Spam Detection	Proofpoint Spam Detection provides bi-directional protection, ensuring that the inbound email channels are adequately protected against spam, and that an organization's reputation is protected by filtering the outbound channel as well.
Bounce management	Protects against the most advanced forms of spam, phishing, and zombie attacks, as well as addresses the newest forms of blended threats where malware is being delivered through an innocuous URL contained with a spam message. Bounce management features block 100% of "backscatter" spam.
No administrative intervention required	Blocks the most spam by examining millions of possible structural, content and reputational attributes in inbound or outbound email, including self-remediation with Proofpoint Smart Send.
Personalized quarantines and personal safe/blocked lists	Individual end users manage their own questionable emails with personalized quarantines and personal safe/blocked lists.

Proofpoint Spam Detection

Multi-layered spam prevention for maximum effectiveness

Proofpoint Spam Detection provides protection across multiple layers to eliminate traffic spikes caused by spam attacks and to ensure that end user mailboxes stay spam free.

Connection-level analysis

Proofpoint Spam Detection starts by testing numerous connection-level data points including DNS, MX record verification, SPF, recipient verification and reputation data. Based on this analysis, SMTP rate control is used to automatically block or throttle malicious connections. This provides outstanding protection against botnets, directory harvest and denial-of-service attacks, while shedding as much as 80% of all incoming SMTP connections when combined with Proofpoint Dynamic Reputation—a part of the Proofpoint Enterprise Protection Suite.

Contextual, lexical and image-based analysis

Proofpoint Spam Detection uses Proofpoint MLX to examine the content and context of messages using structural tests, English and foreign language inspection, pornography detection, malicious (spyware/phishing/pharming) URL detection, image analysis, reputation analysis and any custom policies defined by an organization.

With full support for double-byte languages, Proofpoint MLX provides outstanding protection against even hard-to-detect Asian language spam. Proprietary image analysis techniques included in Proofpoint MLX identify image-based spam that other solutions fail to catch. Additionally, an organization's spam protection is always kept up-to-date, ensuring maximum effectiveness at all times.

Bi-directional spam filtering

Proofpoint MLX powerful spam detection does not rely on reputation for its effectiveness. This makes it uniquely suited to protecting your organization's reputation when filtering the outbound mail stream for spam in the event an internal system is compromised by malware and becomes a source of spam.

Bounce management

Backscatter—the barrage of non-delivery report messages (NDRs) and auto-responses caused by spammers spoofing an organization's email addresses—has become an increasingly serious problem for most organizations. Proofpoint supports the latest BATV (Bounce Address Tag Validation) specification to tag outbound messages and to validate incoming NDRs against those tags to block backscatter.

Advanced anti-phishing protection

Advanced anti-phishing techniques protect end users from scams, fraud, identity theft and malicious code. Destination URLs within the emails are classified and analyzed, and a statistical correlation of various attributes are analyzed so that no single attribute is authoritative. Targeted rules and classifiers for phishing messages allow administrators to take specific actions against these messages.

Powerful end-user controls

Proofpoint Spam Detection checks personal safe and blocked lists for valid and invalid senders. Proofpoint provides various options for end user controls including web, email and plug-ins. End user control features include language selection, individualized spam threshold settings, and safelist/blocked list management. Proofpoint also provides a comprehensive view into a user's personal quarantine.

Administrative flexibility

Different policies can easily be configured for different groups of end users or domains. All policies can be customized at a global, group, or user level with full integration to LDAP or Active Directory to simplify on-going administration. Additionally, messages that contain suspected spam can also be temporarily quarantined for a configurable period of time or until a certain amount of spam updates have been received.

Multilingual

Proofpoint Spam Detection is multilingual and offers outstanding accuracy against spam in any language, including hard-to-analyze, multi-byte character languages, such as Japanese and Chinese.

About Proofpoint

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, Inc.
892 Ross Drive
Sunnyvale, CA
94089

1.877.647.6488