Proofpoint Spam Detection Module

The Proofpoint Spam Detection™ module, a component of the Proofpoint Messaging Security Gateway™ and the Proofpoint Protection Server®, provides the most powerful approach to detecting and eliminating spam in any language. The key to its unrivalled accuracy is the patent-pending Proofpoint MLX™ machine learning technology, a system developed by scientists and engineers at the Proofpoint Attack Response Center. Proofpoint has combined the most effective, traditional spam filtering methods with breakthrough machine learning technology to deliver a system with the industry's highest effectiveness and lowest rate of false positives.

features

Multilayered spam prevention for maximum effectiveness

Proofpoint Spam Detection provides robust, yet simple to manage, protection from spam by combining the most effective spam elimination technologies into one cohesive, easy-to-manage system. Proofpoint's multilayered spam defense combines connection analysis, local and global reputation, and advanced statistical content analysis techniques. Proofpoint Spam Detection inspects hundreds of thousands of attributes in incoming email messages—including IP addresses, envelope headers and structure, image and other attachment attributes, sender reputation data as well as unstructured content in the body of messages—to accurately classify spam and assign a spam score.

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**

  The Proofpoint Email Firewall™ provides a stateful, first line of defense against spam by testing numerous connection-level data points including DNS, MX record verification, SPF, recipient verification, Dynamic Reputation™ information and optional net-MLX data. Proofpoint Dynamic Reputation technology constantly monitors SMTP connections at the IP address level, looking for suspect or malicious activity. Based on this analysis, SMTP rate control is used to automatically block or throttle malicious connections, providing outstanding protection against directory harvest and denial-of-service attacks while shedding 30% to more than 80% of inbound connection load.

- **Contextual, Lexical and Image-based Analysis**

  Proofpoint MLX technology examines the content and context of messages using structural tests, English and foreign language inspection, pornography detection, malicious (spyware/phishing/pharming) URL detection, targeted rules for detecting phish attacks, image analysis, reputation analysis and any custom policies you have defined. 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. The Proofpoint Dynamic Update Service™ keeps the MLX Engine constantly and automatically updated to combat evolving 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.

- **End-user Configuration**

  Checks personal safe and blocked lists for valid and invalid senders.

- **Administrator Customization**

  Checks global safe and blocked lists and any custom-created spam rules; global lists override end-user lists.

Benefits

- Automatically evolves with spamming techniques to help accurately predict and stop never-before-seen attacks.
- MLX is far superior to simple statistical techniques such as Bayesian filters—and it doesn't rely on signatures or fingerprinting techniques, which are easily fooled by spammers.
- Requires no administrative intervention.
- Blocks the most spam by examining hundreds of thousands of structural, content and reputational attributes in every email.
- Bounce management features block 100% of "backscatter" spam.
- Lets individuals manage their own questionable emails with personalized quarantine and personal safe/blocked lists.
- Protects against the most advanced forms of spam including PDF, image and attachment-based spam.
- Advanced anti-phishing techniques protect end users from scams, fraud, identity theft and malicious code.
- Separate adult content scores allow you to enforce zero-tolerance policies against pornographic spam.
- Generates the least number of false positives and stays highly effective over time.
- Policies can be customized at a global, group, or user level with full integration to LDAP or Active Directory.
- Protects your organization from "hash-busting" or randomized spam attacks.
- Confident spam scoring lets you take decisive action against spam.
- Easy-to-configure custom policies.

Proofpoint Spam Detection Module

MLX technology

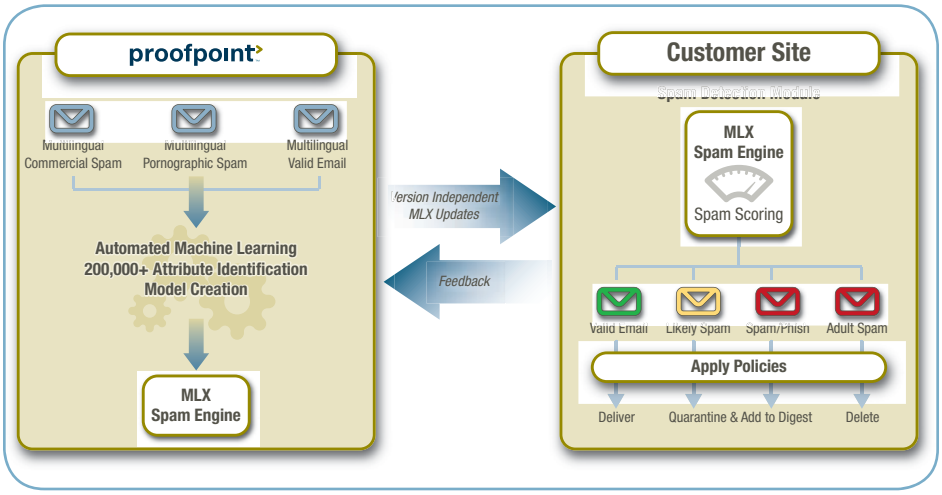
Proofpoint MLX provides complete confidence in defeating spammers

Proofpoint MLX technology goes far beyond the capabilities of competing anti-spam solutions. MLX is far superior to simple statistical techniques such as Bayesian filters—and it doesn't rely on signatures or fingerprinting techniques, which are easily fooled by spammers. It turbocharges traditional techniques with advanced machine learning technologies such as logistic regression and information gain analysis. The result is the highest spam detection rates in the industry.

How MLX works for spam detection

- The process begins at the Proofpoint Attack Response Center, where tools developed by Proofpoint scientists and engineers analyze millions of spam messages and distill them into hundreds of thousands of spam attributes—exposing the underlying characteristics and emerging techniques of current and future spam.
- These attributes are fed into sophisticated, machine learning algorithms such as logistic regression and information gain analysis. The attributes are dynamically balanced so the system understands how important any particular attribute is during the final message classification process.
- This information is then packaged in the form of the Proofpoint MLX Engine and automatically delivered to Proofpoint customers.
- Locally, the Spam Detection module examines multiple structural and content layers, extracting attributes from each incoming email. Then advanced machine learning algorithms compute a final spam score that dictates what action to take.
- Proofpoint's Attack Response Center continually trains the MLX Engine based on new attacks and feedback from deployed Proofpoint systems, constantly retuning for maximum accuracy.

Proofpoint MLX technology can also be enhanced with advanced connection management features, powered by Proofpoint's netMLX global reputation database. See http://www.proofpoint.com/downloads/DS-Proofpoint-Dynamic-Reputation.pdf for more details.



The MLX detection process begins at the Proofpoint Attack Response Center, where scientists and engineers build and refine mathematical models that represent Internet spam. These models are delivered to customers on a frequent basis and are constantly updated to ensure customers stay ahead of the latest spam attacks. Proofpoint examines every aspect of incoming messages, from the sender's IP address, to the message envelope, headers and structure, and finally the content and formatting of the message itself. In all, 20 layers of analysis and hundreds of thousands of attributes—representing both content and structural components—are analyzed. A typical message may trigger more than 300 MLX attributes.

Enterprise Spam Detection

Only Proofpoint's Spam Detection module addresses the unique needs of large enterprise customers. Unlike repurposed hosted or consumer solutions—or hard-to-manage, client-side software deployments—Proofpoint's solution:

- Eliminates spam at the gateway
- Is flexible and adaptable to corporate characteristics and industry terms
- Meets your enterprise's messaging strategy and scaling requirements
- Allows you to easily administer and enforce global, group, and individual spam policies to meet the unique needs of different email users in your organization
- Delivers extremely low false positive rates and extensive end-user controls ensure that your mission-critical business communications are always available
- Is continually and automatically updated to provide maximum protection against even the newest and most evasive forms of spam, including image-based and foreign-language spam

Outstanding End-user Control

Proofpoint provides end users with easy, "self service" control over their personal anti-spam preferences through features including:

- Personalized quarantines and quarantine digest reports
- Personalized safelists and blocklists
- Web-based quarantine and profile administration
- Ability to opt in and out of different spam policies (as permitted by administrator configurable settings)

Learn More about Proofpoint MLX

For more information about how Proofpoint's patent-pending machine learning techniques provide outstanding protection against spam, download a free whitepaper about Proofpoint MLX by visiting:

http://www.proofpoint.com/mlxwp