

# 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. The key to its unrivalled accuracy is the patent-pending Proofpoint MLX™ machine learning technology, a system developed by scientists and engineers at Proofpoint's Anti-Spam Laboratory. 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 uses a multitiered attribute-extraction process that inspects more than 100,000 attributes of incoming email messages—including sender IP addresses, message envelope headers and structure, as well as unstructured content in the body of messages. These attribute-extraction layers include:

#### ○ Connection Level

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, and MLX Dynamic Reputation™ information. The Proofpoint Email Firewall also defends against directory harvest and denial of service attacks.

#### ○ Contextual Analysis

Examines the context of messages using structural tests, English and foreign language inspection, pornography detection, URL inspection, targeted rules for detecting phishing attacks, and a corporate lexicon adapter to customize the solution to your industry.

#### ○ 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.

All of the attributes detected within incoming emails are used by the MLX Anti-Spam Engine™ to ultimately assign a spam score, which represents the probability that the message is spam. To stay ahead of evolving spam tactics, the MLX Anti-Spam Engine is constantly and automatically kept up to date by the Proofpoint Dynamic Update Service.™

## 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 support vector machines. The result is the highest spam detection rates in the industry. What does it mean to you? Complete confidence!



### 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 100,000 structural and content attributes in every email.
- Allows individuals to manage their own questionable emails with personalized quarantine and personal safe/blocked lists.
- 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 ActiveDirectory.
- Stays highly effective over time.
- Protects your organization from randomized spam attacks.
- Confident spam scoring lets you take decisive action against spam.
- Meets your organization's unique needs with a configurable corporate lexicon adapter.

# Proofpoint Spam Detection Module

## How MLX works for spam detection

- The process begins at Proofpoint's Anti-Spam Laboratory, where tools developed by Proofpoint scientists and engineers analyze millions of spam messages and distill them into more than 100,000 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 support vector machines. 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 Proofpoint's MLX Anti-Spam 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 Anti-Spam Laboratory continually trains the MLX engine based on new attacks and feedback from deployed Proofpoint systems, constantly retuning for maximum accuracy.

## Classify messages with high confidence

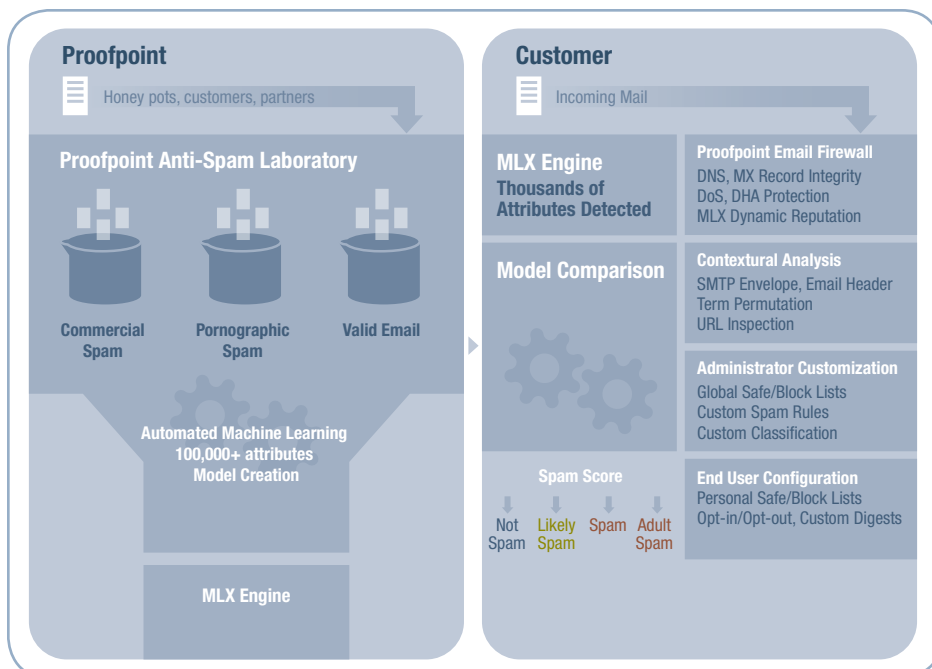
The large number of attributes analyzed by the MLX Anti-Spam Engine ensures that messages are classified with a high degree of confidence. Most messages score very high or very low, with only 1.5 percent falling between 20 and 80 on a scale of 1 (an undeniably valid message) to 100 (assuredly spam). Confident scoring allows you to take decisive action—for example, automatically discarding spam messages before they impact your email servers, quarantining the absolute minimum amount of “probable spam,” and delivering valid messages directly to end users.

Competitors' products are often confused about how to classify messages—upwards of 40 percent of messages typically receive scores between 20 and 80, indicating uncertainty about the validity of the message. As a result, competing products often block valid messages as spam and many spam messages get through to in boxes. Misclassifications such as these annoy end users and generate support calls, greatly increasing the total cost of the solution.

## 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
- Integrates into the 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
- Has no impact on mission-critical business continuity standards



© 2004 Proofpoint, Inc. Proofpoint Protection Server is a registered trademark of Proofpoint, Inc. in the United States and other countries. Proofpoint, Proofpoint MLX, Proofpoint Messaging Security Gateway, Proofpoint Spam Detection, Proofpoint Email Firewall, MLX Anti-Spam Engine, MLX Dynamic Reputation and Proofpoint Dynamic Update Service are trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 11/04