

# Can SPAM without increasing headcount

**Quest provides the most powerful** approach to detecting and eliminating SPAM. Using the most effective, traditional SPAM filtering methods with breakthrough machine learning technology, Quest delivers with the industry's highest effectiveness and lowest rate of false positives.

## Multilayered SPAM prevention for maximum effectiveness

A multitiered attribute-extraction process 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.

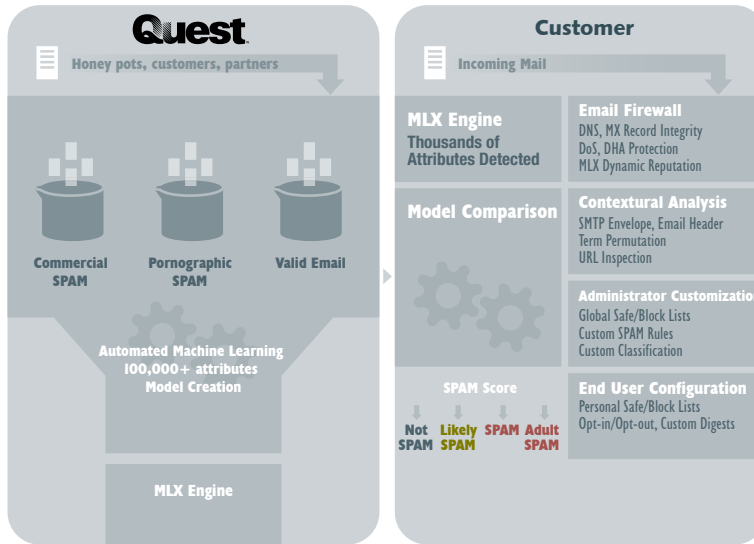
These attribute-extraction layers include:

- **Connection Level**  
An Email Firewall that provides a stateful, first line of defense against SPAM by testing numerous connection-level data points including DNS, MX record verification, and MLX information. The 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 assigned 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.

## MLX technology

MLX provides complete confidence in defeating spammers. 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!



## 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.

Other 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 inboxes. Misclassifications such as these annoy end-users and generate support calls, greatly increasing the total cost of the solution.

## Enterprise SPAM Detection

Quest's SPAM Detection addresses the unique needs of large enterprise customers. Unlike repurposed hosted or consumer solutions—or hard-to-manage, client-side software deployments.

- 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

## 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 utilizing 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

**For more information call 800-326-4220 or visit us at [www.questsys.com](http://www.questsys.com)**

