

Defense-in-Depth Anti-Spam Engine

OVERVIEW

Spam - it has become the email plague of the new century. In 2007, despite assurances from Bill Gates that spam would be eliminated by now, spam had its biggest year on record. The burgeoning volume of spam facing enterprises continues to grow. The distinction between spam and malware is increasingly blurred as complex blended threats, spread by spam botnets, gain prominence. Enterprises need effective tools to counteract spam and all its associated threats. MailMarshal combines proven best-of-breed anti-spam techniques with M86's own innovative technologies to eliminate spam. These layered technology components include:

- RBLs/Reputation services
- SpamProfiler
- SpamCensor
- URLCensor
- Custom Policies
- Zero-Day Protection

Each technology component is applied in successive layers to achieve true defense-in-depth security against the widest range of spam, phishing and other email-borne threats.

Effective anti-spam does not simply block the maximum amount of spam. It also delivers performance, speed, bandwidth, productivity, efficiency and, above all, accuracy. Blocking and then losing legitimate email messages is unacceptable and worse than accidentally letting through a spam message. As is introducing performance bottlenecks which unnecessarily delay important messages.

MailMarshal leads the industry in anti-spam protection, because we:

- Achieve a consistent 99.5% spam catch rate¹
- Minimize false positives
- Provide in-depth reporting
- Are resilient against new forms of spam
- Detect and reject spam messages faster than any other solution
- Provide outgoing spam protection
- Enable flexible management of spam

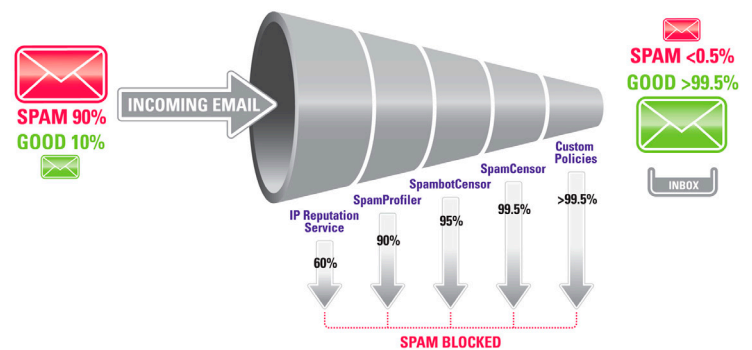
¹ 99.94% spam catch rate in Internal Benchmark Testing

FEATURES

Defense-in-Depth: Multi-layer Anti-spam Defense

Defense-in-Depth protection represents the use of multiple security techniques to minimize the risk of one security component being circumvented. Solutions relying on only one or two techniques are extremely vulnerable to evolving spam tactics. MailMarshal utilizes Defense-in-Depth protection with a range of proven anti-spam and content filtering techniques to provide a multi-layered anti-spam system. With over 10 years experience as a leader in email content filtering, M86 gives administrators unsurpassed choice and flexibility in deploying multiple layers of antispam defense, ensuring the highest possible detection rate and maximum accuracy.

MAILMARSHAL ANTI-SPAM ENGINE



Layer #1 - RBLs/IP Reputation: Real-time IP Checking

An extremely effective way of blocking spam is to check the sender's reputation by comparing the sending IP address against a database of known email senders and spamming hosts. These services vary widely in scope and range from well-known Real-Time Blacklists (RBLs) to full-blown reputation databases that give each email sender a reputation score. MailMarshal performs its queries up-front and on the fly via DNS, caching its results for optimum speed and efficiency. MailMarshal's flexible policy framework allows you the choice of rejecting connections up-front to save bandwidth and server resources, or accepting the message for further analysis.

To minimize the risk of false positives, MailMarshal also incorporates a unique adaptive whitelisting system that is used in combination with RBLs/Reputation services. MailMarshal's adaptive whitelisting automatically builds lists of safe email sources for your organization.

It monitors ratios of spam to good email for all email sources, plus, keeps track of all the email sources that your company regularly sends email to. It then applies sophisticated algorithms to automatically white-list email sources with an established 'good' history with your organization.

Layer #2 - SpamProfiler: Up-front, Fast Message Fingerprinting

MailMarshal's SpamProfiler utilizes intelligent message fingerprinting techniques to accurately identify spam up-front as it is being received. The SpamProfiler works by applying leading-edge fingerprinting algorithms on identified, known spam based on data sourced from an extensive global network of spam sources, honeypots and spam submitters. The SpamProfiler is light on resources, extremely fast, accurate, and is performed up-front prior to any other message processing. This design maximizes message throughput by eliminating the bulk of spam up-front and thereby saving server resources for more in-depth analysis of other messages.

Layer #3 - SpamCensor: Innovative Anti-Spam Filter

MailMarshal's SpamCensor combines over 2000 individual heuristic tests for spam, analyzing message content, size and composition, and attachments for unmatched accuracy. SpamCensor incorporates unique scanning technology that targets footprints left by spambots - devices installed on compromised computers which are responsible for the overwhelming majority of spam sent today. By targeting these 'botprints' and other repeatable characteristics, SpamCensor detects new waves of spam, over and over again, without needing individual spam signatures. SpamCensor is a unique 'preventive detection' filter.

SpamCensor is automatically updated and maintained by our M86 Security Labs team, a group of expert security analysts. The Labs are backed by M86's ThreatNet, a network of spam traps and tools that captures and analyzes spam and threats from around the globe in realtime.

Flexibility and resiliency are paramount in spam filtering. A good anti-spam system needs to adjust to changing spammer technologies. Since it was introduced in 2003, SpamCensor has proved incredibly resilient, constantly changing to counteract new spammer technologies, including such tricks as obfuscation, image spam and PDF spam.

Layer #4 - URLCensor: Real-time URL Blacklist Checking

Over 80% of spam today contains a URL. A proven way of identifying spam is to extract domain information from URLs in the body of the message and check that information against a database of known 'spammy' URLs. MailMarshal's URLCensor is a sophisticated implementation of URL checking that works in realtime, and, like RBL queries, caches results for maximum performance. URLCensor was specifically developed to counter the rising phishing threat where it has performed very well. It is now an integral layer in M86's anti-spam arsenal.

Layer #5 - Custom Polices: Flexible, Complete Email Content Management

MailMarshal has rich customization capability; for example, allowing administrators to:

- Enable personalized email whitelists for each user
- Perform advanced lexical scanning using MailMarshal's unique TextCensor analyzer
- Block email from countries that an organization does not do business in, using CountryCensor
- Deny email addressed to unknown users
- Block executable files, or small, encrypted zip files
- Block illegally constructed messages
- Reject odd or illegal connection behavior
- Employ Denial of Service and Directory Harvest Attack protection

This is by no means a complete list. With a comprehensive email content security toolbox, MailMarshal provides a wealth of other leading features that protect against spam and other email-borne threats.

Zero-Day Protection: Rapid Updates for Significant New Threats

The Zero-Day Protection Framework is a safety net that allows M86 to quickly update your MailMarshal server(s) to protect against significant new threats, including viruses, malware, large spam outbreaks, phishing and other identified exploits. M86 can quickly secure your MailMarshal SMTP server(s) at any hour, even when customer administrators are away from the office, without the need for intervention – providing MailMarshal customers with the ultimate peace of mind.

SUMMARY

As a leader in email content security for more than 10 years, MailMarshal combines proven best-of-breed anti-spam techniques with M86's own innovative technologies to eliminate spam. No single technique is relied upon, and each technique is layered upon the other to provide true Defense-in-Depth protection against spam and all forms of email-borne threats.

MailMarshal provides this security technology within an efficient, scalable framework unmatched in the industry. MailMarshal is one of the most powerful, flexible, easy-to-use and extensible anti-spam products in the marketplace, and one which can be fully customized to suit whatever requirements an organization may have.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 11.02.09