M86 SECURITY™

MailMarshal™ SMTP 6.7

MailMarshal SMTP 6.7 provides key new features for protection against blended email threats, enhanced anti-spam, email authentication and streamlined administration. This release delivers important benefits for security, bandwidth and cost savings, email efficiency and time-saving measures for administrators.

KEY BENEFITS

The Latest in Email Threat Protection

Blended email threats constitute the primary means of infecting a computer with malware. Their success works on the basis of circumventing normal anti-virus measures by delivering the malware via a URL link to an infected website rather than attaching the malware to the email. The new Blended Threats Module for MailMarshal SMTP 6.7 provides reliable protection against malicious links embedded in email. This delivers greater security and protection against malware infections, associated clean-up costs and lost productivity.

Bandwidth Utilization & Spam Protection

Two new additions to MailMarshal's anti-spam engine provide substantial benefits against spam. The IP Reputation Service can reliably reject over ½ of the spam your email gateway would normally receive. Given that spam typically constitutes up to 90% of all email an organization normally receives, the potential benefit is a halving of all incoming email and a substantial reduction in wasted bandwidth. This in turn means lower operating costs, enabling your dollars to go further.

SpamBotCensor recognizes and blocks spam generated by known Botnets. These Botnets are typically responsible for 80% of all spam in circulation.

These additions also provide benefits in improved spam detection performance and more reliable indicators of high probability spam, further reducing chances of false positives.

Improved Administration

New features such as automated user group pruning and the streamlined function for reporting spam/not spam to M86 enable administrators to spend less time managing messages and more time on productive tasks.

WHAT'S NEW AT-A-GLANCE

- **Enhanced Anti-Spam Protection** – Spam is an evolving threat which requires anti-spam solutions to adapt and innovate to meet changing demands. MailMarshal SMTP 6.7 provides key new layers in the Defense-in-Depth Anti-Spam Engine:

  - *Marshal IP Reputation Service* – A real-time IP look-up service which enables MailMarshal SMTP to deny connections from known spam sources before messages are transmitted; resulting in substantial bandwidth savings and more efficient spam protection.

  - *SpamBotCensor* – Botnets play a crucial role in the distribution of the majority of the world's spam. SpamBotCensor is a unique innovation which enables MailMarshal to quickly and accurately identify and block messages generated by known SpamBots.

- **Blended Threats Protection** – Blended threats are arguably the most dangerous email threat facing organizations; they are emails containing malicious URL links. Often organizations are vulnerable to these threats as they circumvent traditional signature-based anti-virus measures. The new Blended Threats Module for MailMarshal SMTP 6.7 is an optional security service which detects known malicious URLs in email messages. The Blended Threats Module (BTM) leverages a cloud-based malware behavioural analysis centre to maintain a dynamically updated database of malicious links to block blended threats.

- **Automated User Group Maintenance** - MailMarshal now provides automated pruning of unused email addresses from automatically generated user groups to help maintain efficiency and server performance.

- **New Outbound SMTP Authentication** – Outbound SMTP authentication has been added in MailMarshal 6.7. You can now configure outbound SMTP authentication for each route within MailMarshal - useful when ISPs require SMTP credentials to combat spammers.

- **Improved Inbound SMTP Authentication** - Inbound SMTP authentication now supports CRAM-MD5 for more secure authentication between servers.

- **And More** – MailMarshal 6.7 provides a wealth of additional enhancements:

  - A new Upgrade Tasks feature informs MailMarshal administrators on recommended actions and newly available features after upgrading to the latest release.
  - A new report spam/not spam feature has been added to facilitate streamlined notifications to M86 Security Labs of missed spam or false positives.
  - Substantial improvements have also been made to key MailMarshal components resulting in increased stability and greater efficiencies in message handling.
  - An email address search tool has been provided to help identify all user groups that an address is associated with by MailMarshal.

Whats New

MailMarshal™ SMTP 6.7

FAQ

Q. Is the Marshal IP Reputation Service free to use?

A. For most customers, the Marshal IP Reputation Service will be free to use. There is an upper limit of 100,000 queries per day provided free of charge to MailMarshal SMTP maintenance customers as part of your entitlements. For the majority of organizations, this should be more than adequate for your needs and there are absolutely no additional costs - in fact, you can expect to see noticeable bandwidth cost savings with the service. For enterprise customers that place higher demands on the service due to larger email volumes, additional fees may apply. Please talk to your local M86 Security representative about your usage requirements and pricing.

Q. How much does the Blended Threats Module cost?

A. The Blended Threats Modules is an optional add-on module similar to optional anti-virus subscriptions available for MailMarshal. It is a subscription service based on your MailMarshal SMTP user license count. Subscription fees start at US$5.40/user/year.

Q. Can I trial the Blended Threats Module before deciding to subscribe?

A. Yes, a free 30-day trial of the Blended Threats Module and full service updates is available for MailMarshal SMTP customers. Simply contact your M86 Security representative to arrange a complimentary trial key.

UPGRADING

MailMarshal SMTP customers with current maintenance contracts may upgrade to version 6.7 at no charge.

If you are a MailMarshal SMTP customer and wish to upgrade to version 6.7, but do not have a current maintenance agreement, please contact your local M86 Security representative.

The procedure for upgrading your MailMarshal SMTP server is documented on the Technical Support section of our website. If you require assistance during your upgrade (and you have a current maintenance agreement), please don't hesitate to contact your local Technical Support representative via our website – www.m86security.com.

If you have any suggestions or requests for our next version, we want to hear them. Simply email us at iwish@m86security.com.

NEW FEATURES IN-DEPTH

**ANTI-SPAM | Marshal IP Reputation Service**
The new Marshal IP Reputation Service from the M86 Security Labs is a real-time spam IP blacklist and a key evolution in MailMarshal's Defense-in-Depth Anti-Spam Engine. It is ideally deployed as the first line of spam defense. In this role, the IP Reputation Service is utilized at the ESMTP layer and can assess the reputation of email servers when first attempting to establish a connection to your email gateway. If the IP Reputation Service recognizes the connecting server's IP as a known spam server MailMarshal will drop the connection and deny spam messages from being transmitted. This provides substantial savings in bandwidth, server load and disk space.

During Beta testing the IP Reputation Service reliably rejected in excess of 60% of incoming spam (your results may vary). Given that most typical organizations see as much as 90% of their incoming email as spam, this can mean a considerable saving on bandwidth for your organization.

The IP Reputation Service integrates with the Automatic Adaptive Whitelist (AAW) feature introduced in MailMarshal SMTP 6.4. The AAW dynamically maintains a list of regular email contacts and uses this to ensure that the IP Reputation Service does not deny connections from servers that your organization normally communicates with; preventing unwanted blocking of email from your customers and partners should they become blacklisted.

The IP Reputation Service is maintained by the M86 Security Labs Team. It leverages real-time spam IP address intelligence from MailMarshal servers deployed around the globe. The IP Reputation list is a dynamic query service so it is always real-time and up-to-date.

MAILMARSHAL ANTI-SPAM ENGINE
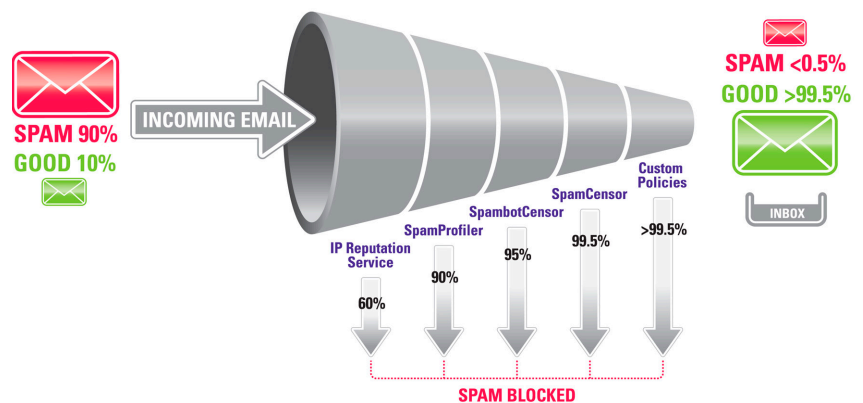
THE DEFENSE-IN-DEPTH ANTI-SPAM ENGINE IS A LAYERED, MUTIFACETED SPAM SOLUTION. AS EMAIL PASSES THROUGH MAILMARSHAL'S SPAM FILTERS SPAM IS WHITTLED DOWN AND REJECTED OR QUARANTINED RESULTING IN A FAST AND CONSISTENT 99.5% SPAM CATCH RATE WITH NEAR-ZERO FALSE POISITIVES.

MailMarshal™ SMTP 6.7
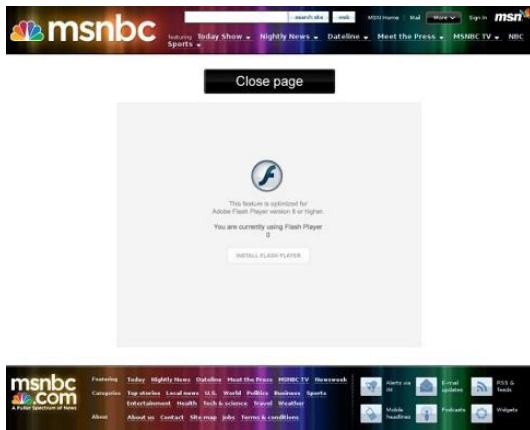
A PRIME EXAMPLE OF A BLENDED EMAIL THREAT –

THE LINK TO THIS WEBSITE ARRIVED IN AN EMAIL WITH THE SUBJECT 'MSN – BREAKING NEWS'. AN EMBEDDED LINK DIRECTS THE EMAIL RECIPIENT TO AN OFFICIAL-LOOKING MSNBC WEBSITE WHERE THEY ARE PROMPTED TO DOWNLOAD A FLASH VIDEO UPDATE. IN THIS CASE THE DOWNLOAD WAS NOT A VIDEO UPDATE BUT MALWARE FOR THE RUSTOCK BOT.

ANTI-SPAM | SpambotCensor

Botnets are networks of compromised computers which can be remotely controlled by criminals. There have been many high profile Botnets, such as Storm, Srizbi, Conficker and Rustock, which command armies consisting of hundreds of thousands of infected computers. Botnets are a fundamental part of spam today. The M86 Security Labs was the first internet security research team to prove that just a handful of Botnets were responsible for over 80% of all the world's spam. We call these Botnets, SpamBots.
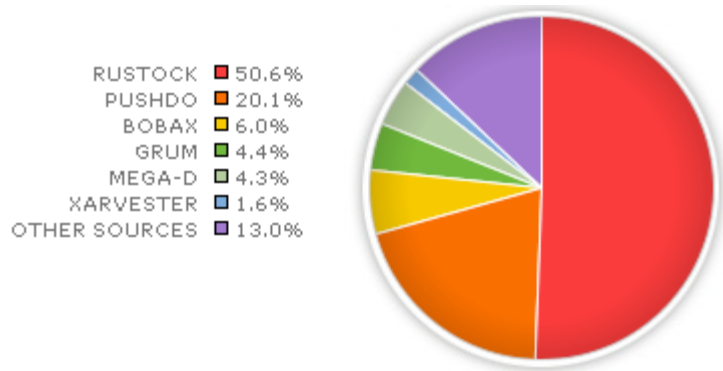
A REPORT FROM THE M86 SECURITY LABS WEBSITE ILLUSTRATING THE DOMINANT ROLE THAT JUST SIX BOTNETS PLAYED IN THE DISTRIBUTION OF 87% OF ALL SPAM DURING OCTOBER 2009.

SpamBotCensor is a new layer in the MailMarshal Defense-in-Depth Anti-Spam Engine which addresses the Spambot problem. It is a proprietary innovation derived from the years of research and analysis put into SpamBots by the M86 Security Labs. Spambots leave tell-tale imprints on the spam messages they send – the email equivalent of leaving fingerprints on an envelope. SpamBotCensor quickly and very accurately recognizes these characteristics, enabling high performance detection of spam from known Spambots.

SpamBotCensor is dynamically updated by the M86 Security Labs with the latest SpamBot signatures and new SpamBot profiles as those Botnets are identified by Security Labs engineers. This ensures that MailMarshal always has up-to-date intelligence on the latest SpamBot characteristics to block their spam.

SECURITY | Blended Threats Module

Blended email threats are a considerable security risk to organizations. They are emails which contain embedded URL links to malicious websites hosting malware and browser vulnerability exploits. They are a serious problem as most traditional anti-malware measures are ineffective against them. Blended threats circumvent normal signature-based email anti-virus solutions by avoiding attachment of the malware to the email. Instead a recipient of a blended threat is encouraged to click on a link in an email through social engineering. Common ploys include links to news headlines, online videos or holiday e-cards. The sites linked to by blended threats often appear legitimate, adding to the social engineering pretence and luring users into clicking on a download and infecting themselves with malware – typically a Botnet client.

MailMarshal™ SMTP 6.7
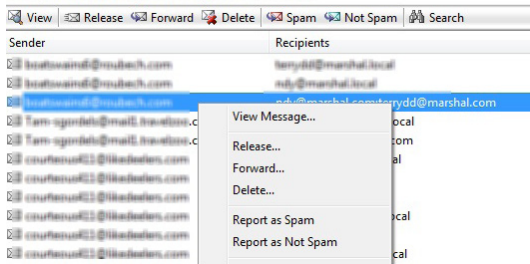
SIMPLY RIGHT-CLICK ON A MESSAGE IN THE MAILMARSHAL CONSOLE TO ACCESS NEW OPTIONS TO INSTANTLY REPORT MISSED SPAM.

The scale of the blended threats issue is significant. Research by Microsoft has revealed that 4% of corporate computers and 30% of home computers are infected with bot code. Blended threats are the primary means of distributing links to sites that enable Botnet infections. Furthermore, clean-up of bot code infections is typically more difficult than anti-virus. Bots are notoriously hard to detect and remove, often disabling locally installed anti-virus products and constantly morphing to avoid signature-based detection. 80% of bot infections result in the need to rebuild the computer due to the difficulties in permanently removing the malware.

The Blended Threats Module for MailMarshal SMTP 6.7 provides unique protection against blended email threats. It is an optional service which uses the M86 Security cloud-based malware behavior analysis datacenter to observe and determine the malicious nature of embedded URLs in email messages. The Blended Threats Module provides a constantly updated library of known malicious URLs to block blended email threats. Please look for the Blended Threats Module Datasheet available on the M86 website for more information.

ADMINISTRATION | Automated User Group Maintenance
MailMarshal provides functionality to automatically populate email user groups. This feature is most typically used to build a list of email accounts that your organization communicates with. This is achieved by harvesting the recipient's email address on emails sent from your organization.

This automated harvesting and populating of email user groups can grow quickly for some organizations if unmanaged. MailMarshal SMTP 6.7 streamlines the management of these automatically generated email addresses by dynamically pruning them. Pruning email addresses can be based on two conditions. User groups can automatically remove email addresses older than a specified time frame (such as 3 months) and/or set a maximum number of email addresses per group and automatically remove the oldest email addresses to maintain this upper size limit. This ensures that user groups remain current, relevant and maintains consistent server performance.

SECURITY | Outbound SMTP Authentication
Outbound SMTP authentication has been added in MailMarshal SMTP 6.7, enabling outbound authentication for each route within MailMarshal. Outbound SMTP authentication can be useful when upstream ISPs require credentials to help combat spammers.

SECURITY | Improved Inbound SMTP Authentication
Inbound SMTP authentication now supports CRAM-MD5 signing which enables more secure authentication between servers.

ADMINISTRATION | Upgrade Tasks
A new MailMarshal Console view provides administrators with information on new features in the latest release. It also streamlines tasks to enable and configure new features if desired; helping to ensure that you receive the maximum benefits from all the latest and greatest capabilities MailMarshal has to offer.

ADMINISTRATION | Report Spam / Not Spam to M86 Security Labs
Occasionally MailMarshal's anti-spam filtering can get it wrong, missing a spam message it should have caught or false blocking a legitimate message. MailMarshal SMTP 6.7 makes it faster and easier for administrators to report these errors to M86 Security so that we have the opportunity to correct the error. Simply right-clicking on a message in a quarantine folder provides options which directly report the error back to M86 Security with no further administrative effort required.

MailMarshal™ SMTP 6.7
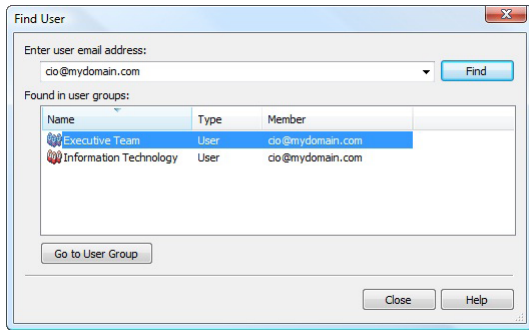
SEARCH BY EMAIL ADDRESS TO FIND ALL ASSOCIATED USER GROUPS.

FOR MORE INFORMATION

The MailMarshal SMTP 6.7 Release Notes can be found on the Support section of our website with a list of all changes in this latest release.

Please also look for our new MailMarshal SMTP 6.7 datasheet available from the Resources section of our website – www.m86security.com – or feel free to contact your local M86 Security representative to learn more about latest features and innovations.

Additional reading available from www.m86security.com:

- Defense-in-Depth Anti-Spam Whitepaper
- Blended Threats Whitepaper
- Blended Threats Module Datasheet
- Marshal IP Reputation Service Datasheet

ADMINISTRATION | Address to User Group Associations Report

Another useful new feature for administrators enables you to search by email address and instantly receive a report of all user groups that email address belongs to. This helps in troubleshooting and administration of users and policies.

ADMINISTRATION | Commit Configuration Scheduling

For larger organizations using MailMarshal in an array, this new feature allows you to specify appropriate times for configuration and update changes to apply. This ensures that servers do not implement changes outside of scheduled update times.

ANTI-SPAM | End User Spam Quarantine Management Update

MailMarshal's end user Spam Quarantine Management (SQM) now provides individual users with the option to turn email digest notifications on or off. Email digest notifications are periodic summary emails addressed to each user with a consolidated report on spam activity and quarantined messages for all of their email accounts. Users can quickly and easily identify potential false positives they wish to receive and release the message by simply clicking on a link in the email. Some users prefer to manage their spam directly within the SQM web interface and prefer not to receive digest notifications. Those users can now set their own individual preferences.

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**

M86
™
SECURITY

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 Center, 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 11.05.09