MARSHAL8e6™

Marshal Email Gateway Security

MailMarshal™ SMTP 6.4 – Best-in-class email security for Enterprise

Protecting your organization against spam and viruses while managing compliance requirements and preventing data leakage may seem a daunting challenge. Finding a way to do all this with a single solution that meets the scalability, flexibility and centralized administration needs of the largest enterprises probably sounds too good to be true. MailMarshal is true email security and management.

OVERVIEW:

MailMarshal SMTP is an email security solution for enterprise organizations. It unifies email threat protection, content security, policy enforcement, compliance and data leakage prevention into a highly scalable, flexible and easy-to-manage enterprise solution. MailMarshal acts as an email gateway to your organization by filtering all incoming and outgoing email at your network/Internet perimeter. MailMarshal blocks incoming email threats such as spam, phishing, viruses, malware and Denial of Service attacks. MailMarshal also enforces acceptable use policies and ensures compliance with data leakage prevention policies. MailMarshal can be deployed as a standalone solution or multiple, distributed MailMarshal servers can be easily configured in an array to support the largest of enterprise environments with minimal administration.

KEY BENEFITS:

Secures your email gateway against all threats

MailMarshal restores the real business value in email by making it safe and efficient to use. MailMarshal protects against all email threats including blocking spam, phishing, viruses, Trojans, worms, Denial-of-Service attacks, Directory Harvesting attacks and spoofed messages.

Rapid Return on Investment

Comprehensive and meaningful management reports highlight anti-spam and security effectiveness as well as identifying attempted policy breaches, enabling system administrators to demonstrate a rapid return on investment.

Low Total Cost of Ownership

Easy deployment, minimal administration overhead, consolidation of all email security functions into a single management interface,along with Zero-Day security updates and detailed but clear reporting, are all part of what makes MailMarshal the ultimate email security solution.

Enables compliance obligations and data leakage prevention policies

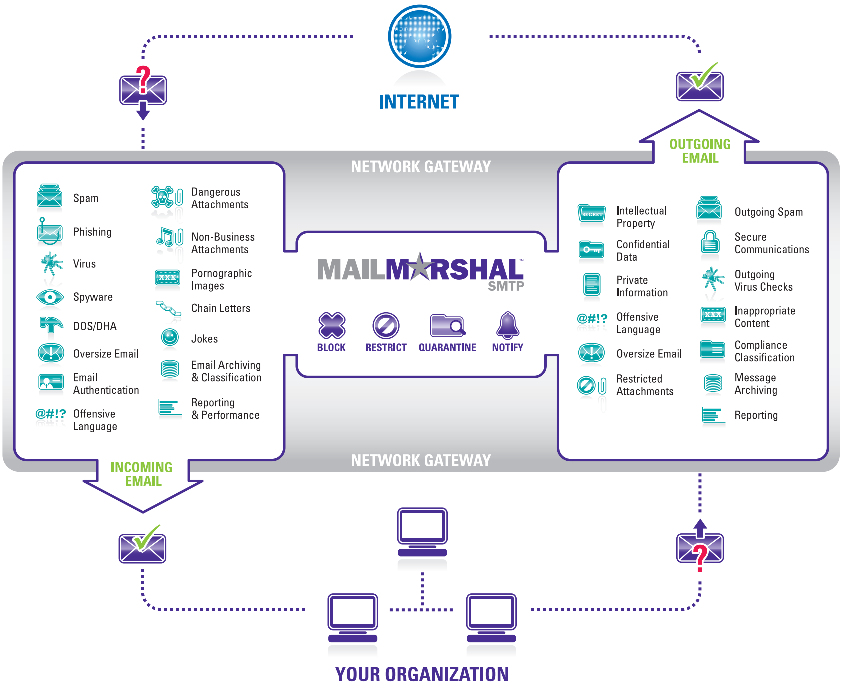
MailMarshal enables organizations to place restrictions on who can send confidential information via email and what data can be sent, and ensures that sensitive communications are secured against prying eyes. MailMarshal also provides contextsensitive email archiving, such as storing all messages on a related topic or all email exchanges with specific domains.

Provides legal liability protection

Inappropriate or offensive content is filtered out of incoming email and outgoing email is automatically checked for policy compliance. MailMarshal allows enterprises to demonstrate that all reasonable measures to protect employees and fairly enforce policies are in place.

KEY FEATURES

- Unsurpassed protection against spam,phishing, viruses and malware
- Denial of Service and Directory Harvesting Attack protection
- Inbound Content Security
- Outbound Policy Enforcement and Compliance Management
- Data Leakage Prevention
- Secure Email Encryption
- Message Archiving
- Pornographic Image Detection
- Reporting and Message Classification
- Comprehensive Enterprise Management



Marshal Email Gateway Security

MailMarshal™ SMTP 6.4 – Best-in-class email security for Enterprise

Improves network efficiency and saves costs

By controlling bandwidth consumption MailMarshal maintains consistent and reliable network performance and prevents excessive non-business email use.

Improves employee productivity

Implementing MailMarshal means that employees spend less time managing spam and helps organizations enforce acceptable use policies, to control sending personal email or other time-wasting, non-business activities.

Safeguards business reputation

MailMarshal prevents the unauthorized distribution of confidential or sensitive information via email and ensures that users are not in a position to embarrass your organization through inappropriate content or data leakage via email.

Creates a safer working environment for employees

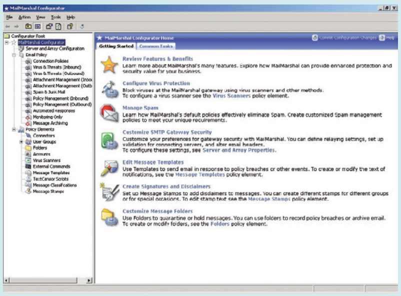
Through consistent and thorough application of security and acceptable use policies, issues such as sexual or racial harassment via email can be prevented.

SOLUTIONS FOR ENTERPRISE ENVIRONMENTS

MailMarshal SMTP is the world's most capable, powerful and scalable email security system. It is renowned for its ease of use, performance and reliability. According to numerous MailMarshal customers, "It just does what it says it does on the box". MailMarshal is utilized by many of the Global Fortune 500 companies.

MailMarshal SMTP can be deployed as a standalone gateway solution or multiple servers can be connected to form an array capable of supporting the largest enterprise environments. MailMarshal's Array Manager architecture allows you to administer multiple, geographically distributed servers and gateways with consolidated management, reporting, performance counters and central policy configuration.

MailMarshal SMTP allows you to build a fault-tolerant, load-balanced environment with a minimum of complexity and cost.



Review Features & Benefits
Learn more about MailMarshal's many features. Explore how MailMarshal can provide enhanced protection and security value for your business.

Configure Virus Protection
Block viruses at the MailMarshal gateway using virus scanners and other methods.
To configure a virus scanner see the Virus Scanners policy element.

Manage Spam
Learn how MailMarshal's default policies effectively eliminate Spam. Create customized Spam management policies to meet your unique requirements.

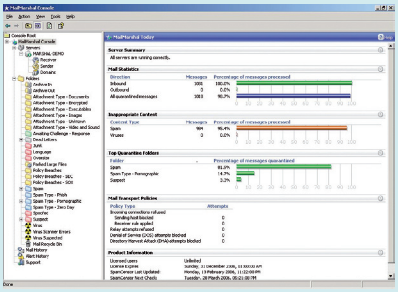
Customize SMTP Gateway Security
Customize your preferences for gateway security with MailMarshal. You can define relaying settings, set up validation for connecting servers, and alter email headers.
To configure these settings, see Server and Array Properties.

Edit Message Templates
Use Templates to send email in response to policy breaches or other events. To create or modify the text of notifications, see the Message Templates policy element.

Create Signatures and Disclaimers
Set up Message Stamps to add disclaimers to messages. You can create different stamps for different groups or for special occasions. To edit stamp text see the Message Stamps policy element.

Customize Message Folders
Use Folders to quarantine or hold messages. You can use folders to record policy breaches or archive email.
To create or modify folders, see the Folders policy element.

THE MAILMARSHAL CONFIGURATOR IS WHERE YOU DEFINE YOUR ORGANIZATION'S POLICIES.



Server Summary

All servers are running correctly.

Mail Statistics

Direction	Messages	Percentage of messages processed
Inbound	1031	100.0%
Outbound	0	0.0%
All quarantined messages	1018	98.7%

Inappropriate Content

Content Type	Messages	Percentage of messages processed
Spam	984	95.4%
Viruses	0	0.0%

Top Quarantine Folders

Folder	Percentage of messages quarantined
Spam	81.9%
Spam Type - Pornographic	14.7%
Suspect	3.3%

Mail Transport Policies

Policy Type	Attempts
Incoming connections refused	
Sending host blocked	0
Receiver rule applied	0
Relay attempts refused	0
Denial of Service (DOS) attempts blocked	0
Directory Harvest Attack (DHA) attempts blocked	0

Product Information

Licensed users	Unlimited
License Expires	Sunday, 31 December 2006, 01:00:00 AM
SpamCensor Last Updated:	Monday, 13 February 2006, 11:22:00 PM
SpamCensor Next Check:	Tuesday, 28 March 2006, 05:21:08 PM

MAILMARSHAL TODAY PAGE PROVIDES A DASHBOARD VIEW OF YOUR EMAIL ENVIRONMENT

If you wish to add more capacity to your email environment, you can simply install MailMarshal SMTP on an additional server, connect the new server to the Array Manager and it is automatically added into the array.

TECHNICAL FEATURES – THREAT PROTECTION

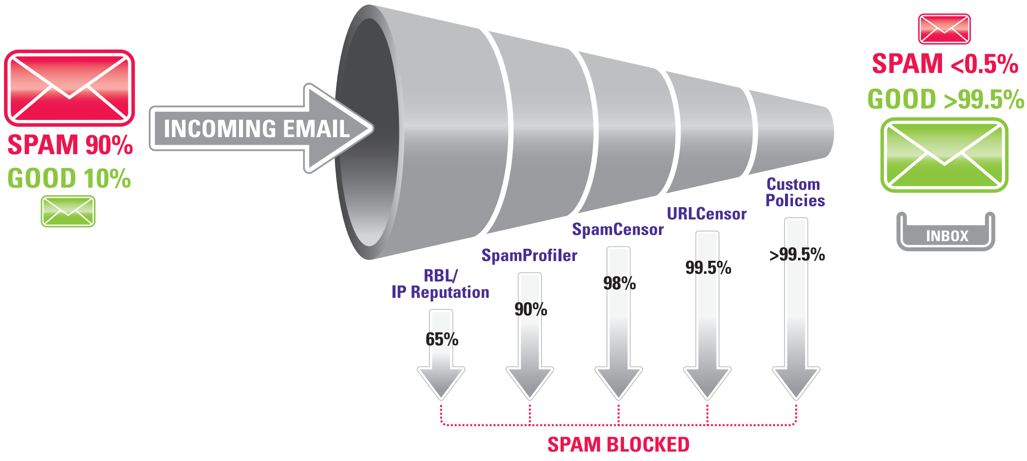
Spam & Phishing Protection

- MailMarshal's anti-spam engine combines layers of spam filters together to provide unsurpassed protection, performance and accuracy.
- Achieves a consistent 99.5% spam catch with <0.001% false positives with no special tuning or ongoing administration.
- Supports IP Reputation services (whitelists / blacklists) and DNSBL databases such as Spamhaus with unique Automated Adaptive Whitelists to ensure you do not block email from common partners.
- Provides complete anti-spam reporting, including individualized reports for employees and end-user spam quarantine release.

Virus & Malware Protection

- Provides a layered anti-virus strategy, based on the seamless integration of a range of supported anti-virus vendors, including McAfee, Norman, Sophos, Symantec and others.
- Supports integration with dedicated antispyware scanners, including CounterSpy and PestPatrol.
- Detects and unpacks archive file types, identifying viruses recursively embedded within attachments

MAILMARSHAL ANTI-SPAM ENGINE



- Identifies and blocks dangerous file types by their content rather than just by file name or extension, thus detecting mislabeled attachments.

- Identifies and quarantines messages containing potentially harmful code or URL links to known malicious websites.

- Applies virus protection to both incoming and outgoing email and provides full virus and malware reporting.

Denial of Service & Directory Harvesting Attack Protection

- Detects and manages suspicious behavior such as rapid concurrent connections from a single IP address or multiple emails sent to invalid email addresses.

- When suspected Denial of Service or Directory Harvesting Attacks are detected, connection attempts from the offending SMTP server are rejected. Normal service resumes automatically after a defined period.

TECHNICAL FEATURES CONTENT FILTERING

Comprehensive Security

- Enforces any policy based on virtually any message attribute. Control messages based on:

- Who the message involves (sender, recipient, source IP address or country of origin)

- What the message contains (spam, malware, keywords and phrases, message size, file attachments, alphanumerical patterns)

- Actions you would like to take (block, delete, archive, delay, encrypt, copy, notify an email address, strip an attachment, classify the message for reporting)

- Essentially any desired policy can be automatically enforced with MailMarshal.

Inbound Content Security

- Take a range of actions on incoming email messages based on any pre-defined condition.

- Reject messages exceeding a specified size limit or messages from any blacklisted IP address, domain or country.

- Control inbound messages based on the presence of restricted file types, the number of attachments of inappropriate keywords (such as profane, racist or sexist language).

- Implement policies by user, department, special group or domain – or across the entire organization.

- Provide visibility of the security of incoming email through comprehensive reporting and email notifications.

- Manage email authentication and antispoofing through Sender ID and Sender Policy Framework standards support.

Outbound Policy Enforcement and Compliance Management

- Automatically applies policy to outgoing messages.

- Enforces policies related to outgoing message size, attachments, keywords or recipient.

- Blocks profane or inappropriate language in outgoing email.

- Upholds corporate policies and ensures messages comply with legal requirements.

- Automatically adds disclaimers or encrypts communications based on policy.

- Automatically archives all outgoing (and incoming) communications to meet any legal obligations.

- Provides full reporting on outbound email content and attempted policy breaches.

- Provides sample policy templates including SOX and HIPAA.

Data Leakage Prevention

- Provides fingerprint technology specifically designed to manage the distribution of confidential files and intellectual property.

- Quarantines any restricted file being sent by an unauthorized user and sends notifications to nominated email addresses.

Secure Email

- Provides built-in gateway-to-gateway TLS encryption to secure confidential communications or ensure regulatory requirements are complied with.

- Interfaces to an optional S/MIME PKI encryption module, MailMarshal Secure. MailMarshal Secure provides comprehensive email encryption facilities with full certificate/key management and automatically maintains encryption user groups though LDAP.

Message Archiving

- Archives incoming/outgoing messages automatically on a daily basis.

- Allows messages to be archived according to conditions such as who the message was from or what it relates to.

- Permits messages to be retained indefinitely or automatically deleted after a defined retention period.

- Locates important messages through comprehensive search facilities and provides full reporting on archived messages.

Pornographic Image Detection (optional)

- Image Analyzer™ is an optional module for identifying inappropriate or pornographic images using deep image analysis.

- Pornographic image detection can be applied to a range of supported image file formats.

- Image Analyzer helps prevent exposure to offensive content and educates users on what is deemed appropriate.

Reporting and Message Classification

- Provides comprehensive security and email activity reporting.

- Review bandwidth reports by sender, recipient, domain and file type.

- Analyze anti-spam performance by user via individualized web-based reports.

- Allows you to sort and store messages based on content and run reports on stored messages for auditing.

- View anti-spam/anti-virus performance, attempted policy breaches and identify potential email abusers through security reports.

Enterprise Management

- Provides administrative features designed to streamline maintenance and minimize administrative overhead.

- Automates importing and maintenance of email account information through comprehensive LDAP and Active Directory support.

- Simplifies configuration changes with single one-click synchronization to all servers via the MailMarshal Array Manager.

- Consolidates logging and quarantine data, so message release can be performed from one central console.

- Enables advanced message management with sophisticated routing and relaying tables and flexible delivery options.

- Summarizes all email traffic information across an array with performance counters and the MailMarshal™ Today interface.

SYSTEM REQUIREMENTS

Processor
Pentium 4 or higher

Disk Space
10GB (NTFS) or higher

Memory
512MB RAM or higher

Operating System
Windows Server Standard or Enterprise 2003 or Windows XP Professional SP1 or later

Database (Optional)
MSDE 2000 SP3a or later or SQL 2005 Express or Microsoft SQL Server 2000 SP3a or later or SQL Server 2005 Microsoft Data Access Components (MDAC) 2.7 or later

Please note: MailMarshal SMTP does not support 64-bit versions of Windows

TRY BEFORE YOU BUY.

Marshal8e6 offers a free ‘try before you buy’ program for MailMarshal SMTP. Please visit us on the Web at www.marshal.com and click on the Evaluation Center to download a fully functional complimentary trial.

MARSHAL8e6™

Corporate Headquarters
Marshal8e6

828 West Taft Avenue
Orange, CA 92865
United States

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

Corporate Headquarters
Marshal8e6

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Marshal8e6

Suite 1, Level 1, Building C
Millennium Center
600 Great South Road
Aukland, New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720