



## Email Gateway Security

# MailMarshal™ SMTP 6.5

Protecting your organization's email environment against spam and viruses while managing complex compliance policies and preventing confidential data leakage can be a daunting challenge. MailMarshal SMTP achieves all this within a single solution that meets the scalability, flexibility and centralized management needs of even the largest enterprises. MailMarshal provides true email security for organizations of all sizes.

### OVERVIEW

MailMarshal SMTP is a versatile, powerful and scalable email security system for use in any network environment. It integrates email threat protection, inbound/outbound content analysis, policy enforcement, compliance and data leakage prevention into a single, flexible and easy-to-manage solution.

MailMarshal acts as a gateway to your organization by filtering all incoming and outgoing email at your network/Internet perimeter. It 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 into an array to support the largest networks with centralized management for streamlined administration.

### KEY BENEFITS

#### Secures your email gateway against all threats

MailMarshal restores the true business value of email, making it safe and efficient to use. It protects against all email threats including spam, phishing, viruses, Trojans, worms, DoS attacks, malware, blended threats, directory harvesting attacks and spoofed messages.

### KEY FEATURES

- Best-of-Breed protection against spam and phishing
- Protection from viruses, malware and blended threats
- Inbound content security (deep content inspection)
- Outbound acceptable use and compliance policy enforcement
- Data Leakage Prevention (DLP) technology
- Secure, automatic email encryption
- Message Archiving
- Pornographic Image Detection (optional)
- Denial of Service (DoS) and directory harvesting attack prevention
- Reporting and message classification
- Comprehensive enterprise management



#### 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 to stakeholders and executives.

#### Low Total Cost of Ownership

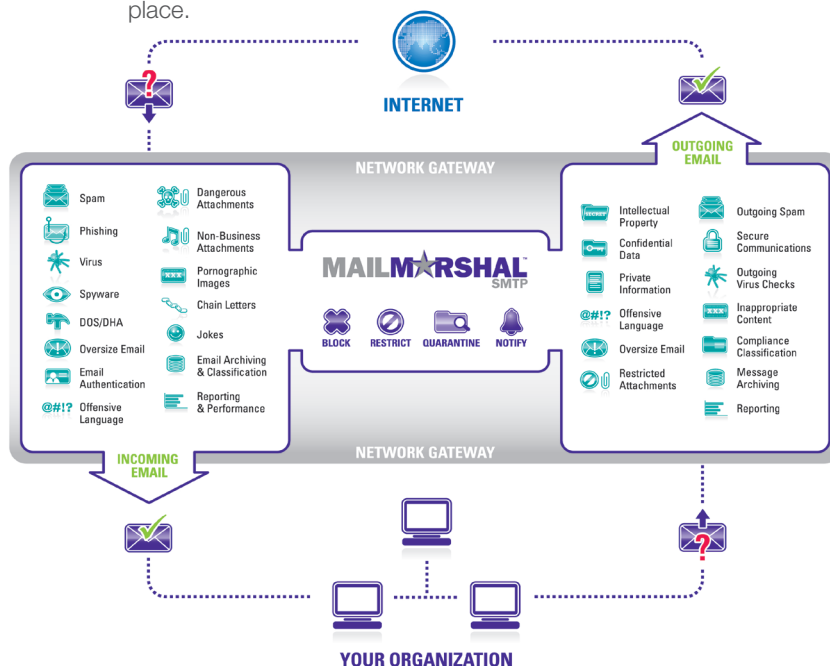
Easy deployment, minimal administration overhead, consolidation of all email security functions into a single management interface along with Zero-Day security and anti-spam updates, and detailed but clear reporting are all part of what makes MailMarshal the ultimate email security solution.

#### Enforces compliance 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. It ensures that sensitive communications are secured against prying eyes. MailMarshal also provides context-sensitive email archiving, such as storing all messages on a related topic or all email exchanges with specific domains.

#### Provides comprehensive 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.



### 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 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 offensive conduct.

### 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.

**"The anti-spam engine has blocked almost all the spam entering our mail gateway. Thanks to MailMarshal, SunRice email users now simply do not expect to receive spam".**

- MICHAEL BROWNING, SENIOR SYSTEMS ENGINEER, SUNRICE

**"We specifically sought a solution that would be easy to manage and update, as well as being highly flexible to seamlessly adapt to changing organizational needs or government ICT legislation, and MailMarshal satisfied all these requirements".**

- ANTHONY SOUTHGATE, GENERAL MANAGER FOR SECURITY DIVISION, INTERNET SOLUTION

## SOLUTIONS FOR ALL TYPES OF ORGANIZATION

Over a decade, MailMarshal has become one of world's most successful and popular email security solutions. MailMarshal is used by more than 10,000 organizations, including 40% of the World's Fortune 500 companies.

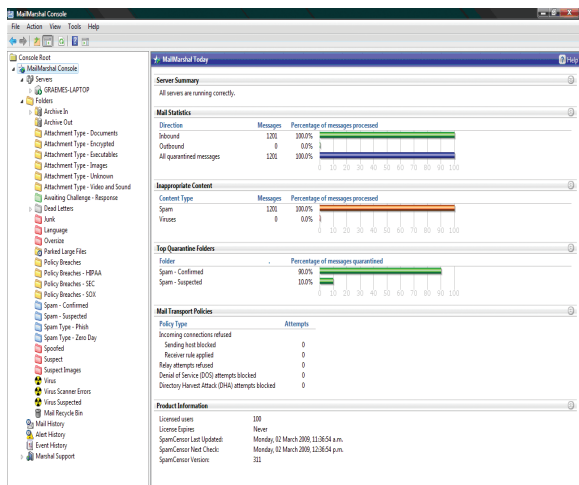
Our customers range from small businesses with fewer than 25 employees to universities, multi-national corporations and government agencies with hundreds of thousands of users. The majority of our customers have used MailMarshal for more than three years and, when asked in a recent survey, 97% said that they would recommend MailMarshal to others. MailMarshal is renowned for its ease of use, performance and reliability. According to many MailMarshal customers, "It just does what it says it does on the box".

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 environments with a minimum of complexity and cost.

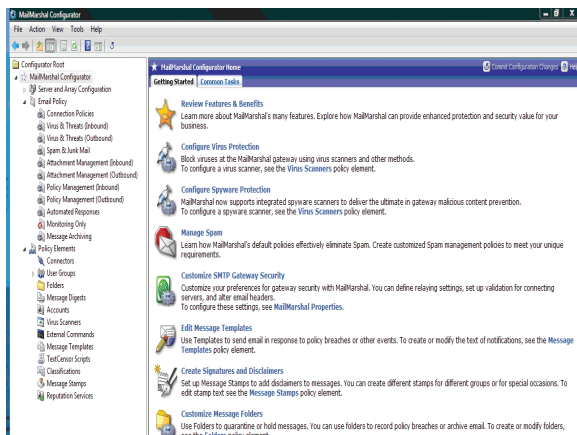
## TECHNICAL FEATURES - THREAT PROTECTION

### Spam & Phishing Protection

- The MailMarshal Defense-in-Depth anti-spam engine combines layers of spam filters for unsurpassed protection, performance and accuracy. It achieves a consistent 99.5% spam catch rate with near zero false positives with no special tuning or ongoing administration.
- Dynamic anti-spam updates are provided via the TRACElabs update service every 60 seconds along with weekly heuristic engine updates.
- Support for IP Reputation Services (whitelists/blacklists) along with DNSBL databases such as Spamhaus.
- Provides proprietary Automated Adaptive Whitelist technology which tracks your email partners to ensure that messages from trusted sources are not blocked as spam. No need to manually create or maintain whitelists.
- Provides complete anti-spam reporting including individualized reports for employees and comprehensive end-user spam quarantine release functionality.

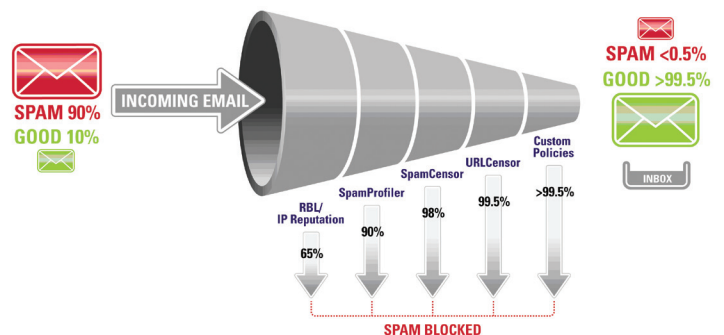


The MailMarshal console provides a dashboard view of your email environment.



The MailMarshal configurator is where you define your organization's policies.

## MARSHAL MAILMARSHAL ANTI-SPAM ENGINE

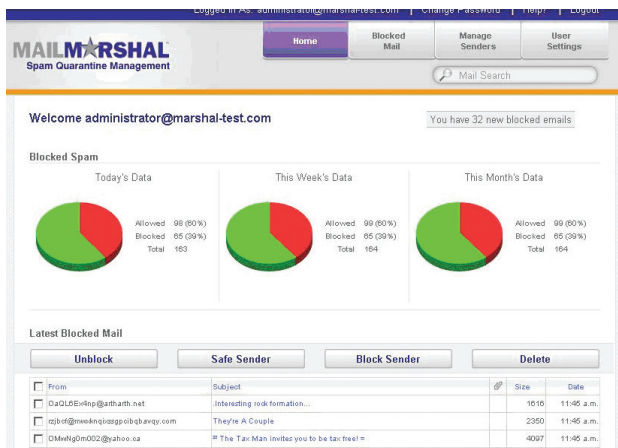


## Virus & Malware Protection

- 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 anti-spyware scanners, including CounterSpy and CA Anti-Spyware for Enterprises.
- Detects and unpacks archive file types, identifying viruses recursively embedded within attachments.
- Identifies and blocks dangerous file types by their content and MIME type rather than simply by file name or extension, thus detecting mislabeled attachments.
- Provides deep content analysis of all email components to identify and quarantine 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.



The MailMarshal spam quarantine management console (SQM) enables end-users to review spam blocked for them and release messages they wish to receive.

## 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, alphanumeric 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 anti-spoofing 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

- Features file 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.



The Marshal reporting console provides web-based access to a wide range of email reports.

## 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 Email Server (SES). MailMarshal SES provides comprehensive email encryption and digital signing facilities with full certificate/key management and automatically maintains encryption user groups through 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
- Schedule reports with email delivery options in a range of output formats including Excel, MHTML and PDF.
- 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 dashboard.

### SYSTEM REQUIREMENTS

<b>HARDWARE</b>	<b>Minimum</b>	<b>Recommended*</b>
<b>Processor</b>	Pentium 4 or equivalent	Pentium Core 2 Duo 3.0 GHz or higher
<b>Disk Space</b>	20GB (NTFS) or higher	160GB (NTFS) or higher
<b>Memory</b>	1GB RAM or higher	2GB RAM or higher
<b>Internet</b>	56Kb/s Internet connection or better	256Kb/s broadband Internet connection or better
<b>SOFTWARE</b>		
<b>Operating System</b>	Windows Server 2008 / Windows Vista / Windows Server Standard or Enterprise 2003 SP2 or later / Microsoft Small Business Server 2003 & 2008 / Windows XP Professional SP3 or later (MailMarshal SMTP supports 32-bit mode running on 64-bit operating systems)	
<b>Database</b>	SQL Server 2008 / SQL Server 2008 Express / SQL Server 2005 / SQL Server 2005 Express	

\*These requirements are recommended for a 100 user organization desiring high performance and sufficient resources for 12 months of report logging and email archiving.

**PLEASE NOTE:** MailMarshal is also available as an appliance (e10000) and hosted services solution. For more information on hardware requirements for larger organizations, please contact your local Marshal8e6 Sales Representative.

### TRY BEFORE YOU BUY.

Marshal8e6 offers a free 'try before you buy' program for MailMarshal SMTP. Please visit us on the Web at [www.marshal8e6.com](http://www.marshal8e6.com) and click on the *Free Product Evaluation* button to download a fully functional complimentary 30-day trial.



**Corporate Headquarters**  
Marshal8e6

828 West Taft Avenue  
Orange, CA 92865  
United States

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

**International 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  
Auckland, New Zealand

Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720