

# MailMarshal™ e10000 Security Appliance

## Unrivalled Functionality, Scalability and Manageability for Enterprises

Securing enterprise email against spam, viruses and other malware while also managing compliance requirements shouldn't present a major headache for large organizations. Finding a low-administration solution that is also flexible and highly scalable is now attainable. It's called MailMarshal e10000 – and it represents the first of a new breed of more intelligent appliances.

### OVERVIEW

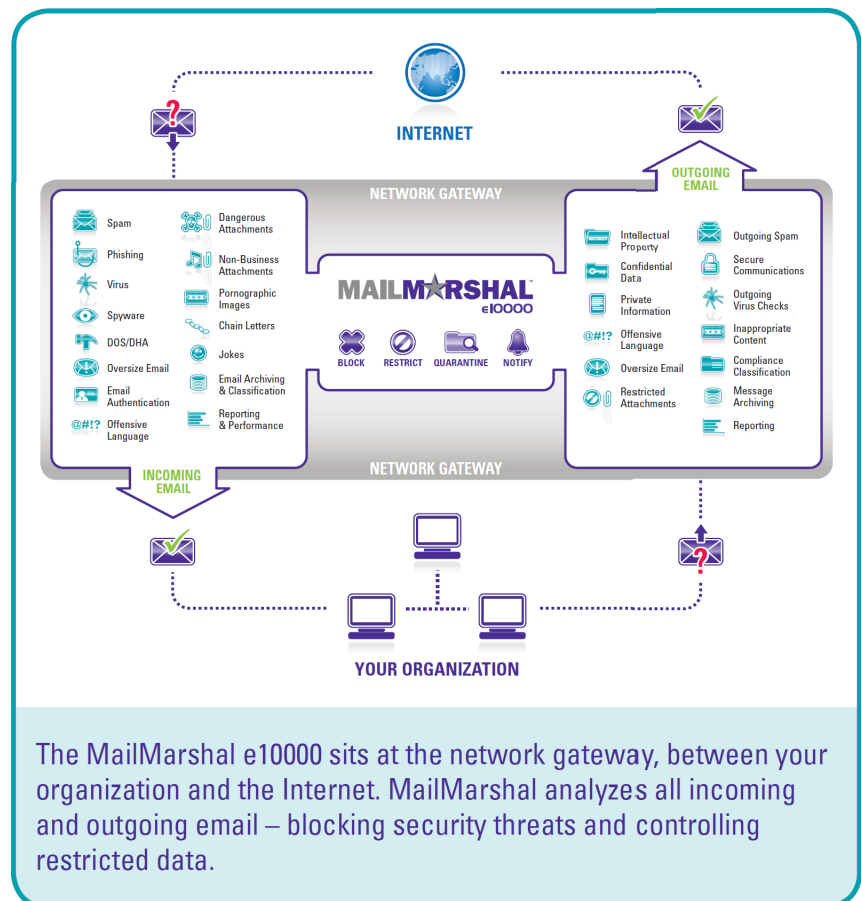
The MailMarshal e10000 incorporates the functionality and scalability of an enterprise software solution in a convenient appliance form factor. The result is the best of both worlds: email threat protection, data leakage prevention and policy enforcement in a single, easy to manage yet highly scalable solution. The MailMarshal e10000 can be deployed as a standalone gateway solution or multiple appliances can be deployed to form an array capable of supporting the largest enterprise environments.

The MailMarshal e10000 eliminates the problems of rapid obsolescence, poor scalability and single-function security traditionally associated with appliances. With the MailMarshal e10000, M86 Security has successfully combined the flexibility and functionality of a software solution with the low administration requirements of an appliance.

### KEY FEATURES

The MailMarshal e10000 effortlessly protects enterprises against multiple security threats while providing complete visibility and centralized management tools:

- Protection against spam, viruses, phishing & other malware
- Denial of Service and Directory Harvesting Attack Protection
- Inbound Content Security
- Outbound Policy Enforcement & Compliance Management
- Data Leakage Prevention
- Secure Email
- Message Archiving
- Pornographic Image Detection (optional)
- Reporting and Message Classification
- Enterprise Management Tools



## KEY BENEFITS

### Rapid Return on Investment

Comprehensive management reports highlight security effectiveness and identify potential rule breakers, enabling system administrators to demonstrate a significant and rapid return on investment.

### Low Total Cost of Ownership

The MailMarshal e10000 is fast and easy to deploy and requires minimal administration overhead. It consolidates all email security functions into a single management interface and provides detailed but clear reporting. The result is a compellingly low total cost of ownership.

### Future-Proofs Your Investment

The MailMarshal e10000 is fully upgradeable, allowing enterprises to add new features and functionality without the need to purchase a replacement appliance.

### Automatically Assures Email Compliance

The MailMarshal e10000 automatically archives any incoming or outgoing email and can classify and take actions on messages according to specific regulatory requirements.

### Improved End-User Productivity

Blocking email-borne threats at the gateway frees up end users from spending time on managing spam. By applying security and acceptable use policies, end users are also protected against issues such as email harassment.

### Increased Network Efficiency

The MailMarshal e10000 blocks 99.5% of spam at the gateway, preventing unwanted messages from getting onto the corporate network. This frees up network bandwidth and restores network performance.

### Minimized Downtime

Multiple MailMarshal e10000 appliances can be deployed and configured in arrays for load balancing and redundancy. This minimizes the potential downtime posed by email security threats.

### Protects Business Reputation

Ensuring that embarrassing or confidential messages are not leaked outside the company helps enterprises protect sensitive information and comply with their acceptable use policies.

### Unrivalled Legal Liability Protection

Inappropriate content is filtered out and outgoing email is automatically checked for policy compliance. This enables enterprises to show that acceptable use policies have been enforced and protects them against potential claimants.

## SOLUTION FOR ENTERPRISE ENVIRONMENTS

### Flexible, Future-Proof Platform

The MailMarshal e10000 offers the best of both worlds; it is easy to deploy and offers robust security with low administration requirements, but also offers the flexibility and versatility of a software platform.

The e10000 is self-maintaining, receiving automatic security and maintenance updates via the Internet. It can be easily upgraded to add new features and functionality, avoiding obsolescence and the need to purchase an upgrade appliance – future proofing your investment.

### Modular and Scalable

The MailMarshal e10000 is an elegant, flexible solution which can be easily adapted to the needs of any organization – from 25 to over 10,000 email users. It is designed to support a fault-tolerant, load-balanced and distributed network environment at minimal cost.

The e10000 is specifically designed to support multiple distributed appliances configured in an array, managed from a single interface – the Array Manager. The Array Manager architecture is fault tolerant, ensuring that no disruption to normal email services occurs in the event of a lost connection.

Scaling the MailMarshal e10000 solution is as simple as connecting to the Array Manager and joining a new appliance. The new appliance is immediately able to begin processing email and will load balance with other nodes in the array. Any configuration changes, updates or upgrades are automatically distributed and managed by the Array Manager with a single click of a button.

## TECHNICAL FEATURES - THREAT PROTECTION

Threat protection is perhaps the most vital piece of an email security solution. In today's world of spam, blended threats and Trojans, all manner of malware and malicious code are attempting to enter your organization. The best place to address this issue is at the point of entry, the network gateway.

**M86 Security's Array Manager Architecture permits system administrators to manage a large number of appliances across multiple locations from a central console.**

## Spam and Phishing Protection

- SpamCensor™ anti-spam engine achieves an average 99.5% spam catch rate with only 0.001% false positives
- SpamCensor supports the use of third party DNSBL databases such as Spamhaus
- Blocks, deletes, tags or quarantines spam for end-user review
- Provides full anti-spam reporting

## Virus and Malware Protection

- Provides a layered anti-virus strategy, centered on the integrated McAfee antivirus scan engine
- Detects and unpacks archive file types, identifying viruses recursively embedded within attachments
- Identifies and blocks restricted file types
- Identifies and quarantines messages containing potentially harmful code
- Applies virus protection to both incoming and outgoing email
- Provides full virus reporting

## Denial of Service and Directory Harvesting Attack Protection

- When deployed as the first receiving email gateway, the e10000 detects and manages atypical behavior (for example, 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 is restored after a predefined period

## TECHNICAL FEATURES - CONTENT FILTERING

Being able to fully inspect all incoming and outgoing content (including email body text, attachments, extracted archived files and any extracted text of those attachments) is necessary to gain control of your messaging system. Providing a safe working environment, protecting the organization from data leakage and ensuring its reputation while also meeting any compliance requirements are growing imperatives.

### Inbound Content Security

- Blocks, rejects, quarantines, strips or marks any incoming message based on any pre-defined condition
- Enables messages exceeding a specified size limit - or messages from any blacklisted IP address, domain or country - to be rejected
- Messages can be controlled based on the presence of restricted file types, the number of attachments or inappropriate keywords (such as profane, racist or sexist language)
- All policies can be implemented by user, department, special group or domain - or across the entire company

- Comprehensive reporting and email notifications help ensure visibility into the security of incoming email
- Supports the Sender ID and Sender Policy Framework standards for email authentication and anti-spoofing

## Outbound Policy Enforcement and Compliance Management

- Automatically applies policies to outgoing messages
- Enforces policies related to outgoing message size, attachments, keywords or recipient
- Blocks profane or inappropriate language in outgoing email
- Upholds corporate standards 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 policies for SOX and SEC requirements

## Data Leakage Prevention

- Provides fingerprinting technology specifically designed to manage the distribution of confidential files and intellectual property
- Any restricted file being sent by an unauthorized email user is quarantined and notifications are sent 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

## Message Archiving

- Automatically archives incoming/outgoing messages on a daily basis
- Messages can be retained indefinitely or automatically deleted after a defined retention period
- Comprehensive search features make it easy to locate important messages
- Full reporting is provided

## Pornographic Image Detection (optional)

- Image Analyzer™ is an optional module for identifying inappropriate or pornographic images using deep image analysis technology
- Image Analyzer helps prevent exposure to offensive content and educates both internal and external email users on what content is deemed inappropriate

## Reporting and Message Classification

- Provides comprehensive security and email activity reporting
- View bandwidth reports by sender, recipient, domain and file type
- Security reports show anti-spam/antivirus performance and attempted policy breaches, and identify potential email abusers

## Enterprise Management

- Provides a wealth of administrative features designed to streamline maintenance and minimize administrative overhead
- Comprehensive LDAP and Active Directory support automates importing and maintenance of email account information
- Array Manager makes configuration changes simple and easy with one-click distribution to all servers
- Logging and quarantine data is consolidated so message searching and quarantined message release can be performed from one central console
- Performance counters and the MailMarshal Today™ interface summarize all email traffic information across an array

## SPECIFICATIONS

<b>Platform</b>	Marshal MTA and Hardened Operating System
<b>Chassis</b>	Standard 1U 19" Rack Chassis with Mounting Rails (16.8"w x 1.7"h x 22.6"d)
<b>Processor</b>	3.4Ghz Pentium 4 CPU
<b>Memory</b>	2GB SDRAM (Two (2) 1GB)
<b>Storage</b>	Twin 250GB 7200RPM Mirrored SATA Drives (hot swappable)
<b>Connectivity</b>	Two (2) GigE Network Interfaces (one for management, one for data)
<b>Power</b>	300W Power Supply, 100/240 Volts
<b>Performance</b>	60,000* messages per hour

\*PLEASE NOTE: Performance values are based on Lab testing. Actual performance may vary.

Please contact M86 Security for sizing and performance advice for your organization or to arrange a free trial.

## 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](http://www.m86security.com).

## TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://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**  
Suite 1, Level 1, Building C  
Millennium Centre  
600 Great South Road  
Auckland, New Zealand  
Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720

Version 08/29/09