

Deployment Options for Exchange

March 2006

Contents

What is Email Scanning?	2
What is Total Email Content Security?	3
The Solutions	3
What are my Options?	4
Key Differences between MailMarshal SMTP and MailMarshal for Exchange	6
Conclusion	11

This white paper examines the various options available to you for the deployment of MailMarshal in a Microsoft Exchange environment. In particular, we will look at the different versions of MailMarshal that are available and how you can combine different MailMarshal versions together to deliver a complete email content security solution.

This white paper is intended for customers of Marshal who utilize or plan to deploy a Microsoft Exchange environment. It is written at a level suited to IT Managers and Chief Information Officers.

This document is intended to explain how MailMarshal SMTP and MailMarshal for Exchange combine to provide you with a complete email content security solution. This includes looking at what makes the two products different but complementary. It also covers the options for deploying MailMarshal for Exchange, as well as the features, benefits and implications of the different deployment environments.

This document also seeks to explain the key differences between MailMarshal SMTP and MailMarshal for Exchange, namely, how the products are used and what benefits they provide. The end objective is to assist you, the customer, in making an informed decision about which MailMarshal solution is right for your needs.

Author: Bradley Anstis

WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

What is Email Scanning?

This white paper discusses two of the solutions from Marshal Family of Products for email content security. Email content security employs a number of security functions and tools to manage email. These functions include:

- Content Analysis (lexical analysis) – checking keywords and phrases in email and attachments, and the context in which they are used
- Attachment Controls – managing the size and type of email attachments
- Anti-Virus – scanning for, identifying and quarantining email suspected of containing viruses, worms, Trojans or other malicious code
- Anti-Spam – scanning for, identifying and rejecting/quarantining email suspected as Unsolicited Commercial Email (UCE)
- Confidentiality Protection – scanning for, identifying and managing email suspected to contain information of a confidential, commercially sensitive or proprietary nature
- Bandwidth Conservation – rejecting, delaying or blocking email that is either of excessive size or non-business in nature to conserve bandwidth and maintain optimum network performance for business use
- Legal Liability Protection – scanning for, identifying and managing email that does not comply with organizational guidelines for acceptable email use. This typically includes email of a harassing, defamatory, libelous, offensive, sexual, racist, profane or an otherwise socially or professionally harmful nature
- Reporting – logging all email activity and events for management review, threat analysis, infrastructure planning, forecasting, fault diagnosis, identifying breaches of acceptable use policy and general usage statistics
- Email Archiving – recording and storing email communications for the purposes of disaster recovery, legal compliance and security
- Message Stamping – append legal disclaimers or brand messages to emails.
- Email Security – Encrypt or decrypt Email at the gateway to protect your business communications

MailMarshal SMTP and MailMarshal for Exchange each offer email content security functionality; however, this functionality differs between the two products for various reasons, as explained in the following sections.

WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

What is Complete Email Content Security?

MailMarshal SMTP and MailMarshal for Exchange perform complimentary security functions. There is however differences between the solutions that become significant when examined in the context of the infrastructure required for complete email content security.

Basically, the difference is this: MailMarshal SMTP is an Internet email security solution, while MailMarshal for Exchange is an internal email management solution. To put this another way;

MailMarshal SMTP is specialized for security against external threats. MailMarshal for Exchange is specialized for management of internal email communications.

The Solutions

MailMarshal SMTP

Internet Email Security

MailMarshal SMTP is a fast, easy-to-use email filtering solution that ensures a safe and productive working environment by enforcing organizational Acceptable Use Policy (AUP) and protecting against spam and viruses.

MailMarshal SMTP is specifically designed to act as an email gateway for an organization. It intercepts email to and from the Internet using the Simple Mail Transfer Protocol (SMTP). MailMarshal SMTP includes its own email Receiver and Sender technology as well as its core technology, the content Engine.

As a gateway product, MailMarshal SMTP is ideally suited to act as a perimeter security solution, isolating your organization's internal network from Internet threats. Threats like email viruses, Spam, oversized emails and Denial of Service Attacks (DOS).

From the gateway, MailMarshal SMTP is strategically positioned to act as a policy enforcement tool for managing outgoing or incoming email. For example: adding message disclaimers to all outgoing email, rejecting outgoing/incoming email with profanity, and analyzing outgoing email for confidentiality risks.

MailMarshal for Exchange

Internal Email Management

MailMarshal for Exchange is a fast, easy-to-use email filtering solution that ensures a safe and productive working environment by enforcing organizational Acceptable Use Policy (AUP) for internal Exchange-based email communications.

MailMarshal for Exchange is specifically designed to provide internal email scanning for email traveling between Exchange 2000/2003 (Exchange) mailboxes. MailMarshal for Exchange is tightly integrated with Microsoft Exchange. It connects directly into the message queue in Exchange and uses the same unpacking content engine to MailMarshal SMTP's engine for email content analysis.



WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

By linking directly into the Exchange message framework, MailMarshal for Exchange is able to filter email that MailMarshal SMTP cannot – email between internal organizational users. This is not limited to just SMTP traffic, but also X.400 and Outlook Web Access (OWA) or any other installed foreign Email connector. Basically, any email that enters the Exchange message framework.

However, because MailMarshal for Exchange relies on the message handling technology already present in Exchange, it cannot use the same Sender and Receiver technology present in MailMarshal SMTP. It is MailMarshal SMTP's Sender and Receiver technology that provides it with the key gateway/perimeter security functionality. Therefore, MailMarshal for Exchange does not possess the same level of email gateway defense as MailMarshal SMTP.

What are my Options?

If your organization is utilizing an Exchange 2000 environment then there are basically three deployment choices for MailMarshal that can be considered

1. Both MailMarshal SMTP and MailMarshal (complete email content security)
2. MailMarshal SMTP (no internal email scanning)
3. MailMarshal for Exchange (no perimeter defense capabilities)

Both option two and three have disadvantages over the first preferred solution.

MailMarshal SMTP and MailMarshal for Exchange combined

If you deploy MailMarshal SMTP and MailMarshal and operate them together in partnership, you will be able to deploy an infrastructure for complete email content security. You will have all of the gateway scanning facilities of MailMarshal SMTP as well as the ability to scan, archive and generate reports for internal email. Basically, you will be able to provide Acceptable Use Policy enforcement for all of the email your organization creates or receives as well as realizing all of the advantages that a combined solution provides. Unnecessary Email will be blocked at the perimeter without the Exchange environment having to process it at all. Remember that on average 60% of today's incoming Email can be classified as Spam and is not necessary.

MailMarshal SMTP

If you deploy MailMarshal SMTP and use it on its own you will receive content security functionality for incoming and outgoing email from the Internet. MailMarshal SMTP also provides the best and most logical platform for anti-spam screening and management, as well as being the most appropriate version for enterprise environments. However, you will not be able to scan the contents of internal Exchange messages. Nor will you be able to generate reports for internal office email that your company's users are sending between themselves (e.g. X.400, OWA or messages from sources other than SMTP).



WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

MailMarshal for Exchange

If you deploy MailMarshal for Exchange and use it as your collective email scanning solution, you will receive a solution that is able to manage much of the core Acceptable Use Policy enforcement for your organization. However, you will sacrifice some of the important perimeter security and Spam management functionality present in MailMarshal SMTP. Furthermore, you will not benefit from MailMarshal SMTP's other added advantage; which is to isolate the internal Exchange environment from external threats, such as spam and viruses. MailMarshal for Exchange is able to intercept any email that is handled by Exchange (SMTP / X.400 / OWA). Therefore, it makes no difference if the email was generated by an internal or external source. Putting this plainly, MailMarshal for Exchange is able to content scan incoming, outgoing, and internal email when used in a standalone configuration. What it does not provide is the many enhanced security benefits that MailMarshal SMTP contributes to a complete email content security solution.

The specifics of these perimeter defenses are explained in the following section.

WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

Key Differences between MailMarshal SMTP and MailMarshal for Exchange

The standalone MailMarshal SMTP benefits are well documented in the MailMarshal SMTP Evaluation Guide, which can be downloaded from www.marshal.com under the MailMarshal SMTP product section, as such we will not cover them here. Instead, this section focuses on MailMarshal for Exchange and the benefits it provides in the two possible deployment options; Combined and Standalone.

Features	MailMarshal SMTP	MailMarshal 5.1 for Exchange
Receiver-rules / ESMTP Blocking	Yes	No
SpamCensor Anti-Spam System	Yes - Full	Yes - Partial
Spam Quarantine Management System for End Users	Yes	No
Enterprise Multi-Server Management	Yes	No
Web-Based Administration Console	Yes	No
Support for DNS Blacklists	Yes	No
Folder Security Permissions	Yes	No
Spam Classifications for Explicit and Suspect Spam	Yes	No
Oversize Message Rejection	Yes	No
Ability to Isolate Exchange Sever from Internet Threats	Yes	No
Header Re-writing	Advanced	No
Anti-Spoofing	Yes	No
Direct Active Directory Integration	Yes	Yes
Gateway Anti-Virus Scanning	Yes	No
Anti-Virus Scanning Between Exchange Servers	No	Yes
Reporting on SMTP Traffic	Yes	Yes
Reporting on X.400 and OWA Traffic	No	Yes
Content Scanning of SMTP traffic	Yes	Yes
Content Scanning of X.400 and OWA Traffic	No	Yes
Gateway Email Encryption (S/MIME) Potential	Yes (optional)	No (not an option)
Performance Considerations	Very High Performance	Increases Load on Exchange Server

WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

MailMarshal SMTP Features Explained

Perimeter Security

MailMarshal SMTP is a gateway email scanning system for the content security of Internet email. Because MailMarshal SMTP operates at the gateway to an organization, it is possible to establish MailMarshal within a traditional DMZ, using a firewall to isolate the trusted network from external threats.

MailMarshal SMTP complements modern firewalls by providing content inspection of traffic permitted to pass through the firewall, much like an x-ray machine at an airport. MailMarshal SMTP also enables you to separate your policies regarding email content management and threat security. MailMarshal SMTP has many features specifically created for perimeter security:

- Receiver-rules / ESMTP support. ESMTP (Enhanced Simple Mail Transfer Protocol) provides functionality that enables MailMarshal SMTP to detect some forms of unwanted email from just the initial packets of information. This includes identifying the size of an email, the sender and the intended recipient. This can allow MailMarshal SMTP to reject a 10MB email at the SMTP negotiation stage, or identify a known SPAM source and reject the message outright by denying the connection. Receiver-rules give MailMarshal a number of key features, including:

- MAPS/RBL support. MAPS/RBL (Mail Abuse Prevention Systems / Real-time Blackhole List) is a popular optional fee-based subscription service for anti-SPAM that MailMarshal SMTP supports. Because of its exceptional effectiveness this is a popular peripheral security option for MailMarshal customers. There are a number of other real-time Blackhole systems that MailMarshal SMTP is able to support through this framework.

- Isolating the Exchange Server. By deploying MailMarshal SMTP at the gateway, you can isolate the internal Exchange network from unwanted Internet email. In this way, MailMarshal SMTP acts like a bodyguard for the Exchange environment, standing in front of your internal systems to block threats from reaching their target. This means that Spam, viruses, DOS attacks, oversized messages and non-business file types can be quarantined and managed at the gateway, away from the internal email environment. This has two key benefits:

- 1) Exchange servers are provided with a forward layer of protection against Spam, viruses and other malicious files meaning that there is less chance of a virus or malicious file entering the internal email network. Remember that on average 60% of incoming Email can be classified as this unnecessary content.

- 2) Exchange servers are spared the processing burden of processing these kinds of messages. There are fewer messages for the Exchange server to manage, as these are isolated at the gateway, making a particularly beneficial defense for keeping Spam away from the Exchange server. By reducing the load (particularly non-business email) you will lessen any performance impact that MailMarshal for Exchange may have on your Exchange systems. As a result you will not only spare the Exchange network from adversely affected processing performance, you will also keep Exchange server disk space clear of large, non-business material. This will lengthen the life of your hardware by reducing the rate at which these resources are consumed, further adding to the ROI benefits of the total MailMarshal solution.



WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

- Advanced header rewriting. Another part of MailMarshal SMTP's Receiver functionality is advanced header re-writing. This is used to manipulate email headers, which is useful to reroute messages (user-based routing) hide confidential information (such as internal server IP addresses).
- Gateway email encryption potential. MailMarshal SMTP is required if you wish to deploy MailMarshal Secure for S/MIME encrypted email. MailMarshal for Exchange does not support this option. This would allow you to deploy PKI-based email encryption at all the Internet gateways to your organization. This means that any email leaving your organization to travel out over the Internet can be automatically encrypted if necessary, without any effort from end users.

Close Active Directory Integration

MailMarshal for SMTP allows direct integration via Active Directory with Exchange users and groups. This makes it easier to use existing email user groups with MailMarshal.

MailMarshal for Exchange Features Explained

Using MailMarshal for Exchange in a standalone configuration (may include multiple Exchange 2000 servers) will allow you to implement a solid content management infrastructure with broad security capabilities.

Internal and external email content security with complete reporting.

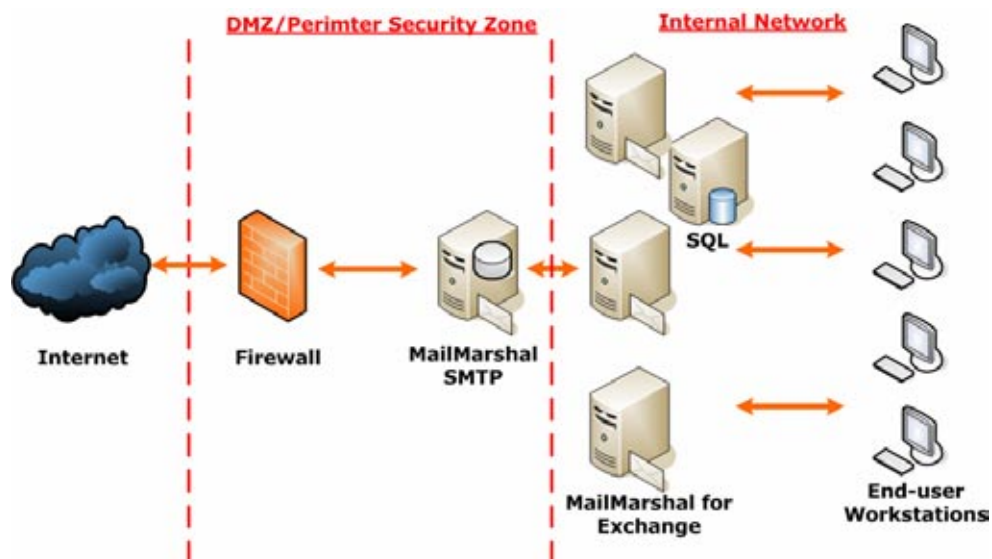
You will have the ability to content filter all email, to, from and within your organization. This is important as typically 70% of an organization's email is sent and received internally (Intranet), while 30% is sent or received with outside parties.

Close Active Directory Integration

MailMarshal for Exchange allows direct integration via Active Directory with users and groups. This makes it easier to use existing email groups with MailMarshal. The differences between the combined deployment and standalone options can also be seen in the following illustrations on page 10.

WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

MailMarshal SMTP & MailMarshal for Exchange – Combined Benefits:



Benefits:

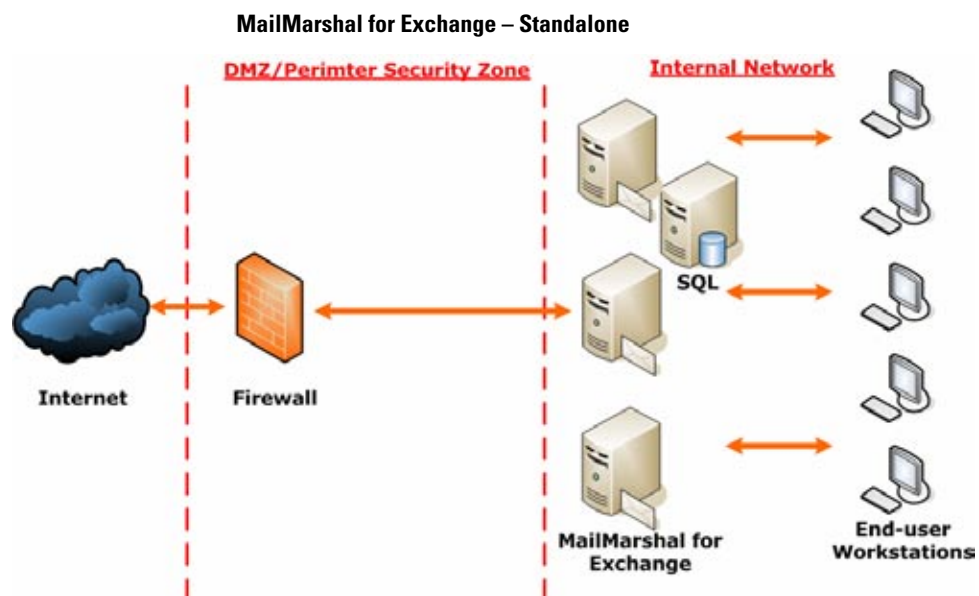
MailMarshal SMTP

- Receiver Rules
- Exchange Server Protection System
- Advanced Header Rewriting
- Gateway Email Encryption Potential
- ESMTP Support
- MAPS/RBL Support
- Close Active Directory Integration

MailMarshal for Exchange

- Internal Email scanning & reporting
- Close Active Directory Integration

WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments



Perimeter Security Benefits are absent

MailMarshal for Exchange

- Internal Email scanning & reporting
- Close Active Directory Integration

WHITEPAPER - MailMarshal Deployment Options for Exchange 2000/2003 Environments

Conclusion

Complete Email Content Security

MailMarshal for Exchange is an effective email content security solution that utilizes much of the award winning security technology present in MailMarshal SMTP. However, MailMarshal for Exchange has been engineered with different principals in mind.

MailMarshal SMTP is first and foremost a security tool and is ideally suited to perform security tasks. MailMarshal for Exchange has been developed to enhance MailMarshal's management capabilities.

At its core, MailMarshal for Exchange provides three very important benefits.

- 1) The ability to filter and report on all organizational email
- 2) The ability to directly utilize Exchange user accounts via Active Directory
- 3) The ability to provide inter-office email virus scanning between Exchange servers

When used to complement the gateway security benefits of MailMarshal SMTP, it provides a complete enforcement infrastructure for Acceptable Use Policy. When used without MailMarshal SMTP, it continues to provide a capable enforcement infrastructure, but lacks the ability to implement fundamental perimeter security principals to email content security.

The bottom line is that for organizations deploying a single Microsoft Exchange server, MailMarshal for Exchange may be adequate for your needs in a standalone configuration. However, for organizations that are more security conscious, receive volumes of Spam/viruses, or utilize multiple Exchange servers, then MailMarshal for Exchange may not fulfill all your needs if used standalone. The better option for these scenarios is the combined offering for complete email content security with MailMarshal SMTP and MailMarshal for Exchange.



Americas
Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404-564-5800
Fax: +1 404-564-5801

Email: americas.sales@marshal.com

Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

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

Email: emea.sales@marshal.com
info@marshal.com | www.marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com