

Email Content Security: Software or Appliance?

August, 2006

Contents

Introduction	2
Key Requirements for Gateway Email Content Security	2
Dispelling The Myths	3
Conclusion	6
Comparing MailMarshal and Appliances: Reference Chart	6

This whitepaper looks at the requirements for gateway email content security solutions, and explores popular claims about appliance solutions, examining the inherent weaknesses that are now becoming apparent to appliance customers. It also compares the strengths and weaknesses of appliances against Marshal's market-leading email content security software, MailMarshal SMTP 2006.

WHITEPAPER – Email Content Security: Software or Appliance?

Introduction

Corporate email is vulnerable. Vulnerable to attack from the increasingly sophisticated and ever-growing number of viruses, spam, spyware and phishing technologies out there. And vulnerable to abuse from within, which could result in: acceptable use policies being compromised; corporate governance and regulatory compliance violations; confidential corporate data being leaked externally.

A plethora of email content security technologies has emerged in recent years to address such vulnerabilities. Today, these technologies are considered essential elements of any business email and IT network environment and are commonly referred to as email content security gateways. Companies currently have the choice of two major types of email content security solution: software or appliances. Software solutions have been available for about ten years, while appliances appeared on the market approximately five years ago. Appliances are purpose-specific email content security servers, typically based on industry-standard server hardware and running a security-hardened Unix/Linux OS to provide the platform for the mail-screening software.

This whitepaper looks at the requirements for gateway email content security solutions, and explores popular claims about appliance solutions, examining the inherent weaknesses that are now becoming apparent to appliance customers. It also compares the strengths and weaknesses of appliances against Marshal's market-leading email content security software, MailMarshal SMTP 2006.

Key Requirements for Gateway Email Content Security

As a global technology solution provider in the Content Monitoring and Filtering Security industry with a comprehensive set of solutions for email and web content security, Marshal understands what enterprises are looking for in this area. There are several key requirements that enterprises look for when selecting an email content security solution. These are outlined below.

Best of Breed

A solution for email content security must be best-of-breed. This means that it must be among the top three products for repelling the security threats that are highest priority with a customer - whether that be spam, viruses or another aspect of content security. For example, most customers expect a best-of-breed anti-spam solution to be capable of detecting better than 95% of spam with barely any false-positives.

Low Total Cost of Ownership

To minimize costs associated with administering a solution, enterprise customers are looking for "plug and play", "set and forget" solutions that can be configured once and then operate automatically without the need for ongoing daily administration. For example, with anti-spam, IT administrators do not want to spend their time constantly releasing emails that have been incorrectly blocked or fine-tuning anti-spam settings to block the latest wave of spam. The solution must be easy to install, set-up, configure, and administer, too.

Flexible Deployment Options

Most enterprises go through the process of updating hardware once every three to five years. Often acquisitions or sudden bursts in email volume require investment in new servers, or re-allocation of existing hardware to different tasks. Most customers look for

WHITEPAPER – Email Content Security: Software or Appliance?

solutions that are flexible and transferable, can scale with the organization's needs and can work on the preferred hardware platform for the organization.

Flexibility also means the ability to work with other existing solutions such as other email servers, anti-virus products, email clients, databases and directories. Flexibility can also mean easy to deploy and administer over multiple sites. A lot of enterprise customers have offices in multiple cities and countries. These customers are looking for solutions that can be managed centrally and deployed easily in all of these locations.

Security policies also need to be flexible. The owners or senior managers of the business often want to be able to work with relatively open email privileges while knowing that staff in other roles are prevented from downloading executable files or sending MP3 files, for example. As a result, the solution must be able to enforce very complicated and granular policies defining who is allowed to do what.

Performance, Scalability and High Availability

Email is a business critical tool for most companies and as such, any email security solution must not become a bottleneck for email processing. Email scanning should be an essentially transparent process, with no perceivable delay in email performance. It should also be scalable, able to manage 10,000 users as easily as it can manage 100. Ideally it should be capable of clustering and load-balancing in an array environment. This is to not only provide high performance throughput scanning but also redundancy for reliable availability.

Return on Investment

An email content security solution needs to demonstrate a return on investment (ROI) as well as a low total cost of ownership. Ongoing maintenance costs need to be reasonable and fixed so that the business can move forward without fluctuating bills exceeding planned budget. It needs to provide reporting that identifies how and where the solution is being effective and saving the organization money, or helping the business to perform better. MailMarshal customers, for example, will see an ROI on their initial investment within the first year.

Dispelling The Myths

Since their inception, appliances have been touted by some as the holy grail of email content security, winning over many SMB and corporate customers in the process. Today, however, the tide is turning, as many appliance customers become disillusioned with the weaknesses and disadvantages inherent in some of these appliances. As is the case with email content software solutions, there is a wide range of appliance options available, ranging from low-cost, inflexible appliances to high-specification, yet very expensive, hardware complete with multiple processors and mirrored hard disks.

Plug and play?

The major selling point for appliances has always been based on the perception that they provided a 'plug and play', purpose built, email security hardware solution. The idea was that a company could order a pre-configured email scanning system that would simply plug into its email environment and instantly start cleaning spam and viruses from email.

In practice, appliances can be very difficult and time-consuming to install. It is not just a simple matter of plugging the appliance in and pointing your email server at it. The biggest selling appliance product in the market can take up to six hours to install, compared to between 1-2 hours for Marshal's MailMarshal software. Quite often, an appliance vendor-approved technician must perform the installation because it is so difficult, with customers

WHITEPAPER – Email Content Security: Software or Appliance?

having to pay extra for this service. By contrast, software such as MailMarshal can be installed by almost any IT person with a reasonable understanding of email configuration, MS Exchange and firewall administration.

Hardened operating system

Another perceived strength of appliances is that they often have a hardened operating system protecting the appliance from common vulnerability exploits. This is certainly a valid security practice. Most viruses and spyware in the wild are designed to exploit vulnerabilities in desktop versions of popular Windows operating systems. So, using another operating system theoretically makes you less susceptible to infection. However, there are still viruses in the wild for other operating systems such as Linux, which is popular with some of the appliance vendors.

More importantly, the argument for hardened operating systems is somewhat overblown. Microsoft provides exhaustive information on how you can lockdown and harden Windows operating systems on dedicated application servers for free and it is relatively easy to do.

Performance

Performance is often claimed as a strength by many appliance vendors on the basis that the hardware is dedicated to a specific task. Performance is really dependent on a range of factors such as processor speed, available memory, disc I/O, volumes of email and the type of email your business sends. Appliances are commonly marketed as suitable for “up to 1000 users,” based on a simple calculation of how much email the average person sends per hour and how much email the server can process. Often this calculation assumes that the average email size is less than 10Kb. In our experience most typical businesses average around 40Kb per email. As a result, a single appliance purchase really only supports 25% of its claim.

In order to actually process the true volume of email the business requires, companies often need to upgrade to a higher specification appliance, or purchase a second or more appliances. Usually, customers have already made a significant investment in the appliance hardware and are compelled to upgrade, again at significant additional cost and installation disruption.

In contrast, MailMarshal is hardware independent and widely regarded as the fastest email content security solution available on the market. Some appliance solutions on the market suffer from significant bottleneck issues because they are not multi-threaded. MailMarshal is multi-threaded and is able to scan emails 4 times faster than most other products. Often when MailMarshal is chosen to replace a competing email scanning solution, it achieves better results on just one server than the competitor was struggling with on four servers.

MailMarshal also has the ability to manage multiple email processing node servers in an array. This can greatly increase performance with load-balancing tools. One appliance vendor has a multi-server controller available which can allow you to link two appliances together and load balance them to share the task of processing large volumes of email. The downside is that you have to pay for this controller separately – yet another additional cost that most customers are unaware of when they make the initial decision to purchase an appliance. Conversely, MailMarshal provides its Array Manager for controlling multiple servers as a standard feature at no additional cost.

Obsolescence

But the biggest problem with appliances is obsolescence. Once you have purchased an appliance, the product is fixed and cannot be transferred to new hardware at a later date. The general consensus is that the viable life of such hardware is something like two to four

WHITEPAPER – Email Content Security: Software or Appliance?

years, depending on the requirements of your organization. With MailMarshal, you can move the software to upgraded hardware whenever you wish.

As mentioned above, appliances are inflexible, and unable to grow with the demands of an expanding business without additional significant investment. Often, new technologies become available which require higher specification hardware to operate. For example, consider you own an appliance and it is already operating at maximum capacity. The hardware may not have the capacity to support modular add-on features such as anti-spyware scanning, encryption, messaging scanning, image classification or new anti-spam technologies. This means you will have to upgrade your appliance to take advantage of new functionality that you wish to use.

Hardware failure

Appliances also have significant problems when there is a hardware failure on the appliance. Often a failure is severe enough to require a return to the manufacturer for repair. Some appliance vendors may provide a replacement appliance while the disabled appliance is being repaired (which may take a few weeks). However, replacement appliances can sometimes take several days to be delivered and installed, leaving your organization vulnerable for an extended period or potentially without email altogether.

Conversely, if you have a hardware failure with the server hosting MailMarshal (and assuming that you have not set MailMarshal up in a redundant array configuration) you can swap MailMarshal onto another box in less than two hours and be up and running again. You can also install MailMarshal on two (or more) standard, affordable PCs and have them running in a redundant, load-balanced configuration and have no downtime at all if one of them should happen to fail.

Redundancy

Redundancy can be another weakness of appliances. In general, there is no method of networking appliances into arrays or multi-server environments. Some appliance vendors do provide this functionality but at additional cost. MailMarshal is the only enterprise email content security solution on the market capable of managing hundreds of servers in redundant arrays, for no additional cost.

Ease-of-use

Ease-of-use is often claimed by appliance vendors. Some appliances can be easy to use, typically because they only have a limited number of features and functions and there is simply not much to configure. Other appliances can be very difficult and cumbersome to use. Some appliances have a particularly difficult user interface which is counter-intuitive and has required fields that unless you know the product intimately, have no meaning and require vendor help to proceed.

Interoperability

Interoperability can also be a problem with appliances. While some appliances have multiple options for anti-virus scanning, most only support one or two anti-virus vendors. By contrast, MailMarshal supports 10 different, leading anti-virus solutions as well as two popular anti-spyware vendors. MailMarshal also works with any SMTP email server on the market.

WHITEPAPER – Email Content Security: Software or Appliance?

Conclusion

In conclusion, the perception that appliances are the holy grail of email content security solutions is changing rapidly. Customers looking for easy-to-use, flexible, scalable and cost-effective email content security products with a good ROI are re-evaluating their choices and realizing that software solutions can often be a better bet for the long term.

Comparing MailMarshal and Appliances: Reference Chart

Requirement	MailMarshal	Appliances
Ease of Use	Excellent - one of the easiest to use. MailMarshal requires minimal training and has an intuitive, simple design. Rules are in plain English and easy to understand.	Varies – most are poorly designed and have overly complicated installation requirements.
Flexibility	Excellent - MailMarshal's depth of functionality, deployment options, interoperability with third-party technologies and powerful policy structure make it tough to beat in this area.	Poor – even the best designed and featured appliances are inflexible because of the hardware platform. They are not transferable. Most do not have the same depth of functionality or power for policy enforcement.
Cost Effective	Very Good - MailMarshal offers the best value and high ROI. Add-in perpetual software licensing, minimal training requirements and regular maintenance updates and MailMarshal is extremely cost effective.	Poor – Appliances can be extremely expensive and quickly become obsolete. They can offer high-spec hardware but often at a premium. They often need specialty installation. Hardware failures can be very expensive. Typically, purchasing a software solution and separate, off-the-shelf hardware will work out to be far more cost effective.
Depth of Functionality	Excellent – anti-spam, anti-attack, attachment blocking, keyword analysis, reporting, archiving, disclaimers, enterprise scalability and multi-server management all for one price. Optional anti-virus and other add-on modules make MailMarshal the best value email security solution available today.	Poor – some appliances offer good functionality but most are only available at additional cost or as subscription add-ons. Typically appliances only perform one or two functions or those functions are very expensive to add on. Typically very poor “bang for buck”.

WHITEPAPER – Email Content Security: Software or Appliance?

Requirement	MailMarshal	Appliances
Performance	Excellent – MailMarshal has a reputation as the fastest email scanning solution on the market. With an off-the-shelf Pentium 4 server, MailMarshal can support over 1,000 mail users on a single server. The advantage with MailMarshal is that you can apply whatever hardware you require for your needs – small or large.	Good – performance from appliances can be very good, but it costs. You need to purchase the vendor’s top specification hardware for high mail volumes and this can be very expensive.
Scalability	Excellent – MailMarshal can support multi-server environments easily and at no additional cost. MailMarshal’s purpose designed Array Manager makes it extremely scalable thanks to ease of management, configuration and reporting.	Poor – most appliances can only handle a set mail throughput. Going beyond this can be difficult and expensive. Some vendors offer multi-server management systems at additional cost and don’t forget you need to buy another appliance.
Redundancy	Excellent – as part of a multi-server environment Marshal can support arrays providing failover redundancy. MailMarshal servers can operate independently from the Array Manager for extended periods if there is a problem.	Fair – appliances that do support redundant server arrangements tend to have sound failover operations, such as connecting to backup databases automatically. However, there are few appliance vendors that provide this functionality.
Reporting	Excellent – MailMarshal provides numerous detailed reports, covering: policy violations, security incidents, mail usage statistics, problem users, bandwidth utilization, anti-spam effectiveness, viruses blocked and traffic patterns over time.	Fair – some appliances offer excellent reporting systems, but most appliances only monitor a small number of email characteristics and simply do not offer the depth of reporting available in MailMarshal.
Administration	Excellent – MailMarshal provides both an MMC administration interface and a web-based interface for remote administration. You can provide multiple levels of administrative logons so that some can only produce reports where others have full admin rights.	Fair – most appliances have fairly basic administration options provided through an HTML interface for remote access. Because these products tend to have fairly limited functionality, administration is quite simple.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, MARSHAL LIMITED PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Marshal, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Marshal. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data. This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Marshal may make improvements in or changes to the software described in this document at any time.

© 2006 Marshal Limited, all rights reserved.

U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the U.S. Government is subject to the terms of the Marshal standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

Marshal, MailMarshal, the Marshal logo, WebMarshal, Security Reporting Center and Firewall Suite are trademarks or registered trademarks of Marshal Limited or its subsidiaries in the United Kingdom and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.



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

Americas
Marshal Inc.
5909 Peachtree Dunwoody Road, NE,
Suite 770,
Atlanta,
GA 30328
USA

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

Email: americas.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