

# Email Content Security for Small and Medium Businesses

August, 2006

## Contents

Introduction	2
What Is MailMarshal?	2
Key Requirements for Small and Medium Businesses	2
Email Security – What Are My Options?	4
Strengths and Weaknesses Of The Three Email Security Options	5
Comparing MailMarshal And Other Options: Reference Chart	9
The Last Word	12

This whitepaper explores the full range of Email Content Security (ECS) systems that are available on the market today. It discusses some of the common requirements for ECS that small businesses often talk about. It examines what separates different ECS solutions, where the strengths and weaknesses are, what makes a good ECS solution and what makes a bad one. Lastly, this whitepaper benchmarks the Marshal ECS solution (MailMarshal SMTP) against these criteria for comparison.

### Introduction

Small and medium-sized businesses (SMB) have special needs when it comes to Information Technology. Large-scale businesses usually have large budgets and are happy to invest in the latest and greatest technology. Small businesses often wait until new technologies have been proven and become more mainstream. One such technology is Email Content Security (ECS). Issues such as spam, phishing and email compliance have raised the profile of ECS. ECS is a security technology that a lot of large businesses have utilized for many years; beginning with the need to control email viruses, then spam, and now adherence to email regulatory and internal Acceptable Use Policy compliance.

Today, ECS is considered an essential element of any business email environment, just as a firewall is considered an essential part of any sound IT security system. As a result a lot of SMB customers are now investing in ECS systems. However, unlike firewalls, where there is really only one general solution, there are many flavors of ECS. This has the effect of making life difficult for an SMB as there are a multitude of choices and wild variances in price and quality.

This is where this whitepaper can assist you as we explore the full range of ECS systems that are available on the market today. We will discuss some of the common requirements for ECS that small businesses often talk about. We will look at what separates different ECS solutions, where the strengths and weaknesses are, what makes a good ECS solution and what makes a bad one. Lastly, we will benchmark the Marshal ECS solution (MailMarshal) to these criteria for comparison.

### What Is MailMarshal?

MailMarshal is a total email content security solution for business networks, combining anti-spam, anti-virus and content security into a highly scalable and easily manageable solution. MailMarshal enables you to apply policies for security, compliance and acceptable use to email at your gateway – providing a safe and efficient working environment.

### Key Requirements for Small and Medium Businesses

Marshal began around 10 years ago with the first version of MailMarshal. MailMarshal was originally conceived and developed as a cost effective ECS solution for SMB. Today, MailMarshal is sold to Global Fortune 500 customers all over the world and protects over 7 million email users.

During the past 10 years, we have listened to literally thousands of different SMB customers talk about their requirements for ECS. What we have learned is that there are several common factors that almost all SMB organizations talk about.

### It Must be Easy to Use

SMBs typically do not have the resources or the expertise to manage complicated systems. There are often only one or two people in IT for the organization who are the “wearers of many hats”. These people will have to administer and configure email security while acting as the IT manager, purchaser, Help Desk and general “jack of all trades”. This means that any email security solution must be intuitive, easy to understand and simple to manage.

There is often a high turnover of staff in IT roles for SMB, therefore any email solution needs to be easy for the next incoming person to understand. Having to send new staff on expensive training courses is something that most SMBs seek to avoid. It also needs to be

## WHITEPAPER – Email Content Security for SMBs

easy for a new staff member to follow the policies and configurations that previous staff members have created.

### **Flexibility**

Small businesses often have to make resources stretch a long way. Servers or old PCs get reused for various tasks as email servers, database storage, web proxies, backup, etc. Any ECS solution should be flexible and deployable in a range of possible methods.

SMBs have sometimes formed through the merger of various smaller companies. They often have different IT systems, domains and requirements. It is difficult enough to merge disparate IT systems together and this can be even more complicated if offices are geographically separated. Routing email to different domains or cities is a common requirement.

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 general staff are adhering to Acceptable Use Policies. For example, users are prevented from downloading executable files, using offensive language or sending MP3s. As a result, the solution must be able to enforce surprisingly complicated policies defining who is allowed to do what.

### **Cost Effective**

When an SMB decides to purchase an email security solution, they want it to be at a fixed cost. They don't want to be surprised with additional or variable costs that they have not counted on. The solution needs to provide a rapid return on investment (ROI) with a low total cost of ownership. Ongoing update costs need to be reasonable and fixed so that the business can move forward without nasty surprises blowing their budget.

### **Bang for Buck**

Being cost-effective leads into another key requirement that we call "bang for buck". Essentially, this is the need to get the maximum out of your dollar. SMBs tend to be the most price-sensitive customers and, in a way, the most demanding. An email security solution needs to be able to perform a variety of functions – not just one or two. Ideally, it needs to provide anti-spam protection while integrating with the organization's preferred anti-virus scanner. It needs to be able to perform a range of keyword scanning tasks. It should be able to block a wide range of attachments and file types. It must provide a range of reports that add value. Ideally, it will perform other tasks such as adding email disclaimers, archiving email and run custom programs. It basically has to work like a utility pocket knife – SMBs want to buy one tool that has all of the features they could conceivably need.

### **Has to Deliver**

Above all, any email security system just simply has to work. It has to deliver what it says it can do on the box. SMBs are not interested in excuses or exceptions where the rules don't apply for them. If it says it can do something, SMB want to see it do it, and keep on doing it hassle-free.

## Email Security – What Are My Options?

For SMBs there are a wide range of options available for email content security. In some ways, there are too many options. It can be difficult for organizations that don't have a lot of time to research all the options available to them, to make the best informed decision.

Essentially there are three main categories of email security:

- Software Solutions (such as MailMarshal)
- Appliances
- Managed Services

Just to complicate things, within these three main categories, offerings from different vendors can vary tremendously. It is not like anti-virus vendors where the main differences are based on brand and reputation. In the email security arena the technologies, quality and performance of various offerings stretch the whole spectrum from very basic to incredibly comprehensive.

### Software Solutions

These are software applications that reside on PCs or servers within your organization. They are typically deployed at the email gateway to your business. There is a huge variety of options that range in price and functionality. Typically, these solutions are sold as perpetual software licenses, but there are some solutions where the basic application is free but you pay for the ongoing security updates (these tend to be focused on one or two issues such as spam and phishing). Software solutions are typically the most flexible, capable of being deployed on whatever hardware you wish to use. They also tend to be highly interoperable, designed to work with other applications such as virus scanners or email servers like Lotus Notes, Groupwise or Exchange. MailMarshal is a software-based solution.

### Appliances

These are task-specific servers that reside within your organization. As with the software solutions, they are best suited for use on the email gateway. They typically have proprietary operating systems and perform specific functions such as purely anti-virus scanning or anti-spam. Again, there is a range of options in both price and quality. It is possible to purchase very high-specification hardware, complete with multiple processors and mirrored hard disks, but these tend to be expensive. Appliances often have limited interoperability, only supporting one or two options for anti-virus scanning. They also tend to have heavy subscription models where you purchase the hardware platform and then pay annual fees for functionality.

### Managed Services

This is sometimes referred to as "mail-scrubbing". It essentially involves re-routing your email so that it goes to another company, where it is "cleaned" first, before it reaches you. Managed Service Providers (MSPs) typically have a range of price options including charging per email cleaned or for a set monthly fee per user. Policy options are fairly basic for simplicity. You also tend to pay for different types of "cleaning". You can pay a set fee for anti-virus and then pay an additional fee to add on anti-spam cleaning. This can be a good option for an SMB that has no IT staff at all (such as a car sales dealership or interior decorating business) and wants to "outsource" their email security.

## **Strengths and Weaknesses Of The Three Email Security Options**

Each of the three main options for email content security has strengths and weaknesses. Some of these issues are relevant for everyone and some will only affect SMBs that have specific requirements where one methodology may be better suited to service than the others.

### **Software Solutions – Strengths**

As mentioned above, software solutions are flexible. This is a key requirement for SMBs. You can deploy most software-based ECS solutions on almost any hardware you have available. Or, if you have a preferred hardware supplier, you can go with their hardware and reap the purchasing and support benefits you have with them.

Software solutions are also flexible because they often work with other software applications as discussed earlier. If you already have an anti-virus scanner, it may be quite cost-effective to license that anti-virus product for use on your email gateway, rather than having to buy an entirely different scanner.

Software solutions also tend to be very cost-effective. As mentioned previously, prices can vary a lot, but for the most part, they can be the best option for price vs. value. Often there are optional subscription modules that you can add on at a later stage. This can be a good option, allowing you the flexibility to put in place the security you need today, while future-proofing yourself against the threats you might want to deal with later. For example, put anti-spam and anti-virus in place now and add anti-spyware, encryption or image classification modules later.

### **Software Solutions – Weaknesses**

It really depends on the quality of the solution you choose. Some software solutions are dedicated to only one or two features whereas some others (like MailMarshal) offer a huge range of features – in which case it is a huge strength.

A commonly talked about weakness of software solutions is that they are designed to work on standard versions of operating systems and this makes them vulnerable to viruses and exploits. Unlike a home user's PC which is being used for various tasks and it is easy for someone to accidentally activate a virus, software solutions are usually performing a dedicated function and are not as susceptible to virus infection or exploits. They are also normally set up at the gateway in a DMZ (Dead Mans Zone) configuration outside the trusted network. This significantly reduces this potential weakness.

In MailMarshal's case, there is a separately available whitepaper on how to lock down the Windows operating system of the machine it is installed on and harden it against exploits\*. So, this really negates this perceived weakness.

### **Appliances – Strengths**

There are quite a few perceived strengths for appliances and this is why they have gained a measure of popularity with large enterprises in the last 3-4 years. However, this popularity has been largely based on some clever marketing by the appliance vendors who have pushed the weaknesses of software solutions and hyped-up the advantages of appliances.

One of these popular claims is around the subject of deployment. Appliances sell on the idea of "plug & play" installation, which basically means you set them up by plugging them into the wall and away you go. This is a great idea in concept as it minimizes the disruption of implementing an ECS solution and saves you time and effort getting up and running.

## WHITEPAPER – Email Content Security for SMBs

However, this plug & play idea is rarely the actual experience as most appliances require significant configuration and tuning before they are effective.

Appliance vendors have pointed at software-only solutions needing to be installed and set-up on hardware first whereas the appliances are all set up at the factory before they are shipped. For the most part, this is not realistic and depends entirely on the specific product being deployed and the preparation or skill of the person deploying it.

For example, almost anyone with a reasonable IT understanding can install and configure MailMarshal in less than an hour. It is simply a result of the work we have done to make this process as easy and painless as possible. On the other hand, the biggest selling appliance vendor routinely takes more than six hours to install and has to be installed by a qualified technician, so you have to pay the vendor to send someone out to set it up. This really turns the appliance “plug & play” claim into a negative if you compare it with MailMarshal.

Another perceived strength of appliances is they 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.

Performance is also a claimed strength by many appliance vendors. This is on the basis that the hardware is dedicated to a specific task and is therefore operating at maximum efficiency. However, performance is really dependant 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.

Most appliance vendors will scale an appliance on the basis that it is “suitable for up to 500 users”. This is founded on a simple calculation of how much email the average person sends per hour and how much email the server can process. Often the appliance vendors assume that the average email size is about 10Kb. In our experience most typical SMBs average around 40Kb per email. As a result, SMB who purchase an appliance that they are told can support 500 users actually only supports 25% of that claim.

Consequently, this leaves an SMB appliance customer in a difficult situation. In order to actually process the volume of email required the SMB needs to upgrade to a higher specification appliance, or purchase a second appliance. You can achieve good performance with appliances, but it can be a lot more expensive to do so with appliances than with some of the better software-based solutions. For the sake of comparison, MailMarshal outperforms the largest selling appliance vendor by around 400%.

The biggest selling 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 issue 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, load-balanced servers as a standard feature and at no additional cost.

### **Appliances – Weaknesses**

One of the biggest weaknesses with appliances is obsolescence. Once you have purchased an appliance the product is fixed and it is not transferable to new hardware. This means the viable life of the solution is restricted by the hardware (in the region of 2-4 years depending on the demands of your organization). With software solutions you can transfer the solution to upgraded hardware whenever you wish.

## WHITEPAPER – Email Content Security for SMBs

As mentioned above, appliances can be inflexible and unable to grow with the demands of an expanding business. 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 additional capacity required 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 may wish to use.

Some appliances can be quite simple to install and configure, but this is really up to the design of the software running on them. Other appliances can be very difficult and cumbersome to install and configure. Whether it is an appliance or a software-only solution, both are going to have some form of user interface. It is important to trial different solutions and gain an appreciation for what makes a product easy to use versus difficult and cumbersome. A number of appliances that we have seen, despite their relatively limited feature set, have poorly designed user interfaces and are surprisingly difficult to use.

Appliances can also have significant problems if there is a hardware failure on the appliance. If the failure is severe enough, it may require a return to the manufacturer for repair. Some of the appliance vendors will provide you with a replacement appliance while yours is repaired (which may take a few weeks). However, this replacement appliance can sometimes take several days to be delivered, leaving your organization vulnerable for an extended period or potentially without email altogether.

If a disk drive or cooling fan fails on the appliance it can be weeks before it can be shipped back to the factory and fixed, or replacement parts and a qualified service technician can be sent to repair the appliance. 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 2 hours and be up and running again. You can also install MailMarshal on two (or more) standard servers 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 can be another weakness of appliances. Many appliance vendors have no method of networking appliances into arrays or multi-server environments. Arrays provide you with the benefits of redundancy and typically load-balancing as well. Some appliance vendors do provide this functionality but at additional cost, so you need to make sure that you price this scenario correctly, if you are considering an appliance-based solution and also want a high-availability, redundant environment.

Interoperability can also be another problem with appliances. Again, some of the better appliance vendors will provide you with multiple options for anti-virus scanning. However, most only support one or two anti-virus vendors, again, you need to make sure you ask which scanners an appliance vendor supports.

### **Managed Services – Strengths**

The key strength with Managed Services is TCO, or Total Cost of Ownership. Total Cost of Ownership refers to what it costs your business to own and operate a particular product. In the case of software solutions and appliances, the TCO covers elements such as administration time, having to employ skilled IT staff, having to supply sufficient hardware to manage email volume, time and thought that goes into configuration, etc. With Managed Services the TCO is practically nil because you are outsourcing the need to filter email to a qualified and experienced third party. There are no hardware requirements, you don't have to administer the system, you don't have to employ knowledgeable staff to maintain the solution.

## WHITEPAPER – Email Content Security for SMBs

As mentioned above, Managed Services have a distinct advantage for SMBs that do not have the staff or resources in-house to maintain an email security solution. This can typically be small service businesses with 5-15 employees. Businesses like mechanics, painters, repair shops, car sales yards, and day-care centers typically don't have skilled IT staff employed or have high-scale IT infrastructure requirements. For these businesses, Managed Services offer convenience and solutions that might otherwise be difficult for them to attain.

### **Managed Services – Weaknesses**

There are several weaknesses with Managed Services and these may or may not be relevant for you, depending on the kind of business you operate.

The first issue, and potentially the biggest, is outsourcing your email environment. If you are a law firm or health clinic for example, this may be unacceptable for confidentiality and privacy reasons. Most Managed Service Providers (MSP) will have very strict customer privacy policies; however, email will still be passing through the MSP and will be observable to their technicians, so this is something to consider if your organization places a high value on confidentiality and privacy.

Cost is another issue with MSP. Over the long-term, software based solutions can be a lot more cost-effective, especially perpetually licensed systems. MSP costs can fluctuate and go up over time but with a perpetual software license you are not subject to the kinds of market cost fluctuations associated with service providers. Also, there will come a point where you have spent so much money on a managed service that you could have purchased a software license for the same money and not have any further ongoing costs. However, this weakness only makes sense if you have the staff and resources to manage your own email security in-house. If you do not have these resources, then this ongoing service cost is simply the price to be paid to attain some level of email content security.

Another weakness of Managed Services is visibility. Because you don't actually control your own email environment, you have little or no information on performance, delays, service outages, lost messages, non-deliveries, etc. For some SMBs, this is information that they don't really want anyway, but if you do wish to have some measure of control over your email environment, be sure to ask how this information can be reported.

Lastly, flexibility can be a problem with Managed Services. Typically there are set services or policies that you can subscribe to and either you can't deviate from these standard rules or it will cost extra to make changes. Some of the better service providers will actually provide you with your own login and a Web site where you can go and manage your own rules, release quarantined messages to yourself, etc. These services offer a good balance between outsourcing your email security, and retaining a measure of control over your own email.

## Comparing MailMarshal And Other Options: Reference Chart

<b>Requirement</b>	<b>MailMarshal</b>	<b>Software Solutions</b>	<b>Appliances</b>	<b>Managed Services</b>
<b>Ease of Use</b>	Excellent - one of the easiest to use. MailMarshal requires minimal training and has an intuitive, simple design.	Varies – most are poorly designed, difficult to configure and understand.	Varies – most are poorly designed and have overly complicated installation requirements.	Typically good – depending on the professionalism and responsiveness of the service provider, ease of use should not be applicable
<b>Flexibility</b>	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.	Varies – there are comparable solutions on offer, but few that can match MailMarshal for price. As for the others, they tend to have limited functionality and reduced policy options making them inferior.	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.	Poor – only the best MSPs offer a customer admin log-in for their services and then access to key features is typically restricted. A good option for those without the technical know-how or need to have flexibility.
<b>Cost-Effective</b>	Very Good - MailMarshal is not the lowest priced solution on the market, but it does offer excellent value and high ROI. Roll in perpetual software licensing, minimal training requirements and regular maintenance updates, and MailMarshal is extremely cost effective.	Good - Most software solutions provide good ROI and value for money. As with anything you get what you pay for. Spend more for better quality and bigger features. Spend less for what you need right now. Ensure that the solution is expandable and future-proof.	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.	Good – for organizations without IT staff or infrastructure, this can be the most cost-effective option. For SMBs that do have staff and resources, MSPs can be cost-effective in the short term but over time the ongoing costs make managed services less cost-effective than most software solutions.
<b>‘Bang for Buck’</b>	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 one of the best “bang for buck” offerings you can find.	Varies – lots of options and various levels of quality. The best alternative offerings are expensive, and features like archiving and multi-server management are optional extras at significant additional cost. Most software offerings only provide anti-spam or keyword analysis with no additional functionality.	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”.	Fair – some mail scrubbing services are restricted to anti-virus and anti-spam in which case you get what you sign up for. Others offer additional features like archiving and reporting. Again you get what you pay for.

## WHITEPAPER – Email Content Security for SMBs

<b>Requirement</b>	<b>MailMarshal</b>	<b>Software Solutions</b>	<b>Appliances</b>	<b>Managed Services</b>
<b>Has to Deliver</b>	Very Good – this really depends on your expectations. MailMarshal has been engineered for 10 years to make good on its promises. It is designed to be a product that you can set and forget with a minimum of fuss and ongoing administration. Over 90% of trial evaluations turn into customer purchases.	Varies – time and again we hear of customers who have bought a competing offering and want to try MailMarshal instead. Some products are very good and do deliver on their promises but many make claims that they simply can't back up – choose wisely.	Good – despite many of the faults we have outlined with appliances, they do tend to be focused products and most deliver what they were purchased to provide. The key is to try before you buy because it is a lot of money to spend on combined hardware and software that doesn't perform.	Fair – the thing with managed services is that so long as you don't tie yourself into a lengthy contract term you are free to discontinue the service and try another option if it doesn't perform. The issue is visibility into this non-performance. If the service is not delivering on its promises, how are you to know?
<b>Performance</b>	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.	Varies – we are unaware of any other software solution that can out-perform MailMarshal. In our own comparison testing, MailMarshal is 3 times as fast as its nearest competitor and as much as 10 times faster than the worst.	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.	Unknown – because the MSP has control of your mail system, how are you to know if it is performing slowly or delaying messages? Most MSPs provide good performance and service, but it can be very hard to tell the good and the bad apart, with no way to measure their performance.
<b>Scalability</b>	Excellent – although this tends to be less of an issue for SMBs, scalability can be important for some. 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 – only a handful of software vendors offer the kind of scalability available with MailMarshal. Most cannot support multiple servers. Those that can charge additional server licensing fees.	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.	Fair – MSPs tend to be able to support some larger environments in terms of mail volume. However, for most larger businesses, the advantages of the MSP start to evaporate. Coupled with a lack of policy flexibility and visibility into how the system is performing, managed services are not ideally scalable.

## WHITEPAPER – Email Content Security for SMBs

<b>Requirement</b>	<b>MailMarshal</b>	<b>Software Solutions</b>	<b>Appliances</b>	<b>Managed Services</b>
<b>Redundancy</b>	Excellent – as part of a multi-server environment, Marshal can support arrays providing failover redundancy. For some SMBs high availability can be a critical requirement. MailMarshal servers can operate independently from the Array Manager for extended periods if there is a problem. MailMarshal provides SMBs with real enterprise capabilities.	Poor – as mentioned above, most solutions do not support basic redundancy. Those that do have limited failover support, and cost even more for this level of support.	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.	Good – any MSP with a good reputation will provide redundancy and minimum service contracts. Be sure to check what levels of service downtime standards they stipulate in their contracts and be sure to read the fine print. Often, late night service outages are considered “scheduled maintenance”.
<b>Reporting</b>	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.	Good – most software solutions provide good reports. A few offer excellent reporting systems but most are relatively basic. This is a key area to examine when evaluating different solutions. Make sure that the solution provides the reporting measures that you require.	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.	Fair – some MSPs provide little or no reporting and these are providers that you want to steer clear of. Most reputable MSPs do provide good reports for those companies that don’t want a torrent of information. Typically the type of reporting information provided by MSPs is limited as they do not log everything about your email.
<b>Administration</b>	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.	Varies – as mentioned previously, you tend to get what you pay for. The better but more expensive software solutions offer good administration options and remote configuration	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.	NA – you pay someone else to administer your email security for you.

### **The Last Word**

During the course of this whitepaper we have examined some of the key aspects of email security and how it affects Small and Medium-Sized Businesses. We have highlighted some of the key requirements that (in our experience) are characteristic of SMB; and hopefully, we have described issues that are relevant to your business.

We have also established the main options available to you for email security and analyzed the strengths and weaknesses of those options. We have attempted to present a compelling case for MailMarshal as a solution to your email security needs while being well suited to your business environment.

From here we hope that you will visit [www.marshal.com](http://www.marshal.com) and accept our offer to evaluate MailMarshal SMTP for yourself. You can use MailMarshal for 30-days at no cost and no obligation. Or, please feel free to contact us to request a demonstration.

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](mailto: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](mailto:americas.sales@marshal.com)  
[www.marshal.com](http://www.marshal.com) | [info@marshal.com](mailto:info@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](mailto:apac.sales@marshal.com)