

Email Content Security: For Small & Medium Businesses

Contents

Introduction	2
What Is MailMarshal?	2
Key Requirements For Small And Medium Businesses	2
Email Content Security – What Are My Options?	4
Strengths And Weaknesses Of The Three Email Security Options	5
Comparison Chart - Mailmarshal And Competing Choices	11
The Last Word	14

WHITEPAPER - Email Content Security: For Small & Medium Businesses

INTRODUCTION

Small and medium-sized businesses (SMB) have special requirements when it comes to information technology. Large enterprises typically have substantial budgets to invest in the latest and greatest technologies. SMBs often have to wait until new technologies have been proven and become more mainstream and affordable. One such technology is Email Content Security. Issues such as spam, phishing and email compliance have raised the profile of email content security. Email content security is a security technology that many enterprises have utilized for a number of years, beginning with the need to control email viruses, then spam, and, now, adherence to email regulatory compliance and corporate Acceptable Use Policy policies.

Today, email content security is considered an essential element of any business email environment, just as firewalls are considered an essential part of any sound network security system. As a result, a great many small and medium-sized businesses are now investing in email content security solutions. Unlike firewalls which have one primary purpose (to act as gateway between the public and private network), email content security solutions today are required to perform multiple security functions. However, there are numerous vendors offering solutions for email content security. Unfortunately, there is significant variance in functionality, price and quality among these many solutions. This, in turn, has the effect of making life very difficult for an SMB searching for an appropriate email content security solution for their needs, as it is difficult to know what to look for and which vendors claims to trust.

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

WHAT IS MAILMARSHAL?

MailMarshal is a complete email content security solution for business networks, combining anti-spam, anti-virus and content security into a flexible 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. MailMarshal is available as an email gateway security software as well as an email gateway security appliance.

KEY REQUIREMENTS FOR SMALL AND MEDIUM BUSINESSES

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



WHITEPAPER - Email Content Security: For Small & Medium Businesses

During the past decade, we have listened to literally thousands of different SMB customers talk about their requirements for email content security. 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 in-house expertise or the desire to manage complicated IT systems. There are often only one or two people in IT who are the “wearers of many hats”. These individuals 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.

It is common to have a high turnover of staff in IT roles for SMBs; therefore, any email solution needs to be easy for the next incoming staff member to understand. Having to send new staff on expensive training courses is something that most SMBs seek to avoid. It also needs to be easy for a new staff member to follow the policies and configurations that previous staff members have created.

Flexibility

SMBs have to make resources stretch a long way. Servers or workstations get re-deployed for various tasks as email servers, database storage, web proxies, backup, etc. Any email content security solution should be flexible and deployable in a range of possible options.

SMBs have sometimes formed through the merger of various smaller companies. There are often 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, by preventing users 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 permitted to do what.

Cost Effective

When an SMB decides to purchase an email security solution, you want it to be at a fixed cost. You don't want to be surprised with additional or variable costs that you 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 unforeseen expenses 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 value out of your dollar. SMBs tend

WHITEPAPER - Email Content Security: For Small & Medium Businesses

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 you 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.

EMAIL CONTENT SECURITY – WHAT ARE MY OPTIONS?

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

Essentially there are three main categories of email security:

- Software Solutions
- 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. 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 with you paying 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.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

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 very expensive.

Appliances often have fixed functionality and interoperability, only supporting one option for anti-virus scanning, for example. This is because appliances come with all the software pre-installed and are designed to operate as a hardened platform where the function of the appliance is fixed. Appliances are designed to be less vulnerable to viruses and malicious code and therefore usually do not permit installation of new programs or removal of installed ones. Appliances tend to be popular with large enterprise customers because they are believed to be easier to deploy and manage. However, generally speaking, appliances are often the most expensive way to deploy an email content security solution. Some appliance vendors 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 normally fairly basic for the sake of simplicity for the MSP. 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 an 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 (software, appliances and managed services) has its 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 their needs.

Software Solutions – Strengths

As mentioned previously, software solutions are designed to be flexible. This links back to a key requirement for many SMBs. You can deploy most software-based email content security 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.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

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 pornographic image detection modules later.

Software Solutions – Weaknesses

Weaknesses in software solutions depend on the quality of the solution you choose. Some software solutions are dedicated to only one or two features and therefore their weakness is their limited functionality. Some others (like MailMarshal) offer a range of features, in which case it is a significant strength.

A key weakness in all email content security solutions (software, appliance and managed services) is around functional capability. Some vendors will claim a particular feature is available in their product, but often this feature is improperly or poorly executed. A good example of this is with a feature such as 'File Type Blocking'. It is common for vendors to claim this feature is present. However, upon investigation it is typical to discover that the method the product uses to identify the type is by the file extension (the three letter suffix at the end of the file name that denotes the file type and the application that should be used to open the file). This is a flawed method to identify a file type. A user can rename the file extension, changing an .MP3 extension to a .PDF extension for example, to fool the email content security solution and circumvent policies. It is also common for virus creators to use something called a double file extension such as "virusname.doc.exe". To a user and the email content security solution the file might appear to be a Word document but the computer may see it as an executable file and activate the virus.

As a result it is difficult to perceive all of the weaknesses that might be present in any email content security solution. SMBs should be cautious of accepting any vendor's claims of functionality and should ask for things like independent customer references and free trials to test the product before purchasing¹. Magazine product reviews should not be relied on as the sole source of information on a product, as the review is often cursory and does not explore the product in depth, or the review may be sponsored by the vendor which introduces bias into the review.

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 exploits². They are also normally set up at the gateway in a DMZ (De-Militarized-Zone) configuration outside the trusted network. This significantly reduces this potential weakness.

¹ Marshal offers a 30-day free trial period on all products and customer case studies are available from the Marshal website (www.marshal.com).

² For MailMarshal SMTP, a special whitepaper is available on how to lockdown the operating system of the computer it is installed on and harden it against exploits – this helps to negate this perceived weakness.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

Software solutions are also sometimes perceived to be difficult to install and setup. This is true in some cases where the software requires a significant amount of technical knowledge to deploy correctly. Some products have very simple and straightforward installation process, no more difficult than installing any other application³. So again, this perceived weakness is isolated to a subset of software solutions.

Appliances – Strengths

There are several perceived strengths for appliances and this is why they have gained a measure of popularity with large enterprises in the last 4-5 years. Generally speaking, the key strengths of appliances are ease of deployment, hardened operating platform and low administration overhead. However, as with the software solutions, some of these perceived strengths are based on vendor claims that do not always measure up under scrutiny. Thus, what may appear to be an advantage of an appliance solution can turn out to be a disadvantage in reality.

One of these popular claims is around the subjects of installation and deployment. Appliances offer the idea of “plug-n-play” installation which basically means you set them up by plugging them into the network and away you go. This is great in concept as it minimizes the disruption of implementing an email content security solution and saves you time and effort getting up and running. However, be wary of any vendor that makes this claim as it rarely reflects the reality. There will always be some measure of pre-installation planning and network configuration required⁴.

Where appliances do have an advantage in the deployment area is that they come on an optimized platform for their specific task. Having everything pre-installed and setup on an appliance means that the vendor can supply you with an indication of performance, so you can have an idea of how many users the appliance will support and how it will perform. From this perspective, appliances have an advantage over software as they have typically been tested and benchmarked on whatever the particular hardware specification is. However, this strength is more applicable for Enterprise customers and is typically less of a concern for SMBs.

Performance is another area that vendors will make claims that do not always measure up to reality. Real-world performance is 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. Use any performance figures that a vendor supplies and one that the vendor has possibly taken some liberties with as a guide.

For example, some appliance vendors will make a claim that their appliance is “suitable for up to 500 users”. This is based on a calculation of how much email the average person sends per hour and how much email the server can process. Often appliance vendors assume that the average email size is about 10Kb. In our

³ MailMarshal is renowned for its simple installation routine, which involves a guided ‘Wizard’ interface and a comprehensive set of pre-configured default policies built into the product

⁴ Depending on your environment, the MailMarshal e10000 appliance can be installed in your network and running in approximately 20 minutes. The pre-configured default policy in the product will immediately block any virus infected message or spam and will automatically begin reporting on any suspicious or unusual email activity.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

experience most typical SMBs average something more like 20Kb-40Kb per email. As a result, SMBs who purchase an appliance that claims to support 500 users may only adequately handle 50% of the volume.

Consequently, this leaves an SMB appliance customer in a difficult situation. In order to process the actual 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 more expensive to do so with an appliance than with a good software-based solution.

Another perceived strength of appliances is that 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. The main strength with hardened appliances is that the operating system is locked down so that unauthorized operations cannot easily occur.

Appliances – Weaknesses

Previously we have explored the perceived strengths of appliances. Often these strengths can turn out to be below expectation. The same can be said of weaknesses. Appliances have a number of weaknesses, but slowly these weaknesses are being addressed by the better appliance vendors. Not all of the weaknesses we are about to discuss hold true for every vendor.

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). Conversely, with software solutions you can transfer the solution to new hardware whenever you wish.

Newer, better appliances are now coming to market that take obsolescence into account. Obsolescence is not just affected by the technology, but also the way that the product is licensed. With some appliance vendors you pay a one-off price which includes the cost of the appliance and a maximum number of users licensed. These licenses are tied to the hardware and cannot be legally transferred, let alone technically transferred, to new hardware⁵.

An emerging trend designed to address the weakness of obsolescence is the idea of virtual appliances. The concept with a virtual appliance is that the appliance comes as a software image that can be run under a virtual server operating environment. This provides for the traditional cost advantages of installation, configuration and maintenance, but also makes the solution easily transferable to new hardware, thus mitigating the obsolescence argument. However, virtual appliances have not yet found mainstream acceptance and at this stage do not represent a viable choice for

⁵ MailMarshal appliance user licenses are transferable so you can move them to a new appliance or even an off-the-shelf server from another vendor at any time without penalty.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

the SMB market. This is an emerging technology so expect to see virtual appliances as a viable option within three years.

Appliances can also have 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 vendors will provide you with a replacement appliance while yours is repaired (which may take a few weeks). However, the replacement appliance can sometimes take several days to be delivered, leaving your organization vulnerable for an extended period or, potentially, without email altogether.

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 vendor solutions. You need to make sure you ask which scanners an appliance vendor supports⁶.

Managed Services – Strengths

The key strength with Managed Services is TCO, or Total Cost of Ownership. This 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, and more. With Managed Services the TCO is practically zero 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, and you don't have to employ knowledgeable staff to maintain the solution⁷.

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, 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.

⁶ The MailMarshal e10000 appliance comes with McAfee anti-virus pre-installed. As the appliance is locked down, you cannot use another brand of virus scanner with the appliance. However, the MailMarshal software option supports over a multiple major anti-virus brands, including McAfee, Symantec, Norman and Sophos, so you can use your scanner of choice.

⁷ MailMarshal is available in certain markets as a hosted email security service offering. Please contact Marshal for details of how you can receive MailMarshal email security as a hosted email security service in your region.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

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.

Therefore, this then becomes a matter of trust which you will have to consider, if your organization places a high value on confidentiality and privacy.

Cost is another issue with Managed Services. Over the long term, software and appliance-based solutions can be a lot more cost-effective, especially perpetually licensed solutions. MSP costs can fluctuate and go up over time, but with software or appliances you are not typically subject to the kinds of market cost fluctuations associated with service providers. Also, because of diminishing returns 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 the ongoing service cost is simply the price that you pay to attain a 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, and more. 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.

Last, 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.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

COMPARISON CHART - MAILMARSHAL AND COMPETING CHOICES

REQUIREMENT	MAILMARSHAL e10000 APPLIANCE & MAILMARSHAL SMTP SOFTWARE	COMPETING SOFTWARE	COMPETING APPLIANCES	MANAGED SERVICES
Ease of Use	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.	Good – depending on the professionalism and responsiveness of the service provider, ease of use should not be a problem
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. Note that the MailMarshal appliance only provides one AV option.	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 as MailMarshal.	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 for flexibility.
Cost-Effective	Very Good - MailMarshal is not the lowest priced solution on the market, but it does offer excellent value and high ROI with all of the security functions you could ever need. With perpetual software licensing, minimal training requirements and regular maintenance updates, 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.	Varies – 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.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

'Bang for Buck'	Excellent – anti-spam, anti-virus, 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.
Has to Deliver	Very Good – this really depends on your expectations. MailMarshal has been engineered for more than 10 years to make good on its promises. It is designed to be a product that you can setup 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. Ask for customer references, independent reviews and a free trial.	Good – despite many of the faults we have outlined with some appliance vendors, 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 if doesn't perform. Ask for references and a free trial.	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?
Performance	Excellent – MailMarshal has a reputation as the fastest email scanning solution on the market. MailMarshal can support over 1,000 mail users on a single Pentium 4 server. The MailMarshal e10000 appliance will support as many as 10,000 email users on a single appliance.	Varies – we are unaware of any other software solution that can out-perform MailMarshal. In our own comparison testing, MailMarshal is 3x 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 – investigate the level of visibility that the provider can give you into their service. 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.

WHITEPAPER - Email Content Security: For Small & Medium Businesses

<p>Scalability</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>
<p>Redundancy</p>	<p>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 enterprise-class capabilities.</p>	<p>Poor – as mentioned previously, most solutions do not support basic redundancy. Those that do have limited failover support, and cost even more for this level of support.</p>	<p>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.</p>	<p>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”.</p>
<p>Reporting</p>	<p>Very Good – 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.</p>	<p>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.</p>	<p>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.</p>	<p>Fair – some MSPs provide little or no reporting and these are providers that you want to avoid. 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.</p>

WHITEPAPER - Email Content Security: For Small & Medium Businesses

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.	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.
-----------------------	--	---	---	--

IN SUMMARY

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 SMBs; 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. Please keep in mind that MailMarshal is available as a software, appliance and managed service solution, so we do provide the choice of deployment platform that you prefer.

We hope that you will visit www.marshal.com and accept our offer to evaluate MailMarshal 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.



Distributed in the UK, Ireland and Channel Islands by Softek.
Tel: +44 (0)8456 443911 Fax: +44 (0)8456 443922
Email: sales@softek.co.uk Website: www.softek.co.uk



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 Rd
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