

The Advantages of a Hosted Messaging Security Solution

An Osterman Research White Paper
Prepared for Microsoft

April 2006

Microsoft®
**Exchange
Hosted Services**



Executive Summary

Messaging management is becoming more difficult. Business requirements are making messaging administrators push their messaging infrastructures to do more than ever before on many levels, including archiving messaging content for regulatory compliance, archiving to support legal discovery and for overall litigation support, providing services to a growing body of mobile users, ensuring business continuity by making email ever more reliable, and managing policies for message encryption.

At the same time, the problem caused by viruses, worms and spam continues to build. A signature-based approach to virus detection no longer provides adequate protection against this growing array of threats, which is driving the need for zero-day virus protection. Further, zombie networks are generating record levels of spam and viruses. Phishing poses a serious and growing threat to personal information and can lead to enormous financial losses.

Hosted solutions can elegantly address the growing array of messaging requirements and threats, and can do so without unnecessarily adding to the cost of current messaging management activities and the complexity of the IT environment.

Messaging Management is Getting Tougher

Messaging Management Before 2002

Prior to 2002, good messaging management consisted primarily of managing email servers well, deploying robust anti-virus defenses, regularly updating anti-virus signatures and making sure that servers ran as efficiently as possible. Viruses, with few exceptions, tended to propagate fairly slowly and good anti-virus defenses from well known vendors were typically adequate to address these threats. Spam existed, but was relatively uncommon and few defenses were even available to address the problem anyway. Phishing was virtually non-existent, as were many of the other problems that messaging managers currently face.

While there were certainly a variety of other messaging and network-related tasks that needed to be performed, messaging management – at least compared to the situation today – was a relatively simple task.

Hosted solutions can elegantly address the growing array of messaging requirements and threats, and can do so without unnecessarily adding to the cost of current messaging management activities and the complexity of the IT environment.

Messaging Management 2002 to the Present

Over the past several years, messaging management has become much more difficult for IT staff and users alike:

- In 2002, spam represented only one in every six messages – today, spam represents at least three out of every five messages sent across the Internet, although the increasing volume of spam is actually much worse than the percentage of email that is spam indicates.
- Phishing is a growing problem and represents a more sophisticated – and potentially more damaging – method of accessing funds from unsuspecting users.
- Zombies – networks of PCs that have been infected with a worm that can allow their control by remote parties – has become an enormous problem for both enterprise and home users.
- Threats sent through IM systems grew dramatically during 2005 and are continuing to become more numerous and more sophisticated. Complicating the problem for corporate IT staff is the significant and growing penetration of consumer IM clients in use in the enterprise which can bypass corporate defenses designed to protect against email threats.
- The vast majority of organizations conduct business transactions via email, including activities like sending and accepting proposals, placing orders and conducting other types of business. Because email is so critical to both enterprises and end users, maintaining extremely high levels of system uptime is critical. Downtime of even a few minutes in length can have very damaging impacts on an organization's business.
- Regulatory requirements for the retention, encryption and management of email are becoming more strict due to regulations like Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), various Securities and Exchange Commission rules and literally thousands of additional requirements.
- Legal discovery is becoming a more important issue as email is increasingly discoverable in legal actions, such as wrongful termination lawsuits, product liability cases and other actions.

Because email is so critical to both enterprises and end users, maintaining extremely high levels of system uptime is critical. Downtime of even a few minutes in length can have very damaging impacts on an organization's business.

- Content compliance is increasingly important, both in terms of managing content within a messaging system, as well as content that is sent outside of an organization through email. There are numerous cases in which organizations have lost legal judgments, lost intellectual property or incurred serious damage to their reputation because of their inability to adequately manage the flow of information leaving their email systems.

The current and future concerns that decision-makers have regarding the management of their messaging systems, derived from an Osterman Research survey conducted in 2005, is shown in the following table.

Current and Future Concerns With Key Messaging Management Issues

There are numerous cases in which organizations have lost legal judgments, lost intellectual property or incurred serious damage to their reputation because of their inability to adequately manage the flow of information leaving their email systems.

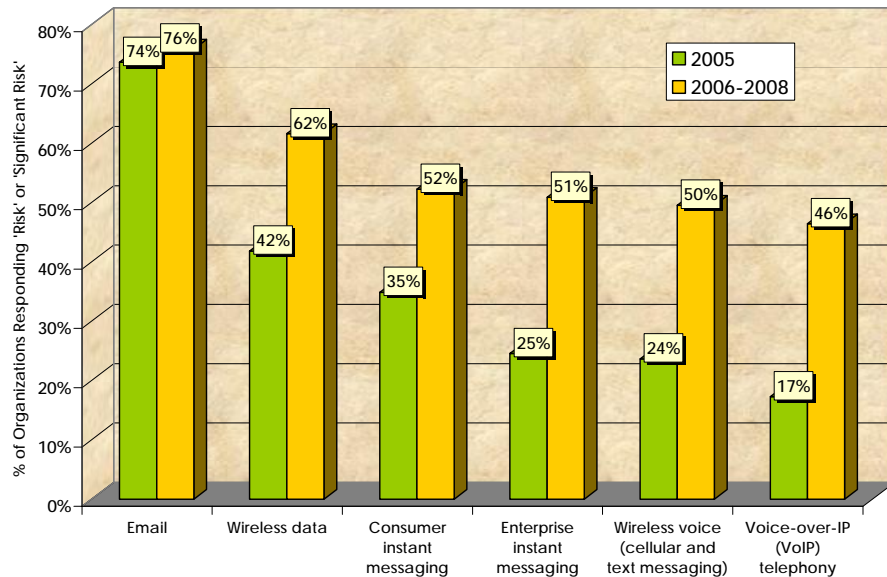
Issue	% Who Are or Will Be Concerned or Extremely Concerned During:	
	2005	2006-2008
Filtering email for spam and objectionable content (e.g., porn and inappropriate content)	74%	75%
Filtering content and attachments for malware (e.g., viruses, Trojan horses, worms, etc.)	88%	85%
Filtering outbound content and attachments for language that violates our acceptable use policies and poses a compliance risk	42%	61%
Providing security defenses for our email system (e.g., denial-of- service attacks, directory harvest attacks, application attacks, etc.)	81%	84%
Filtering content and attachments to identify sensitive language posing a compliance risk, and to route these messages for secure retrieval	40%	59%
Filtering both inbound and outbound emails and attachments for routing compliance language to an email archival system	35%	54%
Retention of email for risk management/in the event of a lawsuit	53%	71%
Managing email storage to improve system performance/reduce restore times, etc.	64%	73%

Messaging Management in the Future

As we look forward over the next several years, the problems described above will undoubtedly become more serious. The absolute volume of spam will continue to increase, placing additional burdens on messaging infrastructures. Phishing and related attacks will become more sophisticated, particularly as the growing influence of organized crime becomes more pronounced in these types of activities. The growth of IM in the workplace will prompt hackers and others to attempt to exploit this channel for their attacks. The risk that organizations perceive these threats to pose to various communications channels is shown in the following figure.

The absolute volume of spam will continue to increase, placing additional burdens on messaging infrastructures. Phishing and related attacks will become more sophisticated, particularly as the growing influence of organized crime becomes more pronounced in these types of activities. The growth of IM in the workplace will prompt hackers and others to attempt to exploit this channel for their attacks.

Perceived Level of Risk that Spam, Virus and Other Threats Pose to Various Communications Media



Business continuity will become even more critical than it is today as organizations of all sizes rely increasingly on email for business activities of all types. Regulators and the courts will increasingly turn their attention to email as a source of corporate records that must be retained and reviewed. Content compliance will become a more serious concern for business managers because of the rapidly growing use of email.

What Organizations Need to Do

The net impact of the problems described above will require organizations to have in place a variety of capabilities in order to adequately manage their messaging capabilities efficiently and effectively, including:

- Basic messaging security
 - Anti-virus, including zero-day threat protection
 - Anti-spam
 - Anti-phishing
 - IM security
- Content management
 - Email and IM archiving for compliance with regulatory and legal requirements
 - Outbound content compliance
 - Encryption
- Business continuity
 - Email and IM archiving for rapid and near real-time content recovery
 - Disaster recovery
- Storage management

It will be critical for organizations to maintain a growing array of capabilities in order to manage messaging systems effectively, to satisfy external requirements and to provide capabilities that will maximize user productivity.

Clearly, then, it will be critical for organizations to maintain a growing array of capabilities in order to manage messaging systems effectively, to satisfy external requirements and to provide capabilities that will maximize user productivity. However, adding these capabilities contributes to the complexity of managing a messaging system because of the interactions between various components and managing the vendors that provide these solutions. Further, all of these capabilities must be provided cost effectively with a minimal impact on IT staff requirements, since driving the cost out of messaging systems will become an increasingly important requirement.

Why Should You Consider Hosted Messaging?

Comparing Software-Based, Appliance and Hosted Models

There are a variety of methods for providing the messaging security and other capabilities described above: software-based systems, appliances and hosted offerings. A comparison of each model is discussed below:

- **Software-based systems**

The traditional model for the delivery of security and other capabilities, software installed on in-house servers provides the greatest degree of flexibility because an organization deploying these systems has a choice of server hardware platforms, operating systems and has a wide variety of available products from which to choose. This permits an organization to use best-of-breed products from a variety of vendors and also to employ unused server platforms, reducing the cost of deployment. Also, because this is the most well established delivery model, it is easy to find well qualified IT staff that are trained and proficient on most of the leading systems currently available in the market.

The disadvantage of the software-based approach is that it generally requires the greatest investment of time by IT staff to deploy and maintain, since both hardware and software must be installed, configured and updated by internal staff. Software-based systems expand the number of hardware platforms that IT staff must manage and can thereby create additional points of failure in the event of a power outage or other situation that can cause system downtime.

- **Appliances**

This model, which is increasingly popular with organizations large and small, combines hardware, operating system and software into a single, rack-mountable package that is generally very easy to deploy and manage. Appliances are often provided as 'plug-and-play' systems that can be easily configured. A growing number of vendors of software-based systems are now offering appliance-based versions of their tools, expanding the breadth of products available. Plus, because an appliance typically requires relatively little management, these tools often have a minimal impact on IT staff time to manage.

The disadvantage of an appliance is that it provides less

The disadvantage of the software-based approach is that it generally requires the greatest investment of time by IT staff to deploy and maintain, since both hardware and software must be installed, configured and updated by internal staff.

flexibility than software-based systems, since the organization deploying an appliance typically cannot choose the hardware platform or operating system used by the appliance vendor. Also, the appliance delivery model also does not allow an organization to deploy excess servers that might be unused and available as is the case with the software model.

- **Hosted offerings**
This model, in which capabilities are provided by a third party, requires that the MX record of an organization's domain be modified so that all messaging traffic is routed through the third party's data center. Traffic is then processed and delivered to the customer, typically with a minimal impact on message delivery speed. While the customer maintains its own messaging servers, all other capabilities are provided by the hosted provider. These capabilities are very easy to set up and modify, typically with not much more than a phone call.

A disadvantage of the hosted approach is that it can provide less flexibility than an on-premise system in terms of the choice of specific anti-virus, anti-spam or other offerings. Hosted solutions, in some cases, can also be more expensive to operate than some on-premise solutions, particularly for very large organizations that can effectively scale on-premise solutions to achieve a very low cost per user.

While there is a traditional resistance to hosted messaging from many IT departments, that resistance is clearly fading over time.

Views on Hosted Messaging

Osterman Research has been tracking the hosted messaging model for more than five years and has conducted extensive research on organizational attitudes toward this model during that period. While there is a traditional resistance to hosted messaging from many IT departments, that resistance is clearly fading over time. Consider the following:

- In a 2005 Osterman Research survey, 18% of organizations reported that they use a hosted service to provide anti-virus, anti-spam and related services. That figure is expected to increase to 24% in 2006 and to 31% in 2007.
- In the same survey, it was discovered that 57% of organizations are considering hosted services as a supplement to their internally managed solutions.

- While only 2% of organizations currently use any sort of hosted messaging archiving solution, 22% of respondents in a 2006 Osterman Research survey found that such a solution would be 'desirable' or 'very desirable'.

The Benefits of the Hosted Messaging Model

While all three of the approaches to messaging management described above have advantages and disadvantages, there are several factors that make the hosted model a very good fit for many organizations:

- Notwithstanding the ability of some very large organizations to achieve a low cost per user with on-premise solutions, hosted services often are less expensive than internally managed solutions since they require very little investment by IT staff to manage. For example, there is virtually no investment of time by IT staff to deploy these services and no investment to upgrade or otherwise maintain them, since the hosted provider manages all of these capabilities. This can result in reassigning IT staff to other initiatives that can provide more value to the organization.

Pricing for hosted messaging security services can often be competitive with the cost of providing these services internally and can often be lower.

Pricing for hosted messaging security services can often be competitive with the cost of providing these services internally and can often be lower. For example, Osterman Research found in a 2005 study that the cost of providing messaging security capabilities internally – including both labor and non-labor costs – is \$117 per user per year for organizations with up to 2,500 employees, and \$63 per user per year for larger organizations. Using the list prices from a major US hosted messaging security provider, the annual, per-user cost for a 2,000-user organization would be under \$56 to provide anti-virus, anti-spam, outbound content filtering and secure messaging functions. Even if we assume that one full-time IT staff member is required to manage these capabilities, the total annual cost per user is still under \$91 – 22% lower than for an internally managed solution.

Using list prices from the same provider for a 10,000-user organization, and assuming that two full-time IT staff members are required to manage these capabilities for this many users, the annual cost per user would be just under \$64 – almost identical to the annual cost of providing these services internally.

- Hosted solutions eliminate the cost of on-premise hardware and software, and almost all of the cost of IT staff time required to maintain defenses. Consequently, management of these defenses is much simpler than is typical with on-premise solutions.
- The hosted model offers the lowest impact on internal infrastructure, since viruses, worms, spam, archiving, etc. are managed by the hosted provider, not internally. This minimizes the internal impact on CPU cycles, storage and bandwidth. This can lead to lower costs, since internal capabilities do not need to be upgraded as often.
- Hosted solutions are characteristically very easy to implement. Once an MX record is modified so that all email is routed through the hosted provider's data center, various services can be turned on or off very easily with virtually no involvement by IT staff.
- A key advantage of the hosted model is that services are continually updated by dedicated staff, typically on a 24x7 basis. New virus signatures, new spam rules and other capabilities are typically updated by hosted providers very frequently. Hosted providers can also provide robust protection from directory harvest attacks which can account for up to one-half of all messaging server CPU cycles. This insulates internal messaging servers from the growing variety of external attacks directed against them.
- Related to the point above is the fact that hosted solutions provide excellent defenses against DNS lookups and related threats because the MX record points to the hosted provider, not the customer's domain. Customers can then lock down Port 25 so that they receive only SMTP traffic from the hosted provider, a source they can trust.
- Hosted providers can offer a variety of disaster recovery capabilities. For example, most hosted messaging security providers include as part of their service automatic spooling of messaging data in the event of a failure of their customers' primary messaging servers. If these servers go down for any reason, such as an electrical blackout or a hurricane, for example, emails are spooled for up to several days (or longer in some cases) until their customers' messaging servers are back online. Messages are then delivered in a flow-controlled

Hosted providers can also provide robust protection from directory harvest attacks which can account for up to one-half of all messaging server CPU cycles. This insulates internal messaging servers from the growing variety of external attacks directed against them.

fashion so as not to overload their customers' servers. The advantage is that even though a messaging system is unavailable, individuals can continue to send email to it without receiving bouncebacks.

Some hosted providers offer more sophisticated disaster recovery capabilities, such as alternate messaging systems using Webmail that allow users to access their email when the primary messaging system is down. These capabilities are useful during full-blown disasters, as well as during more common occurrences, such as when a messaging system needs to be taken down for maintenance or upgrades.

Understanding Return-on-Investment

There are three key points to consider when evaluating the return-on-investment (ROI) provided by a hosted solution versus an on-premise solution:

- Osterman Research has found that many organizations tend to underestimate the cost of providing messaging services internally. For example, as noted above, Osterman Research found in a 2005 survey that most decision-makers do not know the actual cost of providing messaging services in their organization. As a result, an internal evaluation of the cost of an internally managed solution versus a hosted one may not be accurate. In order to perform an adequate evaluation, therefore, it is critical to fully understand all of the costs of an internally managed solution so that an accurate assessment can be made.

In order to perform a thorough and accurate ROI analysis, it is important to identify all of the costs associated with operating a messaging system. These costs would include all of the labor required to manage, troubleshoot and maintain hardware and software platforms; the opportunity costs of labor, hardware and software used to manage messaging systems that might otherwise be repurposed for other initiatives that provide a greater competitive advantage for the organization; and the differential cost of downtime between in-house and externally managed services.

- A hosted solution can offer a faster return-on-investment than an internally managed one because there is typically little up-front cost associated with a hosted service.

Osterman Research has found that many organizations tend to underestimate the cost of providing messaging services internally. In order to perform a thorough and accurate ROI analysis, it is important to identify all of the costs associated with operating a messaging system.

- In performing an evaluation of the costs of an internally managed solution versus a hosted one, it is important to consider the opportunity cost of the former. Because messaging is a 'utility' – an indispensable component of an organization's infrastructure like electricity or water – it provides no competitive advantage to an organization, only a competitive disadvantage in its absence. Therefore, IT staff devoted to maintaining a messaging system, while providing a valuable service, are not performing work that provides a competitive advantage to the organization. Simply put, the use of a hosted provider can free these staff members for work that provides more value to the organization.

Because messaging is a 'utility' – an indispensable component of an organization's infrastructure like electricity or water – it provides no competitive advantage to an organization, only a competitive disadvantage in its absence.

Microsoft Exchange Hosted Services

Microsoft Exchange Hosted Services offer a cost-effective way for enterprises to actively ensure the security and availability of their messaging environment, while instilling confidence that their messaging processes satisfy internal policy and regulatory compliance requirements. A seamless extension of Microsoft Exchange that operates over the Internet as a service, the complete set of services includes hosted filtering for spam and virus protection; hosted archiving to satisfy compliance requirements and internal policies; hosted encryption to preserve email confidentiality; and, hosted continuity for ongoing access to messaging systems during and after disasters. Microsoft Exchange Hosted Services provide value to corporate customers by eliminating upfront capital investment, freeing up IT resources, and removing incoming email threats before they reach the corporate firewall. For more information, visit <http://www.microsoft.com/exchange/services>.

Conclusion

All messaging security delivery models – software-based, appliance and hosted services – have specific advantages and disadvantages. However, a hosted model can provide a variety of benefits to an organization, not the least of which is its ability to provide robust protection from a variety of threats, very easy management of a variety of capabilities, and the ability to free internal IT staff from spending time managing a system that does not provide a distinct competitive advantage to an organization. The table below summarizes the advantages of hosted services relative to on-premise solutions.

All messaging security delivery models – software-based, appliance and hosted services – have specific advantages and disadvantages. However, a hosted model can provide a variety of benefits to an organization.

Summary of Benefits for Hosted and On-Premise Solutions

Benefit	Hosted Service	On-Premise Solution
Automatic updates of virus definitions	YES	YES
Automatic updates of spam rules	YES	YES
Defense against large-scale zombie attacks	YES	POSSIBLE
Global, fault tolerant architecture	YES	POSSIBLE
Stops unwanted email from entering corporate network	YES	POSSIBLE
Predictable reoccurring costs	YES	POSSIBLE
Easily deployed	YES	POSSIBLE
Minimal training time for administrators	YES	POSSIBLE
Standard 24x7 platinum support	YES	POSSIBLE
Reduction in corporate bandwidth	YES	POSSIBLE
Reduction in complexity of IT environment	YES	NO
No software maintenance	YES	NO
No hardware maintenance	YES	NO
No server monitoring	YES	NO
No rack space required	YES	NO
Built-in disaster recovery capabilities	YES	NO

© 2006 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.