Securing the Messaging Infrastructure: Reduce Cost and Risk With a Comprehensive Strategy

an Osterman Research white paper
sponsored by

FaceTime™ BorderWare™

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 253 630 5928 • info@ostermanresearch.com • www.ostermanresearch.com

Why You Should Read This Report

Messaging – the infrastructure that supports email, instant messaging (IM) and voice-over-IP (VoIP) – has become the 'electricity' of the modern enterprise: messaging systems are critical to the success of virtually any mid-sized or large organization because their use is so pervasive and because users rely on them so heavily. Four out of five enterprises use email to finalize orders, accept proposals and conduct other types of transactions. Numerous studies have shown that employees would rather give up access to their telephone than give up access to their email. The use of IM in the enterprise – particularly consumer IM – for business communications is growing significantly. The typical user spends at least two hours each day interfacing with some aspect of a messaging system. In short, messaging has become as vital to the vast majority of enterprises as electricity.

Organizations are realizing that a message is a message, whether it is delivered through the email system, IM or some other transport mechanism.

Nonetheless, messaging does not truly provide a competitive advantage to an enterprise because virtually all enterprises use it as a critical part of their communications infrastructure. However, a messaging system that is less than 100% available or that allows threats to enter the network can provide a competitive *disadvantage* to an enterprise. Consequently, it is critical to protect messaging systems from the growing variety of threats and disruptions facing them.

In short, what is needed is a comprehensive vision of protecting the messaging infrastructure: the choice is either to deploy a growing array of point solutions from a variety of vendors to deal with each new threat as it arises, or deploy a comprehensive solution set that will address current and future messaging security needs. This white paper focuses on the case for the latter.

Messaging Systems Are Under Attack

The goal of a messaging system is to enable communications between multiple parties. A good messaging system does so efficiently and rapidly 24x7x365. However, this seemingly simple task has become much more difficult in recent years due to a variety of issues:

- **Spam**, which has grown from less than 20% of all email traffic in 2002 to as much as 90% of all email today, clogs corporate messaging servers and networks, reduces user productivity and delays message delivery.

- **Viruses, worms and Trojan Horses** – a perennial problem that continues to get worse. Messaging systems have proven to be a natural highway for malicious code. Although early worms were propagated primarily by email, in 2004, eight of the top 10 worms spread using a combination of distribution mechanisms including email, IM, P2P, network shares, exploit scanning and other mechanisms. Because of these "blended" malicious code attacks, just one user with an IM or P2P account can open the enterprise to a potentially devastating virus attack. Viruses spread by IM and P2P will not be detected by email and file server virus scanners and can potentially bypass desktop scanners as well.

- **Consumer instant messaging** (IM) systems bypass corporate messaging security defenses and provide an avenue through which malware and other threats can enter a network. Plus, consumer IM provides no enterprise control over naming conventions, nor do most of these systems natively log conversations for archival purposes.

Outbound content filtering is becoming increasingly important to prevent sensitive information from being distributed to unauthorized parties.

- Spam over IM, or **spIM**, is a growing problem in which IM clients are hijacked for purposes of distributing spam-like messages or malware.

- **Directory harvest attacks** (DHAs), in which spammers attempt to gather valid email addresses and buddy names, impose unnecessary loads on messaging systems. For example, DHAs account for about one-half of all email server processing cycles.

- **Denial-of-service attacks** can bring messaging systems and the network to a grinding halt.

- **Phishing** – apparently legitimate emails and IMs delivered en masse in an attempt to collect credit card numbers, bank account numbers and other personal information.

- **Peer-to-peer** (P2P) systems can introduce viruses and malware into an enterprise network and, as in the case of downloading illegal music, can expose an enterprise to enormous legal liability.

- The transfer of **confidential or inappropriate content** through a messaging system can expose an enterprise's sensitive data to unauthorized parties or create significant legal liabilities, as in the case of distributing offensive material through email. Further, outbound content filtering is becoming increasingly important to prevent sensitive information from being distributed to unauthorized parties.

- A variety of **government regulations** designed to protect personal information and ensure corporate accountability, such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley, are becoming more stringent with regard to content management.

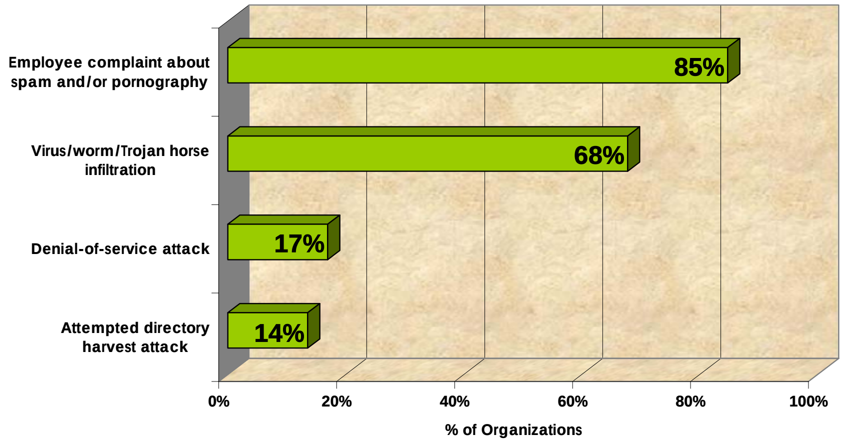
- A potentially enormous threat is posed by **Voice-over-IP** (VoIP) systems that replace traditional telephony. Free VoIP offerings, such as Skype, have quickly become enormously popular – with over 27 million accounts created in the past year alone. Skype bypasses traditional messaging controls, can be used for file transfers and uses an encrypted tunnel through HTTP traffic to pass through firewalls and other security mechanisms.

Messaging storage growth, large attachments and related problems are threatening messaging systems and increasing corporate liability.

As virtually any messaging manager will agree, these problems are getting worse and are making it more difficult and more expensive to manage the costs of messaging systems effectively and efficiently.

Illustrating the danger from the growing threats facing messaging systems is the following figure from an Osterman Research survey that shows the pervasiveness of various messaging system threats.

Enterprise Messaging Problems That Have Occurred in the Enterprise During the Past Month



Why are These Problems Getting Worse?

Messaging threats continue to worsen for a variety of reasons. Spam, for example, is an effective marketing technique because it is extremely inexpensive, because spammers can live with extremely low response rates and because many existing spam-filtering solutions are not able to keep up with spammers' efforts to circumvent these systems. DHAs are getting worse because many messaging systems are simply unable to detect or prevent these attacks as they occur. Viruses, worms and Trojan Horses continue to be a major problem because their creators are increasingly able to penetrate security systems and because of the large number of remote users who can introduce malware into a network.

In addition:

- The use of P2P and consumer IM systems in enterprise environments is growing and allowing users to share information that often is in violation of corporate policies.

- "Zero-day" exploits directed at all types of messaging applications permit hackers to respond with new vulnerabilities as soon as they become public, while enterprise administrators need time to assess the impact of a new patch on other systems in the existing environment and then deploy these patches. During the period between the exploit and the update, enterprise systems are particularly vulnerable.

- Zombie machines – worms spread by messaging systems can turn corporate or home machines into unwitting platforms for launching attacks or generating SPAM inside or outside the enterprise. Though the liability of hosting a zombie network has yet to be explored by the courts, the potential cost is enormous – as is the potential for lost productivity and lost bandwidth due to zombie-infected machines.

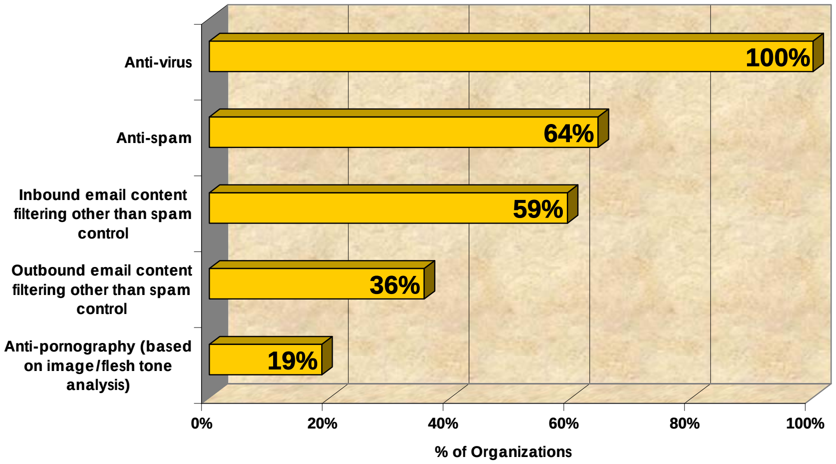
The myriad of threats to messaging – spam, viruses, DHAs, P2P, IM, VoIP exploits and other problems – are causing many enterprises to reassess their current email defense infrastructure.

It is important to note that IM is a threat to the enterprise only insofar as its use is not controlled and secured by the enterprise. IM has proven to be an extremely valuable business tool that is currently used by one in four email users. In fact, the primary application with which organizations want to integrate IM is email, meaning that enterprises must view email and IM as complementary and integrated business tools. However, the wide availability of free and easy-to-install consumer IM systems has created a situation in which security, user identities and IM conversation-archiving are outside the control of the IT department in most companies, making these systems potentially harmful to the enterprise.

What Can Enterprises Do?

To thwart messaging-related threats, virtually all enterprises have deployed point solutions to address the issues outlined above on an ad hoc basis. However, few enterprises have implemented comprehensive messaging security architecture. In addition, few enterprises have deployed any type of effective IM and P2P management or blocking solution and only about one-third of enterprises have deployed outbound content filtering systems. Finally, only one in five enterprises has deployed a pornography-blocking system, as shown in the following figure.

Deployment of Messaging Threat Tools in the Enterprise

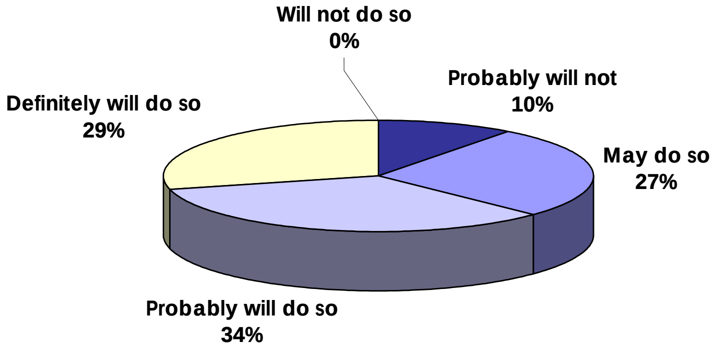


Messaging Defenses Must Be Integrated

Fundamentally, enterprises must realign their messaging security architecture from a collection of point solutions dealing with the growing number of threats to an integrated messaging solution that deals with all threats at the perimeter of the network. Realizing this, many enterprises are beginning to reassess their current messaging defense infrastructure. As shown in the following chart, nearly two-thirds of enterprises will probably or definitely reassess how they handle messaging-related threats at some point in the near future.

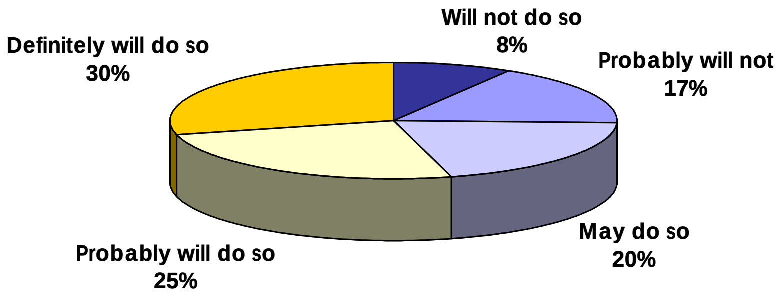
Increasingly, corporations are looking to implement a consistent set of tools and policies across messaging infrastructures – email, IM and VoIP.

Likelihood of Reassessing the Email Defense Infrastructure During the Next 12 Months



An even more difficult – and more expensive – option that will be undertaken by many enterprises will be to reassess the entire messaging infrastructure, which is being driven, at least in part, by messaging-related threats. As shown in the following figure, more than one-half of enterprises will probably or definitely undertake such a reassessment by the end of 2004.

Likelihood Reassessing the Entire Email Infrastructure During the Next 12 Months



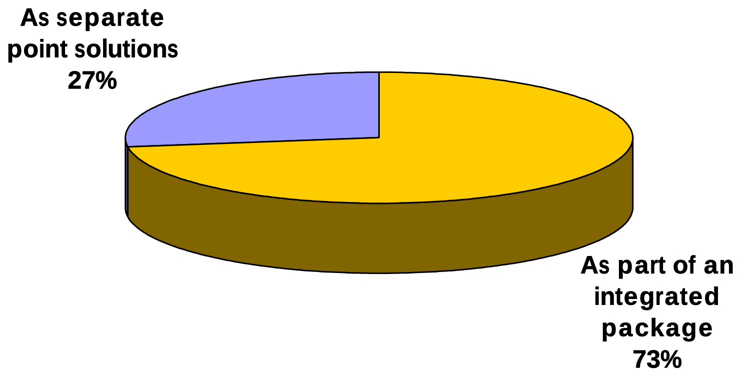
Reassessing either the entire messaging defense infrastructure or the entire messaging infrastructure itself are extremely complex options for enterprises to consider. However, the severity of the problems associated with messaging threats and other messaging-related problems is driving many enterprises to at least consider going through the reassessment process in order to make messaging secure and reliable, and to reduce the liability associated with these threats.

What Should Enterprises Do?

Most enterprises prefer solutions that are integrated into a single offering that will deal with spam, viruses, compliance and other threats and requirements for the messaging system.

Clearly, enterprises need a way to manage their messaging systems efficiently and to prevent threats from negatively impacting the messaging and network infrastructures. Wisely, most enterprises prefer solutions that are integrated and that will deal with multiple threats and requirements for the messaging system. As shown in the following figure, nearly three out of four enterprises prefer such an integrated offering over separate point solutions that deal with specific messaging-related threats.

Preference for Purchasing Messaging Threat Solutions



Messaging Defenses Must Be Integrated

There are a variety of messaging security protections that an integrated solution can provide:

- **Connection-level security** capabilities authenticate legitimate senders of email and IM.
- **Content-level security** capabilities analyze the content of incoming and outgoing messages to detect Spam, viruses, malware and other threats.
- **Intrusion prevention** capabilities protect a messaging system from hacking, denial-of-service attacks and related threats.

While all of these capabilities are critical to protect a messaging system, they must operate in a coordinated fashion. The majority of messaging security products available today do not provide the required level of integration and coordination.

Separate systems are more difficult to manage because they provide different interfaces that administrators and users must learn, they create the potential for 'finger-pointing' when one system fails, and they create additional points of failure.

There are numerous problems associated with managing a variety of point solutions to protect messaging systems from the problems identified above. First, separate systems are more difficult to manage because they provide different interfaces that administrators and users must learn, they create the potential for 'finger-pointing' when one system fails, and they create additional points of failure. Further, a comprehensive messaging security strategy can simplify the management and processing of all incoming and outgoing traffic according to a coordinated set of rules and policies.

What should such a comprehensive messaging security strategy deliver? There are five fundamental attributes that any enterprise system should possess if it is to effectively protect a messaging system:

1. **A message is a message**
   To be effective, a comprehensive messaging strategy must be able to secure email, instant messaging and P2P networks. There are nearly 40 different IM and P2P protocols – all of which should be blocked or managed.

2. **Messaging security**
   Any solution must provide comprehensive protection against viruses and other malware, and it must filter at least 95% of spam while generating virtually no false positives (i.e. legitimate emails that are mistakenly identified as spam).

   A messaging security solution must have the ability to block all files attached to messages, to provide an instant reponse to zero day attacks not yet detectable by anti-virus systems.

3. **Control**
   Any solution must allow administrators to control the messaging system in a centralized fashion so that all aspects of the messaging infrastructure – email, IM, VoIP, etc. – can be controlled in a coordinated fashion. In addition, because some content must be blocked, such as the vast majority of P2P traffic, administrators must have the ability to selectively see and block traffic across the enterprise.

4. **Compliance**
   Because enterprises must comply with a large and growing list of regulations for data retention, and because an increasing proportion of this data is transmitted by and stored in messaging systems, enterprises must ensure that their messaging systems are in compliance with all applicable international, federal, state and provincial laws with regard to data retention. Further, corporate policies regarding data retention and messaging system use, as well as support for legal discovery and other aspects of litigation, make compliance an increasingly important priority for enterprises.

5. **Continuity**
   No aspect of messaging security, control or compliance is meaningful if a messaging system is not available virtually 100% of the time. Therefore, any messaging management system must incorporate stateful failover and other mechanisms to ensure that all of the messaging system components operate on a 24x7 basis.

There are a number of questions that should be asked of potential vendors of integrated messaging security solutions in order to ensure that their solution can adequately protect an enterprise messaging system.

Questions to Ask Potential Vendors

There are a number of questions that should be asked of potential vendors of integrated messaging security solutions in order to ensure that their solution can adequately protect an enterprise messaging system:

- Is the solution cost effective in terms of the initial acquisition and deployment cost and will the solution result in an overall reduction of messaging system costs over the system's lifetime?

- Is the solution scalable to meet the most optimistic anticipated demands that will be placed on the system?

- Can the solution be deployed within the current messaging infrastructure or will significant changes need to be made to accommodate the new solution?

- Is the solution easy to deploy, configure and manage?

- How reliable is the system? Does the vendor guarantee a level of uptime that is consistent with the requirements of the enterprise?

- Does the system meet objective, industry standards and has the system been validated by third parties?

- How financially and otherwise viable is the vendor of the solution?

- Will the solution work with a comprehensive list of email, IM, P2P and VoIP protocols?

- Will the solution work even when the IM system employs an encrypted tunnel or a anonymous proxy to hide its activities?

- Can the solution be easily and automatically updated to support the latest protocols and threats?

What Are the Benefits?

This document has laid out the problems that enterprises face in their messaging systems and what they should do in response. But what are the benefits of deploying a comprehensive messaging security strategy that can deal with current and future messaging threats? There are a number of critical benefits that any enterprise can realize by taking a holistic approach to messaging security:

- **Greater end user productivity**
  Eliminating spam can significantly increase end user productivity by freeing users from the burden of filtering through unwanted content and minimizing the potential for losing valid emails in a sea of spam.

- **More efficient messaging system operation**
  Messaging security reduces email storage and bandwidth requirements and makes messaging servers operate more smoothly.

- **Better messaging system reliability**
  Eliminating messaging threats can significantly improve the reliability of messaging systems by eliminating denial-of-service, hacking, viruses and other threats that can cause a server to fail.

- **Reduced administration costs**
  A complete solution can reduce the number of adminstrators required to manage a messaging security solution, and it can allow an enterprise to postpone the addition of storage and bandwidth necessitated by increased messaging loads caused by spam and other unwanted content.

- **Better administration and management**
  A comprehensive solution for all messaging systems through a centralized control mechanism can make administration easier and more efficient.

An integrated solution can reduce the risk of being out of compliance with government regulations and being unable to satisfy corporate policies.

- **Reduced risk**
  A complete solution can reduce the risk of being out of compliance with government regulations and being unable to satisfy corporate policies.

- **Improved Corporate Visibility**
  By consolidating messaging security and generating detailed reports managers have greater visiblity and access to valuable data to take a proactive stance, identify issues before they impact the enterprise, and make informed budgetary decisions.

A Comprehensive Security Solution

FaceTime and BorderWare offer best-of-breed solutions that address messaging security requirements for email, IM, P2P, VoIP and other systems. These companies work together, both in the development of solutions that address messaging security concerns and through direct and reseller channels, to provide a comprehensive and integrated set of solutions that can address current and future messaging security requirements across the enterprise. Customers benefit by having access to a coordinated set of offerings to address management and security requirements for all corporate messaging--maximizing the integrity of the messaging infrastructure while minimizing the administration costs and policy management challenges associated with a disparate set of solutions.

FaceTime

Founded in 1998, FaceTime provides solutions that help companies secure, manage, and extend IM and P2P to protect technology and intellectual assets, comply with corporate and regulatory requirements, optimize business value from existing systems, increase productivity and lower costs.

FaceTime offers 'Defense-in-Depth' – a comprehensive strategy for end-to-end security, compliance and management of IM and P2P. This approach consists of two key components: RTG500™ in the DMZ to block unauthorized IM and P2P usage and protect against sophisticated workarounds and enforce compliant and authorized use; and IM Auditor™ in the LAN to enable user policy management, hygiene (anti-spIM, anti-virus), regulatory and corporate compliance, archiving and logging, and identity management.

FaceTime solutions help companies within industries such as financial services, life sciences, healthcare, energy, telecom and government address the unique IM security, management and compliance challenges within their organizations.

For more information visit http://www.facetime.com or call 1-888-349-FACE (3223).

BorderWare
Founded in 1994, BorderWare Technologies Inc. is the benchmark provider of messaging security solutions for enterprises and government. The company's flagship MXtreme Mail Firewall is the market leading appliance for securing an organization's email infrastructure. Similarly, BorderWare's SIPassure SIP Firewall delivers the benefits of Internet telephony by managing and protecting the flow of VoIP-specific SIP communications for enterprises and carriers.

BorderWare has more than 6000 customers with systems deployed at various military, intelligence, defense, national security agencies, and corporations worldwide. The company has developed affiliations and partnerships with some of the industry's most prominent companies in Internet infrastructure, security and messaging including Cisco Systems, F5 Networks, Sun Microsystems, FaceTime Communications, RSA Security, Research In Motion (RIM), Symantec and Kaspersky Labs. BorderWare is a private company headquartered in Toronto, Canada with offices in London, Frankfurt, Stockholm, Dubai, Ottawa, Dallas, San Jose, New York, and Washington DC.

For more information visit http://www.borderware.com or call 1-877-814-7900.

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.