



Messaging Security Market Trends, 2005-2008

Report Focus

This report provides an analysis of the desired and perceived customer requirements in the messaging security space. The goal of this report is to assist vendors and others to increase their understanding of market developments and to gain insight into key trends that will shape the messaging security market for the next several years. The primary data sources for this report were two surveys of North American organizations that Osterman Research conducted specifically for this report during May 2005.

Key Findings Presented in this Report

- The cost of providing messaging security capabilities is significant. Osterman Research estimates that the cost of providing these capabilities – including both labor and non-labor costs – is \$117 per user per year for organizations of up to 2,500 employees and \$63 per user per year for larger organizations.
- Almost all organizations have experienced a situation in which a virus, worm, Trojan or other form of malware has successfully penetrated a corporate network through email. Three out of ten organizations have had one or more email messages intercepted, while more than one in five have experienced the successful hacking of an application server.
- Consumer-grade IM client security and compliance are a greater concern for organizations than is security and compliance for corporate email/commercial email clients. IT decision makers increasingly have a greater awareness of the threat presented by consumer-grade IM clients.
- Organizations find security requirements increasing due to various compliance efforts and regulations, often with numerous regulations applying to enterprise systems.
- Organizations are finding that it is not enough to just scan inbound messages; they must now also scan outbound messages for things like content and confidentiality breaches. The same is true for IM as organizations are worried that IM gives staff another option to send out (accidentally or on purpose) corporate intellectual property, including files.
- Integrating security applications with hardened operating systems running on dedicated appliances is becoming more common. Less than one-half of the respondents noted deployment of gateway level systems for anti-virus and outbound content filtering. Almost one-half of the respondents noted that they would have no concern about deploying a messaging security appliance.



- The vast majority of organizations have either addressed the problem of adware/spyware in their networks or they have plans to address the problem during 2005. However, only about one-half of organizations have dealt with problems introduced by consumer IM clients or peer-to-peer file-sharing systems in their networks or have plans to do so during 2005.
- Nearly one-half of organizations are still using their first-generation anti-virus system, but two in five organizations is using their second generation anti-virus capability. More organizations are using a second or later generation anti-spam system than are using their first generation system.
- Many organizations are considering outsourcing their entire email and/or IM system requirements to hosted providers.
- The vast majority of organizations consider it important to establish a secure communications/encryption capability when sending email to business partners or members of their supply chain, when communicating with remote employees and when emailing to customers.
- Osterman Research asked decision-makers to rate a wide variety of messaging management problems in the context of how seriously they impact their organizations. Chief among these is the growth in email storage requirements, followed very closely by the amount of spam that organizations receive, inadequate email archiving, supporting remote users and malware.
- About one-third of smaller organizations and nearly one-half of larger ones are concerned or extremely concerned about their potential to leak sensitive information through messaging systems.
- Most IT organizations believe that C-level line-of-business managers should be more involved in managing policies for confidential information protection and regulatory compliance.
- When asked to rate the reasons for deploying a URL filtering solution, the reasons most often cited as important or very important are to block adware/spyware, sites that contain pornography and that sites that offer online gambling. Of least importance were issues like minimizing Web surfing for personal use and blocking personal Webmail.



Table of Contents

1. Executive Summary	1
2. Methodology and Overview	9
3. Key Messaging Security Issues	11
4. Anti-Virus and Anti-Spam Issues.....	23
5. Instant Messaging Security.....	27
6. Secure Messaging	35
7. Content Filtering, Compliance and Related Issues.....	39
8. Adware and Spyware.....	49
9. Messaging Security Delivery Models	55
10. Vendors of Messaging Security Solutions.....	61

List of Figures

Distribution of Industries Surveyed	9
Distribution of Messaging Systems in the Primary Survey Sample	10
Web Browsers in Use.....	10
Security Violations That Organizations Have Experienced	12
Concerns About Security and Compliance Issues.....	17
Perceived Legitimacy of Various Applications.....	19
Importance of Providing Hygiene, Content Inspection and Logging/Forensics to Maintain the Security and Compliance of Legitimate Applications	20
Annual Spending on Email Security per User (Out-of-Pocket Costs Only, Does Not Include Labor) ..	21
Importance of Zero-Hour Virus Protection	23
Sources That Organizations Would Consider for Purchasing Zero-Hour Virus Protection	24
Organizational Views on Whether or Not Zero-Hour Virus Protection Should be Integrated With Anti-Virus Systems	25
Changes in the Percentage of Spam Blocked by Anti-Spam Filters Over Time	26
Applications of Instant Messaging in the Workplace	27
Organizational Plans for Consumer and Enterprise Instant Messaging	28
Importance of Security in Motivating the Deployment of an Enterprise-Grade Instant Messaging Solution.....	29
Perceptions About the Requirements to Which Instant Messages are Subject	30
Importance of Instant Messaging Management Features.....	31



List of Figures (concluded)

Desirability of Different Deployment Options for Instant Messaging Management	31
Tools Used to Limit or Block Unwanted Instant Messaging Use	32
Tools Used to Limit or Block Peer-to-Peer File Sharing	33
Types of Communications for Which Organizations Perceive it is Important to Have Secure Messaging/Encryption	35
Secure Messaging/Encryption Methods Needed and/or Desired.....	36
Groups That Would Have Funding for Secure Messaging/Encryption Solutions.....	37
Groups to Which Organizations Would Deploy Secure Messaging/Encryption	38
Importance of Various Reasons for Deploying an Email Content Filtering Solution.....	39
Perceived Role of Content Filtering	40
“Should a separate best-of-breed content filtering tool be used for outbound compliance monitoring or should it be a function of an expanded incoming email filtering suite?”	41
“Is it important to perform an email monitoring assessment to determine what is happening in your email environment before implementing a content filtering tool?”	42
Desirability of Integrating Anti-Virus Capabilities into Content Filtering Tools.....	43
Need to Implement Company-Specific Policies for Compliance	43
Corporate or Regulatory Policies That Organizations Need to Enforce with a Content Filtering Solution.....	44
Organizational Concerns About the Leak of Sensitive Information.....	45
IT Agreement With Policy-Related Practices.....	46
Communications Applications/Protocols That Require Content Filtering for Compliance	47
Reasons for Deploying a URL Filtering Solution.....	48
Status of Outbound URL Filtering Today	48
Organizational Views on Adware/Spyware	49
Systems That Are Being Deployed Against Adware and Spyware	50
Reasons for Deploying an Intrusion-Protection Solution.....	51
Concerns About Managing External (Public) Webmail.....	52
Solutions Needed to Manage External (Public) Webmail	53
Current Practices and Preferences for Email Security Solutions	55
Desirability of Various Delivery Models for Email Security.....	56
Current Penetration of Managed Services.....	57
Perceptions About the Use of Managed Service Providers for Email Security.....	58
Likelihood of Using Managed Services During the Next 12 Months Among Organizations That Do Not Currently Use These Services	59



List of Tables

Leading Problems in Messaging Management.....	11
Messaging Security Systems That Have Been Deployed	14
Generations of Messaging Security Systems That Have Been Deployed Among Organizations That Have Deployed a System.....	15
Status of Addressing Various Messaging Security Problems	16
Annual Costs to Provide Email Security per User	21
Perceived Changes in the Performance of Anti-Spam Systems Over Time	26
What Organizations Plan to do About the Leakage of Sensitive Information Via Approved and Supported Applications and Communications Channels.....	45
Concerns About Appliance-Based Products for Messaging Security	60
Perceptions of Vendors in the Context of Whether or Not Potential Customers Would Consider Using Their Offerings	61
Perceptions of Leading Vendors in the Hygiene, Content Inspection And Logging/Forensics for Legitimate Applications.....	62
Leading Anti-Virus Products Deployed.....	62
Vendors of Email and IM Security Products and Services.....	63

About Osterman Research, Inc.

Osterman Research, Inc. provides market research, cost modeling, benchmarking and related services to vendors of technology-based products and services.

We help vendors, IT departments and other organizations make better decisions through the acquisition and application of relevant, accurate and timely data on markets, market trends, products and technologies. We also help vendors of technology-oriented products and services to understand the needs of their current and prospective customers.

Part of what makes us unique is our market research panel: a large and growing group of IT professionals and end-users around the world with whom we conduct our research surveys. This allows us to conduct surveys quickly and accurately.



Messaging Security Market Trends, 2005-2008
was published in July 2005 and is available for \$1,995



For more information on Osterman Research,
or if you have any questions about this
report, please contact us at:

Osterman Research, Inc.

P.O. Box 1058
Black Diamond, WA 98010-1058

Tel: +1 253 630 5839

Fax: +1 866 842 3274

Email: info@ostermanresearch.com

<http://www.ostermanresearch.com>

