

The Advantages of a Hosted Security Model

An Osterman Research White Paper

Published April 2008



Executive Summary

Security is an absolutely critical component for any organization's email or Web infrastructure. The growing volumes of spam, viruses, worms, Trojans, blended threats and other issues, coupled with more sophisticated attacks from spammers and others, necessitates that organizations have robust and adaptable defenses to protect their networks, users and data from a wide range of vulnerabilities. For example, spam represents about 90% of all email, and viruses are found in roughly one in 100 emails. However, because email use is growing at about 20% annually, volumes of spam, viruses and other malware are also increasing over time, requiring organizations to build their messaging security infrastructure in response to this growth.

Further, there has been an enormous increase in malicious Web-borne content, including email messages that contain links to dangerous Web sites, attachments that are little more than stage-one downloaders of other malicious code from the Web, malware that installs and opens a communication channel to the attacking source, and other exploits. Typically, these malware sites succeed in creating more zombie bots that keep feeding the vicious cycle of spam and viruses.

However, managing on-premise email and Web security capabilities is expensive and time-consuming. Organizations must spend a significant amount on hardware, software, training, maintenance contracts, etc. in order to build and maintain their defenses. Further, because the malware industry is making enormous amounts of money, this provides spammers, phishers and others with the resources they need to develop ever more sophisticated attacks and with greater volume. Organizations that do not adequately address messaging security problems face legal liabilities, financial risks, the potential for not being in compliance with statutory and legal requirements and other risks.

Organizations that do not adequately address messaging security problems face legal liabilities, financial risks, the potential for not being in compliance with statutory and legal requirements and other risks.

This white paper, sponsored by Websense, investigates how organizations today are responding to the new amount and the new types of email threats. The purpose of the survey is to assess actual costs of deploying a messaging security infrastructure on-premise vs. using a hosted deployment model. The goal was to determine actual cost differences between deployment models among varying sizes or organizations and network topologies, as well as gather real-world data for best practice recommendations.

Background and Methodology

Websense commissioned Osterman Research to conduct a worldwide survey of messaging decision makers in order to determine their costs of managing email security capabilities, their perceptions of the effectiveness of their on-premise infrastructure, and other issues. A total of 818 surveys were completed with small, mid-sized and large organizations in North America, Europe/Middle East/Africa (EMEA) and the Asia/Pacific (APAC) regions. The specifics of the survey were as follows:

- Online surveys were conducted during February and March 2008.
- 364 surveys were completed in North America, 239 in EMEA and 215 in APAC.
- The median number of employees in the organizations surveyed was 1,500.
- The median number of email users in the organizations surveyed was 1,275.
- All of the respondents were knowledgeable about their organization's messaging security infrastructure.

Key Findings from the Survey

The survey discussed above, which was conducted specifically for this white paper, provided a number of interesting insights into the way that messaging security systems are managed in organizations around the world. These findings show cost results for managing a messaging security solution on-premise; this whitepaper will discuss hosted messaging security further on.

- **On-premise infrastructure costs are significant**

The median number of users supported on anti-virus and anti-spam servers are 250 and 260, respectively. If we conservatively assume that the cost of the hardware and the security software totals \$5,000, then the cost of just the server itself will be roughly \$20 per user, or just under \$7 per user for the typical three-year life span of the typical messaging systems. Anti-virus and anti-spam appliances support slightly more users: the median values were 273 and 338, respectively. If we assume a \$4,000 appliance to support these median numbers of users, then the cost per user will be roughly \$14, or nearly \$5 per user per year.

The approximate cost to manage on-premise messaging security is roughly **\$136 to \$138 per user per year**, or more than **\$11 per user per month**.

However, it is important to note that growing volumes of spam, Web threats and malware will necessitate most organizations' deploying additional hardware during the three-year lifetime for most messaging infrastructure elements, roughly doubling the figures above.

- **IT labor costs for managing security are significant**

The mean number of email users that each security-oriented IT staff member can support is 875. If we assume that the fully burdened salary (salary, vacation, benefits, etc.) for an IT staff member is \$90,000, this translates into an annual IT labor cost of \$103 per email user.

Labor for managing a security infrastructure involves a number of tasks, including deploying hardware, software or appliances; making sure that everything is operating normally virtually 100% of time; deploying patches and upgrades; capacity planning to ensure that the infrastructure does not become overwhelmed as a result of spikes in the volume of spam; and a variety of other tasks.

Interestingly, our research found slightly higher numbers of users supported per IT staff member in North America than in EMEA or APAC, which we attribute to the greater maturity of the North American market, which has resulted in messaging security systems in use for a longer period of time and greater efficiencies for IT labor.

- **Non-labor expenses are also high**

Organizations spend a significant amount on non-labor related expenses for their messaging security infrastructure. For example, North American organizations spend a median of nearly \$28 per user annually on things like maintenance contracts, software renewals, new hardware, etc. Organizations in EMEA spend just over \$29 per user and those in APAC spend nearly \$19 per user.

Based on the costs discussed above, and assuming a three-year life cycle for messaging security infrastructure, the approximate cost to manage on-premise messaging security is roughly \$136 to \$138 per user per year, or more than \$11 per user per month.

- **IT staff members require significant amounts of training**

IT training requirements are substantial, requiring the average IT staff member to spend a median of 30 hours in training initially, followed by a median of 20 hours each year. Over a three-year period, assuming a fully burdened salary of \$90,000, this will translate to a cost of \$3,076 per IT staff member and nearly two weeks of training to learn and stay current on messaging security capabilities.

- **Bandwidth is significantly impacted by messaging traffic**

The mean bandwidth available in the organizations surveyed is 592 Mbit/sec, although bandwidth was highest among North American organizations at 734 Mbit/sec, followed by EMEA (534 Mbit/sec) and APAC (427 Mbit/sec). Not surprisingly, SMTP traffic consumes a significant share of the total bandwidth available, averaging 29% of the total.

This has significant implications on the total cost of ownership for on-premise

messaging security: given that the volumes of spam and malware are increasing, a greater proportion of existing bandwidth will be consumed by unwanted content, requiring organizations to deploy more bandwidth over time. Further, spam spikes can flood bandwidth for short periods, actually bringing down networks in some cases.

- **Confidence in on-premise messaging security is not high**

Many organizations do not have high confidence in the ability of their anti-spam and anti-virus capabilities. For example, 73% of organizations told us that they are confident or very confident in the ability of their anti-virus infrastructure to effectively block all viruses, worms, Trojans and other threats; only 61% of organizations were this confident in the ability of their anti-spam infrastructure to block all unwanted content. This means that a significant proportion of organizations are not confident in their current messaging security defenses.

This data underscores organizations' significant perceived and actual vulnerability to a wide variety of threats, and indicates that organizations are not as well protected as they need to be.

- **What about hosted solutions?**

Most organizations have not yet considered migrating to a hosted email security solution. Many organizations often underestimate the cost of managing their on-premise infrastructure, and so assume that it is always less expensive to manage messaging security in-house; or they do not understand the high level of security provided by hosted providers relative to in-house management.

That said, Osterman Research has found that the decision makers are increasingly open to the idea of hosting critical applications like messaging security and other critical applications.

Many organizations do not have high confidence in the ability of their anti-spam and anti-virus capabilities.

That said, most decision makers do believe that hosted messaging security offerings can provide a number of advantages, including reduced costs for IT labor and upgrades, improvements in the capture rates for spam, viruses and other threats, and greater organizational flexibility.

- **Consolidating on one vendor is perceived to be advantageous**

Roughly one-half of organizational decision makers believe that it would be valuable or very valuable to consolidate Web security, data security, email security and related capabilities through a single vendor. Interestingly, only one in six organizations perceived that such consolidation would provide no value to them.

The Advantages of the Hosted Security Model

Hosted email and Web security can offer a number of advantages for organizations of all sizes, including reduced cost of ownership compared to on-premise solutions, easier management of security capabilities, and the highest level of protection from threats possible.

REDUCING TCO

Many decision makers believe that managing email and Web security internally is less expensive than using hosted services to provide these capabilities. While for large organizations (1,500+ seats) that perception might be accurate, very often it is not. For example, many decision makers often do not consider the complete cost of providing email, security and other functions to their employees. They often underestimate the total amount of labor required to manage the system, the disruptive nature of outages and other unforeseen events on other IT activities, the true and complete costs of capital expenditures, the unanticipated costs of managing a system internally, the power and cooling requirements necessary to manage on-premise hardware, and so forth.

Further, most decision makers simply do not know the true cost of providing email and other services. For example, a 2007 Osterman Research survey asked messaging decision makers how closely they tracked the cost of providing messaging services to their users. The survey found that 8% of those surveyed knew exactly what these costs were, while another 25% could estimate them to plus or minus 10% of the actual cost. That means that two-thirds of messaging decision makers do not know the true cost of providing messaging services in their organizations.

Because many decision makers underestimate the full cost impact of managing an on-premise infrastructure, and because most cannot accurately calculate the cost of deploying and managing it, many do not realize that it is often less expensive to outsource email security capabilities to a third party provider. This is true for the “hard” costs – those for which the organization will incur a direct expense – as well as for opportunity costs. Regarding the latter, because a hosted provider can free IT staff for other work, the use of a hosted service can allow IT staff to generate much more value for their organization by enabling business than if the email security infrastructure is managed internally.

REDUCING COMPLEXITY AND UNCERTAINTY

Email security is complex and becoming more so. New threats, coupled with the growing volumes of these threats and spikes in malware traffic can create a number of problems. For organizations that operate their own security infrastructure, the result can be a saturation of internal capabilities or the compromise of these systems resulting in degraded performance or an outright crash of the internal network. For example, the enormous increase in the volume of spam between May and November 2006 driven by botnets and the use of image spam resulted in many on-premise solutions reaching their maximum capacity. IT staff in many organizations had to scramble to add new servers or appliances and to address the problems caused by the unforeseen explosion in spam.

A hosted solution, on the other hand, can dramatically reduce the complexity and uncertainty associated with new threats or growing volumes of spam, spyware, etc. Because hosted providers bear the brunt of these problems and have a more robust set of capabilities than most organizations could afford to deploy, their customers are insulated from the growing array of problems launched against them.

PROVIDING THE MAXIMUM LEVEL OF PROTECTION

Hosted security providers typically update their capabilities on a near real-time basis. For example, a provider of hosted anti-virus and anti-spam filtering services will typically update its signatures continually, they often have access to the newest threat signatures before they are released to the public, and they have access to information about new threats as they develop. Further, hosted providers typically deploy a broader range of threat-protection technologies and offer expertise that might not otherwise be available or affordable to their customers, particularly their smaller customers.

Further, leading hosted providers will use multiple anti-virus scanners, URL filters to detect phishing attacks, reputation analysis capabilities to determine how likely it is that an IP address is the source of valid or suspect content, and they will analyze global traffic patterns in real-time. These are all capabilities that most organizations – particularly smaller ones – simply cannot afford to deploy and manage in-house.

Most decision makers simply do not know the true cost of providing email and other services – Osterman Research has found that two-thirds of messaging decision makers do not know the true cost of providing messaging services in their organizations.

Also, hosted providers can typically invest more resources into their infrastructure than individual organizations can afford and so can provide extremely high levels of reliability. Because most hosted providers maintain very robust data centers, they can typically offer very high levels of reliability and Service Level Agreements (SLAs) that would be difficult for internally managed systems to match. This allows customers to focus on providing services that offer greater value to their enterprise with the assurance that messaging functionality will be available as close to 100% of the time as possible. It is also important to note that hosted providers' data centers are staffed on a 24x7 basis and that capabilities are monitored continuously, with SLAs around uptime as well as levels of security. This means that problems can be dealt with more rapidly than would be possible for most organizations that operate their own security infrastructure.

Through 2009, Osterman Research forecasts that organizations are planning to deploy a greater proportion of their messaging capabilities using hosted services, as shown in the

following table. While some hosted services will see only flat to modest growth, messaging security will see substantial growth over the next several years.

Percentage of Organizations That Will be Using a Hosted or Managed Solution

Messaging Function	2007	2008	2009
Anti-virus and anti-spam	22%	29%	32%
Hosted and managed email services	13%	14%	19%
Email retention and archiving	14%	24%	31%
Wireless/mobility services	21%	21%	27%

OTHER ADVANTAGES OF THE HOSTED MODEL

Hosted email and Web security offers other advantages, as well:

- The internal network bandwidth required when using a hosted provider can often be significantly less than for an on-premise infrastructure because so much less content is delivered to the internal network after being filtered for spam and other malware. This means that bandwidth upgrades can be postponed, resulting in significant cost savings.

- Most of the leading providers of hosted security services maintain very secure physical facilities, operating video surveillance, multiple access points using two-factor authentication, tracking and monitoring tools and other systems that protect their customers' data from being compromised. Look for providers that have been certified to third party standards such as ISO 27001.

The internal network bandwidth required when using a hosted provider can often be significantly less than for an on-premise infrastructure.

- Using a hosted or managed service provider can make a customer of the service less dependent on a particular vendor's technology, and so will minimize the impact of legacy systems on future technology or vendor choices.
- Hosted providers typically have much more excess mail capacity than an organization that manages its own on-premise email infrastructure. This is simply because it is not economically feasible for organizations to deploy enough excess capacity to maintain operation in the event of a crippling, large-scale spam attack, for example.

IS HOSTED EMAIL SECURITY JUST FOR SMBs?

There is a widely held perception that hosted security providers can offer cost and technical advantages for small organizations that might not have the resources to provide their own, on-premise capabilities; but that it is cheaper and more effective for large organizations to deploy their own security capabilities. However, Osterman Research has

found that even very large organizations can realize cost and technical benefits from the use of hosted security providers.

The Advantages of a Single-Source Security Model

Several years ago, protecting an organization's network against the comparatively small number of threats from notoriety-seeking writers of viruses and worms, and from the small amount of spam sent across the Internet, was fairly easy. However, the growing variety of threats, their rapidly increasing volume and the variety of problems that can impact an organization today mean that a wide variety of capabilities must be deployed in even small organizations. These capabilities include those that protect an organization from viruses, worms, Trojans, spyware, text-based spam, image spam, PDF spam, malicious Web sites and a host of other problems.

There are a growing number of vendors that offer specialized capabilities designed to filter and remediate some of these problems, and a handful of vendors that offer holistic solutions designed to address all of them.

Osterman Research believes that it is increasingly a best practice to implement solutions that can address the entire range of email, Web and other threats that can impact corporate networks. Reasons for this include:

- Point solutions from a variety of vendors require more investments of IT staff time than holistic solutions from a single vendor that can be managed from a centralized interface. Managing a collection of point solutions drives up the cost of IT management, sometimes dramatically.
- Each vendor will have its own upgrade and patch management cycles, again resulting in more IT time investments to upgrade each point solution, and resulting in potential incompatibilities between them.
- Deploying a number of point solutions from different vendors will, in most cases, be more expensive than deploying a single vendor's solution with the same number of capabilities.

IT staff time can be minimized and overall costs reduced in most cases by selecting a single vendor to provide all of the necessary security capabilities to protect an organization against email and Web-based threats.

- Managing relationships with several vendors is more difficult and time-consuming for IT decision makers, purchasing, finance and others than managing a relationship with just a single vendor.

In short, staff time can be minimized and overall costs reduced in most cases by selecting a single vendor to provide all of the necessary security capabilities to protect an organization against email and Web-based threats.

Summary

Hosted security is now a viable solution for organizations of all sizes and is increasingly deployed to ensure better security and reduced costs. A hosted solution offers a number of important benefits, not least of which is the ability for customers to leverage an infrastructure designed to provide very high throughput and to protect against the greatest possible number of threats – duplicating the infrastructure available from a hosted provider would simply not be affordable for most organizations. This can result in lower costs for many organizations, as shown in the following table.

On-Premise Costs of Managing a Messaging Security Infrastructure Over Three-Years
(Based on Data Obtained in the Survey)

Cost Component	ON PREMISE		HOSTED	
	Cost per User	Total Three-Year Cost per User	Cost per User	Total Three-Year Cost per User
Labor 875 users per FTE admin Annual fully burdened labor/admin: \$90,000 5% annual wage growth	\$102.86 (per year)	\$324.27	\$4.73 (per year)	\$14.19
Anti-virus servers/appliances 250 users per server/appliance Cost of appliance: \$5,000	\$20.00 (initially)	\$6.67	\$0	\$0
Anti-spam servers/appliances 250 users per server/appliance Cost of appliance: \$5,000	\$19.23 (initially)	\$6.41	\$0	\$0
Bandwidth devoted to messaging \$3,000 per month/1,000 users 20% devoted to messaging traffic 90% of messaging traffic is spam/malware	\$0.54 (per month)	\$19.44	\$0.06 (per month)	\$2.16
TOTAL THREE-YEAR COST		\$356.79		\$16.35
AVERAGE COST PER YEAR		\$118.93		\$5.45
AVERAGE COST PER MONTH		\$9.91		\$0.45

Note: License and subscription fees are not included in these figures.

Further, integrated solutions that provide both hosted Web security and email security can ensure that organizations have the best protection against the rapidly changing threats that are spreading across these two most widely used communications channels.

About Websense

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, messaging and data protection technologies, provides Essential Information Protection(TM) for more than 42 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and messaging security policies. For more information, visit www.websense.com.

© 2008 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 or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.