

# Why You Should Consider Hosted Messaging Security

**An Osterman Research White Paper**  
*Published February 2009*

**SPONSORED BY**



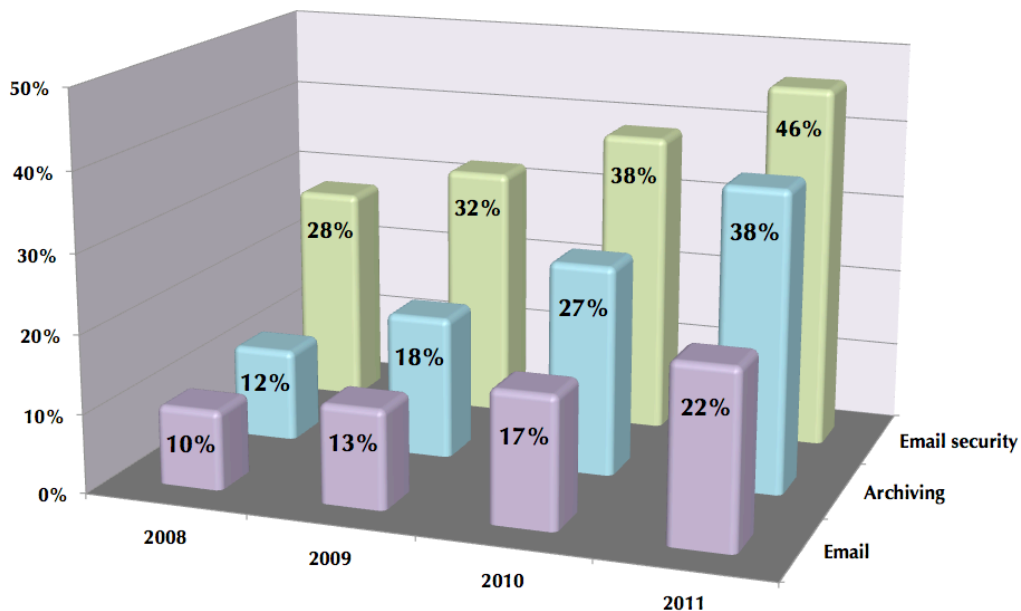
## Save Costs While Improving Email Security

Hosted, or “in-the-cloud”, messaging security capabilities are becoming increasingly popular with organizations of all sizes. Some have already adopted hosted services, while others are becoming more receptive to the notion of using third party services to manage their security infrastructure than they were just a year ago. Particularly driven by the current economic recession, decision makers are realizing that hosted email security can provide a cost-effective solution while actually improving security.

Based on various surveys, Osterman Research forecasts strong growth for hosted messaging services of various types, as shown in the following figure. Strongest growth within the cloud-based services market will be in the email security market, and this market is expected to lead other categories of outsourced services over the next several years. In a major study of the hosted services market conducted by Osterman Research in 2008, anti-spam and virus protection were the two hosted offerings that organizations identified as services that they will likely or definitely deploy to supplement internally managed infrastructure. Although some organizations will have a vendor host their entire email infrastructure, there is a value to using a dedicated hosted email security solution from a vendor that specializes in content security.

**North American Forecast of Outsourced Messaging  
Seats in Mid-Sized and Large Organizations  
2008-2011**

*(% of Corporate Email Users Served)*



## WHAT DRIVES THE DECISION TO USE HOSTED EMAIL SECURITY?

So what does it take for decision makers to consider hosted email security? In a survey of 117 email security decision makers conducted specifically for this report, respondents indicated that cost, privacy, and an offering from a well-founded vendor of on-premise security solutions were likely or very likely to persuade them to consider a hosted email security solution.

Survey question: "To what extent would the following make you more likely to consider using hosted email security?" Response shows the respondents that were likely or very likely to be influenced by the following items.

Response	%
Proof that a hosted email security solution could reduce your email security costs by 50%	71%
Privacy guarantee as part of a Service Level Agreement	61%
Proof that a hosted email security solution could reduce your email security costs by 20%	59%
Proof that a hosted email security solution could substantially reduce your IT labor investments for email security	58%
A hosted email security offering from a major provider of on-premise email security offerings	47%

Most notable is the percentage of businesses that would consider a hosted email security solution if it reduced their costs. Almost 60% said they would consider hosted if it saved them 20% of their costs, while more than 70% said they would consider hosted if it reduced their costs by 50%.

The focus of this white paper is on evaluating the costs of an on-premise solution and comparing it to hosted email security systems, including hybrid systems that combine on-premise capabilities with cloud-based services. This paper is supported by data from a survey conducted specifically for this report, as well as a simple cost analysis showing the cost of on-premise systems.

## THE COST OF ON-PREMISE EMAIL SECURITY

Many decision makers believe that the cost of an on-premise security infrastructure is lower than using hosted services because they are not fully accounting for all of the costs of the internally managed system. The results from the survey conducted for this paper showed that 48% mostly or completely agreed that hosted email security is more expensive than on-premise, gateway email security. In an earlier study in 2008, 66% of smaller organizations and 57% of larger organizations indicated that they do not use in-the-cloud services because they believe in-house management is less expensive than outsourcing. However, detailed cost models built by Osterman Research show that the cost of in-the-cloud security services are significantly lower than on-premise deployments, even for large organizations.

The cost of messaging security solutions can vary widely depending on the size of the organization, the number of users served, the geographical distribution of the organization,

the number of offices it maintains and other factors. Our research found that organizations spend a mean of more than \$63 per email user per year on hardware, software, licensing agreements, physical storage, and other out-of-pocket expenses to maintain their email security infrastructure.

Further, our results showed that there is both a mean and median of one full-time equivalent (FTE) IT staff member per 1,000 email users devoted to managing just the email security infrastructure. If we assume that the fully burdened cost of this dedicated IT staff member is \$80,000 annually, then the cost of providing email security management is \$80,000 per 1,000 users per year, or \$80 per user. When you add this to the cost of hardware, software, and other on-premise infrastructure, the total cost to provide email security internally is \$143 per user per year, or almost \$12 per user per month.

Users	On-Premise Email Security Infrastructure Costs	Email Security Management Costs	Total On-Premise Email Security Costs
1,000	\$ 63,000	\$ 80,000	\$ 143,000
5,000	\$315,000	\$400,000	\$ 715,000
10,000	\$630,000	\$800,000	\$1,430,000

The results above should be put into perspective. Osterman Research has found in numerous studies that many decision makers underestimate the cost of providing messaging and related services to their users. Also, it cannot be overstated that the costs can be *much* higher than this, particularly for smaller organizations, or organizations with highly distributed networks, or those located in urban areas with higher labor rates.

### HOW DO COSTS COMPARE FOR ON-PREMISE VS. HOSTED?

Even if we look only at the infrastructure costs, most hosted email security solutions charge substantially less than the per user cost for on-premise solutions based on these survey results. Businesses should compare the \$63 per person (or higher) cost of maintaining their on-premise solution to the per user cost offered by hosted email security.

Organizations should also keep in mind, savings are not limited to just infrastructure costs, since hosted email security can also save on management. While it does not eliminate email security management entirely, it can reduce management costs significantly. In other research conducted by Osterman, organizations spent a mean of 133 hours per year per content security solution (including email security) on tasks such as managing pattern files, signatures, and other critical updates, as well as upgrading resource capacity to add bandwidth, storage, new servers, or appliances. None of these tasks are required with a hosted email security solution, providing at least a 6.4% savings (133 hours ÷ 2,080 hours in a typical work year) in management costs.

Additional savings can result from reduced downtime, fewer security breaches, and reclaimed staff time that can be allocated to other, more critical projects for an organization:

- Downtime can have a wide range of impacts, from a minimal effect on employee productivity to major losses of revenue arising from lost sales or alienated clients. The research conducted for this white paper found that on-premise messaging security systems experience a mean of over 30 minutes of downtime monthly, or six hours of downtime per year. This means that for six hours each year, users are not protected against spam, malware and other threats, not to mention the significant time investments that are required by IT staff to address downtime issues.

Many hosted email security solutions are backed by Service Level Agreements that promise less downtime than can be supported by onsite solutions, and they are often supported by money-back guarantees.

- Security breaches that arise from inadequate messaging security infrastructure or downtime can cause significant damage. Our research found that 46% of the organizations surveyed had experienced a security breach during the previous 12 months, and that the mean cost of a breach was almost \$63,000 per breach. However, the cost of security breaches can be orders of magnitude higher.

Hosted email security solutions filter out email threats before they reach the network, preventing threats from impacting the business. On-premise email security, however, often leaves a critical security gap for several hours after signature updates are available. Based on survey results, it takes a mean of more than five hours for signature updates to get deployed within the organization's infrastructure. With hosted email security, organizations immediately receive the most up-to-date protection offered by the vendor. These benefits can increase protection and reduce security breaches, saving costs.

- Another important cost that many decision makers often fail to consider is the opportunity cost of using internal staff to manage an on-premise messaging security infrastructure. While messaging security is vitally important, it does not provide a competitive differentiator. On the other hand, if more IT staff time were focused on projects that, for example, reduce technical support wait times or speed responses to prospects' inquiries, that investment would provide a competitive advantage and could provide value far beyond the expenditure on IT staff. The bottom line, hosted email security can help organizations reclaim IT staff time so they can help grow your business.

## **COMPARING HOSTED TO ON-PREMISE EMAIL SECURITY**

This section helps to shed some light on what is currently offered by hosted email security solutions. Hosted solutions are not appropriate for all environments and solution options vary by vendor. However, once decision makers know the questions to ask, they can weigh the true benefits and deployment options of a hosted email security solution.

For starters, many decision makers question whether hosted services can offer as much control and privacy. The fact is, hosted email security can often meet or exceed the benefits or protections required by organizations in these areas. The following summarizes the current perception held by some decision makers and then provides the reality of what is currently offered by hosted email security services.

## CONTROL

- **Perception.** One of the most often-expressed objections to the use of in-the-cloud services is the loss of control that many IT decision makers fear will occur if management of the messaging infrastructure is handed off to a third party. Our research revealed that many control factors are at issue, including security, message tracking, reporting and policy creation.
- **Reality.** Leading hosted providers almost always offer a high level of control over security, generally through the use of web-based management and provisioning capabilities. This allows IT staff to add new users, provision new services for specific users, and provide generally the same level of service they might get with an on-premise system.

Some hosted email security also provides mail tracking, access to logs, and reports, providing insight into the system and control over specific emails. This allows administrators to troubleshoot email issues even though the solution is hosted.

Although functionality varies by vendor, some vendors also provide content control, such as flexible policy creation and content filtering, providing support for compliance and data leak prevention in addition to filtering emails for threats such as spam and malware. Decision makers may wish to look at vendors that offer both on-premise and hosted solutions. These vendors may offer the same granular capabilities in their hosted solution as in their on-premise products, and they may also offer combinations of hosted and on-premise solutions to create hybrid solutions that can put some of these capabilities in the cloud and some on-premise. This provides additional flexibility if organizations wish to maintain content control capabilities on their network while using a hosted service to keep threats off the network.

## SECURITY AND PRIVACY

- **Perception.** Messaging systems house a large proportion of the critical data that organizations need to conduct their business, and many organizations are subject to privacy regulations, requiring that much of this data stay confidential. Many decision makers fear that the use of hosted services will somehow expose this data to rogue employees of the hosted provider who might view or steal sensitive content, or they fear that the privacy of their data could somehow be compromised.
- **Reality.** Hosted email security uses automated processes to scan email, including no human intervention in the process. In addition, some vendors have a Service Level Agreement in place that assures privacy. This may help with privacy regulations that require the business to demonstrate that they are making reasonable efforts to secure email content.

Further, leading hosted providers typically provide a very high level of physical security for their data centers, including multiple access points using two-factor authentication, video surveillance, 24-hour staffing, and more. Also, many data centers have third-party certifications that validate these security measures. Many internally managed systems do not offer this level of security.

## JOB SECURITY

- **Perception.** Some decision makers fear that hosted providers somehow represent a threat to the job security of IT staff that manage an on-premise infrastructure.
- **Reality.** It is unlikely than an organization would lay off IT staff after it migrates to a hosted provider for a variety of reasons. There is an increasingly diverse and complicated set of systems for IT to deploy and manage, and offloading security to a specialist provider is a way to free up IT staff members for tasks that will make better use of their skills and may contribute more directly to an organization's bottom line.

## FINANCIAL VIABILITY OF HOSTED PROVIDERS

- **Perception.** Some are concerned that certain hosted providers might not be financially viable and could cease operations at some point.
- **Reality.** Some hosted providers are more financially sound than others, but this is an issue that organizations can easily address during the due diligence phase of provider evaluations. Further, vendors of on-premise systems can also go out of business, leaving customers without an upgrade path and, hence, just as vulnerable.

## USING BEST-OF-BREED SOLUTIONS

- **Perception.** Some are concerned that hosted providers may not be using the customer's choice of "best-of-breed" providers.
- **Reality.** On-premise infrastructure provides more flexibility because organizations can choose from a large number of providers. However, more leading security vendors are offering a hosted email security solution. Further, the bottom line consideration for messaging security is stopping malware and spam. Choosing the solution that does the best job should be the primary consideration, not having the largest number of choices.

## Benefits of the Hosted Paradigm

---

In addition to offering similar capabilities and benefits as an on-premise solution, hosted email security solutions carry with them a significant number of advantages unique to in-the-cloud security services that decision makers should evaluate and consider:

- **Minimal up-front costs**  
Unlike on-premise infrastructure, the use of hosted security services typically requires little, if any, up-front cost. Some providers will charge set-up fees, but these are generally much lower than the cost of on-premise hardware, the IT labor costs to deploy and configure these systems.
- **No hardware or software to maintain**  
Hosted email security, by definition, does not use on-premise infrastructure, so there is no hardware or software for IT staff to maintain. Upgrades are conducted by the vendor, who has the expertise in security and the particular solution being updated.

- **Easy and rapid deployment**  
Organizations can generally deploy a hosted email security solution by merely redirecting their MX record to route through the service. This makes for simple implementation even across distributed environments and can be installed without impacting other network infrastructure currently in place.
- **Lower IT staff costs**  
Because deployment costs for in-the-cloud services are minimal, and because there is usually no on-premise software to maintain, IT costs are much lower than for on-premise security management. As noted earlier, this allows existing IT staff to be redeployed to tasks that will offer much greater value for an organization than patching software and managing spam filters.
- **More predictable costs**  
The costs of using on-premise infrastructure can be somewhat unpredictable. For example, a rapid increase in the amount of spam often requires that organizations purchase new hardware/software or appliances and deploy them in response to the new threat. This virtually never occurs when using hosted services, since in-the-cloud providers almost always simply absorb the additional malware and spam without passing the storage and bandwidth costs onto their customers. Organizations generally pay a monthly or annual subscription fee per user, providing a stable, predictable cost.
- **Faster response to emerging threats.**  
With hosted email security, the vendor can directly update the solution with the latest protection. A hosted email security vendor can roll out general solution updates without having to package these updates into a new product “release.” Organizations using on-premise email security are often slow to deploy new releases, particularly large businesses that may need to update multiple servers. Using older versions of products can negatively impact effectiveness. With hosted security, customers get the most up-to-date protection offered by the vendor.
- **Other benefits**  
Hosted email security solutions can provide flexible deployment options. They can be deployed as a standalone solution, or can be used in combination with an on-premise system to act as a sort of pre-filter for the on-premise system.

## What Should You Do?

---

Decision makers should understand their total cost of ownership for all aspects of their messaging infrastructure so that they can make well-informed decisions. They should also evaluate the capabilities of leading hosted security offerings compared to on-premise solutions. In most cases, they will find that hosted security meets or exceeds their security, privacy, and control needs while also offering the unique benefits of better protection at a lower cost. The following are some possible questions to ask hosted email security vendors when conducting the evaluation:

- What is the per-user cost for the service for my number of users? Are there other costs in implementing the service?
- Does the service provide a Service Level Agreement (SLA)? Does the SLA guarantee a high-level of availability (i.e., minimal downtime)? Is there a money-back guarantee? Are there other service level commitments in the SLA?
- What capabilities does the service offer for policy management and content filtering? Do they offer mail tracking and reports? How are administrative tasks controlled by the customer?
- Does the service guarantee privacy? Is there any human intervention in the scanning process? Are there any third-party certifications confirming the security of the data centers?
- How long has the vendor been providing security services? Is the hosted service backed by in-house technologies supported directly by the vendor? Are there any independent benchmarks confirming solution effectiveness?
- Does the vendor also offer on-premise solutions? If so, what deployment options are available, such as hosted, gateway, mail server, other?

The answers to these questions can help an organization evaluate if a hosted security solution is appropriate for their business environment. Organizations should consider hosted solutions as an alternative or supplement to an on-premise infrastructure. Not to do so can limit the choices available to them and can result in higher costs of ownership.

## **Trend Micro InterScan™ Messaging Hosted Security**

---

Over the past 20 years, Trend Micro has made content security its sole focus, developing an expertise in securing businesses. For hosted email security, Trend Micro offers InterScan™ Messaging Hosted Security, protecting organizations against spam, viruses, spyware, phishing, and other email threats. Based on the results of this study, Trend Micro hosted email security can save businesses at least 75% in infrastructure and management costs—and the savings can go much higher for larger organizations.

As a hosted solution, InterScan Messaging Hosted Security has immediate access to security updates, accessing the latest protection offered by Trend Micro. The service uses all in-house technologies, with support provided directly by Trend Micro. All threats are kept completely off the network, helping organizations reclaim IT staff time and end-user productivity. In addition, Trend Micro's worldwide team of experts manages all hot fixes, patches, updates, and application tuning to continuously optimize security and performance.

InterScan Messaging Hosted Security provides industry-leading effectiveness. In a recent third-party anti-spam benchmark test by West Coast Labs, InterScan Messaging Hosted

Security received the highest spam catch rate, beating eight popular onsite solutions. InterScan Messaging Hosted Security is powered by Trend Micro Smart Protection Network, which correlates threat intelligence across email, web, and file reputation databases to provide immediate protection at all points of an attack. This protection is backed by one of the most aggressive Service Level Agreements (SLA) in the industry:

- 100% availability
- 95% or better spam blocking
- Fewer than .0004% false positives,
- Less than two minutes email delivery latency
- Zero email-based virus infection
- Email privacy assured through data center certifications

Significant remediation provisions are provided if the SLA commitment levels are not met.

Beyond threat protection, InterScan Messaging Hosted Security also provides flexible policy options to customize security and content filtering to enforce compliance and prevent data leakage. Email Encryption is offered as an add-on service that seamlessly integrates with these content filtering capabilities, allowing organizations to set encryption as a rule action. In addition, mail tracking allows administrators to easily find emails routed through the service and reports provide insight into the system and help to quickly show the value of the service. All of these capabilities are provided through an intuitive web-based console that makes it easy for administrators to manage email security, even in large, distributed environments.

## Summary

---

Hosted messaging security offers a number of advantages over on-premise systems and can serve as either a replacement for, or a supplement to, an on-premise security infrastructure. Hosted offerings can be significantly less expensive than on-premise infrastructure, while offering better protection and the same level of flexibility and control. They can also free up internal IT staff for projects that provide greater competitive advantage.

Decision makers in organizations that want to save money and optimize security should consider the use of hosted messaging security to satisfy some or all of their security requirements and should evaluate all of the issues involved in managing both an on-premise and hosted system when making a purchasing decision.

© 2009 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.