

# Considering the TCO of Messaging and Web Security

---

**An Osterman Research White Paper**

*Published March 2008*



## Why This White Paper Will Be Worth Your Time

---

Messaging and Web-based applications are the most critical tools for most organizations and users, the channels through which most corporate communications flows. For example, a February 2008 Osterman Research survey found that 74% of the information that people send at work on a typical day goes through email. Further, the average user sends and receives 135 emails on a typical day – an average of one email every 3.5 minutes (assuming an eight-hour workday). Plus, users are increasingly reliant on Web-based applications like social networking tools, Web conferencing and the like.

As a result, protecting these channels from external threats – spam, viruses, worms, spyware, phishing attempts, Web-borne threats, etc. – is vital. Deploying capabilities to guard against the growing volume and variety of threats is not an option, but instead a necessary part of doing business. Consequently, just as with any necessary infrastructure element, the key is to maximize performance while driving costs as low as possible.

### JUST WHAT IS 'TOTAL COST OF OWNERSHIP'?

When conducting analysis for critical infrastructure elements and evaluating purchasing decisions, it is important to determine the Total Cost of Ownership (TCO) for all aspects of the investment. Osterman Research has found that many organizations count most of the costs of ownership, but often do not consider all of the costs. They may not consider all of the costs of the labor involved in managing the infrastructure, or they may not appropriately allocate all of the costs of the infrastructure. Plus, many organizations do not consider the opportunity costs – the cost of not deploying scarce IT resources to other tasks that might provide for value for the organization. In short, TCO is about all of the costs of ownership, not just the out-of-pocket costs.

This white paper focuses on the costs of deploying and managing messaging and Web security in two delivery formats: appliances and Software-as-a-Service (SaaS) solutions. It was sponsored by MessageLabs and presents the results of a major, in-depth survey of messaging and Web decision-makers and influencers at organizations of all sizes. It also presents the comparative advantages and disadvantages of both delivery approaches, and offers key issues to consider when thinking about how best to protect an organization's messaging and Web infrastructure.

## Project Background and Methodology

---

### SURVEY METHODOLOGY

Osterman Research conducted an in-depth survey of individuals who are knowledgeable about their organization's email and/or Web security infrastructure. Respondents were queried about the number of employees, email users, physical locations and IT staff; the security solutions that are in place; the number of IT person-hours that are involved in a variety of detailed deployment and management activities; and other issues.

A total of 267 surveys were completed between October 18 and November 4, 2007.

## CALCULATOR METHODOLOGY

To better understand the issues focused on the Total Cost of Ownership for messaging and Web security, MessageLabs developed a calculator that incorporates Osterman Research data developed specifically for this report. This calculator is for organizations to gain a deeper understanding of all the costs and savings associated in purchasing solutions for messaging and Web security. The calculator allows organizations to modify the data to better fit their company's requirements and understand the cost differences for various options.

## Messaging and Web Security Delivery Models

---

There are two basic methods for delivering messaging and Web security capabilities discussed in this report (software installed on in-house servers was not considered in this analysis):

- Appliances deployed in-house
- SaaS solutions

There are variants of these solutions, as well, such as a combination of appliances and SaaS that are offered by some vendors.

### APPLIANCE-BASED SOLUTIONS

Appliances are a hardware solution in which all necessary software has been integrated. Appliances are very easy to deploy, often requiring little more than sliding the appliance into a rack and making some basic configuration changes to the network. The advantages of the appliance approach are that software and hardware are paired by the vendor, eliminating potential incompatibilities between the two; costs of acquisition can be lower than procuring software and hardware separately; and deployment is often faster than deploying software and hardware in separate steps. The disadvantage is that there is less flexibility with this approach, since the vendor pairs the hardware and software, and costs may be higher because existing hardware that an organization might possess cannot be redeployed. Maintenance requirements, in most cases, are higher than for SaaS solutions.

### SaaS SOLUTIONS

Using a SaaS solution, a customer simply points their MX record to the third-party provider without having to deploy any on-premise hardware or software. The provider then processes mail, Web traffic, etc. and passes the filtered content to the customer. The advantages of this approach are that there is virtually no up-front cost, very little IT time is required to manage the service, and costs are more predictable because the spikes in malware volume that might necessitate the purchase of more hardware, storage or bandwidth with an on-premise approach are borne by the provider. Further, leading SaaS providers typically operate very robust, multi-layered defenses that are updated more or less continually.

The disadvantages of the SaaS approach are that the costs can be higher for larger organizations, depending on the pricing provided by particular SaaS vendors, and some

providers offer less flexibility than on-premise solutions. With regard to the latter, customers of SaaS providers will typically not be permitted to choose the anti-virus, spam-filtering or other solutions used.

The cost of labor is a critical consideration for any organization as it plans its messaging and Web security infrastructure, since labor often represents a significant part of the TCO for any system. Further, the cost of labor can vary dramatically based on the location of the company – a full-time IT staff member’s salary can vary by 20% or more even in the same general geographic area. A full-time employee in a large city, for example, will typically earn a significantly higher salary than his or her counterpart in a much smaller metro area.

## Cost of Ownership

---

The research conducted for this white paper was used as the basis for a cost model designed to analyze the TCO for the two delivery models discussed above. The goal was to understand the key differences in TCO between these models, particularly in terms of the impact on the cost of IT labor required to manage messaging security. Osterman Research has found that for on-premise solutions, the cost of labor is the largest component of TCO, whereas for SaaS solutions the per-seat price charged by the provider is the largest component of TCO.

### APPLIANCE-BASED SOLUTIONS

There are four major components to the cost of any appliance-based solution designed to protect an organization against email- and Web-based threats:

- **The cost of the appliance(s)**  
The cost of purchasing the appliance(s), including all software and baseline support subscriptions and the additional miscellaneous expenses of cooling, power, rack space, etc. (which is assumed to be 10% of the capital cost of the appliance box).
- **IT labor costs for deployment**  
The number of hours spent by IT to deploy the appliance(s) into the organization’s infrastructure, including hardware configuration, software configuration, integration into the infrastructure, testing and tuning, IT and end user training, and vendor support.
- **IT labor costs for maintenance**  
The number of hours spent by IT to maintain the appliance(s), including scheduled maintenance, unscheduled maintenance, responding to outages, monitoring the system, running/viewing reports, and vendor support. Further, there is time spent by IT to troubleshoot end user questions/concerns, based on a set percentage of end users, such as those individuals who call IT to address specific issues.
- **Upgrades to the hardware**  
We have assumed that appliance(s) will be replaced in Year 4, necessitating a ‘rip-and-replace’ of the current infrastructure. The replacement of an old appliance also ensures

that organizations have the latest, most robust appliance protecting their networks to help handle the changing threat landscape.

## SaaS SOLUTIONS

There are three major components to the cost of any SaaS solution designed to protect an organization against email- and Web-based threats:

- The up-front cost of the SaaS solution**  
 The initial setup fees (if applicable) and the per user per month subscription cost.
- IT labor costs for deployment**  
 The number of hours spent by IT to deploy a SaaS solution into the organization's infrastructure, including testing and tuning, IT and end user training, and vendor support (there are no hardware or software configuration requirements with a SaaS solution).
- IT labor costs for maintenance**  
 The number of hours spent by IT to maintain the service, including monitoring the system, running/viewing reports, and vendor support. SaaS solutions are plug-and-play; i.e. initially as the service is optimized for the organization, maintenance of the service will require some additional IT resources in the first few months. The IT resource requirement is then reduced once the service is fully optimized for the organization. Further, there is some time spent by IT to troubleshoot end user questions/concerns, based on a set percentage of end users, that call IT for issues.

## COMPARISON OF MESSAGING SECURITY SOLUTIONS

The model that we have developed assumes the following investments, as shown in the following tables.

**Email Security Cost Estimates**  
**\$ Per User Per Month**  
**200 Users**

	APPLIANCE				SaaS			
	Capital	Deployment	Maintenance	TOTAL	Service	Deployment	Maintenance	TOTAL
<b>Year One</b>	\$10.98	\$0.25	\$4.55	\$15.78	\$4.25	\$0.10	\$2.86	\$7.22
<b>Year Two</b>	\$0	\$0	\$4.78	\$4.78	\$4.25	\$0	\$2.79	\$7.04
<b>Year Three</b>	\$0	\$0	\$5.02	\$5.02	\$4.25	\$0	\$2.93	\$7.18
<b>Year Four</b>	\$10.98	\$0	\$5.27	\$16.25	\$4.25	\$0	\$3.07	\$7.32
<b>AVERAGE</b>	<b>\$5.49</b>	<b>\$0.06</b>	<b>\$4.90</b>	<b>\$10.46</b>	<b>\$4.25</b>	<b>\$0.03</b>	<b>\$2.91</b>	<b>\$7.19</b>

**Email Security Cost Estimates  
\$ Per User Per Month  
1,000 Users**

	APPLIANCE				SaaS			
	Capital	Deployment	Maintenance	TOTAL	Service	Deployment	Maintenance	TOTAL
<b>Year One</b>	\$6.02	\$0.09	\$1.25	\$7.37	\$2.55	\$0.04	\$0.77	\$3.37
<b>Year Two</b>	\$0	\$0	\$1.32	\$1.32	\$2.55	\$0	\$0.64	\$3.19
<b>Year Three</b>	\$0	\$0	\$1.38	\$1.38	\$2.55	\$0	\$0.68	\$3.23
<b>Year Four</b>	\$6.02	\$0	\$1.45	\$1.45	\$2.55	\$0	\$0.71	\$3.26
<b>AVERAGE</b>	<b>\$3.01</b>	<b>\$0.02</b>	<b>\$1.35</b>	<b>\$4.38</b>	<b>\$2.55</b>	<b>\$0.01</b>	<b>\$0.70</b>	<b>\$3.26</b>

**Email Security Cost Estimates  
\$ Per User Per Month  
5,000 Users**

	APPLIANCE				SaaS			
	Capital	Deployment	Maintenance	TOTAL	Service	Deployment	Maintenance	TOTAL
<b>Year One</b>	\$12.04	\$0.02	\$0.25	\$12.31	\$2.34	\$0.01	\$0.15	\$2.50
<b>Year Two</b>	\$0	\$0	\$0.26	\$0.26	\$2.34	\$0	\$0.13	\$2.47
<b>Year Three</b>	\$0	\$0	\$0.28	\$0.28	\$2.34	\$0	\$0.14	\$2.48
<b>Year Four</b>	\$12.04	\$0	\$0.29	\$12.33	\$2.34	\$0	\$0.14	\$2.48
<b>AVERAGE</b>	<b>\$6.02</b>	<b>\$0</b>	<b>\$0.27</b>	<b>\$6.29</b>	<b>\$2.34</b>	<b>\$0</b>	<b>\$0.14</b>	<b>\$2.48</b>

**COMPARISON OF WEB SECURITY SOLUTIONS**

The model that we have developed assumes the following investments, as shown in the following tables.

**Web Security Cost Estimates  
\$ Per User Per Month  
200 Users**

	APPLIANCE				SaaS			
	Capital	Deployment	Maintenance	TOTAL	Service	Deployment	Maintenance	TOTAL
<b>Year One</b>	\$34.83	\$0.33	\$3.47	\$38.63	\$5.00	\$0.13	\$2.86	\$7.99
<b>Year Two</b>	\$0	\$0	\$3.64	\$3.64	\$5.00	\$0	\$2.79	\$7.79
<b>Year Three</b>	\$0	\$0	\$3.82	\$3.82	\$5.00	\$0	\$2.93	\$7.93
<b>Year Four</b>	\$34.83	\$0	\$4.01	\$38.84	\$5.00	\$0	\$3.07	\$8.07
<b>AVERAGE</b>	<b>\$17.42</b>	<b>\$0.08</b>	<b>\$3.74</b>	<b>\$21.23</b>	<b>\$5.00</b>	<b>\$0.03</b>	<b>\$2.91</b>	<b>\$7.94</b>

**Web Security Cost Estimates  
\$ Per User Per Month  
1,000 Users**

	APPLIANCE				SaaS			
	Capital	Deployment	Maintenance	TOTAL	Service	Deployment	Maintenance	TOTAL
<b>Year One</b>	\$12.29	\$0.21	\$1.89	\$14.39	\$3.00	\$0.05	\$0.77	\$3.82
<b>Year Two</b>	\$0	\$0	\$1.99	\$1.99	\$3.00	\$0	\$0.64	\$3.64
<b>Year Three</b>	\$0	\$0	\$2.09	\$2.09	\$3.00	\$0	\$0.68	\$3.68
<b>Year Four</b>	\$12.29	\$0	\$2.19	\$14.48	\$3.00	\$0	\$0.71	\$3.71
<b>AVERAGE</b>	<b>\$6.15</b>	<b>\$0.05</b>	<b>\$2.04</b>	<b>\$8.24</b>	<b>\$3.00</b>	<b>\$0.01</b>	<b>\$0.70</b>	<b>\$3.71</b>

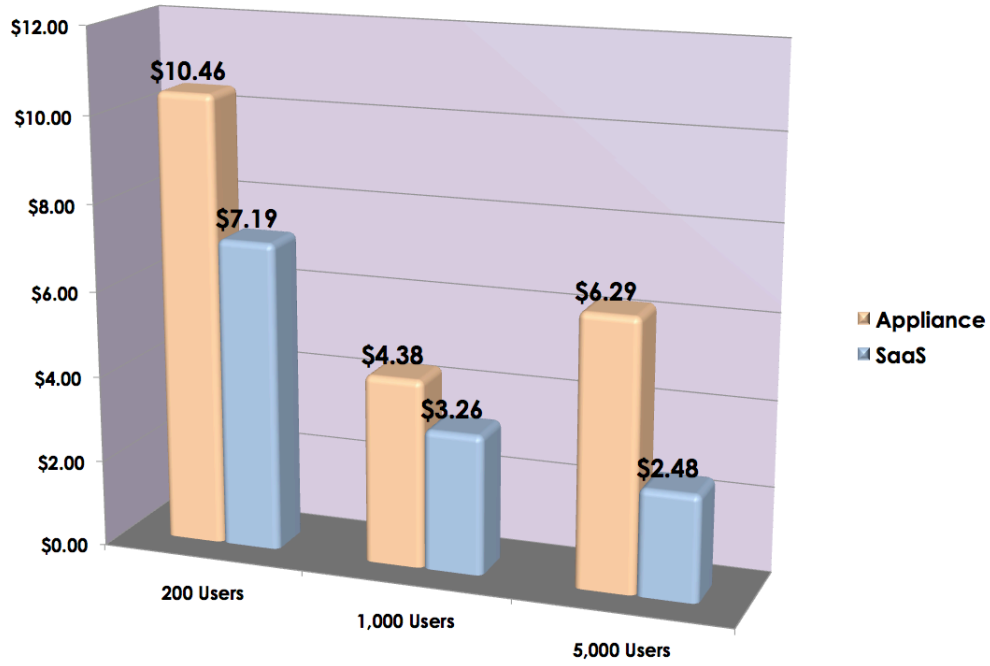
**Web Security Cost Estimates  
\$ Per User Per Month  
5,000 Users**

	APPLIANCE				SaaS			
	Capital	Deployment	Maintenance	TOTAL	Service	Deployment	Maintenance	TOTAL
<b>Year One</b>	\$24.58	\$0.04	\$0.38	\$25.00	\$2.75	\$0.01	\$0.15	\$2.91
<b>Year Two</b>	\$0	\$0	\$0.40	\$0.40	\$2.75	\$0	\$0.13	\$2.88
<b>Year Three</b>	\$0	\$0	\$0.42	\$0.42	\$2.75	\$0	\$0.14	\$2.89
<b>Year Four</b>	\$24.58	\$0	\$0.44	\$25.02	\$2.75	\$0	\$0.14	\$2.89
<b>AVERAGE</b>	<b>\$12.29</b>	<b>\$0.01</b>	<b>\$0.41</b>	<b>\$12.71</b>	<b>\$2.75</b>	<b>\$0</b>	<b>\$0.14</b>	<b>\$2.89</b>

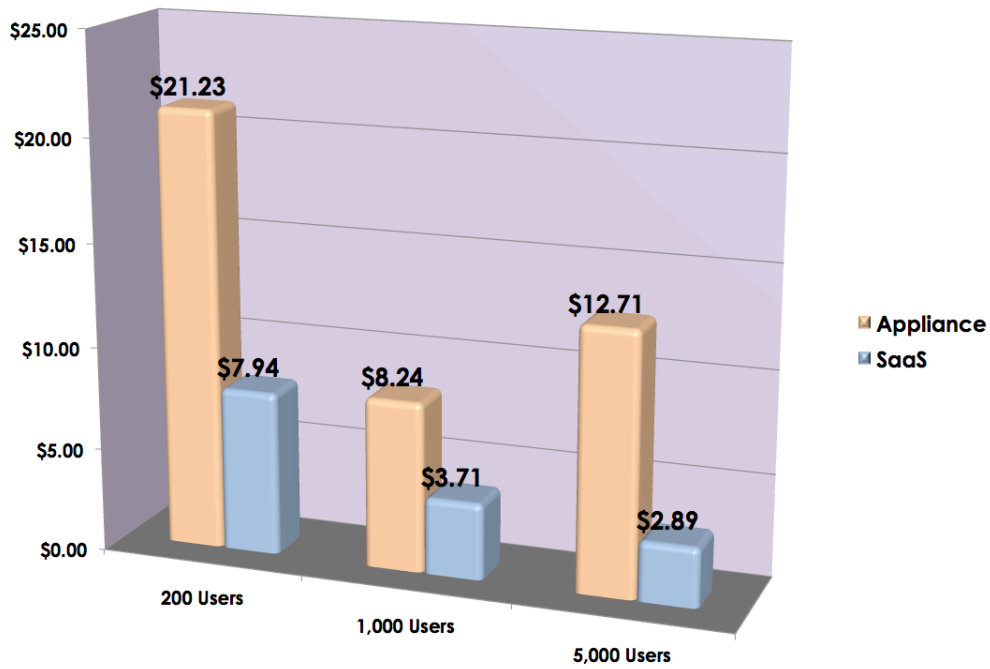
**SUMMARY**

The costs for appliances and SaaS solutions for both email security and Web security are summarized in the following figures.

### Email Security Cost Comparison Average Monthly Cost per User



### Web Security Cost Comparison Average Monthly Cost per User



## OTHER CONSIDERATIONS

In addition to the components of TCO for the various solutions discussed above, there are also a variety of factors that need to be considered in any decision about the optimal choice for messaging and Web security solutions:

- **Redundancy**

Because messaging and Web security is such a critical part of any organization's infrastructure, it must remain up-and-running as close to 100% of the time as possible. Appliance-based solutions are more vulnerable to natural disasters, power outages and other disruptive events than SaaS solutions unless redundant facilities are deployed and managed at a remote location. SaaS solutions, can be just as vulnerable to these types of events if the provider does not operate multiple, redundant data centers through which its customers' traffic is processed.

- **Planning for growth**

The rapid increase in spam during 2006 flooded many on-premise appliance solutions, necessitating the deployment of additional infrastructure at many organizations. Decision-makers need to expect some level of expansion or improvement for their on-premise infrastructure in response to increased volumes of malware, either in the form of more servers/appliances, more capable servers/appliances or some form of reputation analysis/connection management capability that will stem the flow of inbound content. Most SaaS providers, on the other hand, will accommodate this growth without passing along costs to their customers, at least in the short run.

- **Intangible costs**

There are a variety of costs that are not quite as easy to identify, including the costs of waiting for hardware to be replaced if it fails, choosing an appliance solution that might not be compatible with every other part of your messaging infrastructure, the costs of bandwidth for processing spam on-premise instead of dealing with it first 'in the cloud', etc.

## Summary and Conclusions

---

Organizations of all sizes need to deploy messaging and Web security solutions as an essential part of their overall infrastructure. In deciding upon a solution to provide these capabilities, they must achieve the best balance between the performance of the solution and its TCO. The TCO for SaaS solutions is typically lower than for on-premise solutions, particularly for smaller organizations that often do not have dedicated IT staff to manage servers or appliances. Further, SaaS solutions have the advantage of helping organizations to maintain business continuity in the event of a disaster or other disruptive event if a SaaS provider operates multiple, redundant data centers.

© 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.