

# Using SaaS to Reduce the Costs of Email Security

**An Osterman Research White Paper**

*Published February 2009*

**SPONSORED BY**

**proofpoint**<sup>™</sup>



## Executive Summary

---

Software-as-a-service (SaaS) security offerings are becoming increasingly popular in North America and elsewhere. Decision makers are increasingly receptive to the notion of using third party services to manage their security infrastructure, in large part due to the soft worldwide economy that is motivating decision makers to consider the cost of their messaging infrastructure more than ever, and the realization that security must be maintained. In short, decision makers realize that security must be extremely robust, but delivered at the lowest possible cost.

Reasons for this growing interest in SaaS messaging services include:

- **The cost of security is increasing**  
Because providers of SaaS security services can often provide services at lower costs than organizations can provide using on-premise infrastructure and staff (as demonstrated in this white paper), many decision makers are finding use of these services increasingly attractive.

*Because providers of SaaS security services can often provide services at lower costs than organizations can provide using on-premise infrastructure and staff, many decision makers are finding use of these services increasingly attractive.*

- **Security is becoming more complex**  
Security is becoming increasingly complex and more difficult to manage as a result of new regulatory requirements for outbound data protection, increased attacks from more sophisticated malware, new and more sophisticated types of spam, the growth in Web-based threats, greater use of blended threats, and other factors. As a result, many decision makers are seeking to offload some or all of the management of their messaging infrastructure to specialist providers that can manage this complexity.
- **There are more choices available**  
An increasing number of vendors of SaaS security services – including industry heavyweights like Microsoft and Google, as well as many smaller vendors – are delivering compelling marketing messages that are beginning to resonate with decision makers.

### THE BOTTOM LINE

The bottom line is that security is becoming more difficult and more expensive to manage in-house, threats are becoming more sophisticated, and there are a growing number of SaaS alternatives that provide robust capabilities.

This white paper, sponsored by Proofpoint, discusses the key drivers that are motivating organizations to seek SaaS alternatives, and it discusses some sample scenarios of the cost savings that can be achieved through the use of Proofpoint on Demand. These scenarios, generated from a cost model that Osterman Research developed specifically for this white

paper, demonstrate the substantial cost savings that can be achieved through the use of Proofpoint on Demand compared to an on-premise security infrastructure.

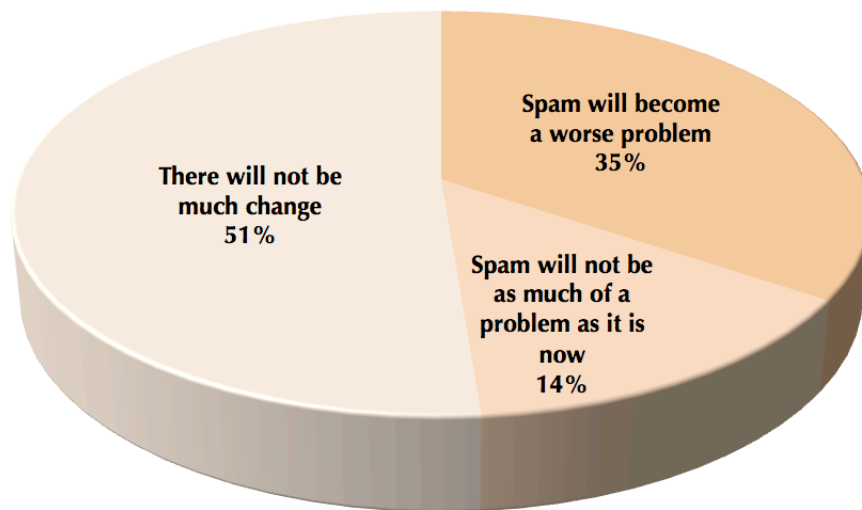
## Why SaaS Security?

### MANY BELIEVE THAT SPAM AND MALWARE WILL GET WORSE

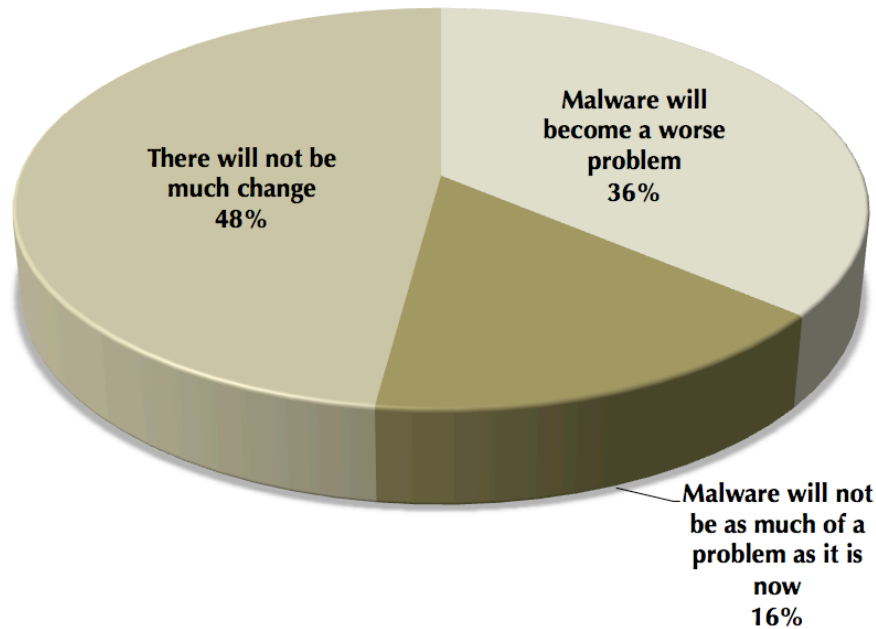
Despite the increasing sophistication of anti-spam defenses that most organizations have deployed, one-third of decision makers in mid-sized and large organizations believe that spam will become a worse problem over the next to three years, as shown in the following figure. Interestingly, while one-half believe that the status quo will be maintained, only one in seven has an optimistic view of the future of the spam threat. Smaller organizations are decidedly less optimistic about the long-term prospects for spam remediation: 40% of decision makers in smaller organizations believe spam will become a worse problem during the next two years, while only 27% of their counterparts in larger organizations believe spam will get worse.

Further, as with the spam problem, slightly more than one-third of organizations believe that malware will become a worse problem over the next three years, as shown in the next figure.

**Anticipated Problems With Spam  
Over the Next Three Years**



### Anticipated Problems With Malware Over the Next Three Years



#### WHAT DOES THIS MEAN?

Will spam actually get worse, or are a third of decision makers overly pessimistic about the future of this ever-present threat? Osterman Research believes that the answer is both yes and no. On the positive side, spam is unlikely to get worse for individual users. The current generation of both on-premise and SaaS anti-spam technology, coupled with the increasing deployment of reputation analysis, connection management systems and other capabilities, means that end users are unlikely to see significant (if any) increases in the amount of spam received in the typical inbox.

More importantly, however, because spammers will largely be thwarted in delivering their content to end users, they will simply continue to increase the amount of content they send through botnets and other spam sources. This means that organizations, SaaS providers, managed service providers, network operators, Internet Service Providers and others will continue to receive more and more spam over time. Similarly, malware poses an enormous threat to the integrity of organizations and their data. Far from the splashy viruses of years past, today's malware threats are intentionally "quiet", intended to extract sensitive corporate data, such as login information, and pass them to unauthorized outsiders. Further, the number of sources for this content is increasing, most notably among infected Web sites, necessitating the use of Web-filtering and other Web-related protection technologies.

#### THE IT INFRASTRUCTURE IS DIFFICULT TO MANAGE

Managing network systems, particularly messaging security, is not easy: the following table shows that maintaining security and compliance, proactive monitoring and other tasks is viewed to be difficult or very difficult by nearly one-half of messaging decision

makers. Even for tasks that fewer decision makers consider to be difficult, a significant proportion still find that there is difficulty associated with managing the IT infrastructure.

**Difficulty of Managing Aspects of the IT Infrastructure**  
*(% Responding Difficult or Very Difficult)*

Attribute	%
Maintaining configuration security and compliance	48%
Proactively monitoring your IT environment	47%
Detecting configuration changes across your network	46%
Managing and deploying software updates in heterogeneous environments	46%
Managing all of your applications and services in a unified way	45%
Troubleshooting network problems	36%
Guaranteeing system uptime for all of your systems (inventory, CRM, etc.)	36%
Service provisioning	23%

**DECISION MAKERS ARE MORE CONCERNED ABOUT SPYWARE**

Further, decision makers are significantly more concerned about spyware infecting their networks, while even more are concerned about Web-based threats and the amount of spam that they receive. Interestingly, the ability to manage and secure mobile devices was even more serious of a concern to decision makers, as shown in the following table.

**Changes in Concerns About Various Security Issues**

Issue	Level of Concern Compared to 12 Months Ago		
	Less	Same	More
Ability to manage/secure mobile devices	8%	66%	27%
The amount of spam we receive	23%	52%	25%
Web-based threats	13%	63%	24%
Spyware infecting our network	17%	62%	21%
Loss of intellectual property through email	10%	77%	13%

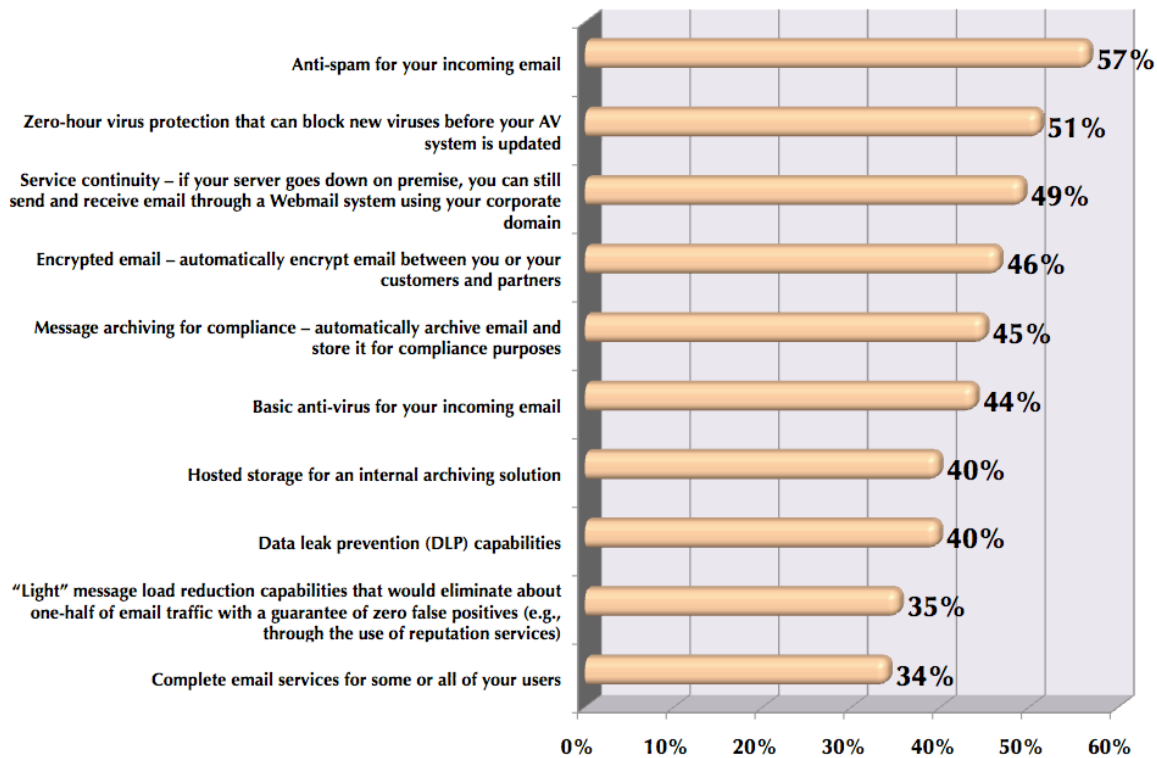
What this table reveals is that there is a significant opportunity for providers of various types of SaaS security services to directly address many of these problems and alleviate burdens for IT departments. While many decision makers will likely not be receptive to outsourcing their entire messaging infrastructure to an outside provider, by selecting key areas for outsourcing that present the most difficulty, IT departments can make their lives significantly easier and free up resources for other initiatives, a particularly important benefit during difficult economic times.

Another important and related consideration that favors the use of the SaaS model is the opportunity cost associated with in-house management. For example, if an organization uses 0.5 full-time equivalent (FTE) staff to manage its messaging security infrastructure, that represents 0.5 FTE that cannot be devoted to initiatives that may generate more value for the organization. While managing messaging security, for example, is a critical task, it does not generate the value that integrating something like instant messaging into a technical support system may create. The decision for organizations, therefore, will be to identify those areas of the infrastructure that are critical, but could effectively be managed less expensively by a third party and that would free up IT staff time in the most efficient way.

### **MESSAGING SECURITY IS THE MOST LIKELY SaaS SERVICE**

While some decision makers are not interested in the use of SaaS services because of their often inaccurate perceptions about the benefits of maintaining the management of the messaging infrastructure in-house, they are least resistant to the notion of using SaaS services for security applications. As shown in the following figure, anti-spam and virus protection are the two SaaS services that organizations identify as services that they will likely or definitely deploy to supplement internally managed infrastructure.

**Likelihood of Evaluating SaaS Services That Would Supplement or Replace Internally Managed Solutions**  
(% Responding Likely or Definitely Will)



## COST OF OWNERSHIP WILL BE A KEY DRIVER

SaaS services for various types of messaging services, but particularly messaging security, will be driven by a number of factors during 2009 and 2010 and beyond:

- Organizations' desire to lower the cost of providing messaging services.
- The growing complexity of the messaging infrastructure.
- The need to provide highly reliable messaging services.

However, Osterman Research believes that one of the chief reasons that organizations will consider the use of SaaS solutions during 2009 and 2010 will be considerations around the total cost of ownership for messaging security. Because organizations of all sizes are facing the dual pressures of a difficult economy and greater security risks, many are seeking alternatives that provide at least the same level of security, but at significantly lower costs. This is particularly true for organizations that are planning a capital refresh cycle and wish to reduce or eliminate their capital expenditures, instead replacing them with operating expenditures distributed more predictably and more evenly over time.

*One of the chief reasons that organizations will consider the use of SaaS solutions during 2009 and 2010 will be considerations around the total cost of ownership for messaging security.*

As we clearly demonstrate in the next section of this white paper, SaaS security – Proofpoint on Demand in particular – offers robust security, but at a much lower cost of ownership.

## Comparing the Cost of Security Options

Osterman Research built a cost model specifically for this white paper that allows a thorough analysis of the costs involved in managing an on-premises security infrastructure. The elements in the cost model permit testing of various scenarios based on a variety of factors, including the level of support provided to end users, the industry in which an organization operates, whether or not downtime should be included in the analysis, anticipated increases in spam, and a variety of other factors.

Using the model, we have developed comparisons for various security deployment scenarios, as shown in the following tables. It is important to note that we focused on a six-year lifecycle for these examples, so that we could include at least one hardware and software refresh cycle in the cost-of-ownership calculations.

## SCENARIO 1: SMALL HEALTHCARE COMPANY

Specifics of this scenario:

- 500 users in Year 1 with email user base growing at 5% per year
- Organization purchases single appliances with no backup/disaster recovery capability
- Provides only 8x5 support
- On-premises system is a market-leading, low-cost provider of appliances
- Three-year capital refresh cycle
- Downtime is not factored into this analysis
- Spam volume is increasing at 100% per year

Cost	On-Premises	SaaS
Average cost per user per year over six years	\$86.79	\$32.07
Average savings per user per year over six years	\$54.72	
<b>% savings provided by hosting</b>	<b>60.6%</b>	
<b>% of total on-premise cost represented by labor</b>	<b>66.5%</b>	

## SCENARIO 2: SMALL MANUFACTURING COMPANY

Specifics of this scenario:

- 750 users in Year 1 with email user base growing at 3% per year
- Organization purchases single appliances with no backup/disaster recovery capability
- Provides 12x7 support
- On-premises system is a market-leading, low-cost provider of appliances
- Five-year capital refresh cycle
- Downtime is not factored into this analysis
- Spam volume is increasing at 75% per year

Cost	On-Premises	SaaS
Average cost per user per year over six years	\$127.44	\$28.43
Average savings per user per year over six years	\$99.01	
<b>% savings provided by hosting</b>	<b>76.5%</b>	
<b>% of total on-premise cost represented by labor</b>	<b>84.5%</b>	

## SCENARIO 3: MID-SIZED FINANCIAL SERVICES COMPANY

Specifics of this scenario:

- 1,000 users in Year 1 with email user base growing at 2% per year
- Organization purchases appliances in pairs for backup/disaster recovery capability
- Provides 24x7 support
- On-premises system is a market-leading provider of appliances
- Three-year capital refresh cycle
- Downtime is not factored into this analysis
- Spam volume is increasing at 100% per year

Cost	On-Premises	SaaS
Average cost per user per year over six years	\$192.88	\$26.48
Average savings per user per year over six years	\$166.40	
<b>% savings provided by hosting</b>	<b>85.3%</b>	
<b>% of total on-premise cost represented by labor</b>	<b>82.1%</b>	

## SCENARIO 4: LARGE SERVICES COMPANY

Specifics of this scenario:

- 5,000 users in Year 1 with email user base growing at 3% per year
- Organization purchases appliances in pairs for backup/disaster recovery capability
- Provides 24x7 support
- On-premises system is a market-leading provider of appliances
- Four-year capital refresh cycle
- Downtime is not factored into this analysis
- Spam volume is increasing at 75% per year

Cost	On-Premises	SaaS
Average cost per user per year over six years	\$154.46	\$21.26
Average savings per user per year over six years	\$133.19	
<b>% savings provided by hosting</b>	<b>83.8%</b>	
<b>% of total on-premise cost represented by labor</b>	<b>72.2%</b>	

## SCENARIO 5: LARGE COLLEGE

Specifics of this scenario:

- 20,000 users in Year 1 with email user base growing at 2% per year
- Organization purchases single appliances with no backup/disaster recovery capability
- Provides only 8x5 support
- On-premises system is a market-leading, low-cost provider of appliances
- Four-year capital refresh cycle
- Downtime is not factored into this analysis
- Spam volume is increasing at 50% per year

Cost	On-Premises	SaaS
Average cost per user per year over six years	\$46.61	\$20.32
Average savings per user per year over six years	\$26.29	
<b>% savings provided by hosting</b>	<b>53.6%</b>	
<b>% of total on-premise cost represented by labor</b>	<b>92.6%</b>	

## CONCLUSIONS ABOUT THE COST OF OWNERSHIP

For all of these scenarios, SaaS email security provides a significantly lower total cost of ownership compared to on-premise security, most notably in the area of reduced labor

costs. Aside from simply the level of savings that a SaaS system will provide, the cost savings are significant in two ways:

- First, of all of the costs associated with managing a security infrastructure, labor is the only cost that will continue to increase over time. A SaaS security solution's ability to eliminate most of the labor involved in managing security will have increasing benefits over time as labor rates increase. This is a particularly important consideration in markets with very high labor rates.
- Second, the significant amount of labor that is freed up as a result of using a SaaS provider means that this IT staff time is now available for other projects and initiatives that can provide more value to an organization. For example, using additional IT staff time to improve an organization's customer service experience or shorten account receivables wait times could be a much better use of these IT resources than managing spam filters and other parts of the security infrastructure.

## About Proofpoint on Demand

---

Proofpoint on Demand™ delivers Proofpoint's unified email security and data loss prevention features as a cost-effective, easy-to-adopt and easy-to-manage SaaS solution. It's the industry's most complete and effective security for enterprise messaging infrastructures. Based on the same enterprise-proven platform that powers Proofpoint Messaging Security Gateway™ appliances and Proofpoint Protection Server® software, Proofpoint on Demand offers the industry's most effective protection against both inbound and outbound email-borne threats, without requiring the installation of on-premise hardware or software.

The benefits of Proofpoint on Demand include:

- Delivers Proofpoint's industry-leading messaging security features-including anti-spam, anti-virus, email policy enforcement and data loss prevention capabilities-as a cost-effective, on-demand anti-spam service.

*Proofpoint on Demand™ delivers Proofpoint's unified email security and data loss prevention features as a cost-effective, easy-to-adopt and easy-to-manage SaaS solution.*

- Proofpoint's Flexible Managed Services Architecture meets any enterprise deployment strategy-from fully SaaS to hybrid on-demand/on-premise installations.
- Flexible customization of your organization's email security preferences, policies, enabled modules, end-user features, alerts and reporting.
- Next-generation hosting platform provides each customer with a fully-compartmentalized, dedicated instance of Proofpoint's service, ensuring complete security of customer data and total flexibility in system configuration.

## Other Benefits of the SaaS Paradigm

---

Clearly, the SaaS model can provide significant cost savings compared to managing an on-premise infrastructure, even for organizations with large numbers of users. However, there are a number of other benefits associated with the SaaS security model, including:

- Very high levels of availability (normally 99.9% or better), typically guaranteed with Service Level Agreements.
- Much lower bandwidth requirements because spam is removed from the email traffic flow. This means that organizations using a SaaS-based security model benefit not only from improved network performance, but can also postpone or eliminate bandwidth upgrades.
- Reduced storage requirements because on-premise storage does not have to be devoted to spam quarantines.
- More predictable costs, since spikes in spam or malware volumes will not necessitate the deployment of new appliances or servers in response. This is particularly advantageous during periods of tight IT budgets in which unexpected expenditures for new security infrastructure might be more difficult to fund.

## About the Cost Model and Methodology

---

The cost model developed for this white paper was designed to account for all of the costs associated with both an on-premise and SaaS security model. It was also designed so that specific soft cost elements, such as downtime, could be “turned off”. Components of the cost model that can be customized by the user to provide various types of comparisons include the following:

- On-premise deployments of appliances can include only single appliances or pairs of appliances for backup and disaster recovery purposes.
- Specific industries can be selected from a picklist of eight different industries.
- Three support options can be selected: 8x5, 12x7 or 24x7.
- A number of leading appliance options can be selected.
- Hardware refresh cycles can be selected from two years to five years, or the user can opt not to include a refresh cycle.
- Growth in spam each year can be modified.
- In addition to downtime, other costs can be included or not included in the analysis, such as the cost of racks, support equipment, annual maintenance, additional support

costs, power, the number of attacks directed against the security infrastructure, and the floor space devoted to the security infrastructure.

- Other parameters can be modified, including IT staff salaries, wage growth over time, the cost of consultants, the amount of training required, etc.

The goal of the model was to create as realistic a comparison as possible between an on-premise infrastructure and a SaaS model.

## Summary

---

Organizations of all sizes need face a difficult conundrum: a) provide robust defenses against a growing set of more sophisticated messaging security threats, and b) do so during a soft economy in which there is pressure to reduce costs as much as possible. While on-premise security solutions can satisfy the first part of this problem, they are less effective against the second part because of the labor investments that are required to maintain appliances or servers. A SaaS solution can provide a markedly lower cost of ownership for the messaging security, while at the same time offering the same level of security and system uptime.

© 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.