

The Cost Effective Migration to Integrated Hybrid SaaS Email Security

An Osterman Research White Paper

Published July 2010

SPONSORED BY



Executive Summary

Security is of paramount importance to any organization that maintains an email infrastructure. A growing proportion of malware and other threats today enter an organization through Web surfing and Web 2.0 applications, so blocking links to these Web sites introduced via email is of utmost importance. In addition, email-borne malware and spam continue to represent dangerous and unwanted content that organizations must manage effectively and as inexpensively as possible.

Traditionally, the approach for organizations to address the problem of email security was to build out a completely on-premise infrastructure using servers and/or appliances that are managed using in-house IT staff.

However, because of tremendous increases in the volume of spam, many organizations have considered a hosted system in which a third party service is used to block malware and spam in conjunction with a minimal amount of in-house IT staff time to manage the vendor relationship, deal with user issues and the like.

What we have seen in practice is that many enterprises are opting for a hybrid system that combines an on-premise infrastructure of servers and/or appliances along with a hosted service that pre-filters malware and spam in the cloud and uses the on-premise system to provide deep inspection of content.

The advantage of a hybrid approach is that the hosted component acts as a sort of cloud-based "shock absorber" for the on-premise infrastructure, absorbing spikes in malware and spam and allowing the on-premise infrastructure to be upgraded more slowly in response to increasing spam levels and the like. Osterman Research believes that the bulk of email security systems in the future will be hybrid solutions.

TWO APPROACHES TO A HYBRID SYSTEM

There are two basic methods for implementing a hybrid email infrastructure:

- Deploy an on-premise system using servers and/or appliances and then use another vendor's hosted offering as a supplemental system in addition to the on-premise infrastructure.
- Use an integrated hybrid SaaS offering combining on-premise and hosted from a single vendor

Osterman Research undertook a research program in which we surveyed organizations about their email security infrastructure. The goal of this research was to understand the cost differences for each of these approaches to building out a hybrid system, and to compare these costs with a purely on-premise solution.

ABOUT THIS WHITE PAPER

The purpose of this white paper is to discuss and analyze the differences between the two approaches to deploying a hybrid email security infrastructure with a particular emphasis on enterprise-level (1,000 or more email user) deployments.

Background on the Research

BACKGROUND AND METHODOLOGY

Osterman Research conducted a primary market research study to understand the approaches that large organizations (1,000+ email users) employ for email security in the context of their use of on-premise and hosted capabilities. Specifically, we examined four different email security architectures:

- On-premise infrastructure only
- On-premise in combination with a different hosted security solution
- On-premise with the same vendor's hosted security integrated into one solution
- Hosted security only

Osterman Research conducted a total 124 surveys with members of the Osterman Research survey panel, but analyzed only the 72 responses that had a minimum of 1,000 email users – what we consider to be “enterprises”. The goal was to quantify the investment in servers, other infrastructure elements and labor that are used to satisfy the email security requirements of these organizations. We then built a cost model to compare the total, three-year cost of ownership for the various models of managing email security.

ASSUMPTIONS USED IN THE COST MODEL

The cost model was designed to provide an accurate comparison between the email security models noted above. Toward this end, we used several assumptions in the model. For a detailed list of the assumptions used in the cost model, please see Appendix A.

LABOR DEVOTED TO MANAGING SECURITY

A key focus of the research for this white paper was the labor investments that are required to manage an email security infrastructure. Specifically, we focused on the following:

- Messaging tracking/tracking email
- Quarantine management
- Dealing with false positives
- Resolving user issues
- Integration report data
- Other tasks

Because labor constitutes a major component in the total cost of ownership for any security system, it was important to determine how much time organizations spend on these activities on an ongoing basis.

Comparing Approaches to Email Security

HOMEGROWN VS. INTEGRATED HYBRID SAAS

Our research found that an integrated hybrid email security solution from a single vendor is substantially less expensive than a hybrid solution comprised of an on-premise infrastructure layered with a different hosted offering (a homegrown hybrid solution), as shown in the following tables and figure.

Three-Year Costs per Seat for Homegrown vs. Integrated Hybrid SaaS Email Security Solutions

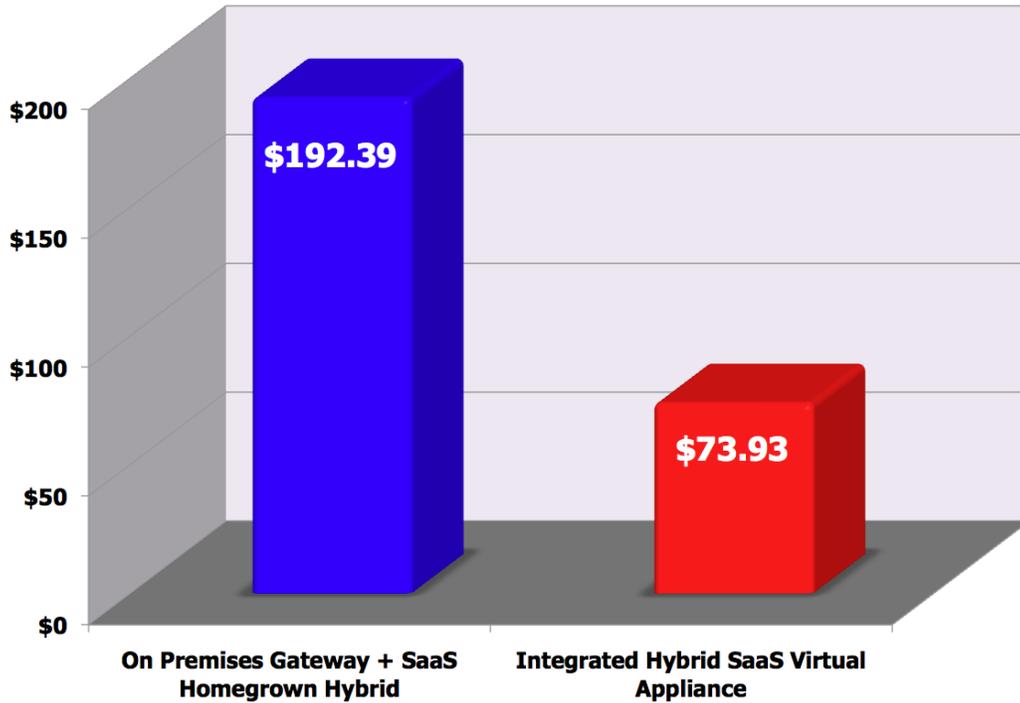
Cost Component	Homegrown Hybrid	Integrated Hybrid
Physical infrastructure, including support	\$64.32	\$44.86 ¹
Hosted security over three years	\$36.00	\$0
SUBTOTAL	\$100.32	\$44.86

Person-Hours Required per 1,000 Users per Week for Homegrown vs. Integrated Hybrid Email Security Solutions (Person-hours per 1,000 Users per Week)

Cost Component	Homegrown Hybrid	Integrated Hybrid
Messaging tracking	5.35	1.35
Resolving user issues	3.68	2.09
Quarantine management	1.75	0.29
Dealing with false positives	1.67	0.57
Other security infrastructure issues	1.45	0.27
Integrating report data	0.97	0.10
Server, OS, etc. management issues	0.02	0.02
TOTAL PERSON-HOURS	14.89	4.70
TOTAL COST OF LABOR, YEAR 1	\$29.79	\$9.41
TOTAL COST OF LABOR, YEAR 2	\$30.68	\$9.69
TOTAL COST OF LABOR, YEAR 3	\$31.60	\$9.98
TOTAL THREE-YEAR COST OF LABOR	\$92.07	\$29.08

¹ Includes cost of cloud-based service and three-year support.

Cost of Homegrown vs. Integrated Hybrid SaaS Email Security Solutions



It is important to note that labor is a major component of the total cost of ownership for both the homegrown hybrid and integrated hybrid solutions, although labor is a much larger component with the former.

WHY IS AN INTEGRATED HYBRID SOLUTION LESS EXPENSIVE THAN A HOMEGROWN HYBRID SOLUTION?

The tables and figure above reveal that the most significant differences between a homegrown hybrid solution and an integrated hybrid solution are on the time and costs spent on message tracking, quarantine management and dealing with false positives. However, an integrated single-vendor hybrid solution can provide timesavings across all of the areas that we analyzed. These differences are due primarily to the fact that an integrated hybrid solution offers a number of advantages relative to a homegrown hybrid solution, including:

- A single console that can be used to manage policy, message isolation queues, and message tracking across both on premises and SaaS components instead of two separate consoles managing two separate products
- The ability to generate reports more easily and more quickly because a single console can be used to produce these reports.
- Resolving user issues, such as lost or missing emails, is easier with a single system with integrated message tracking than when using two separate systems

- Single message quarantine in an integrated system vs. managing two disparate isolation queues in two different systems
- Further, when using a virtual appliance for the integrated hybrid approach, as was the case in our analysis, the physical hardware in use can be used for other server functions, as well, driving down the cost of the integrated hybrid solution.

The primary result of these differences is a significant savings in IT labor required to address these issues, coupled with some level of savings from the use of a virtualized server infrastructure in the integrated approach.

In short, an integrated hybrid SaaS email security solution offered by a single vendor and that uses a single management console can provide substantial IT labor savings over a hybrid solution that is built using competing vendors' offerings.

TRADITIONAL ON-PREMISES VS. SINGLE-VENDOR INTEGRATED HYBRID SAAS

Our research found that an integrated hybrid email security solution from a single vendor is also less expensive than a traditional, on-premise only solution, although the cost delta is smaller, as shown in the following tables and figure.

Three-Year Costs per Seat for Homegrown vs. Integrated Hybrid SaaS Email Security Solutions

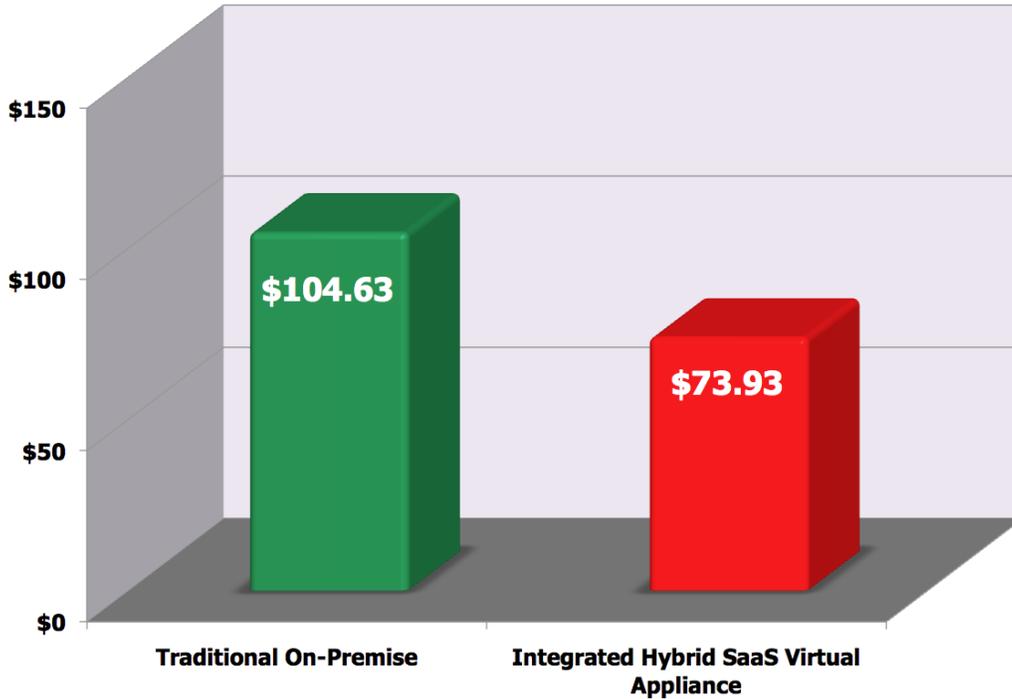
Cost Component	Traditional On-Premise	Integrated Hybrid
Physical infrastructure, including support	\$72.09	\$44.86 ²
SUBTOTAL	\$72.09	\$44.86

Person-Hours Required per 1,000 Users per Week for Homegrown vs. Integrated Hybrid Email Security Solutions (Person-hours per 1,000 Users per Week)

Cost Component	Traditional On-Premise	Integrated Hybrid
Messaging tracking	1.25	1.35
Resolving user issues	0.58	2.09
Quarantine management	0.57	0.29
Dealing with false positives	2.09	0.57
Other security infrastructure issues	0.20	0.27
Integrating report data	0.54	0.10
Server, OS, etc. management issues	0.02	0.02
TOTAL PERSON-HOURS	5.26	4.70
TOTAL COST OF LABOR, YEAR 1	\$10.53	\$9.41
TOTAL COST OF LABOR, YEAR 2	\$10.84	\$9.69
TOTAL COST OF LABOR, YEAR 3	\$11.17	\$9.98
TOTAL THREE-YEAR COST OF LABOR	\$32.54	\$29.08

² Includes cost of cloud-based service and three-year support.

Cost of Homegrown vs. Integrated Hybrid SaaS Email Security Solutions



Our research found that labor represents a smaller proportion of the total cost of an on-premise solution than for a homegrown hybrid solution.

WHY IS AN INTEGRATED HYBRID SOLUTION LESS EXPENSIVE THAN A TRADITIONAL ON PREMISE-ONLY SOLUTION?

So, what benefits do enterprises achieve in moving from an on-premise email security infrastructure to an integrated hybrid approach that uses a combination of on-premise and cloud-based infrastructure? At first glance, the latter approach would seem to be more complex and, hence, more costly simply because it has more moving parts to manage. However, an integrated hybrid security system is actually less expensive – \$73.93 per seat over three years compared to an average of \$104.63 (per seat over three years for a purely on-premise system). There are several reasons for the cost savings:

The chief cost savings from an integrated hybrid approach is the ability to avoid regular additions to the on-premise infrastructure as spam and malware volumes rise for inbound email filtering. For example, when planning an email security infrastructure for a three-year period, capacity planners have two choices:

- Forecast the total volume of spam and malware over three years and build out the infrastructure today to accommodate the anticipated volumes in three years.

- Build out the infrastructure for spam and malware volumes today and then add new servers and/or appliances over time as volumes increase.

Consequently, an on-premise infrastructure will require either a) initial overcapacity or b) regular additions to capacity over time, in either case adding to the cost of the on-premise infrastructure. An integrated hybrid system (or even a homegrown hybrid system, for that matter) will not require these additions to the on-premise component because the hosted system absorbs these increases in spam and malware volumes without cost increases borne by customers.

- Outbound filtering and granular content control is done on a virtual appliance in our analysis, which means the cost of the hardware devoted to email security is actually less than in a traditional, on-premise infrastructure.
- Miscellaneous IT labor tasks associated with server management, such as applying patches and upgrades, are lower in an integrated hybrid system on a virtual appliance.

Summary

An integrated hybrid email security solution from a single vendor is less expensive than either a hybrid solution comprised of an on-premise infrastructure layered with a different vendor's hosted offering (a homegrown hybrid solution) or a traditional, on-premise security solution. The cost savings come primarily from labor savings with the integrated approach, as well as reduced requirements to accommodate growth to meet growing volumes of spam and malware.

About Trend Micro InterScan Messaging Security Virtual Appliance – Integrated Hybrid SaaS Email Security

Trend Micro™ InterScan™ Messaging Security Virtual Appliance is a hybrid SaaS email security solution that integrates proactive protection in the cloud with the privacy and control of an on-premise, virtual appliance.

In-the-cloud security reduces inbound email volumes up to 90% by blocking spam and malware outside your network. This SaaS security is integrated with the VMware Ready virtual appliance at the gateway allowing flexible control over sensitive information. And local quarantines ensure your email stays private because no email is stored in the cloud. With Trend Micro's hybrid SaaS email security you can reduce complexity and overhead to realize significant cost savings.

Purpose-built SaaS-in-the-cloud security

- Trend Micro™ Smart Protection Network™ cloud security infrastructure stops threats before they reach your network

- Web reputation blocks access to malicious websites
- Email reputation blocks unwanted email
- Layered antispam composite engine adds additional filtering
- Industry leading anti-malware ensures emails and attachments are virus free

On-premise VMware Ready virtual appliance

- Customizable rules for scanning inbound and outbound emails and attachments
- Flexible policies to target senders or recipients by company, group, or individual
- Supports data loss prevention, regulatory compliance and corporate governance

For more information, please visit www.trendmicro.com/hybridSaaS.

Appendix A – Cost Model Assumptions

- Fully burdened salary for IT staff members: \$80,000 annually
- Annual salary growth: 3%
- Server used for on-premise only environment: Dell PowerEdge R710 (\$7,294)
- Server used for hybrid environment: Dell PowerEdge 2970 (\$4,692)}
- Appliances used for the on-premise and hybrid environments: the average of three leading solutions from major vendors
- Annual cost of server maintenance: 18%
- Annual cost of software maintenance 35%-40%
- Users supported per server for non-Trend Micro environments: 1,500
- Users supported per appliance for non-Trend Micro environments: 3,000
- Users supported per server/virtualized appliance for Trend Micro environments: 3,000
- Data center costs for non-Trend Micro environments: \$27.01 per user over three years
- Data center costs for Trend Micro environments: \$9.00 per user over three years because one-third of each server/appliance is dedicated to security
- Hosted security cost: \$1.00 per user per month

© 2010 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.