Comparing Leading Email and SharePoint Security Solutions

An Osterman Research White Paper

Published April 2010

SPONSORED BY

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

Why You Should Read This Report

There are new and sophisticated threats directed against email systems from a variety of new sources. Not only are spam volumes roughly doubling every 12 months, but malware is becoming more difficult to detect and remediate. As a result, robust anti-spam, anti-virus and other malware defenses are essential to the health of any organization's email infrastructure.

To improve the effectiveness of these defenses, vendors are turning more to cloud-based capabilities that will supplement on-premise infrastructure in order to provide a more secure environment. Further, organizations will look to make their defenses easier to deploy and manage (an added benefit of cloud-based elements in the defense infrastructure) driving costs as low as possible.

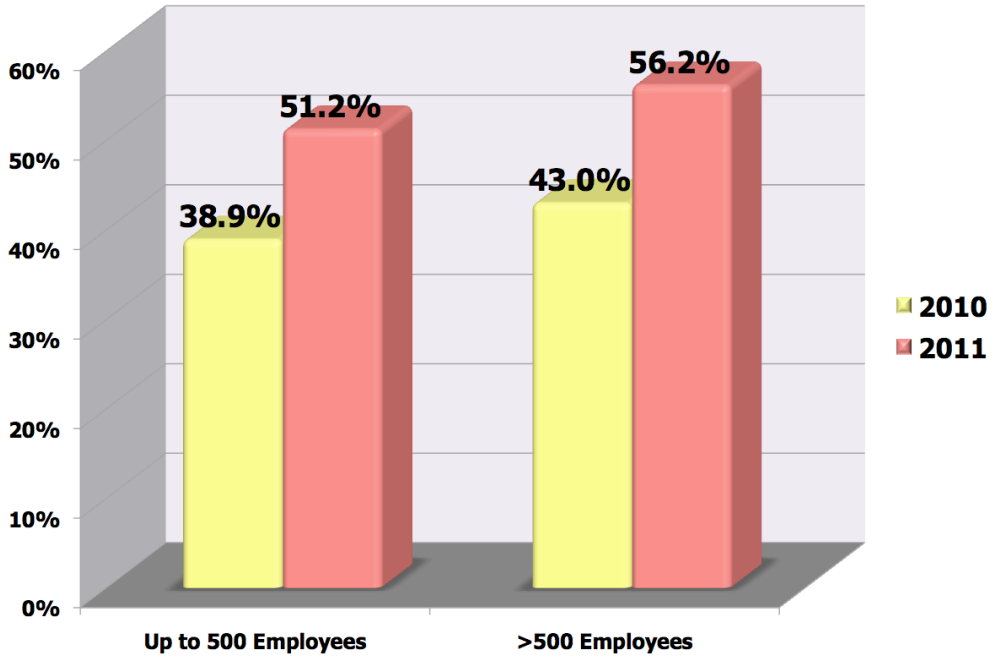
SHAREPOINT IS A GROWING THREAT VECTOR

However, email is not the only threat vector that decision makers must manage. Microsoft SharePoint – rapidly becoming the de facto collaboration environment for Microsoft Exchange-enabled organizations – must also be protected from threats that are potentially carried in the growing number of documents managed in SharePoint environments and/or embedded within its Web 2.0 capabilities (team sites, portals, blogs, wikis, etc.).

It is important to note that because SharePoint sites can include external Web content, it is vital to protect against the growing number of Web-borne threats that might be included in SharePoint portals, team sites, etc.

THE USE OF SHAREPOINT IS GROWING

The importance of SharePoint in the context of security is underscored by the growing proportion of organizations that have deployed it. For example, in a March 2010 survey conducted by Osterman Research, we found that current penetration of SharePoint is at 39% of email users in Exchange-enabled organizations of up to 500 users – in larger Exchange-enabled organizations, 43% of email users employ SharePoint. The survey also found that SharePoint use will grow significantly – to 51% of users in smaller organizations and 56% in larger ones, representing growth of more than 30% in just the next 12 months, as shown in the following figure.



KEY TAKEAWAYS

- Decision makers must study cost of ownership over an appropriate period of time when comparing competing solutions. Osterman Research has found that many organizations do not fully understand their messaging-related costs and cannot estimate them with even reasonable accuracy in most cases. In a slow economy, understanding ownership costs will become even more important.

- Protecting the email and collaboration infrastructure remains absolutely necessary and will become more so given the increasing level of threats. Organizations must focus on solutions that provide the highest level of threat protection.

- At the same time, decision makers realize that deploying capabilities to protect email servers and collaboration tools can be expensive, costs that are driven primarily by the labor required to maintain these systems. Organizations should, therefore, understand the costs of their current solutions and deploy solutions that will lower these costs.

- Decision makers must also study the roadmap of prospective vendors of email- and collaboration-protection solutions. This is a critical step in the due diligence phase for selecting any new threat detection and remediation solution for two reasons. First, it will help decision makers understand whether or not vendors on their short list will stay ahead of malware developers, spammers and other malicious types. Second, understanding a vendor's roadmap – such as knowing how cloud-based services will factor into current and/or future solutions – will help decision-makers know what the long-term impacts of vendor choice will be on their cost of ownership.

Total Cost of Ownership for SharePoint Security

COST OF OWNERSHIP CALCULATIONS

Total cost of ownership (over a three-year period) for SharePoint security varies significantly depending on the solution in question, ranging from $177,575 (Trend Micro) to $269,638 (Microsoft) for the average 2,500-user organization, as shown in the following tables.

Within the total cost of ownership, labor costs to deploy, manage and upgrade the system account for roughly 70-80% of the total cost. Further, that labor cost is primarily (90-93%) driven by time spent for ongoing administration activities.

Given that the majority of total cost of ownership for SharePoint security is in labor rather than software cost, organizations should be sure to take both factors into account when minimizing IT cost is a priority.

Total Cost of Ownership
Over a Three-Year Period
(Median IT person-hours plus public pricing)

	Trend Micro	Symantec	Microsoft	McAfee
TOTAL DEPLOYMENT, MANAGEMENT & UPGRADE EFFORT (3 Years)	**$125,775**	**$134,933**	**$215,638**	**$185,829**
Initial Installation (1)	$5,885	$3,185	$6,314	$6,474
Product Upgrade (1)	$2,278	$2,799	$2,714	$2,209
Annual Ongoing Administration (3 Years)	$113,490	$126,100	$201,760	$173,388
Annual Problem Resolution (3 Years)	$4,123	$2,849	$4,850	$3,759
TOTAL SOFTWARE COST (3 Years)	**$51,800**	**$47,425**	**$54,000**	**$73,875**
Initial Purchase Cost (2,500 users)	$32,350	$22,475	$18,000	$41,025
Annual Software Renewal Cost	$19,450	$24,950	$36,000	$32,850
TOTAL COST OF OWNERSHIP	**$177,575**	**$182,358**	**$269,638**	**$259,704**

Total Cost of
Ownership per User

Cost	Trend Micro	Symantec	Microsoft	McAfee
Total three-year cost per user	$71.03	$72.94	$107.86	$103.88
Average annual cost per user	$23.68	$24.31	$35.95	$34.63
Average monthly cost per user	$1.97	$2.03	$3.00	$2.89

TIME SPENT DEPLOYING, MANAGING AND UPGRADING SYSTEMS

Looking more closely within that labor cost, we see that total effort over a three-year period, on average, ranges from just over 3,100 hours over three years to just over 5,300 hours (a delta of 71%) to manage a large-scale deployment for SharePoint security.

This variability is almost entirely a function of the time spent on ongoing SharePoint security management (roughly 90% of total effort spent managing each product), which ranges from roughly 2,800 hours for Trend Micro product to almost 5,000 hours for Microsoft's (a delta of 78%).

Most respondents reported roughly the same installation effort, except for Symantec's offering which seemed to be the easiest to install. Upgrade effort was reported to be largely the same across all vendors.

IT Person-Hours Required
Over a Three-Year Period
(Median IT person-hours)

	Trend Micro	Symantec	Microsoft	McAfee
TOTAL DEPLOYMENT, MANAGEMENT & UPGRADE EFFORT (3 Years)	**3,116.7**	**3,339.8**	**5,340.2**	**4,603.4**
Initial Installation (1)	153.0	82.8	164.2	168.3
Product Upgrade (1)	53.7	66.0	64.0	52.1
Annual Ongoing Administration (3 Years)	2,808.0	3,120.0	4,992.0	4,290.0
Annual Problem Resolution (3Years)	102.0	70.5	120.0	93.0

With the majority of labor cost spent on ongoing administration, those organizations with limited IT staff and/or those seeking to free up staff for other projects should pay close attention to this aspect of SharePoint security.

Given the weak economic conditions worldwide at the time of this writing, Osterman Research anticipates that there will be particular emphasis on cost containment and operational efficiencies during 2009.

ONGOING ADMINISTRATION IS THE MOST CRITICAL CONSIDERATION

Regardless of vendor, 90-93% of the total management time required for SharePoint security is spent on ongoing administration. All efforts – system monitoring, reporting, group/configuration management and quarantine management – require substantial time, rather than one effort in particular taking the majority.

Overall, administrators reported spending between 18 (for Trend Micro) and 32 (for Microsoft) hours per week (or 936 to 1,664 hours per year) on such management, a difference of up to 78% more depending on vendor. Problem resolution each year was

roughly the same, ranging from 23 (for Symantec) to 40 (for Microsoft) hours.

IT Person-Hours Required
for Ongoing Management
(Median IT person-hours per week unless otherwise noted)

	Trend Micro	Symantec	Microsoft	McAfee
TOTAL ONGOING MANAGEMENT	**18.0**	**20.0**	**32.0**	**27.5**
General System Monitoring	5.0	5.0	8.0	8.0
Creation of Reports	5.0	3.0	8.0	5.0
Quarantine Management	2.5	4.0	5.0	4.0
Group or Configuration Changes	3.0	4.0	6.0	6.0
Other Ongoing Administration	2.5	4.0	5.0	4.5
TOTAL ONGOING MANAGEMENT (per year)	**936**	**1,040**	**1,664**	**1,430**
PROBLEM REMEDIATION (per year)	**34.0**	**23.5**	**40.0**	**31.0**
TOTAL PERSON-HOURS	**970.0**	**1,063.5**	**1,704.0**	**1,461.0**

With organizations bringing on, or gaining central control over, new electronic communication and collaboration systems like SharePoint, minimizing the administration- including security administration- related to such systems is critical.

While organizations always want to avoid unforseen issues with their communication and collaboration systems, from a level of effort standpoint, the time spent addressing them is negligible within even the ongoing administrative efforts over the course of a year, regardless of vendor.

ONE-TIME DEPLOYMENT/UPGRADE EFFORT ALSO VARIES

In general, the initial deployment of SharePoint security generally takes three times as much time as an upgrade- except in the case of Symantec, where administrators reported roughly the same amount of time for both activities. That time for installation ranges from 83 hours (for Symantec) to 168 hours (for McAfee). Regardless of vendor, product configuration is generally the most time consuming activity- even compared to pilot testing- of installation.

IT Person-Hours Required
for Initial Deployment Activities
(Median IT person-hours per year)

Activity	Trend Micro	Symantec	Microsoft	McAfee
Initial installation	40.0	10.0	34.0	40.0
Initial configuration	53.0	40.8	71.7	63.3
Other initial efforts	44.0	12.0	18.5	25.0
Initial pilot testing	16.0	20.0	40.0	40.0
Upgrade installation	19.0	20.0	26.7	6.7
Upgrade configuration	23.0	20.0	24.0	32.5
Other upgrade efforts	11.7	26.0	13.3	12.9
TOTAL – INITIAL	**153.0**	**82.8**	**164.2**	**168.3**
TOTAL – UPGRADE	**53.7**	**66.0**	**64.0**	**52.1**

There is no one vendor that excelled at both the initial task of installation and the later task of upgrade (inclusive of configuration and testing), but there was definitely more variability in the installation effort, so this is something organizations should consider at the time of their first purchase. In terms of the complexity of these activities, a mean of 24% of respondents reported that complexity of these activities was "high". However, only 12% of Symantec respondents reported that these activities were highly complex, while 36% of Microsoft respondents did so. Of course, looking at the bigger picture, given that these one-time administrative efforts account for roughly 100 hours, compared to the roughly 1,000 hours or more of ongoing administration each year, organizations should keep them in perspective.

Total Cost of Ownership: Mail Server Security

As with collaboration server security, total cost of ownership varies widely, and can almost double, depending on the solution, ranging from $141,237 (for Trend Micro) to $271,513 (for Microsoft) for the average 2,500-user organization, as shown in the following tables. The largest determinant of mail server security is, again, TCO is administrative effort (generally 65% to 70% of TCO). Within total administrative effort, ongoing, day-to-day administration of the solution accounts for the majority (80%-90%) of that effort.

Total Cost of Ownership
Over a Three-Year Period
(Median IT person-hours plus public pricing)

	Trend Micro	Symantec	Microsoft	McAfee
TOTAL DEPLOYMENT, MANAGEMENT & UPGRADE EFFORT (3 Years)	**$92,157**	**$167,908**	**$190,513**	**$117,698**
Initial Installation (1)	$4,077	$11,231	$6,885	$4,250
Product Upgrade (1)	$2,841	$3,053	$6,351	$2,989
Annual Ongoing Administration (3 Years)	$75,660	$145,015	$173,388	$104,033
Annual Problem Resolution (3 Years)	$9,579	$8,609	$3,880	$6,426
TOTAL SOFTWARE COST (3 Years)	**$49,080**	**$69,200**	**$81,000**	**$84,825**
Initial Purchase Cost (2,500 users)	$30,675	$43,250	$27,000	$40,725
Annual Software Renewal Cost	$18,405	$25,950	$54,000	$44,100
TOTAL COST OF OWNERSHIP	**$141,237**	**$237,108**	**$271,513**	**$202,523**

Total Cost of
Ownership Per User

Cost	Trend Micro	Symantec	Microsoft	McAfee
Total three-year cost per user	$56.49	$94.84	$108.61	$81.01
Average annual cost per user	$18.83	$31.61	$36.20	$27.00
Average monthly cost per user	$1.57	$2.63	$3.02	$2.25

Organizations should carefully evaluate all of the costs of ownership for any messaging security solution, taking care not to underestimate any of these costs. This is particularly true for the costs of administrative labor, since these are a significant percentage of TCO, but often less visible during evaluation.

TIME SPENT DEPLOYING, MANAGING AND UPGRADING SYSTEMS OVER A THREE-YEAR PERIOD

There was great variability across vendors in time spent on mail server security management (initial installation, subsequent upgrade and ongoing administration), as shown in the following table. Variability in the amount of administration time required by mail server security solutions ranges from 2,282 hours (for Trend Micro) to 4,715 hours (for Microsoft) over the three-year period (a delta of 106%). This variability is largely a function of ongoing administration, which accounts for 80%-90% of total effort. Time spent on installation, upgrade and problem resolution does vary as well, but accounts for a relatively small percentage of administration.

IT Person-Hours Required
Over a Three-Year Period
(Median IT person-hours)

	Trend Micro	Symantec	Microsoft	McAfee
TOTAL DEPLOYMENT, MANAGEMENT & UPGRADE EFFORT (3 Years)	**2,282**	**4,165**	**4,715**	**2,914**
Initial Installation (1)	106.0	292.0	179.0	110.5
Product Upgrade (1)	67.0	72.0	150.0	70.5
Annual Ongoing Administration (3 Years)	1,872.0	3,588.0	4,290.0	2,574.0
Annual Problem Resolution (3Years)	237.0	213.0	96.0	159.0

While organizations are naturally hesitant to change security solutions, in many cases an extra one-time effort to install a new solution (even more so when an upgrade of the current solution is planned) can result in a dramatic reduction in overall administrative effort.

ONGOING MANAGEMENT IS THE MOST CRITICAL CONSIDERATION

Regardless of vendor, ongoing management accounted for roughly 80%-90% of the total management effort. While all activities represented substantive effort, system monitoring and creation of reports seemed to be more labor intensive than quarantine or configuration management. Overall, organizations reported between 12 hours (for Trend Micro) and 27.5 (for Microsoft hours per week (624 to 1430 hours per year) for ongoing administration- more than twice as much time depending on product. Regardless of vendor, administrators reported spending the most time on system monitoring, although for certain vendors configuration and report creation also required substantial effort. For problem resolution, time spent ranged from 32 (for Microsoft) to 79 (for Trend Micro) hours per year.

IT Person-Hours Required
for Ongoing Management
(Median IT person-hours per week unless otherwise noted)

	Trend Micro	Symantec	Microsoft	McAfee
TOTAL ONGOING MANAGEMENT (per week)	**12.0**	**23.0**	**27.5**	**16.5**
General System Monitoring	5.0	8.0	7.5	5.0
Creation of Reports	2.5	5.0	9.0	4.5
Quarantine Management	2.5	5.0	5.0	4.5
Group or configuration changes	2.0	5.0	6.0	2.5
TOTAL ONGOING MANAGEMENT (per year)	**624**	**1,196**	**1,430**	**858**
PROBLEM REMEDIATION (per year)	**79.0**	**71.0**	**32.0**	**53.0**
TOTAL PERSON-HOURS	**703**	**1,267**	**1,462**	**911**

Because organizations are continually trying to do more with less, in many cases a change in mail server security products can free up substantial staff time.

ONE-TIME DEPLOYMENT EFFORT ALSO VARIES GREATLY

Administrators reported that initial deployment took between 106 (for Trend Micro) and 292 (for Symantec) hours. Initial deployment time was largely spent on the initial installation, although configuration and pilot testing were also substantial efforts. For an upgrade, administrators reported between 67 (for Trend Micro) and 150 (for Microsoft) hours.

IT Person-Hours Required
for Initial Deployment Activities
(Median IT person-hours per year)

Activity	Trend Micro	Symantec	Microsoft	McAfee
Initial installation	37.0	200.0	70.0	48.0
Initial configuration	30.0	36.0	53.5	26.5
Other initial efforts	8.0	11.0	15.5	10.0
Initial pilot testing	31.0	45.0	40.0	26.0
Upgrade installation	29.0	25.0	81.0	34.0
Upgrade configuration	30.0	36.0	53.5	26.5
Other upgrade efforts	8.0	11.0	15.5	0.0
TOTAL – INITIAL	**106.0**	**292.0**	**179.0**	**110.5**
TOTAL – UPGRADE	**67.0**	**72.0**	**150.0**	**70.5**

With the new installation time for Trend or McAfee taking the same (or less) time as a Symantec or Microsoft upgrade, the latter times provide opportunities for organizations to consider a change in vendor to one of the former. Interestingly, 60%-70% of respondents indicated that they were either satisfied or very satisfied with the time

reported for product installation (including product configuration) except for Symantec customers, less than half (46%) of whom were satisfied or very satisfied.

Conclusions

From this research as a whole, a number of higher level insights can be drawn.

- While published software prices do vary, they have a relatively small impact on total cost of ownership.
- On average, enterprises are spending between roughly $319,000 and $540,000 on messaging and collaboration security together, depending on the products they choose (a delta of 70% more).
- Between two-thirds (65%) and three quarters (75%) of that cost is related to staff time reported for the deployment and ongoing administration of security, with the remainder spent on software costs.
- Time spent on deployment and management varies between ~5,400 hours and 10,000 hours managing security over a three-year period – a difference of 4,656 hours or 2.5 person years depending on vendor selected.
- This variability is predominantly a function of the amount of time spent on routine, ongoing administration of the respective products which accounts for 86% to 93% of the total effort reported by administrators.

Total Cost of Ownership
Over a Three-Year Period
(Median IT person-hours plus public pricing)

	Trend Micro	Symantec	Microsoft	McAfee
TOTAL DEPLOYMENT, MANAGEMENT & UPGRADE EFFORT (3 Years)	**$217,932**	**$302,841**	**$406,151**	**$303,103**
Initial Installation (1)	$9,962	$14,416	$13,199	$10,724
Product Upgrade (1)	$5,119	$5,852	$9,074	$4,774
Annual Ongoing Administration (3 Years)	$189,150	$271,115	$375,148	$277,420
Annual Problem Resolution (3 Years)	$13,701	$11,458	$8,730	$10,185
TOTAL SOFTWARE COST (3 Years)	**$100,880**	**$116,625**	**$135,000**	**$158,700**
Initial Purchase Cost (2,500 users)	$63,025	$65,725	$45,000	$81,750
Annual Software Renewal Cost	$37,855	$50,900	$90,000	$76,950
TOTAL COST OF OWNERSHIP	**$318,812**	**$419,466**	**$541,151**	**$461,803**

Organizations should be sure to consider the total (both staff and software) cost of ownership when making a decision about mail server or collaboration server. Even more so when relying on both mail and collaboration server security and especially in today's economic environment.

Our findings indicate that Trend Micro offers a clear cost advantage based on the data generated from this research, most notably for mail server security. For example, the cost of combined mail server and SharePoint security is shown in the following table.

Total Cost of Ownership per User
Mail Server Security and SharePoint Security

Cost	Trend Micro	Symantec	Microsoft	McAfee
Total three-year cost per user	$127.52	$167.79	$216.46	$184.72
Average annual cost per user	$42.51	$55.93	$72.15	$61.57
Average monthly cost per user	$3.54	$4.66	$6.01	$5.13
DIFFERENCE COMPARED TO LOWEST COST SOLUTION	**100%**	**132%**	**170%**	**145%**

Background and Methodology

Trend Micro commissioned Osterman Research to conduct blind surveys of enterprises that have deployed one or more of the following solutions:

MAIL SERVER SECURITY

- Trend Micro ScanMail for Microsoft Exchange 7.0 or later
- Symantec Mail Security for Exchange 5.0 or later
- Microsoft/Sybari Antigen for Exchange 8.0 or later
- McAfee GroupShield for Exchange 5.0 or later

SHAREPOINT SECURITY

- Trend Micro PortalProtect 1.5 or later
- Symantec Antivirus for SharePoint 4.3 or later
- Microsoft/Sybari ForeFront/Antigen for SharePoint 7.5 or later
- McAfee PortalShield for Microsoft SharePoint 5.0 or later

In order to qualify for inclusion in this research program, respondent organizations had to have (with a few minor exceptions):

- The system deployed for at least six months
- At least 500 employees
- Microsoft clusters in place
- Deployed both anti-spam and anti-virus protection

Further, the organizations surveyed could not be a reseller of security solutions.

The median number of employees in the organizations surveyed was apprxomately 2,500.

A combination of telephone and Web-based surveys were conducted with members from the extensive Osterman Research survey panel database. These individuals, from organizations in the US and Europe, were selected randomly. In addition, secondary information was used for pricing data.

A total of 101 mail server security surveys were completed, distributed as follows:

- Trend Micro ScanMail – 31 surveys
- Symantec Mail Security – 31 surveys
- Microsoft/Sybari Antigen – 16 surveys
- McAfee GroupShield – 23 surveys

A total of 112 mail server security surveys were completed, distributed as follows:

- Trend Micro PortalProtect – 23 surveys
- Symantec Antivirus for SharePoint – 38 surveys
- Microsoft/Sybari Forefront/Antigen for SharePoint – 35 surveys
- McAfee PortalShield for Microsoft SharePoint – 16 surveys

Cost elements quantified through the survey included:

- Product installation
- Product configuration
- Pilot testing
- Product upgrade
- Routine operational administration
- Other administration

ABOUT THIS WHITE PAPER

This report discusses the results of two separate research programs that were focused on four leading mail server security solutions designed for Microsoft Exchange environments, as well as SharePoint collaboration server security solutions. The four solutions – from Trend Micro, Symantec, Microsoft and McAfee – were the focus of a research program conducted with messaging decision makers.

Osterman Research conducted independent surveys of enterprise-level IT administrators from the United States and Europe. The majority were surveyed online, while some were surveyed by telephone. The goal of this research was to assess the time and other investments that their organizations have made in the testing, licensing, deployment and ongoing management of their mail server and collaboration security solutions. Based on these inputs, two cost models (one for email and one for collaboration) were developed to analyze the total cost of ownership for the various solutions. The data generated from the research, as well as the conclusions of the cost model, are presented in this document.

Survey respondents were chosen randomly and no culling or selection of respondents was conducted to give one vendor an advantage over any other. A full discussion of the methodology for this research is provided at the end of the report.

It is important to note that while there are significant differences in the cost of ownership among the various offerings discussed in this report, these are all established offerings from well-respected vendors – albeit with differences in technology and effectiveness, but those are factors outside the scope of this survey.