WHITE PAPER

A Cloud-Client Architecture Provides Increased Security at Lower Cost

An Osterman Research White Paper

Published January 2012

SPONSORED BY

TREND MICRO™

OSTERMANRESEARCH

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

Reducing Security Costs and Improving Protection

Despite improvements in Internet security over the past several years, malware, spam and a growing variety of other threats are creating an even more dangerous threat landscape for organizations of all sizes:

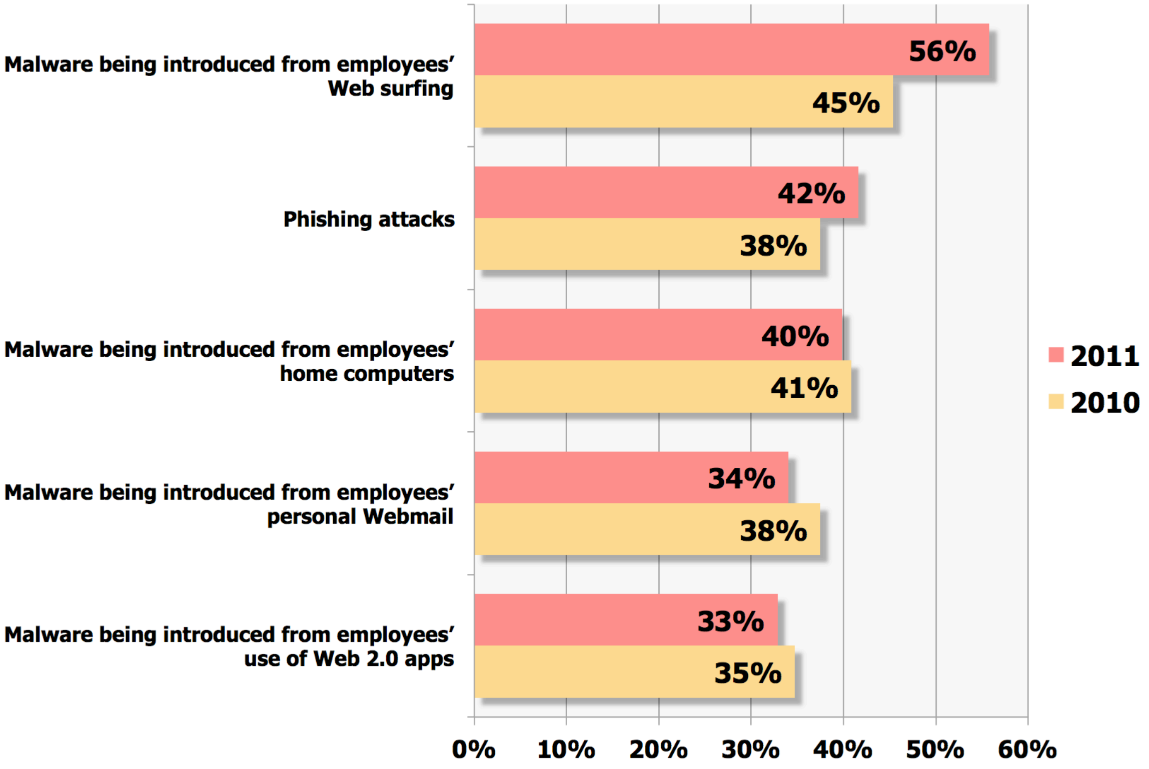
- Spammers have reduced their emphasis from the traditional "carpet bombing" of messages delivered through email and are now more focused on targeted phishing and spearphishing attacks to deliver malware. This, along with the takedown of a couple of major botnets, has resulted in a significant reduction in the amount of spam that is being delivered relative to a year ago.

- However, because attacks are now more targeted and more likely to lead to the infection of malware, the reduction in spam has coincided with a significant increase in the threat level faced by email users.

- Moreover, the past few years has seen a significant increase in the sophistication and severity of Web-based threats.

- The result has been growing concern about both Web-based threats and advanced targeted attacks during the past year, as shown in the following figure.

IT Decision Maker Concerns About Various Security Issues, 2010 and 2011



KEY TAKEAWAYS

All of this said, if an organization of any size could significantly reduce the length of time required to access threat intelligence using in-the-cloud reputation databases to block new malware and spam variants before they even reach the network, it could reduce the rate of endpoint infection, lower overall security management and lost productivity costs, and reduce the likelihood of security breaches. Moreover, if an organization opted to combine these activities with the consolidation of its Internet content security infrastructure to just a single vendor, the advantages and cost savings would be even greater.

In an enterprise with 5,000 employees:

- *52% of endpoints get infected each year*
- *$230,880 in employee productivity and IT labor is lost from these infections*

If the enterprise employed a cloud-client security architecture from a single vendor:

- *It could save $49 per employee per year*
- *It could reduce its security costs by 41%*

This white paper discusses the various benefits of more rapid access to threat intelligence, using a cloud-client architecture for immediate protection, as well as the benefits to enterprises of consolidating to a single vendor for Internet content security infrastructure. Together these benefits can save more than 40% of an enterprise's total security management costs, not to mention savings on reduced productivity loss, a reduced number of security breaches and other, less tangible costs. The paper discusses the calculations developed by Osterman Research specifically for this white paper, as well as the solutions offered by Trend Micro that can significantly improve an organization's Internet content security infrastructure.

BACKGROUND AND METHODOLOGY

A key part of this white paper development effort was an Osterman Research survey conducted during October and early November 2011 with more than 100 organizations. The goal of this survey was to determine the costs of IT labor focused on security management, the likelihood and cost of data breaches arising from security problems, the perceived benefits of improved pattern updates, the perceived benefits of using a single vendor for security management, and other issues. The organizations surveyed have a median of 1,500 employees and 1,350 email users.

Security Must Address New IT Trends

CONSUMERIZATION OF IT = MORE ENDPOINTS

There are a growing number of endpoints through which malware can enter an organization's network, including servers, traditional email clients on desktop and laptop computers, corporate and personal Webmail, Web browsers, collaborative tools, smartphones, tablets, instant messaging clients, employees' home computers, USB storage devices, and other systems.

We hear a significant amount about the consumerization of IT (which we could also call the democratization of IT) although there may be some difference of opinion about what that actually means. In essence, the consumerization of IT encompasses three basic concepts:

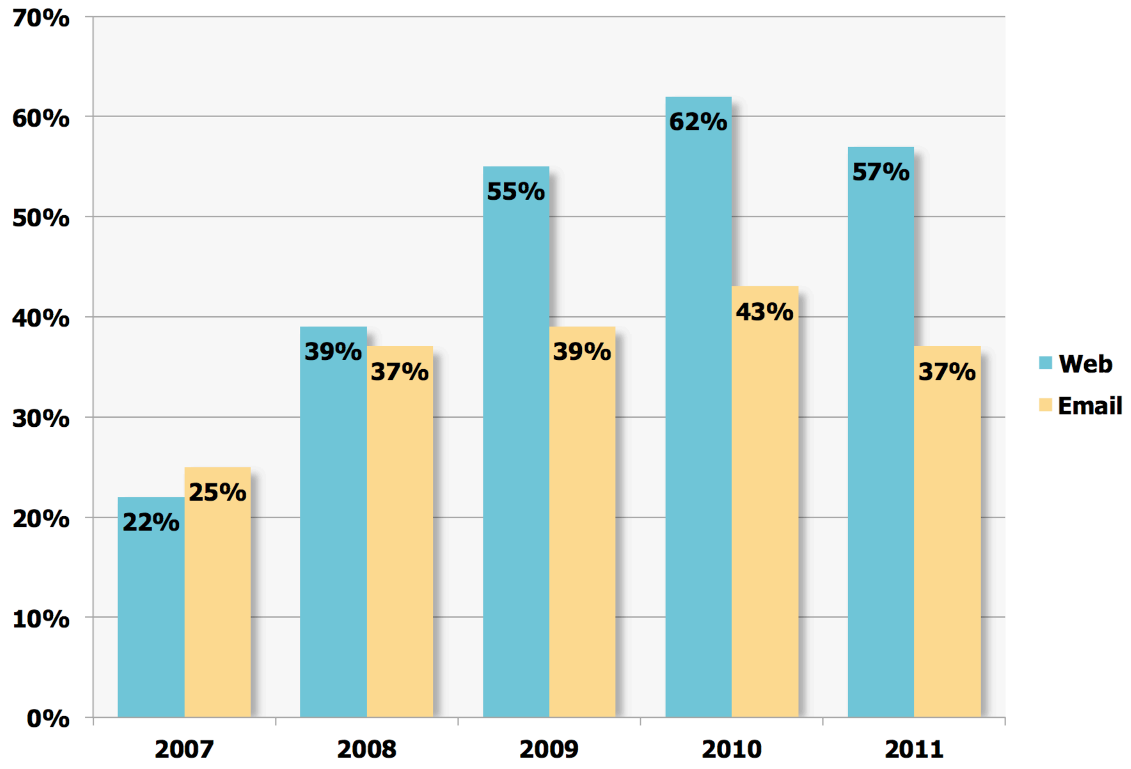
- The use of non-traditional, "consumerish" tools in a workplace environment, including Facebook, YouTube and other Web 2.0 applications.
- The mixed use of personal devices for work-related applications, such as smartphones, tablets, personal Webmail, etc.
- The notion that IT's role is changing from one of dictating the infrastructure to a role more like that of a traffic cop – simply trying to manage anything and everything that users employ to access work-related resources.

Every endpoint represents a potential entry point for a virus, worm, Trojan horse or some other form of malware to gain a foothold in the corporate network. Today, malware is part of a cybercrime economy and cyber criminals are using multiple endpoints and delivery mechanisms to steal data and resources. The more popular the use of the business tool, the more often it is targeted by the cyber criminals.

MALWARE IS GETTING WORSE

Gone are the days when single variants of spam, viruses, and worms were created and propagated slowly over the Internet, spreading over the course of several weeks. Instead, today's malware can morph into hundreds or thousands of variants and can propagate in minutes, infecting large numbers of endpoints in a very short period of time. The result has been growing penetration of both Web-based and email-based malware, despite a slight drop in 2011, as shown in the following figure.

Proportion of Organizations Reporting a Successful Security Violation by Mode
2007 through 2011



MORE THAN 50% OF ENDPOINTS ARE INFECTED EACH YEAR

The result of the growing number of endpoints, coupled with more virulent and more capable malware, is that endpoint infections are numerous. Our research found that during a typical month, 4.3% of endpoints are infected with malware, resulting in more than 50% of endpoints becoming infected over the course of 12 months. This means that in an organization of 5,000 endpoints, 2,580 will be infected over a year's time.

CLEANING INFECTIONS IS TIME-CONSUMING AND EXPENSIVE

Our research also found that a mean of 77 minutes of elapsed time is required to clean an infected endpoint from the time the infection is detected until it is completely resolved. This results in both employees being much less productive during the time that their endpoints are being restored, as well as lost IT time to remediate the problems.

The result for a 5,000-endpoint company is that an average of 215 endpoints will become infected during a typical month and 276 hours of elapsed time will be consumed addressing the problem. If we assume that the average, fully-burdened, annual salaries for non-IT and IT staff members is $65,000 and $80,000 respectively, this translates into a monthly productivity loss of $8,625 for non-IT staff[1] and $10,615 for IT staff, or a total monthly cost of $19,240.

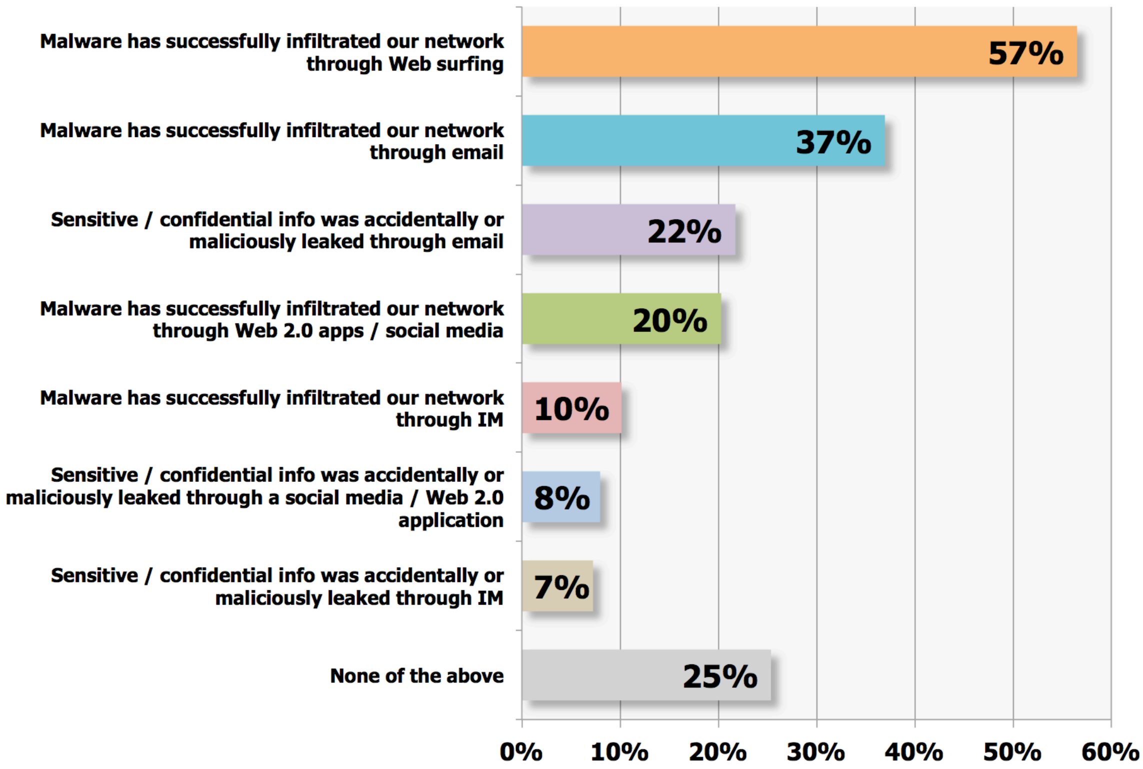
[1] Assumes that end users are not productive while waiting for their computer to be repaired.

The bottom line is that organizations spend significant amounts just on cleaning endpoints from various types of malware infections: the combination of non-IT and IT costs totals $230,880 in a typical 5,000-employee company each year.

SECURITY BREACHES ARE ANOTHER THREAT

Our research has also found that security breaches are very common, with nearly three out of five reporting a Web-based security breach during the past 12 months and more than one-third reporting an email security breach during the same period, as shown in the following figure.

Security Incidents That Have Occurred During the Previous 12 Months

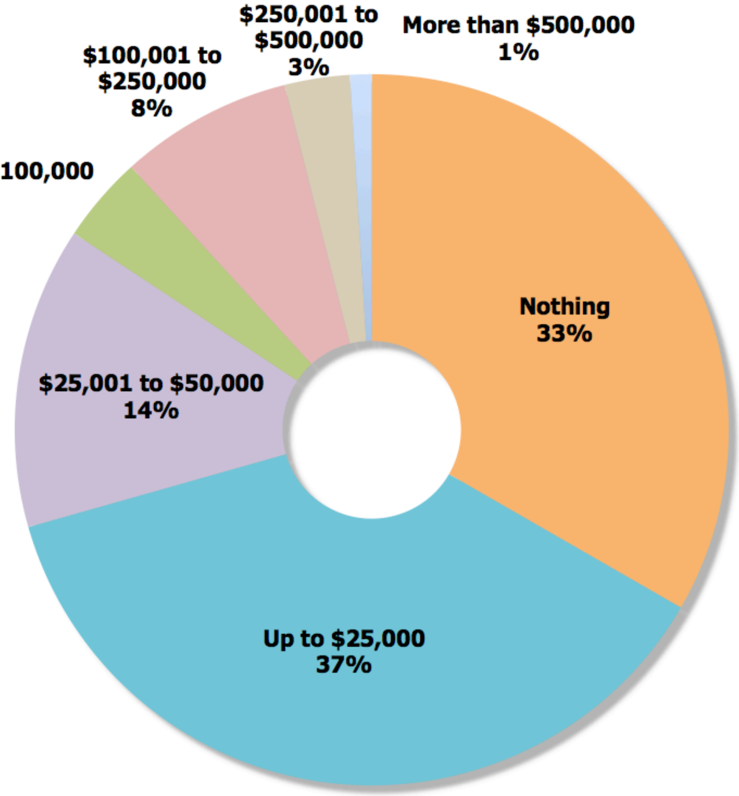


DATA BREACHES ARE EXPENSIVE

Our research also investigated the potential cost of a security breach. As shown in the following figure, more than one-third of survey respondents told us that a typical, single security breach would cost up to $25,000, while 12% believe that a security breach would cost in excess of $100,000.

Based on an average of the data shown in the figure below, Osterman Research estimates that the average cost of a security breach is $44,363. This was calculated by taking the midpoint of each cost range shown below (and estimating an $800,000 cost for the "more than $500,000 range") and multiplying by the likelihood of each cost.

Estimated Cost of a Single Security Breach



We also asked organizations about the likelihood of a security breach occurring during the next 12 months. Only 4% of respondents told us that there is virtually no chance of such a breach occurring, while 60% told us there is a "moderate" to definite likelihood that such a breach will occur.

Using traditional quantitative business analysis methods, if we multiply the average cost of a security breach by the likelihood of its occurrence, then the average cost of a security breach that organizations will experience during the next 12 months is $21,294 ($44,363 * 48% chance based on the data in the figure above). However, this represents the low end of the cost of potential security breaches. For example, a breach of personally identifiable information can result in a requirement to send each victim a postal letter explaining the breach, the cost of credit reports, lawsuits, bad press, lost future business with affected customers and other consequences. A single breach can actually cost millions of dollars, not to mention the tremendously negative impact on an organization's reputation.

INTERNET CONTENT SECURITY MANAGEMENT IS ALSO EXPENSIVE

The survey program that we conducted for this white paper found that security-related IT labor expenditures are quite significant: during a typical week, IT makes the following investments in managing the security infrastructure:

- 15.2 person-hours per week per 1,000 users for managing pattern files, signatures and other critical updates for endpoints. For an organization of 5,000 endpoints, the weekly IT labor cost is $2,923.

- 9.7 person-hours per week per 1,000 users for upgrading resource capacity to add bandwidth, storage, new servers/appliances, etc. For an organization of 5,000 endpoints, the weekly IT labor cost is $1,865.

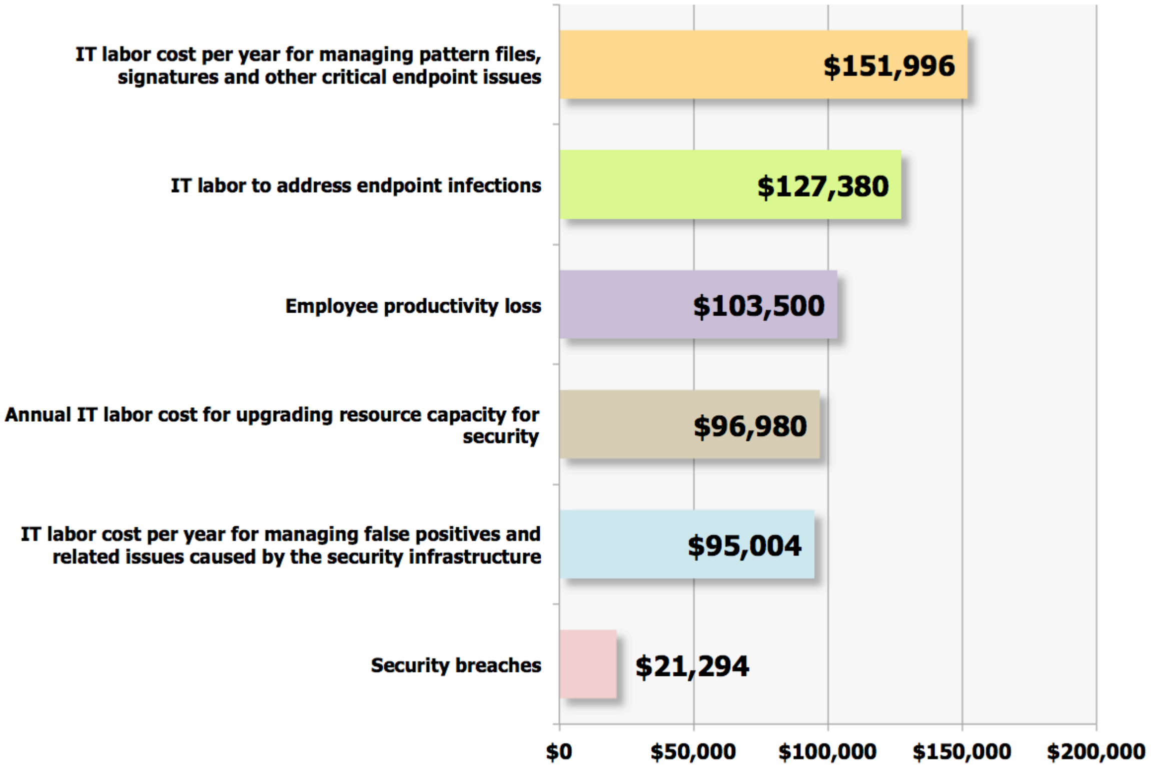
- 9.5 person-hours per week per 1,000 users for managing false positives and related issues caused by the security systems. For an organization of 5,000 endpoints, the weekly IT labor cost is $1,827.

What this means is that in an organization of 5,000 users, the total annual IT labor cost to manage endpoints based on these three activities will be $343,980, which translates to a total of 4.3 full-time equivalent (FTE) staff members to manage.

COST SUMMARY

Based on the analysis above, the annual costs experienced by organizations of 5,000 employees are shown in the following figure.

Costs Associated With Managing and Remediating the Security Infrastructure for an Organization of 5,000 Users



Internet content security management is expensive and much of this cost is related to anti-malware-focused tasks and resources. Organizations spend a considerable amount trying to defend against malware, including labor costs to manage pattern files, deal with false positives as well as additional bandwidth, storage, new servers or appliances, and other network upgrades needed to support the increasing size of pattern files and signatures downloaded to the endpoints to protect against the numerous spam and malware variants. Despite these efforts, more than 50% of endpoints become infected each year. Moreover, these costs also do not take into consideration the additional benefits that an enterprise would receive if the IT staff could be used on higher priority initiatives that increase productivity and generate more revenue.

The Benefits of More Rapid Protection

SECURITY UPDATES ARE NOT FREQUENT

One of the fundamental problems with the security status quo is that many of these systems are not updated frequently. For example, our research found that:

- 91% of respondents employ a security infrastructure that requires pattern file or signature updates.

- A mean of 7.2 hours of elapsed time is required to update pattern files and signatures for anti-malware systems across all endpoints, while 5.6 hours is required for anti-spam updates.

- Pattern files and signatures are updated less than once per day in 14% of the organizations surveyed and only once per day in 37% of them. Only 22% of organizations have pattern files and signatures updates more than four times per day.

This creates a serious problem in a world in which malware lifetimes can be measured in minutes, but most organizations update their security systems only once or twice a day. With few updates there is a security gap between when malware is released and when the protection is deployed across clients and servers. The result is that a new malware variant can appear, do its damage, and then be replaced by a new variant before the first pattern file or signature can be deployed to combat it. As cybercriminals become even more adept at creating their wares, the problem will get significantly worse.

FASTER UPDATES MEAN BETTER PROTECTION

The obvious method for combating the problems caused by slow pattern file/signature updates is to provide faster access to threat intelligence, ideally as close to real time as possible. However, as threat volumes increase, so do the size of pattern files. An approach that relies solely on traditional methods to distribute pattern files and signatures is simply not sustainable because the traditional deployment mode is just too slow and cumbersome.

Instead, threat intelligence should be maintained in the cloud, using queries from a lightweight client. This type of cloud-client architecture saves on resources and provides faster security with enterprises no longer waiting for pattern file deployment to be protected. This approach allows security systems to detect and remediate newly discovered threats more quickly, thereby reducing the number of infected endpoints and security breaches. This will result in lower costs and fewer negative consequences for users and organizations alike.

To address this issue, we asked survey respondents the following question: "Imagine that your server and endpoints could be updated 10 times faster with new pattern files/signatures after a new threat has been detected (for example, going from eight hours to update signatures to 15 minutes)." Note that the survey phrased the faster access to threat intelligence as a pattern file/signature update instead of trying to explain a cloud-client architecture in the survey. However, the key to the survey response is that the organization has access to threat intelligence within 15 minutes instead of eight hours.

Our research found that even with this minimal introduction to dramatically faster pattern file/signature updates, respondents believe that the chance of a data breach would be reduced. For example, with faster updates the number of respondents who believed they would "almost certainly" be breached fell by 30%, while those who felt there would be "almost no chance" of a breach increased by 60%.

FASTER ACCESS EQUALS LOWER COSTS

Not only can faster access to threat intelligence reduce the risk of data loss and the cost of IT labor spent on remediating endpoint infections, it can also reduce the overall cost of managing security.

Osterman Research developed a cost model specifically for this white paper that allows an organization to estimate the cost advantages it might obtain from having faster access to threat intelligence. For example, we have estimated the following for an organization of 5,000 employees:

- Endpoint infection rate would go from 4.3% to 2.0%.

- There would be a 40% reduction in IT staff investments in managing pattern files, signatures and other critical endpoint issues.

- There would be a 10% reduction in IT staff investments for upgrading resource capacity to add bandwidth, storage, servers or appliances, etc.

- There would be a 5% reduction in IT staff investments for managing false positives and related issues.

Based on these assumptions, Osterman Research estimates that these reductions would mean that the total security costs – including productivity losses – for an organization of 5,000 employees would go down by 32%, or $38.15 per employee per year.

THE BENEFITS OF USING A SINGLE SECURITY VENDOR?

Many organizations use multiple vendors for their Internet content security infrastructure – our research found that there is a mean of 3.8 vendors used to provide

Internet content security (median of three). However, many organizations are attempting to reduce the number of vendors to lower costs by obtaining volume discounts, reducing IT labor investments in managing multiple vendors' products, simplifying patch management, and so forth.

We asked organizations that are using multiple Internet content security vendors, "If you could use just one best-of-breed vendor for all of your server and endpoint security requirements, what percentage of IT staff time devoted to Internet content security management do you think you might save during a typical week?" While 30% of respondents assumed there would be no savings from the consolidation of vendors, 25% estimated the savings to be more than 10% per year – 8% estimated the savings at more than 25%. The mean estimated savings was 9.6%. This can result in major cost reductions, particularly for large organizations.

THE BOTTOM LINE

Faster access to threat intelligence, coupled with the use of a single Internet content security vendor, can result in significant savings. For example, in the 5,000-employee organization discussed above:

- Total annual security costs would go from $596,154 to $405,385 – or $119.23 per user per year down to $81.08 – a 32% savings in both IT labor and overall employee productivity.

- In addition, the use of just one best-of-breed vendor that could provide faster updates and other benefits would offer *additional* savings of $55,187 annually, or $11.04 per user.

- The total savings, therefore, would be $245,956 ($190,769 from more efficient administration and reduced infection plus $55,187 from the use of a single vendor), representing a 41% reduction in the current cost of managing security for this 5,000-seat organization.

Trend Micro Cloud-Client Architecture

TREND MICRO SMART PROTECTION NETWORK

Trend Micro Enterprise Security offers Internet content security that provides immediate protection in a tightly integrated offering of products, services, and solutions. At the core of these products and services is the Trend Micro Smart Protection Network, a cloud-client architecture designed to provide fast data and threat protection with minimal network resources. This approach combines in-the-cloud reputation databases and lightweight client infrastructure to quickly and automatically protect information wherever and however an enterprise's employees connect.

Threat information is analyzed using the global knowledge of over 1,000 dedicated Internet content security experts at TrendLabs, Trend Micro's global network of research, service, and support centers. This data is correlated across three types of reputation databases – Web, email and file. If one element shows a bad reputation, it is automatically blocked across all threat delivery methods – providing immediate protection at every point of attack – spam sources, embedded links, dangerous files, and web sites with malicious content. These reputation databases are constantly updated and mutually reinforcing to provide significantly better protection than would be possible using any of these technologies by itself.

THE BENEFITS OF A CLOUD-CLIENT ARCHITECHTURE

With a cloud-client architecture, Trend Micro can update the in-the-cloud reputation databases in real time and the light-weight client can quickly access this information as needed – no longer waiting for periodic downloads of static pattern files to be protected. And this protection can also be accessed by roaming users when both on and off the network. This immediate access to threat intelligence lowers exposure to dangerous spam and malware, reducing malware infections and security breaches. The reputation databases also stop threats at their source, limiting the amount of spam and malware on the network and saving on costly resources.

A UNIFIED DEFENSE: ONE VENDOR FOR INTERNET CONTENT SECURITY

The Smart Protection Network powers Trend Micro Web, messaging, server and endpoint security, creating a unified defense throughout the network between the reputation databases. Whether an enterprise chooses one Trend Micro product or a complete security solution, businesses can access the correlated threat information between these reputation databases to get network protection faster. Trend Micro's comprehensive Internet content security enables customers to use one vendor for immediate, effective protection built into flexible security that is easy to acquire, deploy, and manage.

TREND MICRO ENTERPRISE SECURITY SAVES COSTS

Trend Micro's cloud-client architecture provides faster protection than conventional approaches that rely solely on pattern file updates. Trend Micro also provides a comprehensive solution that enables enterprises to use one vendor for Internet content security. This combination supports the benefits discussed earlier in this paper. Based on the survey results, here is a summary of the amount enterprises can save with Trend Micro Enterprise Security over conventional Internet content security solutions across multiple vendors.

Cost Savings for Conventional vs. Trend Micro Security Solutions

Employees	Conventional Security Costs	Savings from Use of Cloud-Client Architecture	Savings from the Use of a Single Vendor	Total Savings	Annual Savings per Employee
1,000	$119,231	$38,154	$11,037	**$49,191**	**$49.19**
5,000	$596,154	$190,769	$55,187	**$245,956**	
10,000	$1,192,308	$381,539	$110,374	**$491,913**	

** Costs include security management, productivity loss, and security breach*

Summary

Malware is serious and is getting worse over time. Malware variants are becoming more numerous, more sophisticated, more difficult to detect and their lifecycle is becoming much shorter. Organizations that employ a traditional Internet content security infrastructure whose pattern files and signatures are updated only once or twice each day are at a serious disadvantage, since malware variants can enter a network, do their damage and then disappear before the enterprise even receives the latest pattern files or signatures to combat them.

To address these deficiencies, organizations should employ an integrated Internet content security infrastructure that accesses the latest threat intelligence through a cloud-client architecture, providing immediate protection against the latest spam and malware threats. This will reduce the chance of security breaches, reduce the number of servers and endpoints that become infected and reduce IT labor costs focused on security management. Coupled with the use of a single Internet content security vendor, the savings from doing so can be significant.

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, statue, 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.