WHITE PAPER

# The Cloud Advantage: Increased Security and Lower Costs for SMBs

**An Osterman Research White Paper**

*Published August 2012*

***SPONSORED BY***



**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

# EXECUTIVE SUMMARY

By enabling faster access to threat intelligence through a cloud-client architecture, resellers can improve their customers' security posture while reducing their security management costs, employee productivity losses, and the number of security breaches that customers would otherwise suffer.

Osterman Research conducted a survey specifically for this SMB Security white paper that focused on the time and costs associated with remediating malware infections and other ramifications from dealing with malware and related issues. A total of 108 surveys were completed during June and July 2012.

# THE CURRENT STATE OF SMB SECURITY

## BYOD—MORE AND MORE ENDPOINTS

The typical SMB employee uses a number of endpoint devices – a desktop computer, a laptop, a smartphone, a tablet, and home computers with various applications on them. Each of these endpoints represents a vector through which malware can enter their SMB organization's network. The Bring Your Own Device (BYOD) trend of employees using personal mobile devices and laptops for work is accelerating the problem by introducing devices with an even greater likelihood of introducing malware into a company network.

## THE GROWING PROBLEM OF MALWARE

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 a very short period of time, infecting large numbers of endpoints in as little as a few minutes. Malware nowadays is part of a rapidly growing underground economy with cyber criminals employing multiple compromised endpoints and social networking to reach large numbers of targets. The more popular a mobile device (Android or iOS) or the business tool (DropBox, Skype, or FaceBook), the more often it is targeted with delivery mechanisms to steal personal and company data and resources.

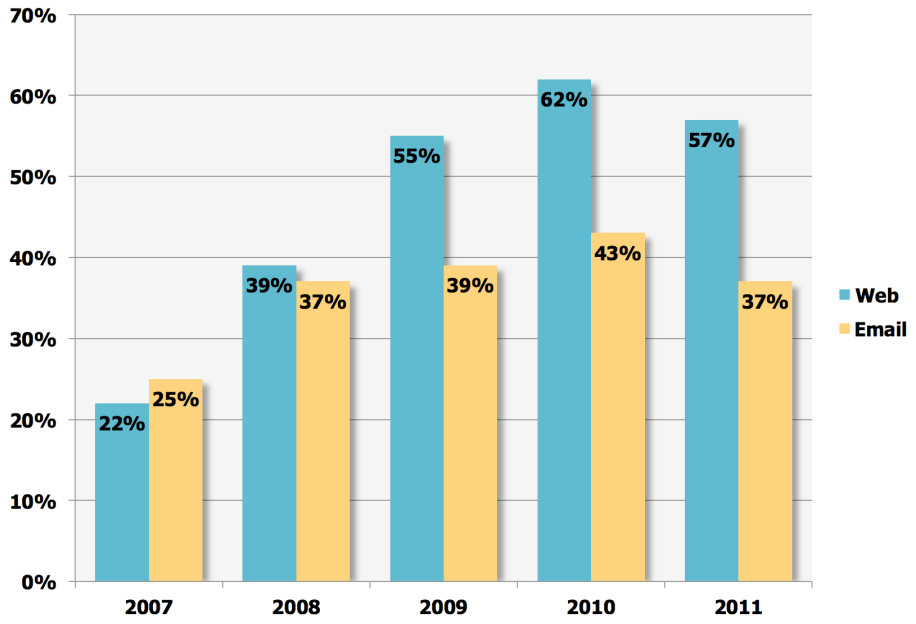
As a result of the growing number of endpoints, coupled with more virulent and more capable malware, the number of endpoint infections is enormous. For example, Osterman found during a typical month that 4.3% of endpoints become infected, which translates to an infection rate of 52.1% annually. That means that in an organization of just 100 endpoints, an average of 4.3 endpoints will become infected in any given month, or 52 endpoints each year.

## THE THREAT LANDSCAPE IS GETTING MORE SERIOUS

During the past several years, we have seen significant and growing numbers of organizations report security violations through their use of Web and email, as shown in the figure below[i].

***By enabling faster access to threat intelligence through a cloud-client architecture, resellers can improve their customers' security posture.***

**Organizations Reporting a Successful Security Violation by Mode**
2007 through 2011




The data in the figure above suggest security violations – malware, phishing and related types of attacks – are growing steadily over time.

Compounding the problem is the fact that malware is becoming more virulent, more stealthy and more difficult to detect. Worse, the lifecycle for many malware variants can now be measured in minutes, not hours or days – many variants appear, do their damage and then disappear long before new pattern files or signatures can be deployed and propagated to endpoints.

Using more advanced tools like automatic transfer systems (ATSs)[ii] – the latest addition to widely used cybercrime toolkits – attackers have streamlined their list of targets to only online banking customers in countries like Germany, the United Kingdom, and Italy. Carefully choosing targets was also evidenced by findings on advanced persistent threat (APT) campaigns like IXESHE[iii]. Android malware like fake spying tool apps[iv] continue to increase in number due most likely to the continued rise in the OS's popularity for more than 400 million active Android-based devices.

## IT SERVICE STAFF TIME IS BEING WASTED

In addition to the serious consequences of SMB's customer data loss, financial loss, or the potential interception of sensitive content; when an endpoint is infected, IT service providers must spend time cleaning customers' endpoints. For example, our research found that it takes a mean elapsed time of 72 minutes to remediate a malware infection on a single endpoint – time that the IT service provider must spend dealing with a problem that could have been avoided with better security. Add to this the partial or complete downtime for a customer's employee as he or she waits for their endpoint to be fixed.

Using these figures, a reseller managing an organization with 100 endpoints will spend more than five hours per month remediating endpoint infections – at a fully burdened annual salary of $80,000 per year for an IT service technician, this translates to a monthly cost of $199, or nearly $2,400 per year for a single customer. Adding in the cost of downtime for customers' employees – something for which they might hold a reseller service provider at least partially responsible – can add

***A reseller managing an organization with 100 endpoints will spend more than five hours per month remediating endpoint infections – at a fully burdened annual salary of $80,000 per year for a reseller's technician, that translates to a monthly cost of $199, or nearly $2,400 per year for a single customer.***

dramatically to the cost of endpoint infections for the customer. In addition, add in the loss of employee productivity and potentially the negative impact on the reputation of the customer organization if data is lost or stolen. SMB organizations have smaller budgets and would rather spend their money on new technology investments than malware infection remediation.

## THE HIGH COST OF CONTENT SECURITY MANAGEMENT

Our research found that IT labor costs are high; for example, the survey found that:

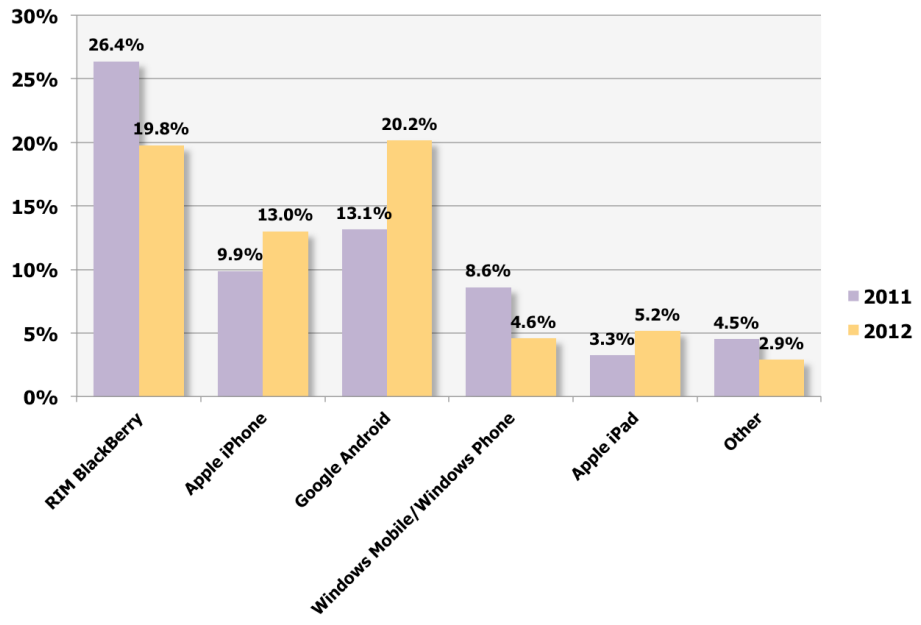
- Each IT staff member supports only 33 endpoints, resulting in a total IT labor cost per endpoint of $2,400 or $79,200 per year.
- When internal IT staff manages an organization's infrastructure, 5.2% of staff time during a typical week is spent on email security management.

However, there are many other costs associated with email security, such as the appliances, software, servers, cloud-based services and other elements that make up an overall email and Web security infrastructure.

A significant proportion of the cost of security management is related to antimalware-focused tasks and resources. Resellers spend a considerable amount of resources trying to defend against malware, including labor costs to manage pattern files, deal with false positives, add additional bandwidth, update storage, and deploy new servers or appliances. In addition, they must perform 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.

The bottom line: IT consultants spend significant amounts of money addressing endpoint infections when their time and customers' money could be spent on more strategic projects with a higher return on time invested. The problem will clearly become worse as endpoints multiply substantially and as the number of mobile devices used within SMB organizations grows over time, as shown in the following figure. (The data in the figure represents the results of an Osterman Research survey with organizations in North America that have up to 150 email users.)

**Penetration of SMB Users by Mobile Platform**
Organizations with up to 150 email users, 2011 and 2012




*IT consultants spend significant amounts of money addressing endpoint infections when their time and customer's money could be spent on more strategic projects with higher return on time investment.*

### THE GROWING PROBLEM OF SECURITY BREACHES

Data stealing cybercriminals are taking advantage of the popularity of social media by delivering malicious threats and content online. These data breaches are becoming so costly that many organizations are at risk of being put out of business through direct financial losses or the high cost of direct or indirect data loss.

For example, many organizations have been targeted with keystroke loggers that steal passwords to allow criminals to transfer funds out of an organization's financial accounts. Last year alone, more than a billion dollars was stolen from small and mid-size bank accounts. Here are a few examples from the United States over the recent past:

- Western Beaver County School District: $700,000[v]
- The Catholic Diocese of Des Moines: $600,000[vi]
- Hillary Machinery: $800,000 (its bank was able to recover only $600,000[vii])
- Patco: $588,000[viii]
- Experi-Metal, Inc.: $560,000[ix]
- Village View Escrow: $465,000[x]
- An unidentified construction company in California: $447,000[xi]
- Choice Escrow: $440,000[xii]
- The Government of Bullitt County, Kentucky: $415,000[xiii]
- The Town of Poughkeepsie, New York: $378,000[xiv]
- An unidentified solid waste management company in New York: $150,000[xv]
- An unidentified law firm in South Carolina: $78,421[xvi]
- Slack Auto Parts: $75,000[xvii]

The cost of a single data breach can total in the hundreds of thousands of dollars, as evidenced by the examples above. Moreover, a previous survey conducted by Osterman Research for Trend Micro in October 2011 found that 15% of respondents felt it was at least very likely that a security breach would occur during the next 12 months in their organization.

The cost of these breaches can include the direct costs of notifying customers via postal mail or email, litigation, lost revenues from customers who no longer want to do business with a victimized firm, and lost goodwill resulting from publicity surrounding the breach.

## THE BENEFITS OF FASTER PROTECTION

### SPEEDING THE DELIVERY OF SECURITY UPDATES

A fundamental problem for many SMBs who update their pattern files/signatures only a few times per day is a higher likelihood of malware-related infections. Because two new threats are discovered every second[xviii], the less frequently that updates occur, the greater the chance an endpoint has of becoming infected.

With infrequent updates there is a security gap between when malware is released and when the protection is deployed across the various endpoints. This results in new malware variants having an opportunity to do their work and get replaced by a new variant before the first pattern file or signature can even be deployed to combat the original threat. As cybercriminals become even more adept at their craft, the problem will only worsen.

### THE BENEFITS OF FASTER UPDATES

The obvious method for combating the problems caused by infrequent pattern file/signature updates is to update them more regularly, 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 their deployment is too slow.

***With infrequent updates…new malware variants [have] an opportunity to do their work and get replaced by a new variant before the first pattern file or signature can even be deployed to combat the original threat.***

The better alternative is to leverage solutions that manage threat intelligence and pattern files/signature updates in the cloud using queries from a lightweight client. This type of cloud-client architecture saves on endpoint computing resources and provides faster security as opposed to waiting for pattern file deployments. This approach allows security solutions 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 infections, coupled with fewer IT resource requirements and less time spent on cleaning devices, as well as less time spent managing email and Web security.

### THE ADVANTAGE OF USING A SINGLE VENDOR

Many IT service providers and resellers use multiple vendors for their customers' content security infrastructure because they perceive there are benefits in a "best-of-breed" approach to email and Web security. However, many are trying to reduce the number of vendors they use in order to lower costs by obtaining volume discounts, reduce IT labor investments in managing multiple vendors' products, simplify patch management, and so forth.

Interestingly, we found that more than twice as many SMB end user customers (56%) felt it was important or extremely important to use a single vendor to manage email security versus a multiple vendor strategy (24%). The benefits of using a single vendor for both service providers and their SMB customers alike include the ability to achieve volume discounts, realize potentially faster updates, and improve integration across on-premise and cloud-based services.

***The benefits of using a single vendor for both resellers and their customers alike include the ability to achieve volume discounts, realize potentially faster updates, and improve integration across on-premise and cloud-based services.***

### WHAT DOES THIS MEAN FOR YOUR BUSINESS

Faster access to threat intelligence, coupled with the use of a single content security vendor, can result in major cost savings:

- A significant reduction in the amount of time spent required for service providers to manage email security. For example, if the amount of time spent on email security could be halved, that would result in IT labor savings of roughly $20.67 per end user per year.
- Cutting the endpoint-infection rate in half would reduce the IT labor cost of endpoint remediation from a mean of $16.27 per user per year to roughly $8.00.
- Cutting the endpoint-infection rate in half would also result in a significant reduction in the productivity loss experienced by end users who are either unable to work while their endpoint is infected, or whose productivity is hampered during the infection and remediation period.
- Perhaps most importantly, reducing endpoint infections could lead to dramatic reductions in the risks associated with data loss, since the potential for breaches of data or financial accounts would be significantly reduced.

## SUMMARY

Malware is a serious issue and the problem is getting worse as cyber criminals become more adept at penetrating corporate defenses. Malware variants are becoming more numerous, more virulent, more difficult to detect and their lifecycle is becoming much shorter. Traditional pattern file/signature update processes that rely on updates that occur only once or a few times per day are simply not adequate to address the problem because of the pattern files can't keep up with the malware variants.

Consequently, resellers should employ an integrated content security infrastructure that accesses the latest threat intelligence through a cloud-client architecture, providing immediate protection against the latest spam and malware threats. Using this approach will reduce the potential for security breaches, reduce the number of

endpoints that become infected and reduce IT labor costs focused on security management. Coupled with the use of a single content security vendor, the savings from doing all of these things can be significant.

# WHO IS DOING IT RIGHT?

## TREND MICRO SMART PROTECTION NETWORK

Only one security vendor manages threat intelligence in the cloud: Trend Micro. Trend Micro offers content security that provides immediate protection in a tightly integrated offering of solutions. At the core of these products is the Trend Micro™ Smart Protection Network™. The Trend Micro™ Smart Protection Network™ cloud security infrastructure rapidly and accurately identifies new threats, delivering global threat intelligence to secure data wherever it resides. Trend Micro looks in more places to collect massive amounts of threat-specific data from multiple sources including a global network of sensors. Data mining and big data analytics are used to identify, correlate, and analyze new threats, producing actionable threat intelligence across mobile, physical, virtual and cloud environments. This intelligence is delivered to Trend Micro products and services through its proven cloud infrastructure to ensure customers' data is protected.

Trend Micro Smart Protection Network powers the cloud security solutions, which protect the SMB, including hosted endpoint security, hosted email security, and hosted mobile device management. IT service providers can manage the entire cloud security portfolio from a cloud-based central management console, with visibility into multiple customers' deployments from one central command post.

Trend Micro protected small and medium-sized businesses (SMBs) against more than 142 million threats in the first half of 2012 alone.

***Trend Micro protected small and medium-sized businesses (SMBs) against more than 142 million threats in the first half of 2012 alone.***

[i] *Messaging and Web Security Market Trends, 2011-2014*; Osterman Research, Inc.
[ii] http://blog.trendmicro.com/evolved-banking-fraud-malware-automatic-transfer-systems/
[iii] http://blog.trendmicro.com/taking-a-bite-out-of-ixeshe/
[iv] http://blog.trendmicro.com/beta-version-of-spytool-app-for-android-steals-sms-messages/
[v] http://www.post-gazette.com/pg/09195/983738-57.stm
[vi] http://krebsonsecurity.com/tag/catholic-diocese-of-des-moines/
[vii] http://rixstep.com/1/1/20100126,00.shtml
[viii] http://www.networkworld.com/news/2009/092409-construction-firm-sues-after-588000.html
[ix] http://www.computerworld.com/s/article/9156558/Michigan_firm_sues_bank_over_theft_of_560_000_
[x] http://krebsonsecurity.com/2010/06/e-banking-bandits-stole-465000-from-calif-escrow-firm/
[xi] http://www.technologyreview.com/computing/23488/?a=f
[xii] http://www.bankinfosecurity.com/articles.php?art_id=3159&opg=1
[xiii] http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html
[xiv] http://www.computerworld.com/s/article/9153598/Poughkeepsie_N.Y._slams_bank_for_378_000_online_theft
[xv] http://www.suite101.com/content/protect-yourself-against-banking-crimeware-a156086
[xvi] http://www.abajournal.com/news/article/doj_says_massive_decade-old_botnet_helped_web_thieves_steal_millions/
[xvii] http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html
[xviii] Source: Trend Micro