

WHITE PAPER

The Business Benefits of Hosted Email Security for the SMB

Sponsored by: Trend Micro

Brian E. Burke

Gerry Pintal

Christian A. Christiansen

December 2008

IDC OPINION

All businesses face a daily bombardment of email spam that consumes valuable IT staff time as well as end-user productivity. In addition, email is an attack vector for many types of security threats to businesses, including phishing, viruses, spyware, and malicious URLs. Given that all businesses are experiencing the financial pressures of a tightening world economy, coupled with the uncertainty of any near-term recovery, small and medium-sized business (SMB) managers are searching for ways to cut costs while continuing to maintain a consistent level of service and protection for their businesses.

SMBs face unique challenges in combating these threats, in that they have very limited IT staff resources available when compared with larger businesses. Because SMBs are confronted with having to deal with other critical issues on a daily basis, the frequent maintenance required by IT staff to keep messaging security products effective can very often be neglected, resulting in an increased exposure to malicious security threats. In contrast, large enterprises are able to establish, fund, and staff security-specific groups whose charters are directed at architecting, managing, and maintaining secure corporate infrastructures.

SMBs, by necessity, focus the lion's share of their financial and people resources on funding, managing, growing, and competing for market share in their respective industries. Consequently, the resources available to implement, maintain, and manage security infrastructures are, in many cases, in short supply. As a result, information security among SMBs is primarily approached reactively rather than proactively, and critical tasks such as ongoing maintenance of messaging security products can often go by the wayside.

IDC believes that it is imperative for SMBs to seek security solutions that proactively address not only the emerging threat environment but also their operational cost and maintenance issues.

For SMBs looking to address these critical issues, hosted messaging services have become an attractive platform of choice for their messaging security approach. Driven by the explosive increase in the volume of spam and the increasing sophistication of malicious attacks, hosted messaging security services are quickly being adopted by many organizations that want to stop threats "in the cloud" before they reach the network.

IDC estimates that in excess of 95% of unwanted messaging traffic can be stopped in the cloud before it enters the corporate network. IDC predicts that by 2012, hosted messaging security services will overtake both software and appliances as the most widely deployed new SMB messaging security platform.

Hosted messaging security services are becoming an attractive platform because they stop threats before they reach the network and ongoing upgrades and tuning are conducted by the vendor, providing up-to-date protection against the latest known and unknown threats. Hosted email security is also more cost-effective for SMBs due to the additional support provided by the vendor. Having an experienced security vendor provide the support saves on IT resources as well as reduces the risk of costly security breaches. Overall a hosted email security solution offers higher cost savings over other SMB email security approaches.

METHODOLOGY

To gain insights into the emerging security challenges and costs facing SMBs and to learn more about how organizations address these challenges, IDC conducted in-depth interviews with executives at companies in several industry sectors to identify SMB customer and market trends for hosted software as a service (SaaS) solutions. The participating organizations operate in education, manufacturing, food services, and security services industries. In addition, IDC met with Trend Micro's management team to review its goals and strategies for addressing customer challenges. This white paper uses all of these research perspectives to create a view of real-world challenges and solutions for SMB customers.

IN THIS WHITE PAPER

This white paper provides small business owners, midsize company executives, and functional IT staff with a deeper look at how hosted messaging security can help address and manage a dynamically changing threat environment. It also offers a realistic view of the business benefits associated with implementing hosted messaging security. This document presents perspectives on the evolving demands for messaging security solutions (including whether to continue maintaining an on-premise solution), how even small declines in end-user productivity can have significant cost implications, and how to address current and emerging regulatory requirements.

SITUATION OVERVIEW

The Challenges for SMB Information Technology

Finding the Optimal Balance

As discussed earlier, SMBs in many cases, especially in tight today's economic conditions, have to work with limited available human and capital resources while also being required to overcome ongoing challenges of establishing high levels of security in a dynamic and rapidly evolving threat environment. Too often, SMBs are forced to accept lower end-user productivity due to spam and other email-based threats because IT staff simply do not have the time to provide critical ongoing maintenance to on-premise messaging security products such as traditional software and appliances.

The Emerging Threat Environment

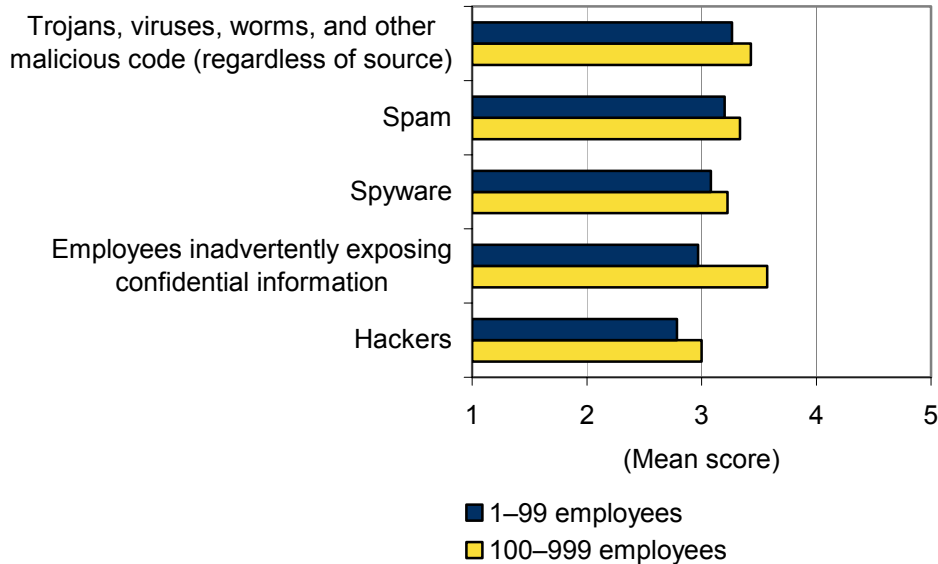
In the past, hackers and malware developers competed for notoriety by wreaking havoc on computer systems just for the "fun of it." Today, a new generation of cybercriminal, often affiliated with organized crime, has emerged. Financial gain is the primary driving force behind this generation's development of spam, harvesting email addresses from mail directories and launching spyware, phishing attacks, worms, and other forms of malware.

A serious security breach resulting from one of the aforementioned attacks can damage a company's reputation and brand, consequently resulting in the loss of customers, revenue, and profitability. Other potential business risks include loss of intellectual property and investor confidence, the potential for regulatory fines, and even costly litigation.

In IDC's 2007 annual security survey of IT and security professionals, participants were asked to rate the top threats to their company's network security. Figure 1 displays IT's view of the top 5 security threat categories to their businesses. This data clearly shows that the top 3 threats for small to midsize companies are directly related to messaging security.

FIGURE 1

Top Threats by Company Size



n = 430

Note: Threat sources are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC, 2007

According to this IDC survey, malware, spyware, and spam top the list of leading security concerns among SMB IT management and administrators. Spam is an issue that is prevalent across the spectrum of all businesses but affects SMB end-user productivity disproportionately due to persistently limited available SMB IT staff resources. Spam may also be driving unnecessary purchases by SMBs of additional mail servers and contributing to a perceived need for increased network bandwidth requirements.

Trojans, viruses, and worms are increasingly being created by for-profit criminal enterprises, and they are specifically targeting SMBs to steal confidential data such as credit card numbers, personal identification numbers (e.g., social security numbers), and other personal information having value on the Internet black market. IT security staff are also increasingly becoming concerned that employees may be inadvertently exposing confidential business information.

All of these factors provide a clear signal to SMB management that providing SMB IT staff with sufficient resources to establish continuously effective security is a critical issue that requires serious consideration.

The following is a summary description of the most common email threat types with a brief description of methods of defense against them.

Spam

As we have seen, spam is an ever-increasing threat to businesses and has become a cost-effective vector for criminal attacks on individual businesses. Traditionally, spam has been unsolicited bulk email that is selling a product or service for a wide variety of items, including drugs, mortgage rates, and so forth. The biggest impact of traditional spam is the time it takes end users to clean out their inboxes to stay under mailbox size limits and be able to find and respond to valid emails. Adding to the user productivity impact, spam also depletes IT resources by increasing server storage, backup time, and network traffic.

☒ **Spam as a threat delivery mechanism.** Today, the term "spam" is used to describe unsolicited bulk email that delivers any type of unwanted content. Spam is no longer limited to promoting products and services; it can also deliver malicious content such as attachments with viruses or spyware and embedded URLs to dangerous Web sites with spyware, phishing attempts, and other forms of malware intended to infect a company's machines. Spam emails with malicious content are a significant threat to SMBs, particularly given IT's concern over end users inadvertently exposing confidential data.

☒ **Phishing.** Phishing is a vehicle for attempting to trick people into revealing confidential information such as passwords, bank and credit card information, or other confidential data. Aggressive email campaigns are driving unsuspecting users to counterfeit Web sites where they are duped into revealing their confidential information. Although phishing was originally more of a consumer threat, the number of phishing attacks aimed at businesses is increasing. Some are very targeted, appearing to originate from the company's Human Resources or IT department and requesting confidential data about the employee or organization.

- ☒ **Spyware.** One of the most prevalent mechanisms for stealing confidential data is spyware. Unlike phishing, where the recipient usually has to divulge some type of data, spyware is malware that uses malicious code to steal information unbeknownst to the user. Spyware is a particularly dangerous threat because it can monitor keystrokes, eavesdrop on email, and scan files on hard drives. Spyware can be delivered through attachments or by the user following a link to a malicious site where the code can be silently downloaded just by opening the Web page. IDC estimates that 40% to 50% of all help desk calls are currently related to spyware.

Antispam systems are able to significantly reduce the number of these email threats, preserving resources and protecting against costly security breaches. However, it is critical to deploy an effective antispam solution, one that keeps threats off of the network entirely — not one just scanning onsite. For example, if end users spend even 15 minutes a day deleting spam, that will cost businesses significant productivity over time.

In addition, SMB IT staff may not have available time to provide the maintenance necessary to keep on-premise antispam systems effective. With maintenance of existing antispam systems being neglected (e.g., not installing new versions, not adjusting for company growth), spam blocking effectiveness can slowly decline to the point where an increase in spam can easily occur. SMBs can benefit from solutions that are maintained by the vendor, ensuring the latest threat protection and reducing IT resource requirements.

Available Solutions

Given the tight squeeze in which SMBs find themselves, it is obvious that an efficient, effective messaging security solution is needed to address their unique situations. A variety of messaging security solutions are available, such as:

- ☒ **On-premise messaging security solutions.** In general, on-premise messaging security solutions — including both traditional software and appliance products — are often selected because businesses believe they enable more control over the messaging security application and also avoid concerns that routing email through a third party will result in lower email availability and performance. In truth, companies often get as much insight into their email traffic with a hosted solution with mail tracking capabilities, reports, and flexible policy options. In addition, hosted solutions generally provide higher availability. Hosted security vendors have more infrastructure resources, allowing them to prevent extensive downtime, with many providing availability guarantees through service-level agreements (SLAs).

Hosted security vendors provide and house all security software and hardware, deploy all updates, and tune the systems to provide optimal effectiveness. Hosted vendors are also able to scale the service when a business adds new employees or over time is experiencing increased email and spam volumes.

- ☒ **Hosted messaging security solutions.** In general, hosted messaging security solutions enable customers to effectively outsource the ongoing maintenance required to preserve solution effectiveness. In addition, most hosted solution vendors charge one fixed price per user with unlimited email filtering capacity, with the result that companies do not have to purchase additional hardware or software as email and spam volumes grow. Some hosted messaging security vendors even offer service-level agreements that not only provide contractual guarantees for service availability and email delivery latency but also provide contractual guarantees for spam blocking effectiveness, false positive rates, and zero virus infection.

SMBs should seriously consider implementing hosted messaging security, and in their search for hosted messaging vendors, they should consider the following criteria for evaluating vendor hosted messaging solutions:

1. What is the total volume of emails that the vendor scans on a daily basis?

The more emails a vendor scans, the more effective that vendor's hosted messaging security solution will likely be in stopping known email threats and in stopping emerging email threats.

2. Does the vendor provide other security solutions such as antivirus or Web security in addition to messaging security?

The more data that a vendor has visibility to across differing threat vectors, the more effective in general each of its solutions, including messaging security, will be.

3. Is the technology included in the hosted messaging security solution created and owned by the vendor or OEMed from another vendor?

Vendors that own their own technology continually experience, analyze, and devise protection against all forms of attacks under a variety of local and international conditions and as a result are better able to provide a higher degree of protection for their customers than vendors without homegrown technology. Vendors with homegrown technology have the edge because they have direct control over the effectiveness and support of their technologies and are up to date at any given time to more effectively address emerging threats that now make up the majority of email threats.

4. Does the vendor provide a service-level agreement that contractually guarantees the following?

- ☒ High availability
- ☒ Spam blocking effectiveness
- ☒ Minimal false positive rates
- ☒ Zero virus infection occurrences
- ☒ Minimal mail delivery latency

5. Does the vendor provide aggressive credits as part of the service-level agreement guarantees?

Remedies specified in SLAs can be a significant differentiator (e.g., remedy credits offered in minutes versus hours can be a strong indication of the vendor's commitment to providing a high-quality and effective security service solution).

THE BUSINESS IMPACT

To assess the business and financial benefits that a hosted messaging security solution offers SMBs, IDC interviewed several SMBs to gain a firsthand understanding of the primary issues involved in the decision process and the resulting economic benefits achieved from their implementations of a hosted messaging solution.

The Decision Process

The primary drivers behind the SMBs implementing a hosted messaging security solution included:

- The need to significantly reduce overall spam traffic
- Limited availability of dedicated and trained IT staff to deal with an increasing volume of messaging related issues and threats
- The need to reduce their vulnerability to sophisticated messaging-borne threats
- Legacy equipment failing to perform effectively

The participating SMBs, which operate in education, manufacturing, food services, and security services industries, selected Trend Micro's hosted messaging solution, InterScan Messaging Hosted Security (IMHS), on the basis of the overall effectiveness of spam reduction, ease of implementation, and low ongoing maintenance costs. "We implemented InterScan Messaging Hosted Security on Friday, and on Monday our end users saw no spam! The switchover was seamless, and because the interfaces are intuitive, no training was necessary."

"We implemented InterScan Messaging Hosted Security on Friday, and on Monday our end users saw no spam! The switchover was seamless, and because the interfaces are intuitive, no training was necessary."

Considerations

The information presented in the following sections reflects specific results of this research effort activity in concert with IDC's institutional knowledge in the areas of security and solution trends. The data presented in this research provides a view into the overall benefits gained by participating SMBs in their efforts to increase their overall success in reducing undesired email traffic while reducing their overall cost of ownership.

Because many variables and conditions are associated with these studies, quantitative results of other similar cases may vary considerably from the results presented in the following cost analysis.

Participating SMBs' Background Information

- ☒ **Industries.** The businesses participating in this study included companies in education, manufacturing, food services, and security services industries.
- ☒ **Employees.** The businesses represented in this research employed 8 to 2,500 people.
- ☒ **Budgets.** Overall IT budgets, including security line items for companies interviewed in this research, have remained flat over the previous and current years. Overall IT budgets are expected to remain under pressure for the foreseeable future.
- ☒ **Security staff.** Dedicated security staffs in companies participating in this research ranged from one to two full-time equivalent professional staff members.

Table 1 presents a summary of the average per-employee cost savings gained by the participants in this study.

TABLE 1										
Annual per-Employee Cost Savings with InterScan Messaging Hosted Security										
Cost Type	Security Products Reseller		Manufacturing		International Food Distributor		Education		Typical SMB Average	
Number of employees	8		200		510		2,500		406	
	Without IMHS	With IMHS	Without IMHS	With IMHS	Without IMHS	With IMHS	Without IMHS	With IMHS	Without IMHS	With IMHS
Employee productivity spam costs	\$169	\$2	\$361	\$14	\$57	\$0	\$87	\$0	\$168	\$4
IT/help support costs	\$243	\$81	\$454	\$5	\$178	\$3	\$73	\$2	\$237	\$23
Subtotal	\$412	\$83	\$815	\$19	\$235	\$3	\$160	\$2	\$405	\$27
Cost savings per employee	\$329		\$796		\$232		\$158		\$378	

Source: IDC, 2008

As can be seen in the preceding cost analysis model, significant per-employee savings, on an annualized basis, can be derived from the implementation of an effective and comprehensive hosted messaging security solution.

THE TREND MICRO SOLUTION

Trend Micro™ InterScan Messaging Hosted Security (IMHS) offers SMBs a cost-effective approach to securing their businesses.

As indicated earlier in this white paper, SMB IT staffs are confronted with the challenge of providing continuously effective messaging security at the same time they are also being asked to provide support for multiple other projects that contribute directly to the company's bottom line.

To address these unique SMB security needs, Trend Micro provides a hosted messaging security solution — InterScan Messaging Hosted Security — that includes a contractually binding service-level agreement with:

- 100% availability
- At least 95% spam blocking
- Less than .0004% false positives
- Less than two minute email delivery
- Zero email-based virus infection
- Remediation provisions

As a hosted messaging security solution, set security options stop spam before it reaches the customer's network.

The following section provides a more detailed summary of the Trend Micro InterScan Messaging Hosted Security solution.

InterScan Messaging Hosted Security

Trend Micro InterScan Messaging Hosted Security stops spam, malware, and other email threats before they reach a company's networks. InterScan Messaging Hosted Security will stop denial of service (DoS) attacks and directory harvest attacks (DHAs) before they take down a business' network. Backed by dedicated experts in messaging security, InterScan Messaging Hosted Security is designed to provide a continuously effective messaging solution that enables companies to reclaim IT staff time and end-user productivity as well as reduce mail server storage and network bandwidth requirements. All maintenance, including patches, updates, hot fixes, and application tuning, is done by Trend Micro experts with little to no maintenance required from customer IT staff. In addition, as a hosted solution, there are no hardware or software costs.

Trend Micro offers two InterScan Messaging Hosted Security implementation options, both backed by an aggressive service-level agreement:

- Standard option.** This option provides an easy, cost-effective way to eliminate at least 95% of spam using default network-level connection controls without any administrator intervention. Using Trend Micro Email Reputation technology to evaluate the source of emails, this service protects against the most egregious spammers and emerging spam sources such as botnets and zombie networks.

Key features include:

- ❑ Smart Protection Network to provide immediate protection against attacks by correlating threat information across Email, Web, and File Reputation databases, collecting intelligence at all points of the attack
- ❑ Email Reputation to block IP addresses generating spam, phishing attacks, spyware, and other malware attacks, including blocking attacks from botnets
- ❑ Antispam composite engine to block spam using statistical analysis heuristics, threat signatures, whitelists, blacklists, Web Reputation applied to embedded URLs, and other innovative technologies
- ❑ End-user quarantine management to save IT staff time by enabling end users to manage their own spam folders, approved sender lists, and blocked sender lists
- ❑ Multilingual antispam and antiphishing to better protect businesses outside the United States
- ❑ Zero day protection to guard against unknown and targeted virus attacks

As a hosted solution, Trend Micro InterScan Messaging Hosted Security can protect any existing mail system, be rapidly and easily deployed, and help to immediately stop spam and other email threats after implementation.

- ☒ **Advanced option.** This option delivers all of the hosted security features provided in the standard option and enables customers to create their own rules for spam and malware, setting sensitivity and actions as well as customizing protection for groups within the company. This enables customers to optimize spam blocking while minimizing false positive rates and, according to Trend Micro, stopping up to 99% of spam. The advanced option also provides content filtering to support data leak prevention (DLP) and help enforce regulatory compliance requirements.

In addition, the advanced option offers an email encryption add-on service that provides policy-based encryption. This encryption service integrates with the content filtering capabilities of InterScan Messaging Hosted Security to easily apply encryption to desired groups or emails with specific types of content, making it easy for SMBs to secure confidential communications.

Key features include:

- ❑ The spam, malware, and phishing protection described for InterScan Messaging Hosted Security Standard is applied to both inbound and outbound emails to protect against both external and internal email threats.
- ❑ Customizable policy filtering that can set rules for specific senders, recipients, groups, or individuals to optimize spam blocking effectiveness, false positive rates, and other threat protection.

- ❑ Content filtering capabilities allow administrators to set rules that scan email content and attachments by characteristics, keywords, lexicons, and customized data rules with flexible action options to prevent data leaks and enforce compliance.
- ❑ Optional policy-based email encryption to enable secure message delivery to anyone with an email address.

More information is available at www.trendmicro.com.

CHALLENGES

As with most important business decisions today, the cost of investing in any existing or new technology, even in prosperous economic times, is a major consideration facing SMB executives. With IT budgets coming under increased pressure because of current tight economic conditions, deciding where and how an organization can derive the biggest bang for the buck out of limited and often shrinking budgets is an ongoing balancing act that many business owners, IT managers, and senior business managers must deal with.

It is clear from current research that spam, spyware, viruses, phishing, worms, and other forms of malware are becoming more sophisticated and dangerous. Establishing highly effective defenses to stay ahead of these increasingly complex and sophisticated messaging threats must be among SMBs' top priorities.

The challenge for Trend Micro is to present convincing arguments backed by quantitative evidence to assist SMBs in recognizing the overall business benefits InterScan Messaging Hosted Security can deliver by reducing their messaging security costs, providing substantial gains in opportunity costs by freeing up valuable IT resources to address core business-related IT objectives, and at the same time improving overall employee productivity. The research conducted in this effort provides SMBs with compelling quantitative evidence of Trend Micro's successes in helping SMBs identified in this research to cost-effectively achieve their messaging security objectives.

CONCLUSION

SMB business managers and executives face a variety of challenges every day. Many of these challenges require shoot-from-the-hip decision making if SMBs are to successfully compete in highly competitive markets and industries. At a minimum, the critical factors that must be included in SMBs' planning and decision-making processes are the profitability, efficiency, and security of their operations.

Planning, designing, and implementing a continuously effective security infrastructure that provides a high degree of protection from the various messaging threat vectors described earlier must be an essential part of an SMB's success-oriented business planning process.

Trend Micro InterScan Messaging Hosted Security offers SMBs a comprehensive and cost-effective way to provide continuously effective protection from Internet-borne threats.

For more information, see www.trendmicro.com.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.