Enterprise Strategy Group | Getting to the bigger truth.™

White
Paper

“Good Enough” Email Security Is No Longer Good Enough

By Jon Oltsik, Senior Principal Analyst

January 2013

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Executive Summary

Large organizations have email security defenses in place today yet malware continues to sneak through and compromise servers and endpoints, leading to the theft of valuable information in some cases. Clearly something must be done, but what? Are security risks around email increasing? At the same time, some vendors are touting new email server versions featuring native security features and functionality. Will these elements address email security risk on their own? This paper concludes:

- **Email is getting more hazardous.** Aside from traditional viruses, worms, and Trojans, email has become a popular vector for advanced malware propagation as part of Advanced Persistent Threats (APTs). In these cases, malware is often distributed via spear phishing, malicious URLs, or compromised files that circumvent traditional email security controls.
- **Native email server security may be a step in the wrong direction**. New email server platforms with basic security functionality will likely be attractive as many business managers perceive that they can now get security protection for free. As the saying goes, "You get what you pay for." Security protection included in email servers may have been adequate ten years ago, but it is no match for today's insidious threat landscape. The old notion of "good enough security" for email may save a few dollars, but it can increase IT risk to an unacceptably high level. A few dollars of email security savings could pale in comparison to a multimillion-dollar security breach.
- **Large organizations need to think of email security as part of an enterprise security architecture**. Hackers and cyber criminals consistently exploit numerous gaps in today's security defenses. To address this, CISOs need a security architecture that can coordinate policies and controls with security analytics and intelligence on-premises and in the cloud. This type of architecture will help improve email *and* enterprise security simultaneously.

Email: More Dangerous Than Ever

When Ray Tomlinson sent the first email message by using the "@" sign to separate user from machine name, he could not have imagined the communications revolution to follow. Not long after this initial message transmission, email became the "killer app" of the Internet. The rise of the public Internet in the 1990s only fueled the email fire. As of 2012, there were nearly two billion email users and hundreds of billions of individual email messages sent on a daily basis.

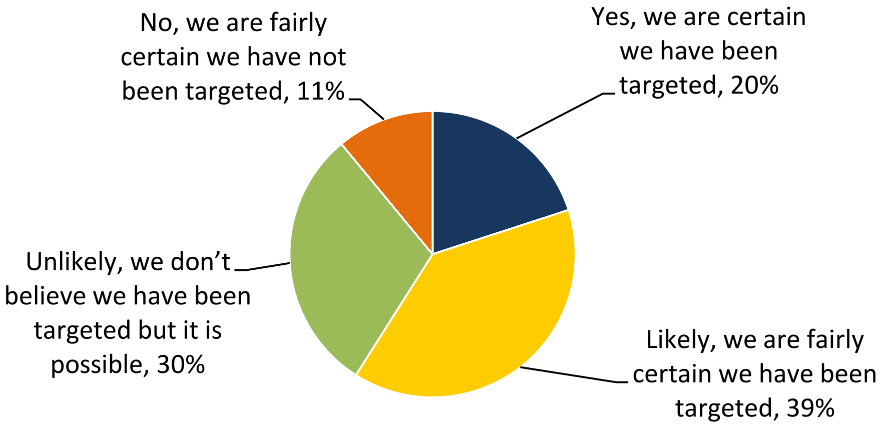
Similar to the mail service, telegraph, and telephone, email has served to transform communications. In spite of this extraordinary accomplishment, email also made the Internet a more dangerous place. This first became apparent in 1988, when the "Morris worm" infected approximately 6,000 major UNIX systems. As the Internet became more mainstream, email viruses and worms had an even greater impact (i.e., Melissa, Iloveyou, etc.). More recent malware variants associated with email include Koobface, Zeus, Black Hole, and various types of ransomware. Meanwhile, spam continues to make up 80% to 90% of total email volume while hackers have improved phishing attacks for social engineering exploits.

It's clear that 13 years after the Melissa virus, email remains a threat vector commonly used to distribute viruses, worms, and Trojans. Additionally, email-borne malware continues to grow in volume and sophistication. As frightening as this is, however, email is also used for even more sinister purposes. Cyber criminals often use email as part of Advanced Persistent Threats (APTs). In this scenario, hackers target individual users by using social engineering attacks and email as a means for malware distribution. When a user receives a spoofed email from a seemingly trusted source, it is not at all unusual for them to open the message, execute the malware, and unwittingly act as "patient zero" for an ongoing APT that ultimately results in the exfiltration of valuable data.

APTs represent a serious and unprecedented type of threat to enterprise organizations. Furthermore, APTs are far more common than most people think. According to ESG Research, 20% of enterprises are certain they have been the target of an APT while 39% of enterprises are fairly certain they been the target of an APT (see Figure 1).[1]

Figure 1. Belief that Organization Has Been Targeted by APTs

Based upon what you know about APTs, do you believe your organization has been the target of a previous APT attack? (Percent of respondents, N=244)



Source: Enterprise Strategy Group, 2013.

Advanced Malware Can Circumvent Traditional Email Security Tools

APT authors go to great lengths to research user profiles, use social networking techniques, and create credible email messages to appear trustworthy. In addition to fooling users, cyber criminals are also well aware of the limitations of most email security technologies. To evade email security controls, hackers use a multitude of methods for malware distribution including:

- **Spear phishing.** This scheme fools the user and the security controls. A spoofed email from a supposedly trusted source evades spam filters and proceeds to a user's inbox. These sophisticated scams often trick users into opening emails and taking actions that lead to a malicious code infection.
- **Drive-by downloads.** Rather than include malware in an email itself, many APTs will use email and social engineering to prompt a user to click on an infected web link. When naïve users take this action, it acts as a drive-by download, executes malware, and compromises their system. Many email security technologies scan messages for malware or spam filtering while embedded web links sail through.
- **Malicious content.** Cyber criminals have become adept at embedding malware within common files such as Microsoft Office documents and PDFs. In many cases, email security controls are configured to block certain types of attachments (i.e., .vbs, .ws, .wsc file extensions) but all other attachment types such as PDFs are almost always "white listed" so malware goes from cyber criminals to endpoints and remains undetected.

Even enterprise organizations with advanced security controls and layered security architectures can be vulnerable to these types of exploits. Why? Hackers take advantage of protection gaps and the lack of integration of many security tools. For example, many organizations have email, web security, and antivirus gateways, but these technologies often operate in isolation. By inserting malicious code within acceptable email messages and

[1] Source: ESG Research Report, *U.S. Advanced Persistent Threat Analysis*, November 2012.

attachments, hackers can remain invisible to discrete safeguards deployed for alternative tasks in other network locations.

It is also worth noting that cyber criminals often use 0-day vulnerabilities, blended threats, and/or polymorphic/metamorphic malware to easily sneak by most AV gateways. Since advanced malware may be designed to infect one system in the world, AV scanners and engines may not have a signature that matches a unique advanced malware variant used for an APT attack. AV scans based upon signatures alone are no match for today's threat landscape.

"Good Enough" Email Security Is a Step in the Wrong Direction

In the past, security professionals had a colorful way of describing the way executive management viewed security. The thought was that CEOs didn't want good security; they merely wanted "good enough" security. In other words, corporate executives were willing to fund basic security technology safeguards but were unwilling to invest in people, processes, and technologies to help them manage risk, detect suspicious activities, or respond to actual security incidents in an appropriate manner.

Over the last few years, many executive managers have become much more amenable toward information security. CEOs have learned about cybersecurity the hard way through a combination of publicly disclosed security breaches and visible news headlines. Cybersecurity is no longer just a technology issue, it's a business issue.

Business and Executive Managers Have Security Limitations

Executive-management attention on information security is a positive development for the most part, but CEOs, CFOs, and COOs aren't security or technical experts. Yes, they are willing to invest in security safeguards but they really don't understand requirements or product differences, and they still have financial obligations at hand. This knowledge gap and financial pressure can lead to instances where security technologies are viewed on a generic basis, leading once again to "good enough" security decisions.

ESG sees the potential for these kinds of "good enough" decisions around email security over the next few years. Why? Email vendors are adding basic email security capabilities into their server platforms. Business executives and purchasing managers may hear the words "email security," "antivirus," and "integrated" and assume that they no longer have to pay for additional email security safeguards. ESG believes this "good enough" email security strategy could be a big mistake, given the threats described above. Basic security feature/functionality in email servers tends to:

- **Lack the right analytics for advanced malware detection.** Many email security engines still depend upon AV signatures for malware detection while others have basic heuristics to detect common malware families with slight variations. These defenses are fine for pedestrian viruses and Trojans but will miss advanced malware at an alarming rate. What's needed here is a combination of network defenses and advanced analytics to execute malware in a sandbox environment, analyze content, quarantine suspicious files, and monitor networks for other suspicious behavior such as DNS patterns or host communication to a command-and-control server. These capabilities are completely absent.
- **Scan messages upon network ingress only**. Baked-in email security scans email messages upon arrival to the mail server only. Yes, this will catch blatant malicious code but advanced malware will inevitably sneak around signature-based filters. Full-featured email security systems provide for this possibility by performing ongoing scans on all messages stored on the email server on a regular basis. By doing so, email security can find malware previously classified as false negative. Regrettably, basic security features on email servers do not have this capability.
- **Fail to provide deep file type and web filtering.** As described above, basic email protection may offer some filters for file types, but they do so by looking at file extensions rather than the actual file content. This gives content-based malware a free pass to proceed to a user's inbox. As for malicious URLs, email server security assumes that other security defenses are in place to detect and block these threat vectors.

- **Have insufficient reporting from their UI.** Strong security depends upon continuous monitoring of system behavior in order to judge the effectiveness of security policies and controls. This is also critical for regulatory compliance and general IT audits. This type of reporting is not included in the basic security provided with email servers.

Email servers are designed to process, store, and forward email; leading email servers perform these tasks quite well. While it is admirable that these vendors would include basic protections for customers, CISOs must understand that "good enough" email security is completely inadequate and places the organization at an unacceptable level of risk.

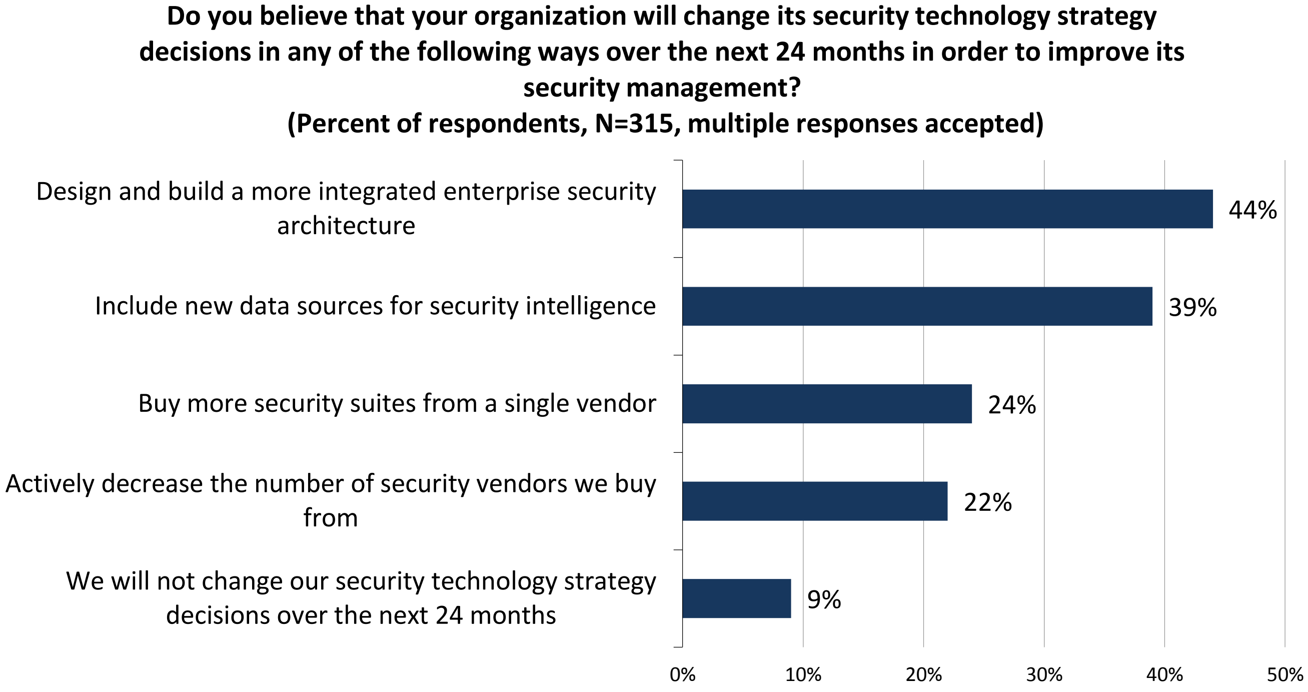
CISOs must make sure that executives are properly educated so they aren't making security choices based upon false assumptions. Given the threat landscape, it would be a shame for enterprises to make "penny wise and pound foolish" email security decisions which expose the organization to a security breach or problems costing millions more than they saved.

Email Security Should Be Tightly Integrated Into Enterprise Security

Large organizations built their security infrastructure organically over time, adding security appliances to address the threat Du Jour. These types of defenses encourage CISOs to view security in well-defined categories: email security, web security, Advanced Malware Detection/Prevention, etc. The strategy was adequate when security breaches typically led to downtime and system remediation, but this is no longer the case. Today's APTs and targeted attacks are used as a stepping stone and can lead to highly damaging data exfiltration. Advanced malware propagation may even be used to attack critical infrastructure, destroy equipment, and interrupt vital services.

So what's needed? A security architecture that tightly integrates email security with additional layers of defense and security analytics. This type of activity is already happening. According to ESG research, 44% of large organizations plan to design and build a more integrated enterprise security architecture over the next 24 months (see Figure 2).[2] Email security will certainly be included in the overall security architecture plan.

Figure 2. How Security Technology Strategy Decisions Will Change



Source: Enterprise Strategy Group, 2013.

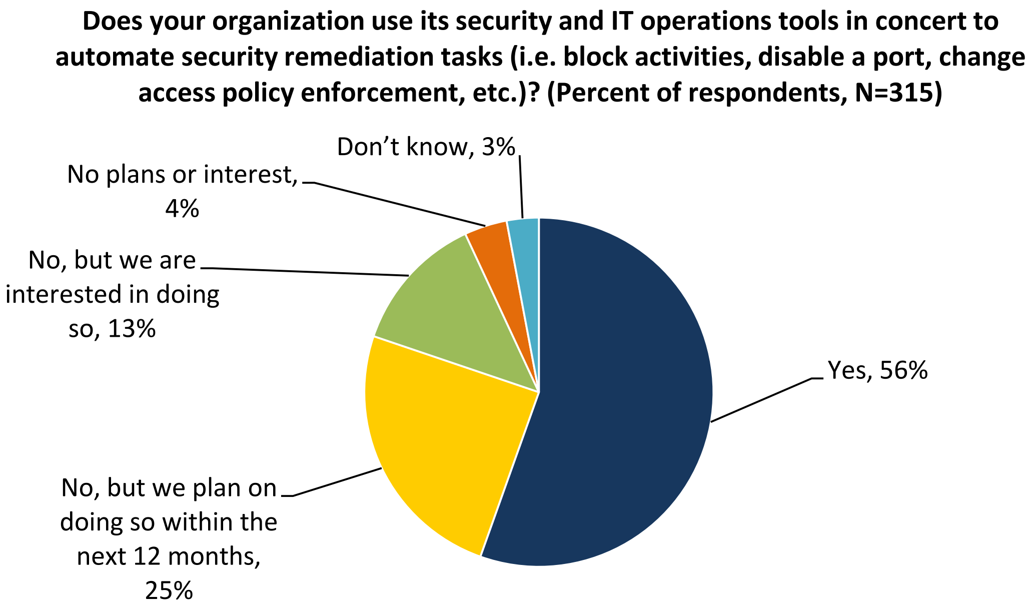
[2] Source: ESG Research Report, Security Management and Operations: Changes on the Horizon, July 2012.

As a standalone security function, email security products must be full-featured and offer high performance, easy deployment and operations, and best-of-breed security protection against all types of threats. When email security becomes part of an enterprise security architecture, it can become even more effective because:

- **Threat management can extend across email, file, and web content.** As previously mentioned, email can spread advanced malware through a number of tactics such as spear phishing, infected documents, and malicious URLs. Integration between email and other security services could be extremely helpful for detecting and blocking these email threat vectors. Upon detecting a web link, email security could check with a web reputation service or web threat gateway to check whether the URL, domain, or IP address is a known threat or carries a high-risk score. Leading web threat management gateways get real-time threat and reputation updates from the cloud so this information is likely to be up to date. With this type of integration, security administrators can detect threats, block email transmission, and do further analysis to see whether this was random malware distribution or evidence that suggests a targeted attack in progress.
- **DLP can be tuned for email usage.** Many large organizations have DLP gateways on their networks to prevent data leakage. Typically, DLP looks for standard data types such as Social Security numbers and customer account data. If DLP were more tightly integrated into email security, it could provide much more granular policy enforcement. For example, it could allow certain types of data to be emailed based upon user role. Rather than simply block an email between a physician and an insurance provider, DLP could also coordinate with email security to encrypt the email so it is allowed to go through.
- **Email gains AMD/P capabilities.** Even with email, web, and file content integration, stealthy advanced malware can remain undetected. What are needed here are specific Advanced Malware Detection/Prevention (AMD/P) defenses. Typically, these are deployed as network gateways that have the ability to scan content, analyze executables in virtual sandboxes, determine the properties and functions of the executable, and make a decision to forward or block the file. These types of AMD/P services should be deployed within the email security network infrastructure or become a callable service based upon email security policies or suspicious content detection.
- **Email provides and consumes security intelligence to fine-tune controls.** All components of the security infrastructure should log events and share security information with security analytics systems that reside onsite or in the cloud. When security analytics uncover new threats or vulnerabilities, they should be able to use this intelligence to automate security-controls adjustments for better protection. For example, when cloud-based security analytics see a pattern of advanced malware attacks against the financial services industry, it should be able to share this information to update rules, change reputation scores, and blacklist files immediately. This type of integration would be welcome—as ESG research indicates, 56% of large organizations already use security and IT operations tools in concert to automate remediation tasks today (see Figure 3).[3] Greater integration with on-premises and cloud-based security analytics and intelligence would likely accelerate this type of security controls automation.

[3] Source: Ibid.

Figure 3. Large Organizations Are Automating Security Remediation Tasks



Source: Enterprise Strategy Group, 2013.

Enter Trend Micro

Many email security point tools and services are available, but few of them qualify as best-of-breed and even fewer are an integrated component of comprehensive enterprise security architecture. One notable exception here comes from Trend Micro with its ScanMail Suite for Microsoft Exchange.

Trend Micro has many years of experience in this area as it has been providing security protection for Exchange servers since 1998. Trend Micro provides best-of-breed email and enterprise security integration with:

- **Content scanning.** ScanMail recently enhanced file filtering capabilities to detect and block malware embedded in Office documents and PDF attachments. Given the rise of APTs and advanced malware, this is an email security requirement.
- **Web content filtering.** Other mail server security vendors scan for malicious URLs only as part of spam filtering. This method doesn't work for enterprise Exchange servers which are not deployed as a gateway (i.e., Exchange Edge role). Trend Micro has a different philosophy and believes emails with malicious URLs are not just annoying spam but a threat that should be checked for at every email security layer.
- **Enterprise security integration.** ScanMail integrates with Trend Micro enterprise security in a number of areas such as DLP, monitoring/reporting, and its cloud-based Smart Protection Network. To detect and block sophisticated malware, ScanMail also provides an optional sandbox for execution analysis of attachments and feedback of local threat intelligence (via integration with Deep Discovery Advisor).

With full email security protection and enterprise security integration, Trend Micro provides what large organizations need: a comprehensive security architecture. CISOs should take note of this, research Trend Micro products and services, and assess how Trend Micro aligns with their email and enterprise security strategies.

The Bigger Truth

In 2005, many security professionals lamented over their organizations' decision to eschew their recommendations in favor of "good enough" security. While these decisions may have been foolish from a security perspective, business managers did base them on some logic. Security attacks were fairly mundane at the time, so a few best practices and security technology safeguards could significantly lower the risk of a damaging security breach. This wasn't an ideal situation but business managers were willing to accept the risk.

Fast forward to the end of 2012, and everything has changed. Threats are more targeted and sophisticated. Security defenses are increasingly porous. Risk has increased to an unacceptable level. Fortunately, business executives understand this new landscape and are more willing to get involved with security decisions and invest in the right training, processes, and defenses.

Ultimately, CISOs must act as educators, communicators, leaders, and cheerleaders to make sure that business managers understand the difference between "good" security and "good enough" security at all times. Email servers offering basic security functionality are examples of where organizations confuse free security with good security, but in reality, free security can just barely be classified as "good enough" security and even that may be a stretch. Since email is often a vector for advanced malware, it is critically important to avoid the temptation to place small financial gains over security protection and risk management. ESG believes that email security must be full-featured, best-of-breed, and part of an internal and cloud-based security architecture. Sacrificing any of these requirements will only increase IT risk—or lead to something much, much worse.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com