WHITE PAPER

Rethinking endpoint and email security for the BYOD era

ENJOY SAFER TECHNOLOGY™

RETHINKING ENDPOINT AND EMAIL SECURITY FOR THE BYOD ERA

It seems like nearly every day we hear about another company falling prey to a cyber threat, often resulting in data loss.

The attacks can and do hit organizations of all sizes and are only becoming more widespread and difficult to detect. The consumerization of IT and Bring Your Own Device (BYOD) only exacerbates the issue since companies now have many more endpoints to protect—many of which they don't own.

In a survey of more than 500 IT professionals conducted in the spring of 2012 by Savitz Research Solutions, one in five companies said they had been the victims of cyber crime in the previous two years. Of those, 71 percent said the culprit was malware and 55 percent said the attack involved phishing or social engineering.

Malware and phishing attacks occur most often via email. Given the high incidence of attacks, it's clear that the traditional method of fighting them—antivirus software installed on endpoints—is no longer enough. What's now required is an integrated approach that combines email and endpoint security solutions.

In the spring of 2012

1 in 5

companies said they had been the victims of cyber crime in the previous two years.

The power of integration

A layered approach to security has long been considered a best practice among security professionals, who often cite the need for "defense in depth." The idea is analogous to a home that has door locks and deadbolts but also a security system. Should an intruder make his way past the locks and open a door, the security system will trigger an alarm that will likely send the intruder fleeing.

In the same way, businesses need to apply multiple security technologies to effectively thwart cyber intruders. Endpoints need protection with antivirus, antispyware, firewall, antispam and Web-filtering tools, while simultaneously protecting email systems. Given that email is one of the tools knowledge workers use most often, it is one of the most attractive attack vectors for cyber intruders.

The sheer volume of mail that workers receive also makes email an enticing entry point, making them prone to errors that lead to successful social engineering tactics. As users try to quickly get through their inbox, they become more susceptible to phishing attacks and may open a nefarious piece of mail that appears to be from a trusted source. If the attacker is successful in getting the recipient to click on a link in the email, the door is open for the installation of malware that gives the intruder entry to the company's network. It is now essential that companies protect their mail servers as well as user endpoints.

Protecting both the endpoint and the mail server provides a dual-layer defense, an in-depth strategy that is important to effective

security. To be successful, an attack must succeed in thwarting both defense mechanisms; no single weak link can lead to an intrusion. But these types of security tools are only truly effective if they are highly efficient, able to do their job without slowing down the network or server and hindering end user response time—and hence, productivity. The tools must also be simple for IT to deploy and manage, minimizing complexity.

SMB challenges with integrated security

In practice, few small or medium-sized businesses (SMBs) use both endpoint and email security solutions. Of those companies that do use both, many use security solutions from different vendors, which makes them more difficult to manage.

Multivendor solutions increase complexity

Each security tool has its own proprietary management console, and administrators will have to be trained on how to use multiple products, with no transfer of operational knowledge between products.

Many SMBs also consider such a configuration to be too expensive. The products must support multiple endpoint operating systems and potentially multiple mail systems, driving up costs. Additionally, they have to pay support costs to both vendors, often for products that have many overlapping features.

Performance concerns

SMBs are also concerned about security solutions being a drag on performance. In the Savitz Research survey, when asked to detail difficulties with their current endpoint security solution, 31 percent of businesses reported system slowdowns, while 25 percent said their software was a "resource hog."

Poor performance can be a significant problem and can devastate the effectiveness of an endpoint security solution. End users will often find ways to get around the tools by canceling system scans and opting out of updates to avoid productivity losses. As a result, the security tool isn't up to date and can't detect against recently released known virus signatures or the increasing number of "zero-day" threats—those released in the wild before vendors are able to identify them and write signatures that traditional antivirus tools utilize to detect them.

Given the importance of and demand on mail servers, SMB IT managers share similar concerns when it comes to security tools. A solution that hinders performance will not be tolerated for long.

Dealing with BYOD

The BYOD phenomenon may be the trickiest issue for SMBs, but it is now unavoidable. Companies can no longer simply dictate what devices their users may employ. A recent Harris Interactive survey of some 1,300 adults in the United States who are currently employed found that more than 80 percent of them "use some kind of personally owned electronic device for work-related functions." What's more, 66 percent of those who use a personal device for work say their company has no BYOD policy.

This is a recipe for disaster, as many of those employee-owned devices, such as smartphones, have no antivirus software whatsoever, while maintaining direct access to corporate mail

systems. Such devices are fully capable of spreading email-borne threats to the corporate network.

Personal use, real threats

Threats can also be spread when employees use public computers to access the Web-based version of corporate email, such as from conferences and client networks.

Similarly, users can spread threats when they're on the company network checking personal email and visiting social media sites. Many SMBs lack the kind of security tools that can effectively deal with these threats, such as content filters and device control tools that enable companies to block access to sites and removable media that may be against company policy.

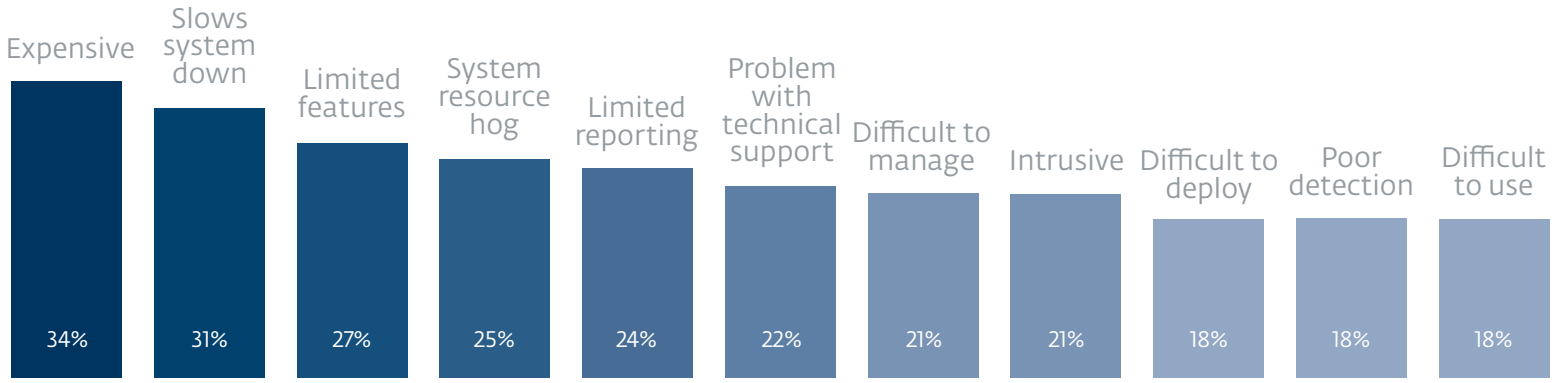
A proven and effective combination

ESET recognizes these various challenges and has a solution that is both effective and easy to deploy: the combination of ESET Endpoint Security and ESET Mail Security.

ESET Endpoint Security provides comprehensive protection for endpoints, packaging antivirus, antispyware, firewall, antispam, Web-filtering and device-control software. ESET Mail Security eliminates all types of email-borne threats and unsolicited email, with harmful content filtered away at the server level—before it can do any damage. Both tools take advantage of ESET's advanced heuristics technology, which enables them to catch the growing number of zero-day threats because they don't rely on signatures for detection.

DIFFICULTIES WITH CURRENT ENDPOINT SECURITY SOFTWARE

Over 30% of IT security managers currently have problems with endpoint software being expensive and slowing the system down, while roughly 25% say it has limited features, is a system resource hog and has limited reporting.



Simple to use

While its tools are highly advanced and effective, ESET understands that SMBs often have limited IT resources at their disposal. ESET has taken pains to ensure its solutions are simple to deploy and operate day to day. One key to this is the ESET Remote Administrator, which enables IT to manage both the ESET Endpoint Security and Mail Security solutions from a single console.

This approach helps to limit the amount of training required, as the Remote Administrator maintains the same interface of both products, reducing complexity and, consequently, the errors that complexity can breed.

Yet the package offers complete control. With the Remote Administrator, operators can update signature databases, run reports and generally enforce consistent security policies across the entire network. The system also includes a built-in task management system that allows for timely and complete responses when malware is discovered.

Less taxing

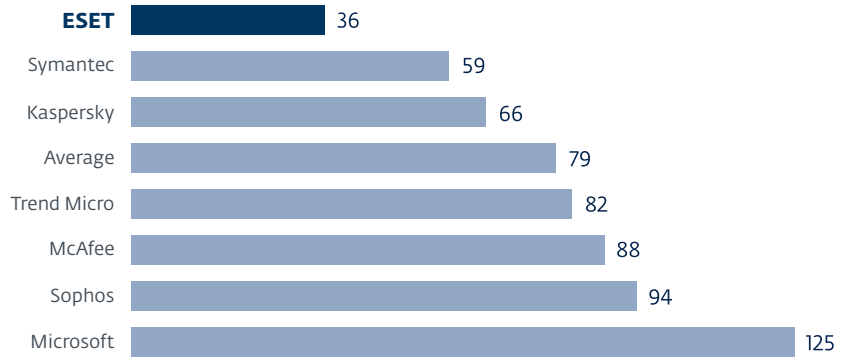
ESET successfully deals with the performance issue by delivering a solution that is highly effective yet light on network bandwidth and email server resources. Both ESET Mail Security and Endpoint Security are engineered to use minimal system resources, leaving more processing power dedicated to the applications employees need to be productive. ESET virus scans are also far faster than competing tools (see chart).

This kind of performance can be a major factor, as many SMBs don't have ample spare network or server capacity. If a security solution slows down the network or puts too much of a burden on servers, it may create more problems than it solves.

Building a business case

ESET makes it easy for customers to build a business case for an integrated endpoint and mail security solution. It results in a lower-cost solution, taking advantage of a single vendor and eliminating duplicate support costs. This type of solution also involves less training since the products have a similar look and feel, and administrators can operate both platforms from a single console. Additionally SMBs can ensure their investment is protected even if they change platforms, as ESET has Mail Security solutions for Microsoft Exchange, IBM Lotus Domino and multiple variations of Unix, including Linux, BSD and Solaris.

FULL SYSTEM ENDPOINT SCAN TIMES (MINUTES)



Source: www.passmark.com | B2B Report, August 2012

ESET benefits

The increasing volume and complexity of cyber threats combined with the surge of devices to protect as a result of BYOD presents a challenge for SMBs that cries out for a layered security solution. Only by securing both endpoints and mail servers can companies rest assured that their networks are protected from malware and other threats.

But employing endpoint and mail security packages from different vendors may only add to the complexity. ESET offers a different approach that brings numerous benefits:

- An integrated product line all managed from one console to simplify and drive efficiency of daily operations.
- A small footprint for lower overhead and less demand on scarce network and system resources, making security transparent to end users and IT administrators.
- A best-in-class antivirus solution that can find viruses even before signatures describing them are available—a must to protect against the rising number of zero-day attacks.
- Support for multiple mail systems and operating systems.

ESET's email and endpoint security solutions provide the flexibility SMBs need to combat today's threats while offering strong ROI and lower total cost of ownership.

Learn more about how ESET can protect your organization.
Visit: www.eset.com/us/business