WHITE PAPER

Market Pulse

Endpoint Security Must Get Better

SURVEY FINDS IT LEADERS READY TO CONSIDER MORE EFFECTIVE, EASIER-TO-USE TECHNOLOGY.

Endpoint security is at a critical juncture. Increasingly, employees at organizations of all sizes are using a wider variety than ever of desktop and mobile devices, including smartphones, tablets and laptops, as they work from broadly dispersed locations, including home offices. Often, organizations are permitting and even encouraging employees to use their own devices under BYOD (bring your own device) policies. With these devices, employees are accessing not only corporate data and applications, but also social media, banking and shopping sites.

In a 2014 IDG Research Services survey of IT leaders, 83% say endpoint security is critically important—and with good reason. As recent news events have demonstrated, the scope and cost of data breaches can be very high. For IT professionals, including CIOs and CISOs, corporate/career survival hangs in the balance.

Mobility and BYOD aren't the only factors placing new importance on endpoint security. Cloud-based applications such as corporate productivity suites and storage require tight security for the endpoints accessing those services. In addition, many organizations are gravitating toward data-centric business models in which business intelligence and operations data are critical—and that data must be accessed from a wide variety of endpoints.

According to the IDG survey, CIOs and CISOs also understand that as the number and variety of attacks have increased, no single technology is sufficient to keep an organization safe. Consequently, a multilayered approach to security is needed, covering such techniques as anti-malware/anti-virus, email security, secure Web gateway, encryption, application whitelisting/control, data loss prevention (DLP), advanced threat protection, virtual patching/host IPS and mobile security. Notably, DLP, ATP, virtual patching and mobile security will nearly double in the next year, the survey finds.

» Dissatisfaction

Despite recognizing the importance of endpoint security, survey respondents are unhappy with the technology in several respects—most importantly, the complexity of the products and the difficulty of security policy enforcement. In a telling response, less than half highly rate their organizations' current endpoint security solutions in any one area. The amount of staff training required garners a particularly negative response, with nearly 30% ranking it only 1 or 2 on a scale of 1–5, where 1 is poor and 5 is excellent.

The reason for the large amount of time needed for staff training is the sheer number of tools. The use of separate management consoles for each of several security tools, such as email security, Web security, DLP or other packages, mandates distinct education regimens for each. In addition, the use of a large number of tools means that management tasks are duplicated. For example, every time a policy is changed, that change must be implemented on each management console—a costly and time-consuming process.

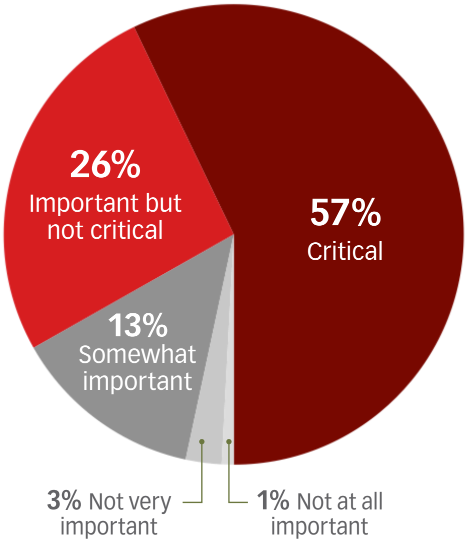
Huntington Memorial Hospital in Pasadena, Calif., uses four different endpoint security products. "Each solution appears to be reasonably simple to set up and install. It is when combined that it becomes a pain for IT to manage," says Henry Jenkins, director of information services at the hospital and a survey respondent, in an email message.

CIO Strategic Marketing Services

TREND MICRO™

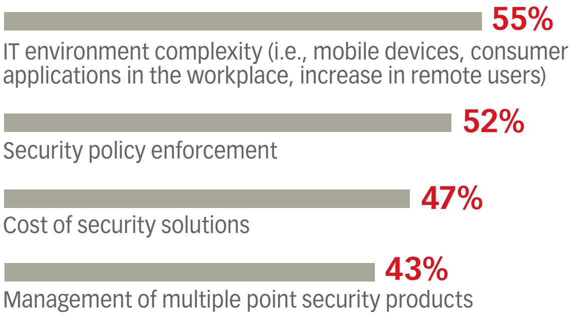
FIGURE 1. Endpoint Security as IT Priority

Endpoint security is reported as a ***critical*** or ***important*** IT priority at 83% of organizations.



As cloud-based solutions gain popularity, endpoint security solutions must effectively handle endpoints whether they are connected to corporate networks or to public or private clouds. However, the ability of endpoint security solutions to evolve with organizations' cloud strategies does not fare well in the survey. Only 34% rate their solutions at 4 or 5; 23% rate their solutions at 1 or 2; while 14% say they "don't know," indicating lack of knowledge of a cloud progression path.

FIGURE 2. Top Challenges of Endpoint Security



» Openness to change

The perceived importance of endpoint security and the dissatisfaction with current tools combine to create openness to change among those surveyed. Two-thirds (67%) of organizations are likely to consider alternate security vendors within the next year.

"We want something a whole lot easier to administer and integrate, via standards, to allow a 'best-of' solution for our environment, and greater functionality," says survey respondent Richard Buss, senior vice president of technology at EMSL Inc., a nationwide environmental testing lab headquartered in Cinnaminson, N.J., in an email exchange.

Meanwhile, Jenkins of Huntington Memorial Hospital voices similar thoughts in an email exchange. "I would like to see a better, integrated approach that provides the same kind of controls that we are getting from each point solution at a price lower than the sum of our current security solution parts."

The survey finds that price aside, ease of management, better threat protection and better endpoint performance are the key factors that are likely to lead respondents' organizations to switch security vendors. And survey respondents will seek out security vendors that can deliver the benefits they view as most important to their businesses: protection against attacks and the ability to avoid the costs of potential security incidents.

» Trend Micro

Answering the need for a broad range of threat protection that can be managed from a single console, Trend Micro Smart Security Suites bring together a full complement of security capabilities, including endpoint, email and Web security. From one console, you gain complete visibility across all components of the solution, and can see a time-based view of policy compliance and security incidents for a given user across all of that person's devices. You can deploy on-premise, in the cloud or in a hybrid model—and can change the mix at any time. This flexible deployment capability means your investment is future-proofed should your infrastructure move increasingly to the cloud.

Trend Micro endpoint solutions deliver the most complete user protection available against today's evolving threat landscape, featuring outstanding performance and straightforward licensing. With the broadest range of anti-malware techniques, Trend Micro delivers multiple layers of threat protection and data security to protect your users and your corporate information across every device, application and network.

If you are seeking a better endpoint security solution, you can find more information on Trend Micro products here: **www.trendmicro.com/switch**