E-guide

PRO+ Content

Endpoint Protection Planning Guide

How will you prepare for unexpected attacks?

In this e-guide

In this e-guide:

Endpoint protection software has made many recent improvements, but it still seems to be falling short.

In fact, a recent TechTarget survey shows that IT and security pros are concerned about undetected threats, false alerts, and data breaches with their current endpoint protection.

Vendors are taking various approaches to increase endpoint protection. Innovation continues, but methods remain imperfect.

You must use available technology to lower risk as much as possible. Combining such tools and software can improve endpoint security protection.

Explore methods and technology options through this e-guide to create a protection plan that works for you.

In this e-guide

IT security trends: 2017 prioritizes cloud, network, endpoints

Diana Hwang, Content Development Strategist - TechTarget

Prioritizing endless cybersecurity initiatives is not an easy task for infosec teams.

Endless attacks, such as the recent WannaCry ransomware virus or other innovative types of ransomware that can potentially wreak havoc on businesses, represent one of many IT security trends professionals need to think about when protecting their organizations.

Indeed, as IT security trends are showing a growing number of organizations deploying cloud services, infosec professionals have revealed their top 2017 cybersecurity initiatives in the latest TechTarget survey. It's no surprise that securing the network and ensuring the protection of the abundant number of endpoints in enterprises were considered among the top security priorities for 2017.

TechTarget's ninth annual 2017 IT Priorities Survey reveals the top tech initiatives IT professionals intended to focus on for the year. Among the 971

IT professionals interviewed, 21%, or 207 respondents, represent North American IT professionals who spend the majority of their time on security-related tasks for their organizations.

IT security trends: Cloud is a hot button

This year's IT security priorities show cloud service deployment, network-based security and endpoint security among other key initiatives for 2017. The survey reports 45% of respondents are planning to deploy a cloud-based storage initiative this year, requiring infosec teams to focus on cloud security and to ensure their company's data remains safe from would-be hackers.

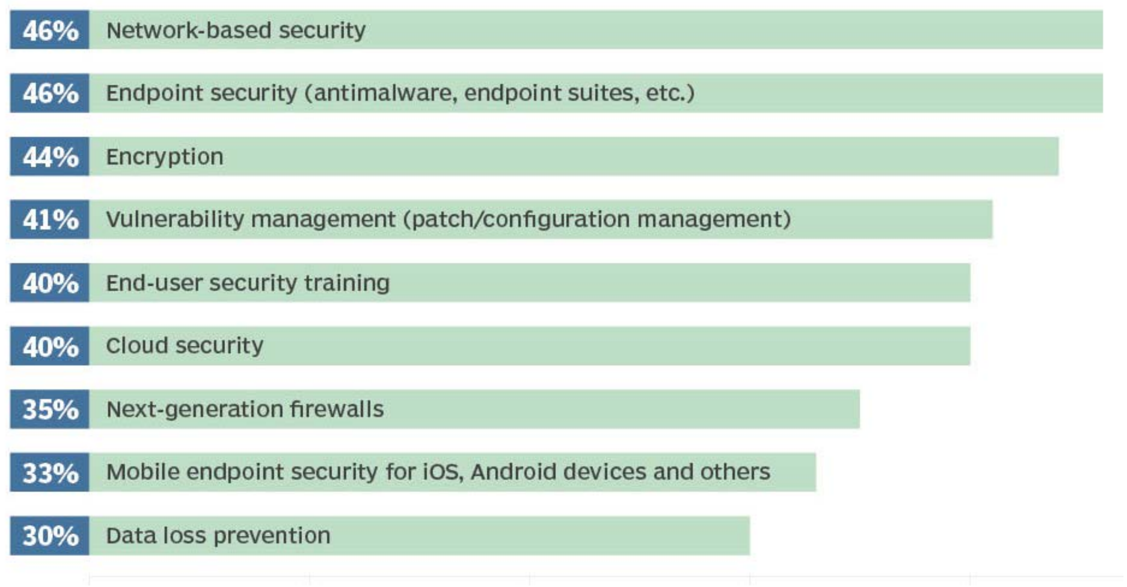
The survey also shows IT security trends revealing the differences between small-, medium- and large-sized business cloud deployments.

2017 IT Security Priorities

Security crosses tech boundaries, and IT security pros are shifting their attention to include cloud, network and endpoint security initiatives in their main priorities.

In this e-guide

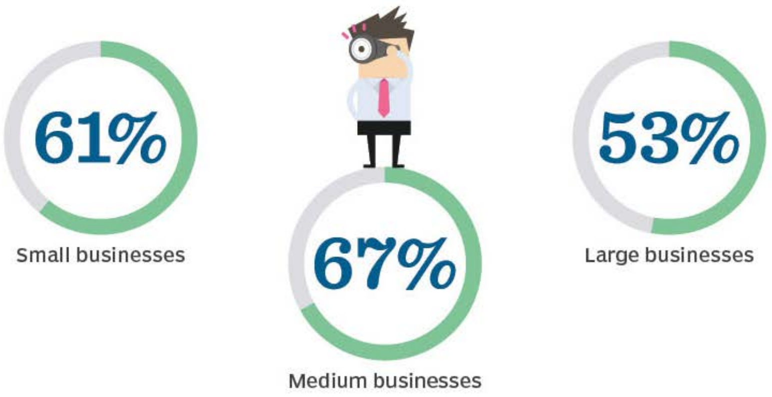
Top security initiatives IT security pros plan to focus on in 2017



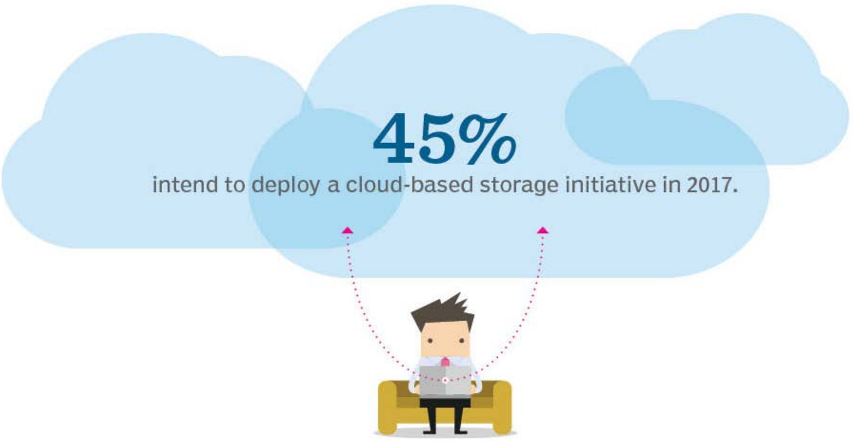
In this e-guide

Where's the money going?

Cloud services represent one of the most important areas of investment IT security pros intend to place their business in small-, medium- and large-sized businesses.

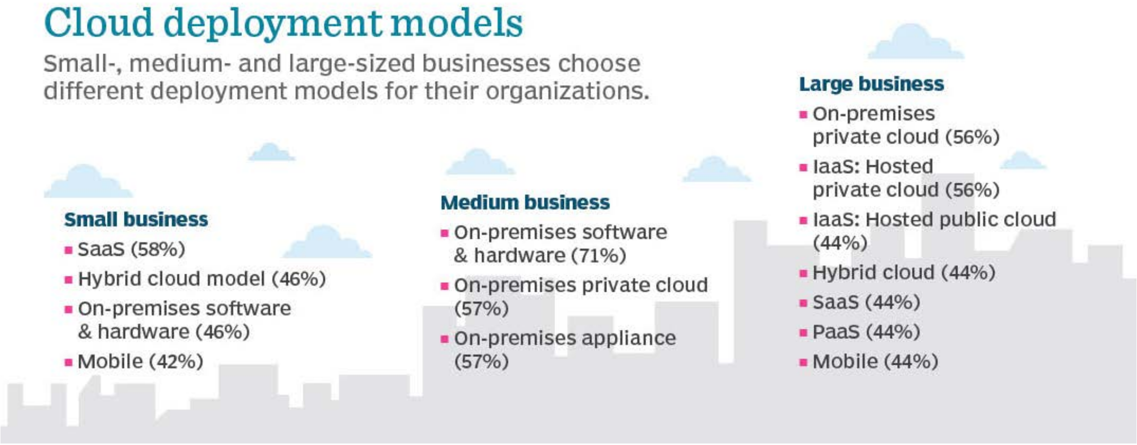


Organizations increasingly rely on the cloud to store data



intend to deploy a cloud-based storage initiative in 2017.

In this e-guide



Cloud deployment models

Small-, medium- and large-sized businesses choose different deployment models for their organizations.

Small business

- SaaS (58%)
- Hybrid cloud model (46%)
- On-premises software & hardware (46%)
- Mobile (42%)

Medium business

- On-premises software & hardware (71%)
- On-premises private cloud (57%)
- On-premises appliance (57%)

Large business

- On-premises private cloud (56%)
- IaaS: Hosted private cloud (56%)
- IaaS: Hosted public cloud (44%)
- Hybrid cloud (44%)
- SaaS (44%)
- PaaS (44%)
- Mobile (44%)

Budgets

In today's tight economy, IT spending must be carefully considered before making the decision to increase or decrease an organization's budget.

SMALL BUSINESSES ARE BIG SPENDERS

25% said they will increase their 2017 budget by 10%

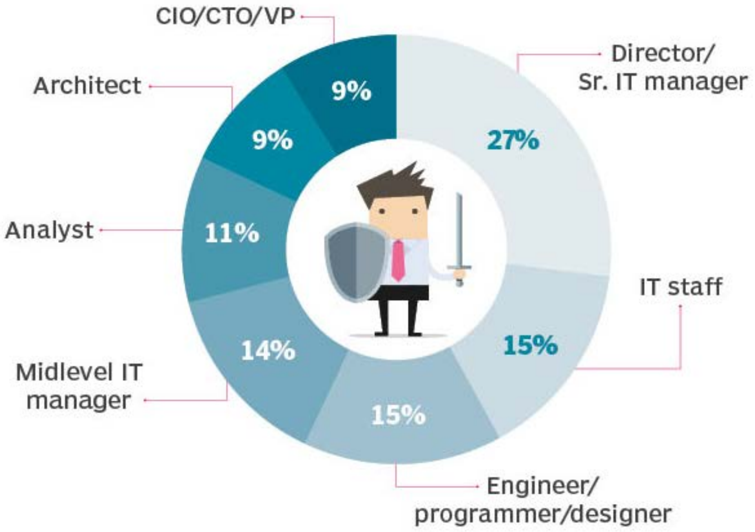
MEDIUM BUSINESSES ARE MODERATE SPENDERS

24% intend to increase their 2017 budget by 5-10%

LARGE BUSINESSES ARE THRIFTY SPENDERS

29% intend to keep their 2017 budgets the same

Who are the security survey respondents?



Small businesses lean toward a hybrid cloud model (46%), while medium-sized businesses prefer an on-premises private cloud model (57%). Large businesses have a variety of choices, with most respondents leaning toward on-premises private cloud (56%) or an infrastructure as a service (IaaS) hosted private cloud model (56%).

Thrifty spending in 2017 also requires that IT review their budgets. According to the survey, small businesses are the biggest spenders, with

25% increasing their 2017 budget by 10%. Medium businesses are moderate spenders, with 24% increasing their 2017 budget by 5-10%. Large businesses are thrifty, with 29% keeping their 2017 budgets the same as the previous year.

↘ Next article

In this e-guide

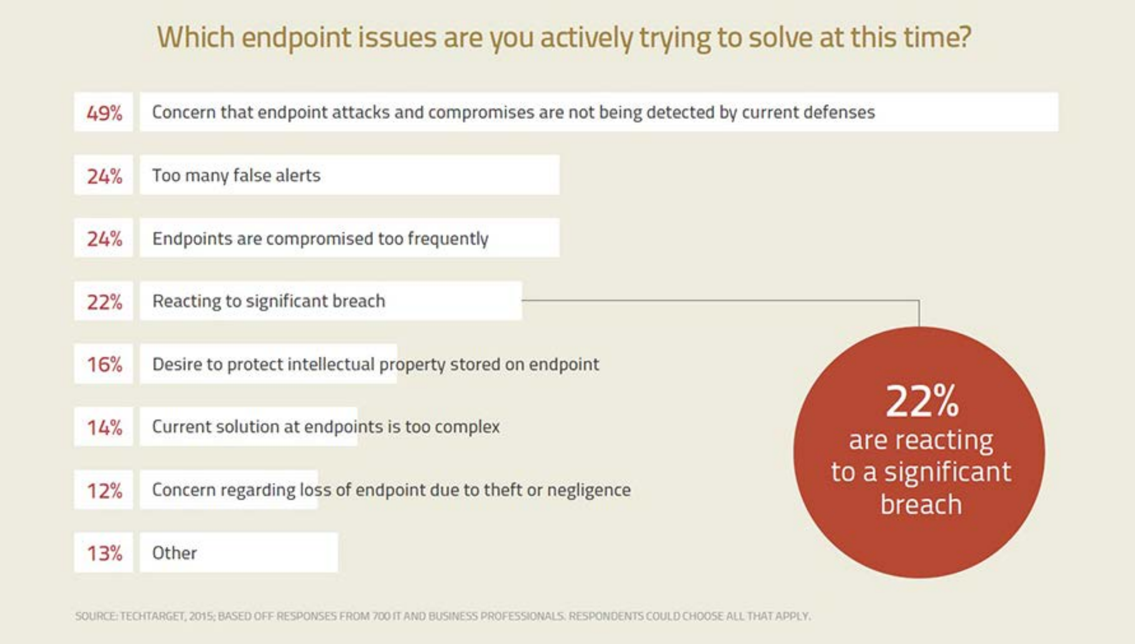
What endpoint protection software is on your short list?

Kathleen Richards, Editor - Information Security

Endpoint protection software for desktops and servers is adding more and more functionality to respond to the challenging threat climate. Many endpoint protection suites also offer policy integration and data protection for the tablets and smartphones of an increasingly mobile workforce. But according to the North American readers we surveyed, the changes may not be enough.

TechTarget polled 700 IT and security professionals at medium-to-large enterprises, who told us that they had active endpoint security projects or technology purchases in the next 12 months. Nearly half of the respondents said their security investments are being driven by the need to protect against threats not detected by traditional endpoint security products; 24% are concerned about too many false alerts or endpoints that are compromised too frequently. For 22%, it's the all-too-common scenario -- they are reacting to a significant breach.

Which endpoint issues are you actively trying to solve at this time?

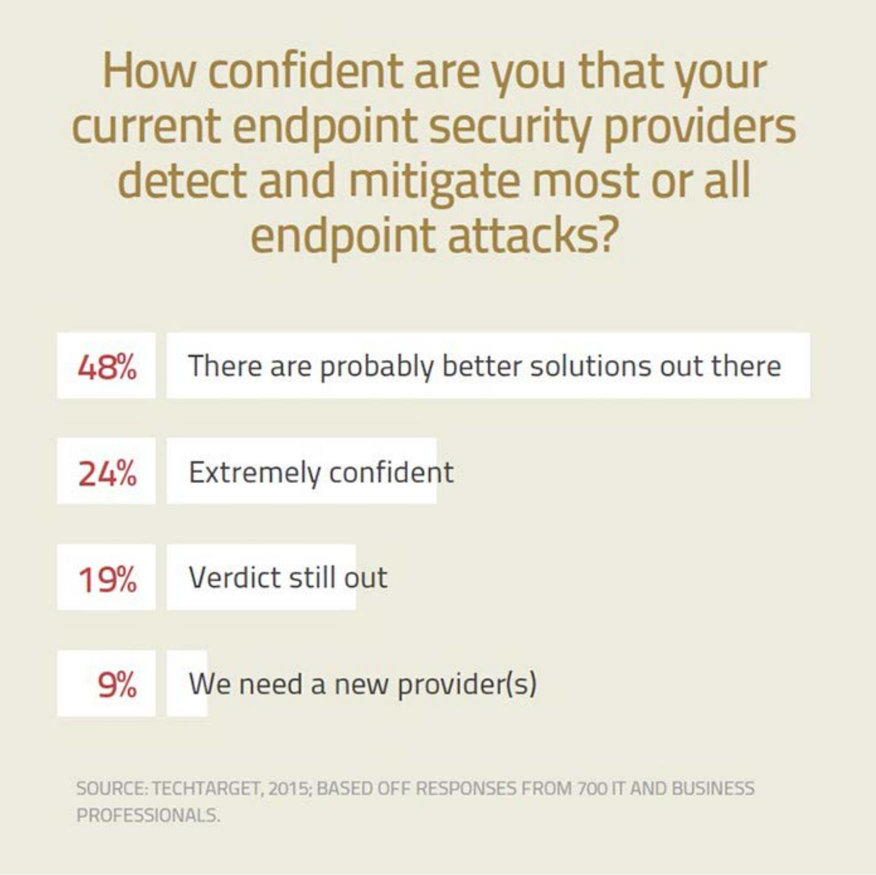


SOURCE: TECHTARGET, 2015; BASED OFF RESPONSES FROM 700 IT AND BUSINESS PROFESSIONALS. RESPONDENTS COULD CHOOSE ALL THAT APPLY.

Many organizations are still in search of effective protection techniques against unknown threats and malware. Whether that requires layering network and endpoint security products, using existing technologies properly, integrating policies across multiple environments or switching endpoint protection software providers; almost half of those surveyed said, "There are probably better solutions out there." Desktop virtualization is part of the endpoint protection of 50% of the organizations surveyed. However, less than half (42%) have an endpoint strategy for employee-owned (BYOD) devices.

In this e-guide

Enterprises can adopt proactive approaches, according to analyst firm Gartner, by using technologies that support application controls, vulnerability analysis and patching on endpoints. Tools that offer a range of protection techniques, whose "efficacy" is evidenced by independent test labs, may also help.



SOURCE: TECHTARGET, 2015; BASED OFF RESPONSES FROM 700 IT AND BUSINESS PROFESSIONALS.

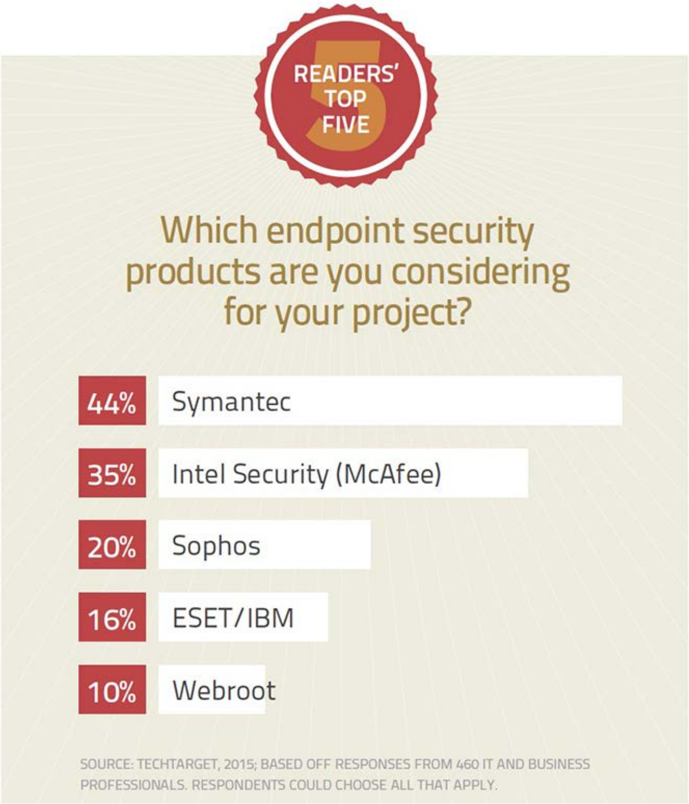
Traditional endpoint security products have moved well beyond antivirus and personal firewalls, and more products have focused on closing the gap between endpoint detection and response. This shift reflects the growing need to identify and remediate threats in less time.

Roughly half of survey respondents indicated that their organization is shifting away from static scanning as the primary protection for endpoints. When asked which approach was most effective for securing endpoints, one third said anomaly detection coupled with quick containment and response; 22% indicated traditional virus scanning tools; 20% said tighter account controls preventing admin-level use of systems; and 8% favored whitelisting applications.

Which criteria of an antivirus/antimalware product are most important? Price ranked first (53%), followed by efficiency of signature scanning with minimal performance degradation (51%); behavior blocking and monitoring of system calls made by unrecognized software (50%); ease of remediation, including removal and cleanup of detected attacks (48%); and inclusion of a personal firewall (20%).

Despite the calls for change, when we asked readers which enterprise endpoint protection software they were considering for their current project or purchase, traditional market leaders (with the highest usage among those surveyed) topped their short lists.

In this e-guide



SOURCE: TECHTARGET, 2015; BASED OFF RESPONSES FROM 460 IT AND BUSINESS PROFESSIONALS. RESPONDENTS COULD CHOOSE ALL THAT APPLY.

In spite of sweeping organizational changes in 2015, Symantec's Endpoint Protection software remains on the short list of 44% of readers. The company split its information management and security products into two businesses after announcing the strategy in October 2014. Version 12 of the company's antivirus and personal firewall software for desktops and servers running Windows, Mac OS X and Linux, was released in November. The software is tied to other technologies, namely Symantec Online Network Advanced Response, or SONAR, to monitor application behaviors to address unknown threats beyond antivirus signatures. Endpoint Protection 12 also supports the company's Security Technology and Response for scanning endpoints and Advanced Threat Protection for servers, but some technologies require separate management consoles.

Intel Security (McAfee), another heavy hitter in this category -- it has the second largest market share worldwide, according to Gartner -- was shortlisted by 35% of the readers surveyed. Sophos Endpoint Protection software, ranked third with 20%, is focused on prevention and faster detection and remediation. The company uses an evolving network-to-endpoint strategy based on heartbeat synchronization and context-aware security. Like other vendors, Sophos is building on its endpoint security with mobile, and shifting through sensor and threat information with help from its SophosLabs cloud. Webroot also landed on the shortlists of 10% of those surveyed. In a somewhat unique approach, the Webroot SecureAnywhere technology relies on behavioral analysis to detect anomalies and malware. Its back-end databases are stored in the cloud, which offers enterprise users a lightweight client.

Gartner expects enterprise protection platforms to continue to integrate more functionality such as enterprise mobility management and data loss prevention. "In the longer term, portions of these markets will be subsumed by the EPP market, just as the personal firewall, host intrusion prevention, device control and anti-spyware markets have been," according to Gartner research analysts Peter Firstbrook and Eric Ouellet, who published a report on endpoint protection software in February. Many companies already invest in endpoint and mobile data protection, their research shows. More endpoint protection suites are also integrating application controls and vulnerability analysis into their mobile offerings, which could satisfy the EMM requirements of smaller-size organizations.

Next article

In this e-guide

Improve endpoint security protection with advanced tools and techniques

Michael Cobb, CISSP-ISSAP

Given the diversity of devices, combined with the wide assortment of users who now connect to an enterprise network, *absolute* security may be impossible. But better endpoint security protection *can* be attained. There are various technologies that can help safeguard data stored on endpoints while protecting the network from devices that may be vulnerable to attack or already compromised. Network access control, data loss prevention and robust data destruction can work together for better endpoint security protection and prevent devices from putting enterprise data at risk.

What NAC does

Network access control (NAC) is a key technology for admission control, based on the overall security posture of users and their devices. Preadmission security policy checks, and the ability to automatically remediate noncompliant devices, ensure that each endpoint meets a minimum level of compliance before it can fully connect to the network. This not only ensures that endpoints are capable of protecting themselves from attack by malware, but also stops them from putting the rest of the network at risk. NAC can leverage user and device profiles in back-end data stores, such as Lightweight Directory Access Protocol, RSA and Active Directory. This enables routers, switches and firewalls to work together to determine who or what is trying to connect to the network and assign the appropriate access. This provides better endpoint security protection through greater coordinated defense-in-depth with security controls able to share their knowledge of network and device behavior.

NAC products can provide detailed information about the status of an endpoint's security: Are all necessary patches applied? Is hard-drive encryption enabled? Is the host-based firewall running? Which ports are open? While answering these concerns, and more, context-aware capabilities provide ongoing protection during each network session. Support for more specialized equipment -- such as point-of-sale systems, kiosks, supervisory control and data acquisition systems that may connect to the network -- is also important, as is integrating NAC with mobile device management technologies so that the security status of mobile devices can be checked.

Where DLP fits

While NAC can keep endpoints compliant and control their access to resources, data loss prevention (DLP) technologies provide better endpoint security protection by defending the data on devices from unauthorized attempts by careless or malicious users to copy or share it. DLP tools use deep content filtering to inspect and control the data a user or device is trying to download, copy, print, share or transfer to both prevent unauthorized use and stop sensitive data from leaving the network. This provides real-time data protection as user accounts can be automatically disabled or devices quarantined as soon as a suspicious data -- e.g., large uploads or downloads, odd login times and so on -- transfer begins.

They can be stand-alone or cloud-based tools, or integrated into existing endpoint security suites. Extending data loss prevention to mobile devices, whether corporate- or user-owned, usually requires some form of mobile device management product. Many of these can also ensure data on mobile devices is always encrypted.

Required: Data Destruction

Encryption should, of course, be used on all endpoints, but the less sensitive data left on devices, the better it is for endpoint security. The turnover of network endpoints has never been higher, and data destruction polices need to be applied to all devices that have the ability to store data. Correctly sanitizing an endpoint's drive or flash storage when it is reassigned or decommissioned is essential to destroying all the electronic data on it; normal file deletion commands only remove pointers to the data, which means it takes only a trivial effort, using common software tools, to recover the actual data.

Better endpoint security protection requires reducing the number of endpoints holding forgotten copies of classified information, which reduces the chances of enterprise data being leaked or exposed. Combining robust data destruction with NAC and DLP technologies will greatly improve the overall security of endpoints and the data they store or process.

Next article

To find the best endpoint security tools, focus on these features

Kevin Tolly, Founder - The Tolly Group

When McAfee was formed in 1987 to sell the first commercial antivirus package, it set a baseline approach that has persisted to this day: Have a list of character strings that are unique to particular viruses and then scan files (and those files in memory) for the strings. Generally, if the scanner found one of the strings (the virus's signature), it had very probably found a virus.

As other vendors emerged, they battled over their effectiveness at various aspects of this passive scanning approach. They focused on compiling the biggest, most comprehensive database of virus and malware signatures. The best endpoint security software available simply scanned for “bad” signatures every time a file was downloaded or opened. Vendors would boast about having better research teams to catch more viruses.

A number of additional virus-hunting techniques were introduced over the years -- heuristic scanning to deal with polymorphic viruses that purposefully avoided having consistently scannable signatures, allowing the software to run but cordoning off its requests to the operating system to watch for malicious behaviors, and the introduction of reputation-based ratings to score the likelihood that a given executable could be relied on to be safe. But the basic pattern held: A monolithic software package at the endpoint watched all the new files and called out known bad actors.

Recently, though, the enhancements have begun to overtake the core static scanning components of antivirus software. "Next-gen" endpoint security tools have emerged as a new product category with specific characteristics.

Real-time a defining trait of next-generation endpoint security

Signature files are static and threats are dynamic. At a certain point, it simply became impractical (if not impossible) to update signature files incessantly and instantaneously in an attempt to contend with zero-day threats. These are by definition threats that no virus collector has yet catalogued as of the moment they are launched.

So, if anything, "real-time" is the defining characteristic of the best endpoint security offerings in the next generation of tools. For many products, this means jettisoning the endpoint-resident signature file altogether and using different means to ferret out viruses and malware.

Analysis replaces signature matching

In next-gen tools, the best endpoint security offerings replace signature matching with analysis (in real-time, of course). Different products, naturally, will analyze different aspects and attributes to determine if a piece of code represents a threat to the endpoint.

Some of the analysis techniques have evolved from traditional endpoint products. For example, reputation analysis has been in use for a number of years. This technique generally involves searching a database containing lists of known "bad actor" IP addresses and websites that have been confirmed to be sources of malware.

For some traditional vendors, moving to next-gen tools means taking various techniques that they have developed over the years within their traditional product line and integrating to provide a more effective solution.

Many security products will evaluate multiple attributes of a piece of code. Each piece of information would be used to build a risk score that, ultimately, would help the tool determine whether the code should be blocked. One next-gen vendor claims to have developed over six million possible indicators of malware and uses that information to determine whether a given piece of code is malware.

Isolation aids analysis

Another variation of analysis involves simply letting the suspect code run on your system, to analyze what it does. If it tries do something bad, like erase files or make outbound network contact without authorization, then by definition it is malware and should be contained.

This approach, known generally as *sandboxing,* is not new. What is new is the implementation: One vendor leverages the high-performance virtualization features built into most PC hardware these days. That vendor creates a micro VM that can be termed a *one-sample sandbox*. The code is run, its behavior analyzed, a threat decision is made and the VM is discarded. Every sample gets its own fresh VM within which to run and be analyzed.

Even best endpoint security tools can't do it all

In the realm of next-gen endpoint security, niche vendors are continually coming up with new takes on the issue. There are always new features being added. But it's also important to understand what next-gen endpoint security is *not*. It is not a one-size-fits-all solution to your endpoint security woes. Nor is it a "me, too" list of vendors all doing the same thing. And, importantly it is not necessarily meant to be a total replacement for traditional endpoint security. It is simply a means to obtain the best endpoint security possible which is, in turn, a key element of an overall approach to keeping your systems secure.

Next article

In this e-guide

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at http://SearchSecurity.com/

Images; Fotalia