Can We Say Next-Gen Yet? State of Endpoint Security

A SANS Survey

Written by G. W. Ray Davidson, PhD

March 2016

Sponsored by
Sophos

Executive Summary

The perimeter continues to dissolve, and the definition of endpoint is evolving, according to results of the SANS 2016 Endpoint Security Survey, now in its third year. In it, respondents say their organizations continue to connect new and different types of endpoints, including point-of-sale (POS) devices, printers, mobile devices, building security systems and even wearables to their networks.

As we might expect, 90% or more consider desktops, servers, routers, firewalls and printers to be endpoints that need to be protected. After that, respondents include other less-typical devices in their definition of endpoints that warrant protection: 71% include building security (access/surveillance), 59% include employee-owned mobile devices and 40% consider industrial control systems as endpoints that need to be protected. Some respondents also consider POS devices, smart cars, emulated endpoints in the cloud and wearables as endpoints needing protection, highlighting the diversity of thinking among respondents.

Respondents still put most of their security efforts into desktops, laptops and several types of servers, which they reported as the most commonly exploited endpoints. In the past 24 months, 85% of respondents reported compromises of desktops, with 13% of respondents considering their desktop compromise "widespread." Another 68% reported compromised laptops. These two types of endpoints are likely to have login and access credentials, the most commonly exfiltrated information reported by respondents who had been breached. These types of endpoints are attractive to most attackers because the credentials can provide access to more valuable information in the enterprise network.

Of the organizations hosting nontraditional endpoints such as printers, POS devices and even wearables, many already appear to be wrapping these devices into their enterprise security programs. For example, 9% allow wearables into their network, and 8% actually include them in their programs. Other responses show there is increasing desire to cover new forms of endpoints in security and incident response (IR) programs.

About Their Breaches

44% admitted one or more of their endpoints had been compromised in the past 24 months

57% of compromises (the majority) are discovered as a result of antivirus/IPS alerts at the endpoints, with **36%** discovered via automated security information and event management (SIEM) alerts

27% of compromises were detected through third-party notification, reinforcing the need for additional endpoint monitoring and protection

21% of compromises are being detected through hunting for compromised endpoints using indicators of compromise learned from threat intelligence

About Their Security

86% consider desktops to be endpoints that should be managed and protected, while **79%** feel the same way about servers; and **74%** include desktops and/or servers in their security and incident response programs

72% consider employer-owned mobile devices to be endpoints worth protecting, but only **54%** cover these devices in their security and incident response programs

9% said wearables are connecting to their networks, and just over **8%** cover wearables in their security and response policies

Survey Demographics

Respondents indicated that they have endpoints located on almost every continent, with the highest concentrations in the U.S. (76%), Europe (34%) and the Asia-Pacific region (31%). They represented small to very large companies, having a range from fewer than 100 user accounts and endpoints to 500,000 connected to the network. The sample was fairly evenly split, with 30% representing organizations with more than 10,000 endpoints connecting, 34% from organizations with 1,000 to 9,999 endpoints, and 28% with fewer than 999 endpoints connecting (another 4% didn't know). See Figure 1.

How many unique user accounts and endpoints are currently connecting to your organization's network?

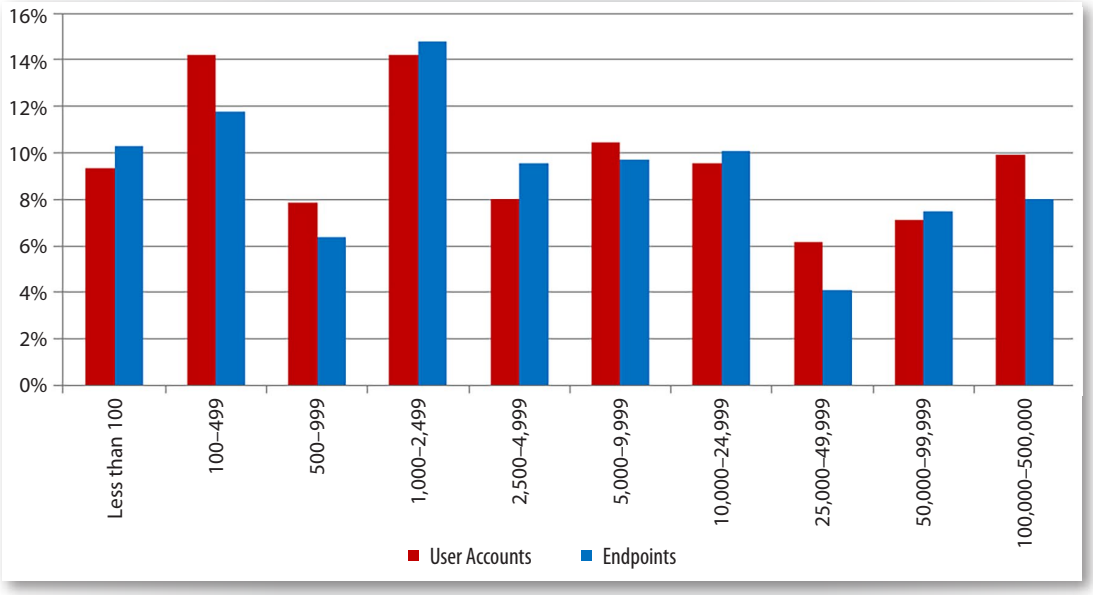

Figure 1. Network Size

As with most SANS surveys, the survey respondents represent a wide variety of network sizes, from small and midsize enterprises to large corporations, indicating that awareness is not confined to a particular size or type of organization.

Industry Type

Similar to last year's survey,[1] financial services and government made up about one-third of survey participants. High tech represented 10% of respondents, 9% came from health care, and 8% from education. Figure 2 shows the top 10 industries represented in the survey.

What is your organization's primary industry?

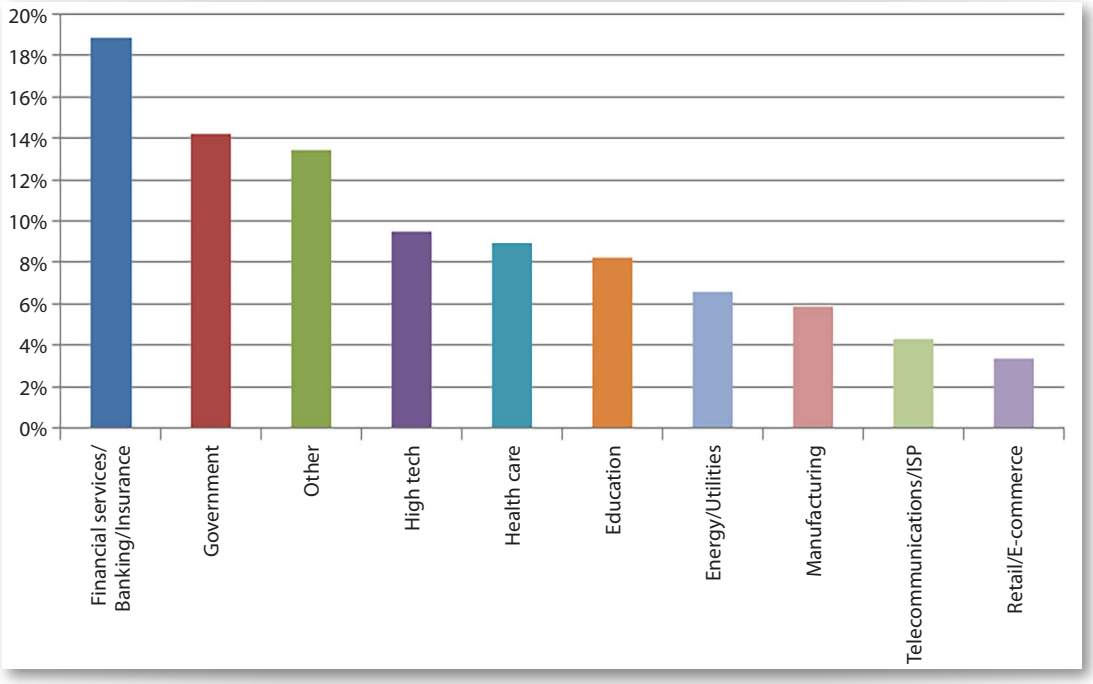

Figure 2. Top 10 Industries Represented

The wide variety of respondents corresponds to an assortment of different drivers for their endpoint programs. Given that they are in the business of protecting peoples' money, financial organizations have historically built robust security programs. As Willie Sutton knew,[2] "That's where the money is." The U.S. government, including Department of Defense networks, represents the largest network in the world, and access credentials make tempting targets for attackers aimed at this demographic. The rest of the main industries represented in this survey have their own burdens to protect their intellectual property, student information, patient data and even the national critical infrastructure.[3, 4, 5, 6]

[1] Williams, Jacob, "The Case for Visibility: SANS 2nd Annual Survey on the State of Endpoint Risk and Security," www.sans.org/reading-room/whitepapers/analyst/case-visibility-2nd-annual-survey-state-endpoint-risk-security-35927

[2] www.fbi.gov/about-us/history/famous-cases/willie-sutton

[3] "Federal Information Security Modernization Act," www.dhs.gov/fisma

[4] "Health Insurance Portability and Accountability Act," www.hhs.gov/hipaa

[5] Family Educational Rights and Privacy, www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33

[6] "Framework for Improving Critical Infrastructure Cybersecurity," www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Respondent Roles

The majority of respondents (62%) have roles directly related to security, including job titles such as security analyst, security manager, CISO, incident responder and compliance manager. Another 29% of respondents specified somewhat more general operational roles, such as system administrator, network engineer or IT manager. See Figure 3.

What is your primary role in your organization?

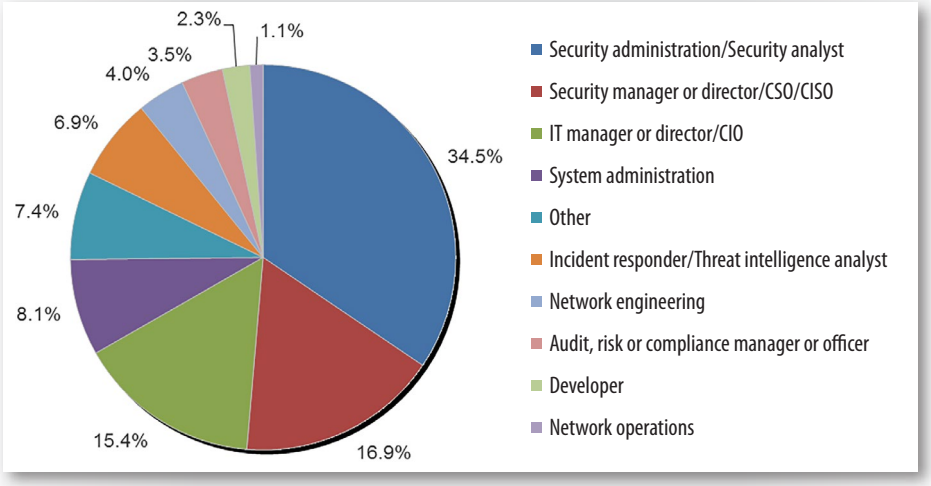

Figure 3. Roles Represented

The understanding of what constitutes an endpoint is changing rapidly, as the network perimeter is dissolving. As technology evolves to address changing business needs, a wider variety of devices is being connected to the network.[7] The most common connected endpoints are still desktops, servers, laptops, printers and network devices such as routers and switches. However, in this year's survey 78% of respondents report connecting employer-owned mobile devices, and 59% report connecting employee-owned mobile devices.

Nontraditional Endpoints

Although retailers represent only 3% of responders, 27% report connecting point-of-sale (POS) devices. As these results show, POS devices are used by more than retailers. For example, three other industries most likely to have POS devices on the network are (from highest to lowest) education, health care and financial services, comprising 57% of the total. Public-facing government agencies, such as motor vehicle departments, courts and others, also host POS terminals. See Figure 4.

If it can be networked, docked, tethered or attached, it needs endpoint security.

—Survey Respondent

Of the devices connected to your network, what device types do you consider to be endpoints that need security management and protection?

Indicate whether or not these device types are included in your security and incident response (Sec/IR) programs.

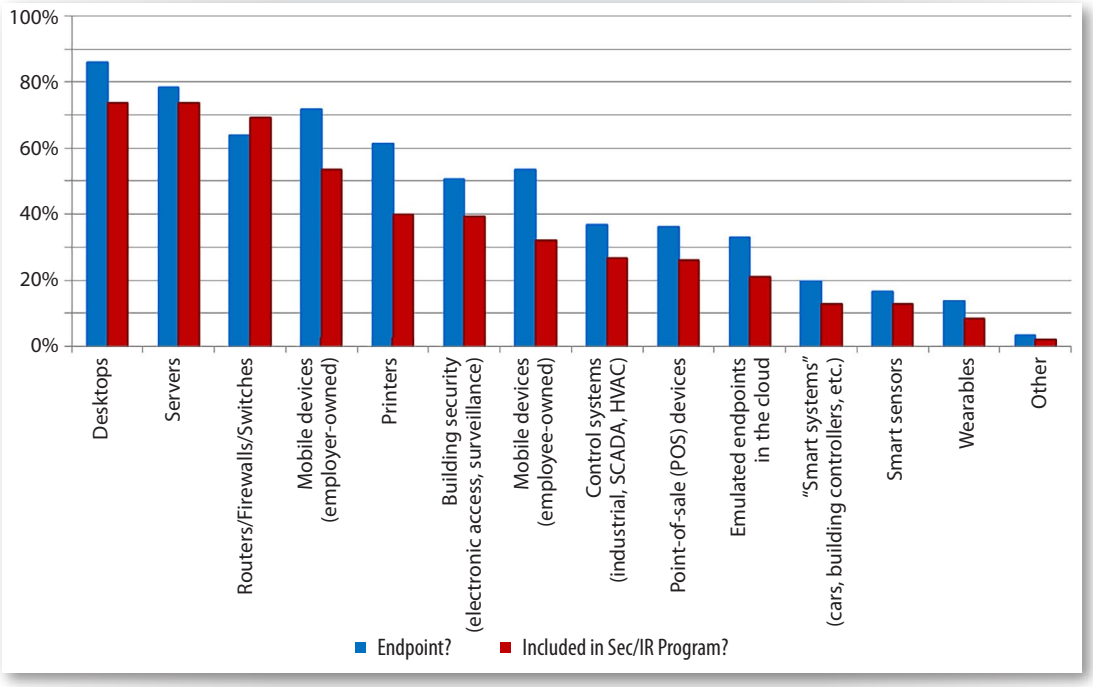

Figure 4. Devices Connecting to the Network and/or Covered by Security Programs

Also interesting is the fact that 9% of the respondents said wearables are connecting to their networks, 14% consider wearables to be endpoints needing protection, and just over 8% cover wearables in their security and incident response policies.

[7] http://arstechnica.com/information-technology/2016/01/how-the-smartphone-changed-everything-or-the-rise-of-byod-in-the-workplace

Covering New Devices

The data point to an interesting trend: Organizations that are onboarding new types of endpoints are more often covering those unusual devices in their programs (with the exception of printers). For example, if we consider coverage of specific types of endpoints by security programs, newer devices such as POS devices, emulated endpoints in the cloud, and wearables are more likely to be covered in management programs than desktops and employer-owned mobile devices. Table 1 illustrates the trend.

Table 1. Percentage of Device Types Connected vs. Coverage of Endpoints by Security/IR Programs

Device	Connected to the Network	Included in Sec/IR Program	% Covered
Point-of-sale (POS) devices	26.6%	25.5%	95.9%
Emulated endpoints in the cloud	23.0%	20.8%	90.6%
Wearables	9.4%	8.2%	86.5%
Servers	94.7%	72.5%	76.5%
Desktops	96.4%	72.5%	75.2%
Routers/Firewalls/Switches	94.6%	68.3%	72.2%
"Smart systems" (cars, building controllers, etc.)	17.6%	12.7%	72.2%
Smart sensors	17.8%	12.7%	71.4%
Mobile devices (employer-owned)	78.1%	52.7%	67.5%
Other	3.3%	2.2%	66.7%
Control systems (industrial, SCADA, HVAC)	40.0%	26.3%	65.6%
Building security (electronic access, surveillance)	70.5%	38.6%	54.8%
Mobile devices (employee-owned)	58.9%	31.5%	53.5%
Printers	89.7%	39.3%	43.8%

The endpoints least likely to be covered are building security systems, employee-owned mobile devices, and printers, according to results.

Different device types present different challenges in endpoint security coverage. For the first and oldest type of devices, which includes desktops, laptops, servers and most networking devices, the technology is mature and well characterized. Solutions typically include an agent or other monitoring component, a communications protocol such as **`syslog`** or some proprietary design, and a collection and reporting capability. While some incompatibilities exist, the device architectures and communications protocols are sufficiently well characterized to allow integration of monitoring capabilities, which facilitates management of the endpoint security. In addition, these devices generally come under the jurisdiction of a single organizational area, so business responsibilities are relatively well defined and clear-cut.

A second category of endpoints—control systems and building security devices—has also been around for some time and has been connected to networks in substantial numbers. But sophistication of the devices themselves is growing, along with recognition that these endpoints are an attack vector. Unfortunately, the embedded technology in these endpoints is often substantially different from that in conventional end user devices. For that reason, the protection technology is also different. Endpoint agents are not as standardized, and sensors are not as easy to integrate into a larger endpoint protection solution. In addition, because building security and the manufacturing/operations associated with control systems have historically been organizationally separate from IT security, they are less likely to be covered by policies than classic devices. It may not even be clear which part of the organization is responsible for the security of these devices. So, for these types of devices, both technical and organizational challenges need to be overcome.

Printers are a common vector used by hackers to establish a foothold elsewhere in the organization. ... It's critical for organizations to include connected printers (often with outdated operating systems) in their endpoint inventories and wrap them into their vulnerability management programs.

The latest devices to be connected to the network include employee-owned mobile devices and wearables. For them, the situation is evolving rapidly, mostly because bring-your-own-device (BYOD) policies and controls are still maturing. While more and more users are demanding the ability to supply their own devices, and some organizations are requiring this or moving to virtual desktop environments, much change is still afoot. Complicated policy issues must be addressed, including data privacy, access and ownership. Although mobile device management (MDM) solutions are maturing, the environment hasn't yet reached the state of the desktop/laptop/server environment. From an organizational standpoint, because these endpoints are generally associated with individual end users, there are usually precedents in policies and processes. As long as existing policies can be extended to cover these devices, it may be possible to apply protection without change. Depending on the organization, there may be varied challenges in adapting existing policies and processes, but the same stakeholders are generally involved, and the principles are similar, if more varied, for these new device types.

It's surprising to see printers are the least commonly covered devices in security programs. Printers are a common vector used by hackers to establish a foothold elsewhere in the organization, and professionals have known about this risk for years. It's critical for organizations to include connected printers (often with outdated operating systems) in their endpoint inventories and wrap them into their vulnerability management programs.

Pathway to Maturity

The sorted data in Table 1 in the previous section describes an organization (and an industry) that is maturing but still struggling to cope with the past. Policies are being created and implemented to cover newer technologies and identified vulnerabilities, such as POS devices and emulated endpoints, but there are still gaps for older endpoint types, including desktops and laptops.

The Endpoint Security Maturity Model, introduced in a previous SANS whitepaper, describes a security model that respondents to this survey are clearly following.[8] The model, illustrated in Figure 5, describes five levels of maturity:

Level I: Random, or Disorganized. Organizations display little to no policy, no endpoint inventory, low user awareness of security, and ad hoc installation, configuration and management of endpoints.

Level II: Reactive, or Tactical. Policy is weak, overbroad and/or poorly communicated; endpoint inventory is nonexistent or out-of-date; some user awareness but no training; no configuration standards or management.

Level III: Preventative. Formal policy exists, but may or may not have been updated recently; policies lag technology; hardware and software inventory exist, but updates are irregular; some user training but no testing of awareness; endpoint protection uses signatures but not heuristics; mobile device management (MDM) and mobile agent tools may be in use.

Level IV: Organized, or Directed. Formalized, functional policies, with a formal and active review cycle; automated and up-to-date hardware and software inventories; formal user training that is assessed and tracked; continuous monitoring and updating of endpoints, including mobile devices.

Level V: Proactive, Comprehensive, Continuous and Measurable. Security program is designed and executed to anticipate change; aligned with IT, procurement and business risk; endpoints are configured and provisioned according to standards, locked down and monitored continuously; initial incident response is fully automated; and the organization participates with relevant computer emergency readiness teams (CERTs) and information sharing and analysis centers (ISACs).

[8] Hardy, G. Mark, "Behind the Curve? A Maturity Model for Endpoint Security," www.sans.org/reading-room/whitepapers/analyst/curve-maturity-model-endpoint-security-36342

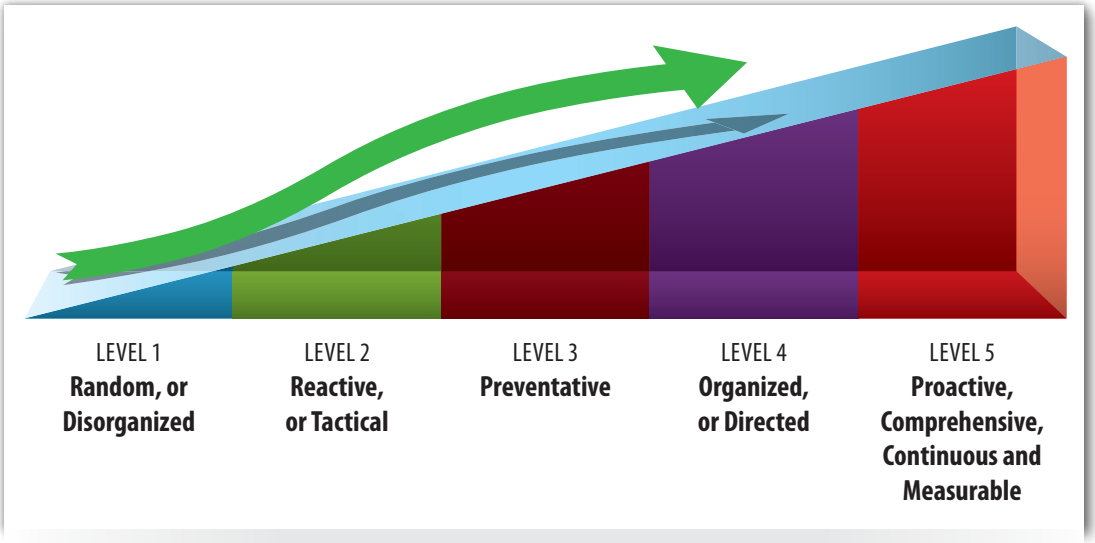

Figure 5. The Endpoint Security Maturity Model[9]

Just as with the general IT Security Maturity Model[10] from which the Endpoint Security Maturity Model is derived, most organizations are in the lower levels of maturity, but they are progressing.

[9] "Behind the Curve? A Maturity Model for Endpoint Security," www.sans.org/reading-room/whitepapers/analyst/curve-maturity-model-endpoint-security-36342, Figure 2, page 9.

[10] Tom Scholtz and Jay Heiser, "ITScore for Information Security," Gartner, June 21, 2013, www.gartner.com/doc/2507916/itscore-information-security (Gartner account required)

Breaches and Consequences

An indicator of maturity is how frequently an organization is compromised and how well and thoroughly it responds when its endpoints are breached. In this survey, 44% of respondents say one or more of their endpoints had been breached in the past two years, mostly on a limited scale.

Systems Breached

Desktops and laptops represented the most breached systems, with those breaches also reportedly involving more widespread compromise. Of the breaches reported by the 44% of respondents who indicated they had had an endpoint compromised within the past two years, 85% involved desktops, 68% involved laptops, and 55% affected servers. Breaches of desktops and laptops were also the most likely to be considered widespread (13% and 10%, respectively), although the majority were limited to a small number of endpoints per breach. Servers, too, are attractive targets because of the likelihood that they contain sensitive data, intellectual property and administrator credentials. See Figure 6.

Over the last 24 months, what types of endpoints and endpoint apps have been compromised?
Please indicate if these were widespread or limited in scope to either a small number of endpoints or just one endpoint.

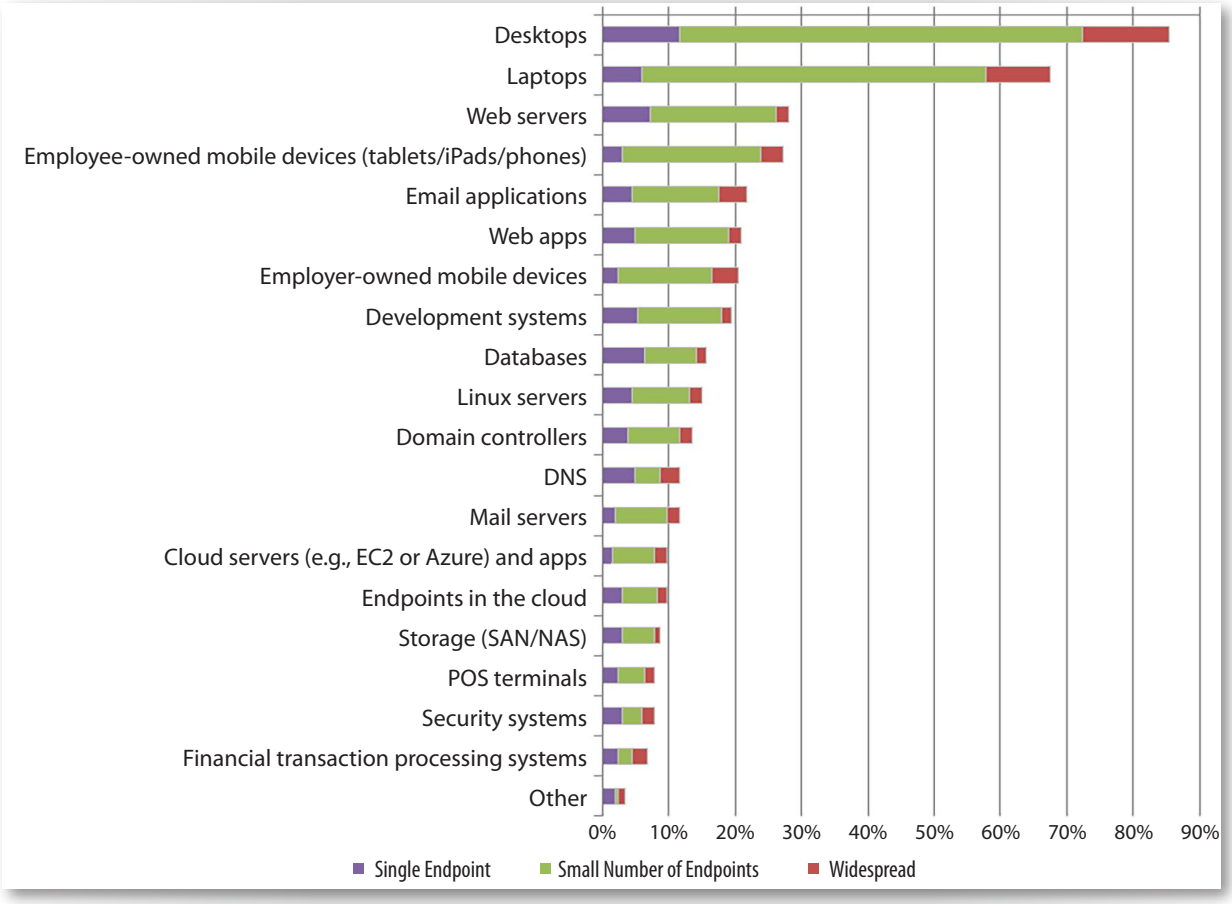

Figure 6. Types of Endpoints Breached and the Related Extent of Compromise

TAKEAWAY:

Assume an attacker is already inside your network. Determine the path to the most valuable target and guard the endpoints along the way especially well.

Breaches on less traditionally deployed endpoints aren't as common, according to results. For example, only 8% of breaches affected POS terminals, although 27% of respondents report connecting these to their networks.

One point of concern is that employee-owned devices are already being reported as having been breached as frequently as web servers, despite being relatively new additions to the endpoint universe. Web servers have been a very popular and successful vector of attack for some time. The rapidity with which employee-owned devices have risen to the same level should give pause to security personnel.

Data Breached

Desktops and laptops are most likely to contain access credentials and are the easiest to compromise, usually by targeting the user. Not surprisingly then, the most common type of data compromised (49%) was login and access credentials, which can be used to gain access to other systems containing more valuable enterprise information, such as personally identifiable information (PII), intellectual property, trade secrets, source code and so on. These types of information were also reported as compromised in the survey, although at a lower rate. Figure 7 illustrates the types of data breached or exfiltrated in the reported incidents.

What data was breached or exfiltrated as a result of the incident? ***Select all that apply.***

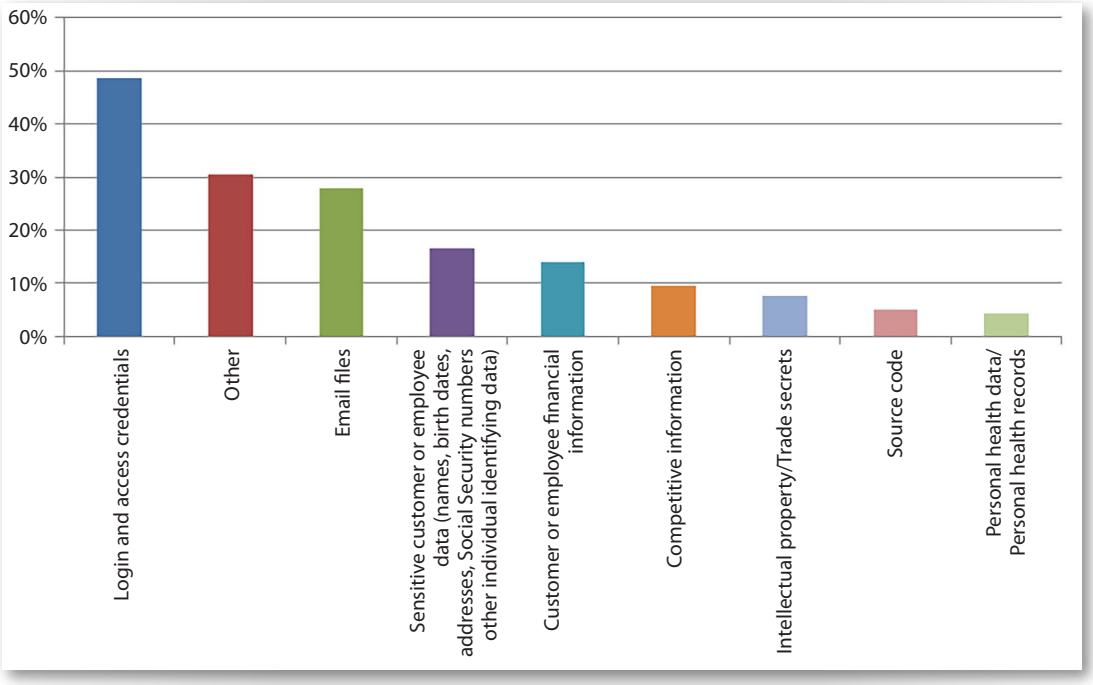

Figure 7. Types of Data Compromised

The "Other" category includes compromise of a web server so it would act as a command and control node, crypto/ransomware attacks, exfiltration of Microsoft logs and a Global Address List, and many responses of "unknown" or "nothing taken."

Detection

As one might expect, the vast majority of compromises are detected reactively—either via an alert from endpoint antivirus or IPS directly, or via a SIEM or similar system. Unfortunately, 27% were discovered via notification from a third party, such as law enforcement, affected customers or business partners. This situation reflects a relatively low level of maturity; reactive behavior falls within Level II of the Endpoint Security Maturity Model.

The good news is that 21% percent of respondents indicated they had detected compromises through use of hunting techniques, a proactive approach that involves searching for potential incidents rather than waiting for alarms to tell you something's wrong. This is a step in the right direction. In last year's survey, only 16% of respondents used proactive techniques to ferret out threats before they became breaches. Figure 8 illustrates how respondents detected compromises.

How did you detect the compromise? ***Select all that apply.***

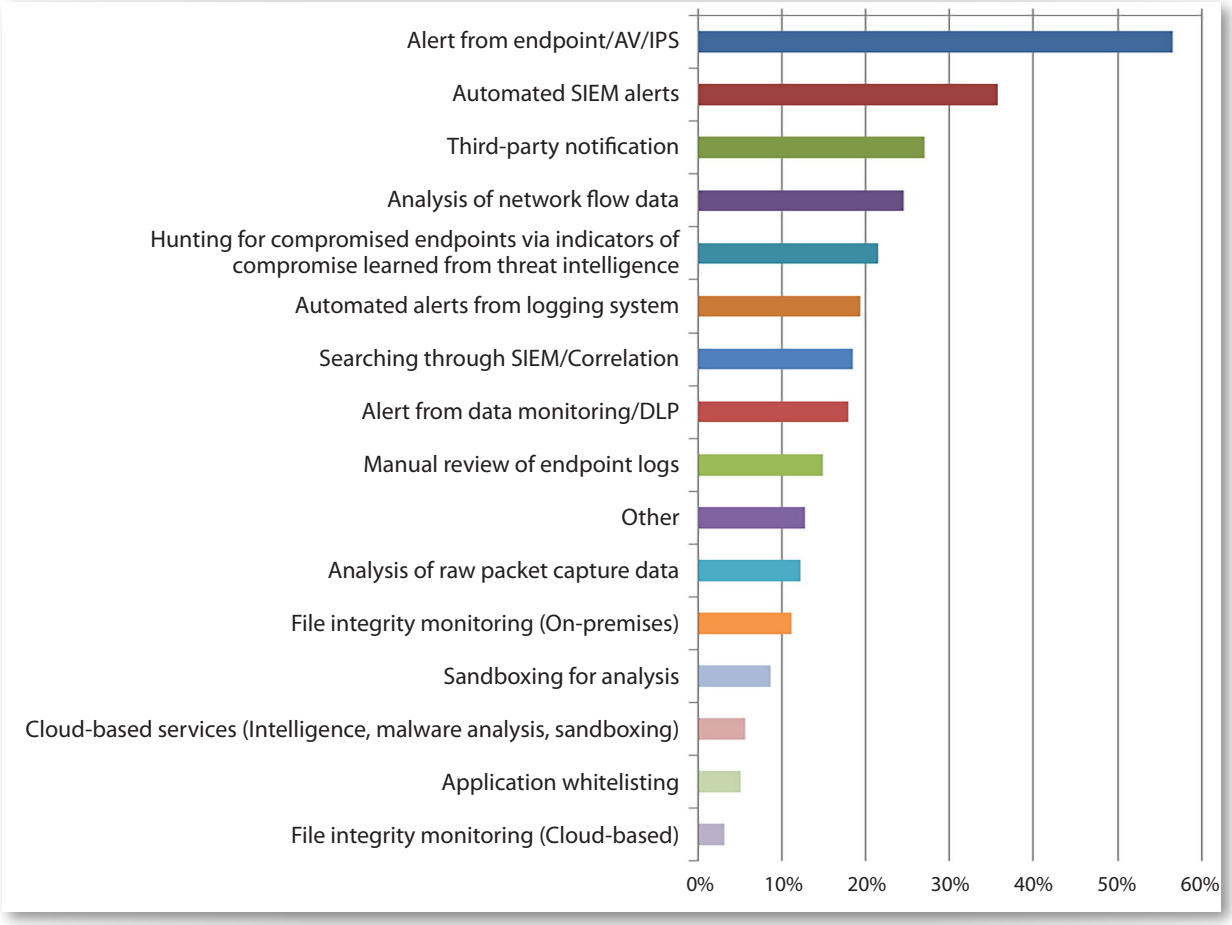

Figure 8. Methods Used to Detect Compromises

This increase in proactive activity is further supported by the decrease in respondents who didn't know whether or not they had used proactive discovery techniques to detect threats from 34% in 2015 to 15% in this year's survey. Moreover, in 2015, only 15% of respondents detected more than half of their threats proactively, whereas 32% of respondents reached the same milestone in 2016.

These results represent an increase in maturity. Proactive behaviors, such as using hunting techniques, are associated with Levels IV and V in the Endpoint Security Maturity Model.

Time Invested

Most of our respondents (55%) reported it takes them on average three or more hours per compromised endpoint. Alarmingly, 7% stated it takes more than 24 hours per endpoint! See Figure 9.

When responding to an incident, how much time (in man-hours) do you spend (on average) per compromised endpoint?

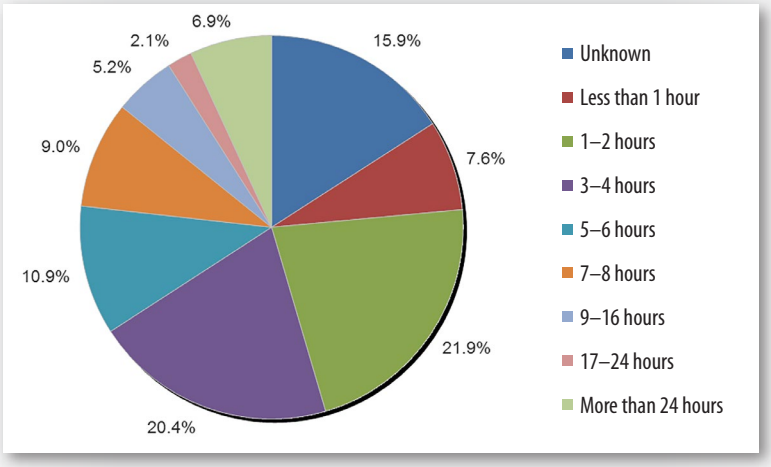

Figure 9. Time Spent per Compromised Endpoint

Note that these endpoint breaches occur across the enterprise, so you can quickly get a sense of the impact these incidents have on an enterprise in both lost time and productivity.

Visibility

During investigations, the majority of respondents say they were able to collect basic information about their endpoints, including operating system and version, applications, type of device, login information, ports and interface data. However, 41% of respondents reported they were unable to acquire endpoint information regarding unauthorized possession of sensitive data. This was the highest reported unmet need and is consistent with the increasing presence of employee-owned devices on the network. See Figure 10.

Indicate whether or not you are able to acquire the endpoint information you need most when detecting threats.
Leave a choice blank if you do not need the information.

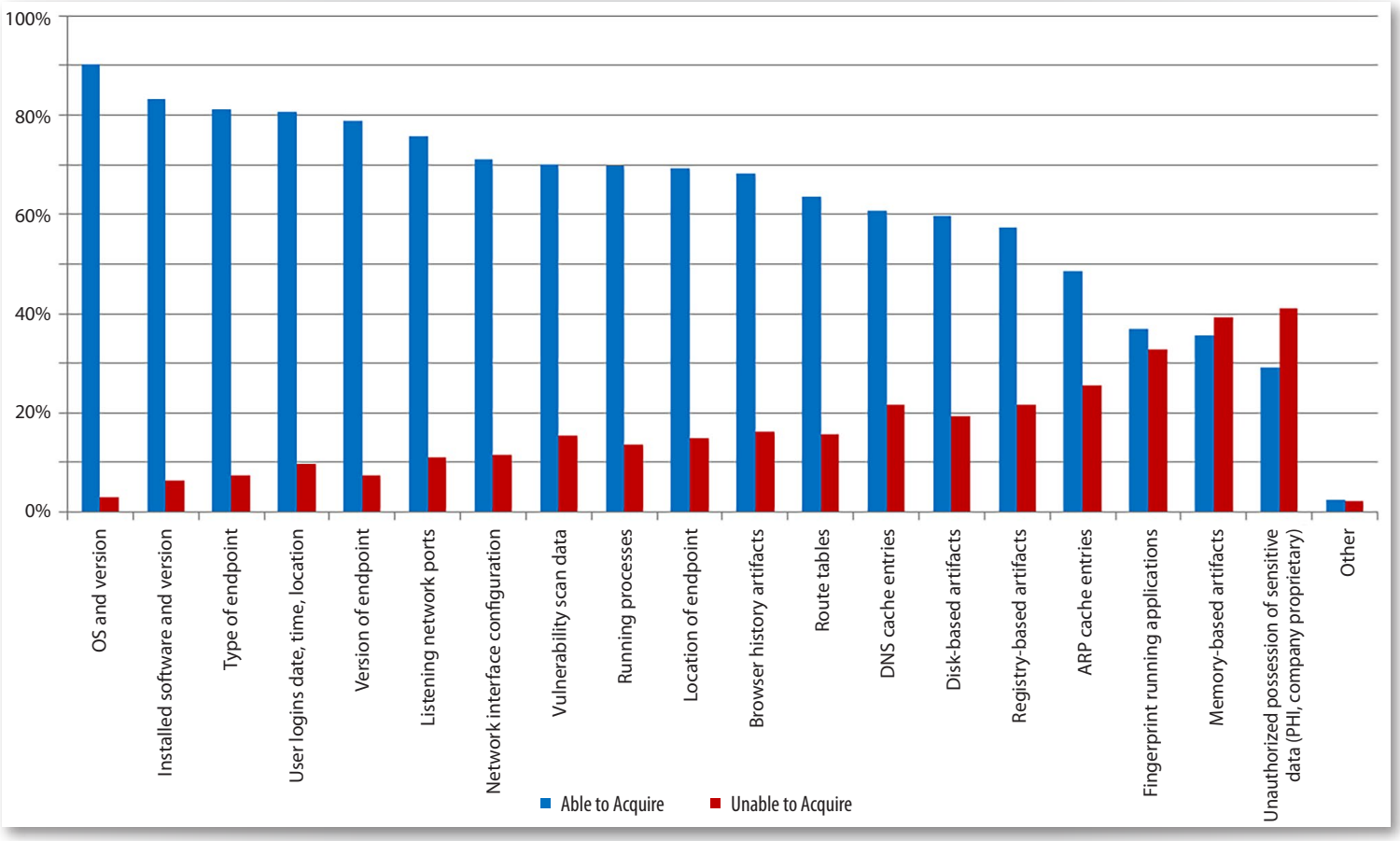

Figure 10. Ability to Acquire Information Needed

Attackers know how to create attacks that do not leave traces on disk, and defenders are scrambling to keep up. Yet 39% of respondents reported they were unable to acquire necessary memory-based artifacts as part of their endpoint threat response. However, respondents are at least aware of the need for memory analysis, and this is a positive development.

Desktops and servers continue to be primary targets even though they are covered in a security/IR plan because they likely contain valuable data and are relatively easy to compromise via the end user. Although mobile devices are somewhat more likely to be covered by security programs, they are also prime targets for exploitation, for these same reasons. The increased use of mobile devices is likely to exacerbate the problem. As organizations continue to add endpoints, the attack surface will continue to expand for attackers.

Table 2 shows the key categories of endpoints being used in enterprises and the gaps that exist between what is connected, what security personnel believe should be managed, and whether those endpoints are actually covered in the organization's security/IR program.

Table 2. Endpoint Management of Selected Key Devices

Device	Connected to the Network	Endpoint Should Be Managed	Included in Security/IR Program
Desktops	96.4%	84.8%	72.5%
Servers	94.7%	77.4%	72.5%
Control Systems (industrial, SCADA, HVAC)	40.0%	36.2%	26.3%
Building Security (electronic access, surveillance)	70.5%	49.8%	38.6%
Employee-Owned Mobile Devices (BYOD)	58.9%	52.7%	31.5%
Wearables	9.4%	13.6%	8.2%

TAKEAWAY:

If the organization is not designed to support changes as necessary, security will lag behind both technology and business process.

These results are interesting in that the perception of which endpoints should be managed is lower than the percentage that actually appears on the organizations' networks. Further, the percentage of devices covered in security programs is significantly lower than both the devices actually in use and the perceived need to protect them.

With regard to wearables, the perception that such devices need to be managed is greater than their implementation on respondents' networks. This increased perceived need for management makes sense, given that the devices are relatively new entrants into organizational networks.

As noted in the section "Covering New Devices," the challenge for these devices is on the technological side. The increasing prevalence of BYOD acceptance means that procurement is no longer making all the purchasing decisions based on standards, and users are connecting a wider variety of devices to the network. These devices may have different technical characteristics, such as operating system and filesystem structure, so the protection technology likely varies. Security is always more difficult in a varied environment, adding challenges for the security department. The various devices that comprise this new type of endpoint require multiple solutions, all of which must be integrated into the overall strategy for protecting the enterprise.

Next-Generation Protection

Tools themselves are maturing and meeting the varied demands that respondents ask of their endpoint security systems. Not surprisingly, these demands include fairly common technologies such as antivirus/IDS, application whitelisting and encryption, but increasingly users are also demanding vulnerability assessment, application awareness, threat intelligence and support for incident response. See Figure 11.

The challenge for next-gen endpoint protection is ensuring C-level awareness of and funding for technology to address gaps on the endpoint, and configuring these technologies to work together to protect endpoints both proactively and reactively.

Please indicate which features and functions you would expect to be included in next-generation endpoint protection? *Select all that apply.*

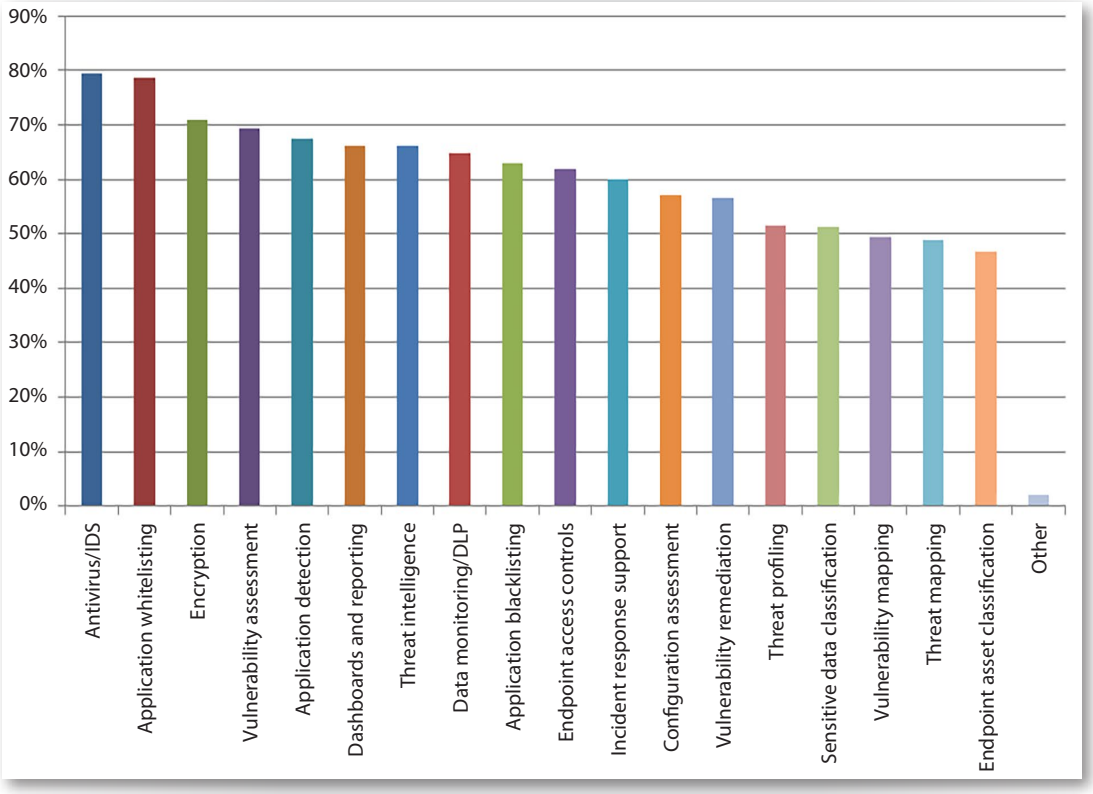

Figure 11. Features and Functions Needed in Next-Generation Endpoint Protection

Write-in responses included such items as browser activity sandboxing, integrity checking, auto-containment and resolution, and categorization of vulnerabilities.

All of these technologies exist today through different vendors. The challenge is twofold: ensuring C-level awareness of and funding for technology to address gaps on the endpoint, and (often an even bigger challenge) configuring these technologies to work together to protect endpoints both proactively and reactively, which is why their level of achievement varies. The majority of respondents (96%) are still running antivirus: 75% are doing so internally, 3% are using only cloud providers for this function and 19% are doing so with both cloud and internal endpoint protection. Another 77% assess vulnerabilities on their endpoints, 73% say they are encrypting data on endpoints, and 72% have implemented access controls.

The majority of these functions are performed internally. However, more respondents are indicating they use cloud services for threat intelligence (12%), threat profiling (10%), threat mapping (9%) and vulnerability assessment (9%) than the other endpoint services, as shown in Table 3.

Table 3. How Respondents Achieve Needed Features and Functions

Answer Options	Achieved Internally	Achieved with Cloud Service	Achieved with Both	Not Achieved
Antivirus/IDS	74.7%	3.2%	18.5%	2.2%
Application blacklisting	38.0%	4.6%	9.5%	37.0%
Application detection	50.1%	3.9%	9.7%	25.5%
Application whitelisting	35.8%	3.2%	8.8%	41.1%
Configuration assessment	49.1%	4.1%	8.3%	26.5%
Dashboards and reporting	47.4%	6.3%	17.0%	18.0%
Data monitoring/DLP	37.5%	5.6%	11.9%	34.5%
Endpoint access controls	57.4%	3.9%	10.9%	18.0%
Endpoint asset classification	42.8%	4.1%	9.0%	31.4%
Encryption	57.9%	3.2%	11.9%	18.5%
Incident response support	41.1%	3.6%	15.3%	28.2%
Sensitive data classification	33.3%	3.4%	7.8%	41.6%
Threat intelligence	23.6%	12.2%	17.0%	34.1%
Threat mapping	19.5%	9.0%	11.9%	44.5%
Threat profiling	21.4%	9.5%	10.0%	43.8%
Vulnerability assessment	53.3%	9.0%	14.6%	13.6%
Vulnerability mapping	36.3%	6.3%	13.4%	29.0%
Vulnerability remediation	44.0%	4.9%	12.4%	24.3%
Other	2.7%	0.7%	2.4%	2.7%

Moving Up the Maturity Model

A perfect endpoint management program is impossible without IT being a partner with the core business.

Just as the Endpoint Security Maturity Model can be used to characterize the current state, it also provides suggestions for increasing maturity and improving endpoint security management for all three of the endpoint categories discussed above. Specific guidance can be gleaned from the description of Level V maturity:

1. Foster good relationships among IT and business leadership and procurement to align goals, risks and policies. Gaps and problems occur when business solutions are implemented without security involvement. And business will include security in decisions only if security is perceived to add value. A discussion of how to accomplish that is beyond the scope of this survey analysis, but suffice it to say that a perfect endpoint management program is impossible without IT being a partner with the core business.

2. Involve all stakeholders whenever making decisions about endpoint management. The evolution of endpoints means that processes for managing them will also evolve. Encourage all stakeholders to anticipate future directions, both in technology and in business use of that technology. Where possible, design the endpoint management process so it can be easily adapted to those anticipated changes.

3. Improve user awareness and training, and assess the results of that training. Endpoint devices are often the user's interface with IT, which makes them a very attractive target for attackers. Train and empower users to protect the endpoints.

4. Implement the CIS Controls for Effective Cyber Defense.[11] Again, a full treatment of this suggestion is well beyond the scope of this survey analysis. However, implementation of the top five controls represents "quick wins" and will provide major benefits for endpoint protection.[12] Those controls are:
   - Inventory of Authorized and Unauthorized Devices
   - Inventory of Authorized and Unauthorized Software
   - Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
   - Continuous Vulnerability Assessment and Remediation
   - Controlled Use of Administrative Privileges

TAKEAWAY:

Users can be either the weakest link or the first line of protection. Good awareness training —repeated at frequent intervals, with assessments— can make the difference.

[11] www.cisecurity.org/critical-controls

[12] Adapted from Lewis, James A., "Raising the Bar for Cybersecurity", http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

Conclusion

The survey results show that although conventional devices such as desktops and servers represent the largest segment of endpoints connected to the network, the variety of endpoints is growing quickly. Building security and control system devices are being gathered under the umbrella of endpoint management, and business needs are driving the inclusion of both employer-owned and employee-owned mobile devices.

Organizations are still being compromised, with the primary target data being logins, access control and sensitive information. Accordingly, the most common device targets are desktops, laptops and servers, since they are most likely to contain that information. As mobile devices become more prevalent on company networks, these devices are likely to become targets more often.

The development of endpoint management strategies and processes can be described with the help of the Endpoint Security Maturity Model. Although there are no "magic bullet" solutions, technical or otherwise, the model provides helpful guidance for developing a long-term strategy for endpoint management. A critical aspect of this strategy should also be implementation of the relevant CIS Controls for Effective Cyber Defense.

About the Author

G. W. Ray Davidson, PhD, is the former dean of academic affairs for the SANS Technology Institute. He continues to serve as a mentor, subject matter expert and technical reviewer for the SANS Institute and holds several GIAC certifications. Ray started his career as a research scientist and subsequently led global security projects for a major pharmaceutical company. He has taught at the college level and worked at a security startup. Ray currently works with clients to develop and implement network security monitoring and threat intelligence capabilities. He is also active in the leadership of the Michigan Cyber Civilian Corps.

Sponsor

SANS would like to thank this survey's sponsor:

SOPHOS