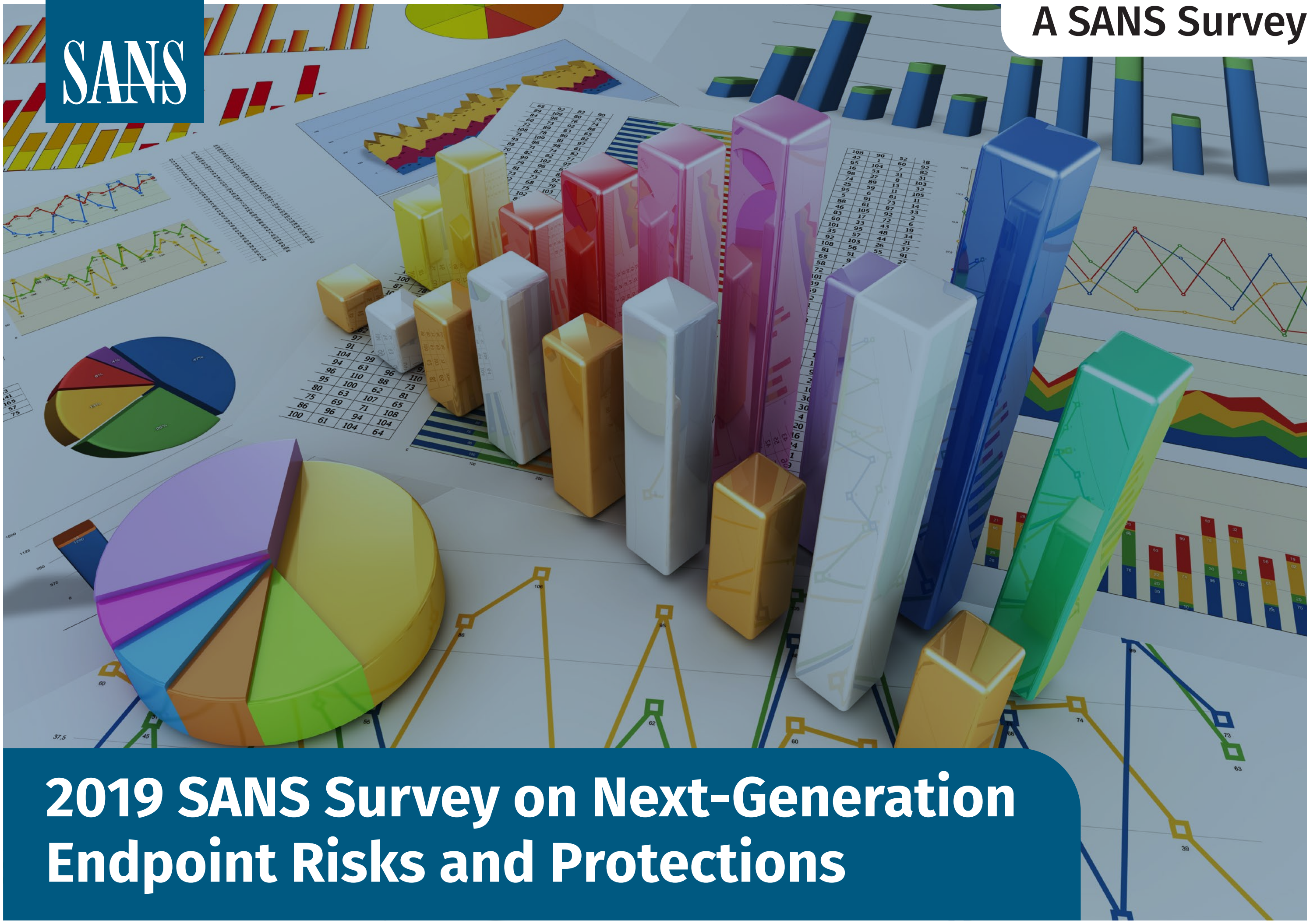
A SANS Survey



2019 SANS Survey on Next-Generation Endpoint Risks and Protections

Written by **Justin Henderson**
and **John Hubbard**

December 2019

Sponsored by:

opentext™

Analyst Program

Executive Summary

Central visibility and automation solutions are a necessity to detect, defend and respond to modern attacks. These solutions include data analytics tools (such as security information and event management [SIEM] and endpoint detection and response [EDR]), as well as automated detection and response technologies (such as user behavior monitoring and machine learning), according to the SANS 2019 Endpoint Protection and Response Survey.

In this year's survey, as in prior years, respondents reported difficulty in being able to observe or identify a compromised asset. While having properly trained staff and sufficient budget are ongoing issues, the adoption of modern endpoint assets—many of which are mobile—as well as the lack of technologies offering prevention and detection capabilities exacerbate the problem. Organizations need to stay abreast of current hardware and software solutions that emphasize automated processes, central visibility and decision-making powers.

Key Results

- **39%** of respondents have concerns about mobile devices and lack processes for them
- **27%** of laptops and mobile devices are centrally managed
- **28%** of respondents cannot collect logs from assets that are off company-controlled networks
- **11%** of respondents report an inability to identify what data has been breached and **66%** find it difficult
- **62%** of breaches can be identified within the first 24 hours
- **28%** of survey respondents confirmed that attackers had accessed endpoints

Understanding Endpoints and Our Respondents

Attacks often start on endpoints such as workstations, then pivot to critical data sources on servers. While network controls and analysis tools provide quick visibility across many assets, they are often hindered by encryption and might lack additional host-level details. For maximum visibility, more insight is necessary at the endpoints.

However, cost, complexity and not knowing what data to collect from an endpoint hinder organizations trying to move from traditional network controls to endpoint controls. Combine these factors with the popularity of cloud solutions—such as containers and serverless code execution as well as IoT and smart devices—and it can seem unclear where to start.

Many organizations don't seem to be using solutions that offer auditing or advanced endpoint detection and response (EDR) capabilities. EDR is gaining popularity and answering some of the problems, but it has tradeoffs. This year's survey is designed to provide insight into what organizations are doing, as well as offer meaningful steps that organizations can take to improve the situation.

The response pool represented a global group of security professionals from within various organizations. Figure 1 on the next page provides a snapshot of those respondents.

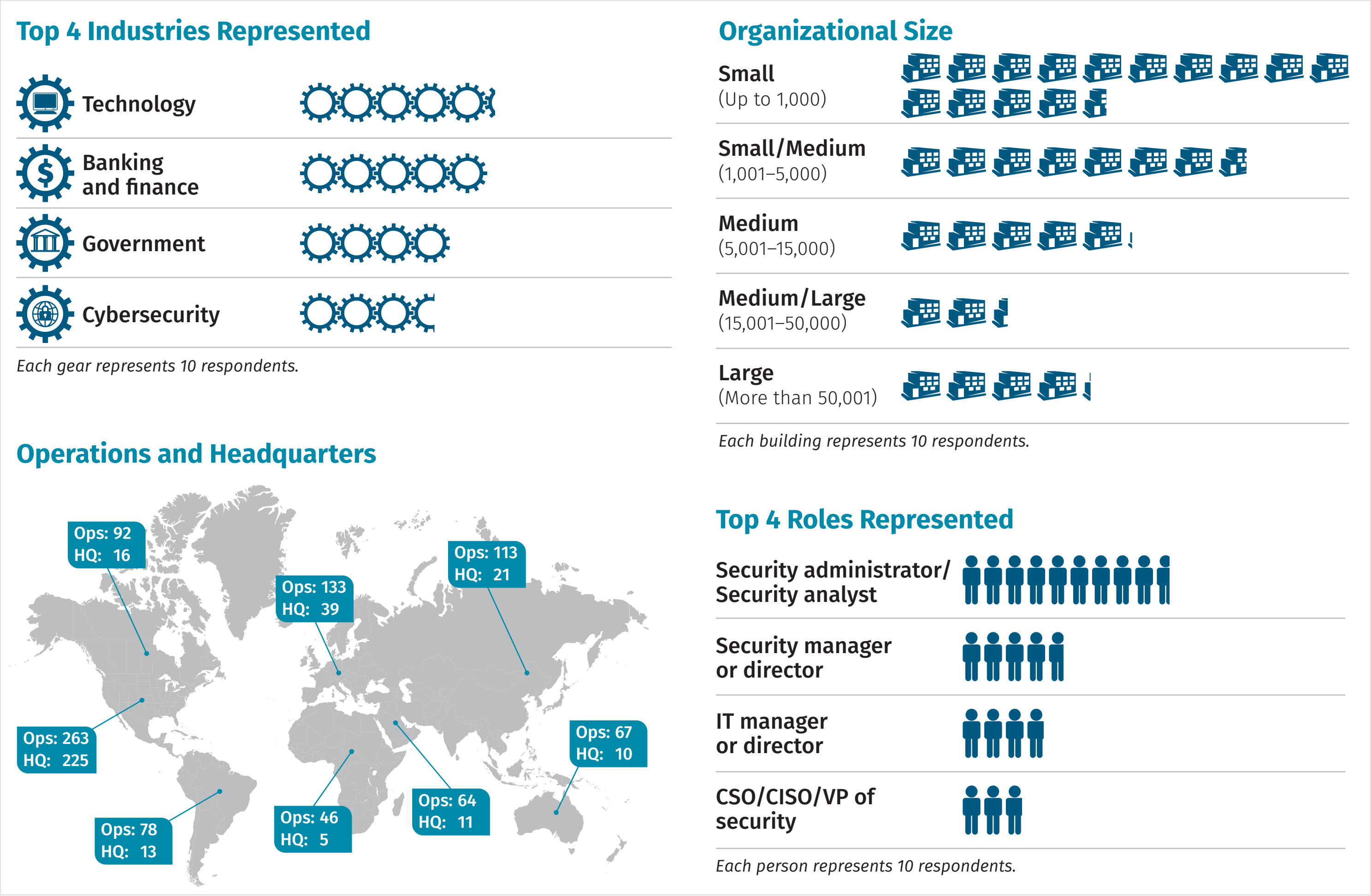


Figure 1. Key Demographic Information

Managing Endpoints

Endpoints cover a vast range of hardware types and underlying operating systems. As part of the survey, questions were devised to identify challenges and opportunities around endpoints. The questions ranged from central management capabilities to detection and prevention controls that organizations might or might not have. The following sections cover endpoint types and capabilities that organizations report around maintaining them.

Types of Endpoints

Each year the survey asks respondents what types of endpoint devices connect to their corporate networks. For the most part, the types of endpoints remain consistent year-over-year with spikes or declines limited to only a few categories.

In 2019, there was a decrease in cloud-based endpoint device by approximately 12 percentage points when compared with the 2018 survey.[1] With all the talk of organizations migrating to the cloud, it is unclear why the 2019 survey shows a decline. In contrast, the volume of desktops reported is lower than the 2018 survey by 18%. The

[1] "Endpoint Protection and Response: A SANS Survey," June 2018, www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460 [Registration required.]

drop in desktops may be due to the increase in employee-owned devices, leading to the possible conclusion that BYOD is trending. See Table 1.

Also notable: The 2019 survey shows increased use of smart systems and wearable technology. These categories are likely to include the implementation of smart technologies such as augmented reality into various industries such as healthcare and engineering. Ultimately, this means that security professionals will have to learn new methodologies and tools for securing such devices. The influx of non-standard endpoints is likely to introduce new pain points, as training and documentation around securing new technologies is limited. Organizations need to be aware that new endpoint types need segmentation and security considerations as they are already being compromised (covered later in this report).

Table 1. Comparison of Device Types (2018 vs. 2019)

	2018	2019	% Change
Cloud-based systems (emulated or virtualized)	60.6%	49.1%	-11.5%
Desktops (employer-owned)	74.1%	56.0%	-18.1%
Environmental controls (HVAC, water treatment)	43.1%	35.4%	-7.6%
Industrial control systems (SCADA, plant floor manufacturing)	27.4%	25.9%	-1.5%
IoT devices/Sensors	43.1%	41.4%	-1.7%
Laptops (employee-owned)	50.0%	43.5%	-6.5%
Laptops (employer-owned)	70.8%	60.4%	-10.4%
Mobile devices (employee-owned; tablets, notebooks/iPads, smartphones)	60.6%	56.3%	-4.3%
Mobile devices (employer-owned; tablets, notebooks/iPads, smartphones)	67.5%	55.7%	-11.9%
Other	4.7%	3.9%	-0.9%
Physical perimeter security systems (electronic access controls, surveillance systems)	60.6%	48.5%	-12.1%
Point of sale (PoS) devices	28.8%	22.6%	-6.2%
Printers	70.1%	60.4%	-9.7%
Routers/Firewalls/Switches/Other network devices	71.2%	60.4%	-10.8%
Servers (development, database, email, web, DNS)	71.2%	56.5%	-14.6%
Smart sensors	25.9%	22.3%	-3.6%
Smart systems (cars, building controllers)	17.5%	23.2%	5.7%
Wearables	16.4%	26.8%	10.4%

Centralized Management

Central management of endpoints is often raised as a concern among those responsible for endpoint security. Survey results show that, of employer-owned devices, 77% of servers and approximately 73% of both laptops and desktops are centrally managed, while employer-owned mobile devices are centrally managed only 53% of the time, as shown in Figure 2 (on the next page). The fact that large portions of these devices, by category, are not centrally managed will be an ongoing deficiency for organizations trying to consistently harden, patch and know their environment. Figure 2 represents mainstream endpoint devices such as laptops, desktops and mobile devices where mature endpoint management suites are available. The figure demonstrates even though mature technologies exist to manage common assets, adoption of such technologies is far from complete.

When it comes to employee-owned devices, BYOD presents additional challenges, and respondents indicated that only 27% of mobile devices and 18% of laptops are centrally managed. While technologies such as VMware Horizon, Citrix Virtual Apps and Desktop and Microsoft Virtual Desktop can serve as a connection broker between untrusted personal devices and organizational assets, the personal devices are running at a lower security posture and provide little to no visibility for security teams to detect a compromise. This can lead to the potential compromise of data, usernames and passwords without an organization's knowledge due to introduction of malware utilizing keyloggers or man-in-the-middle techniques combined with the installation of malicious root certificates. Without visibility into personal devices, it is not possible to evaluate how often such compromises are occurring or are likely to occur.

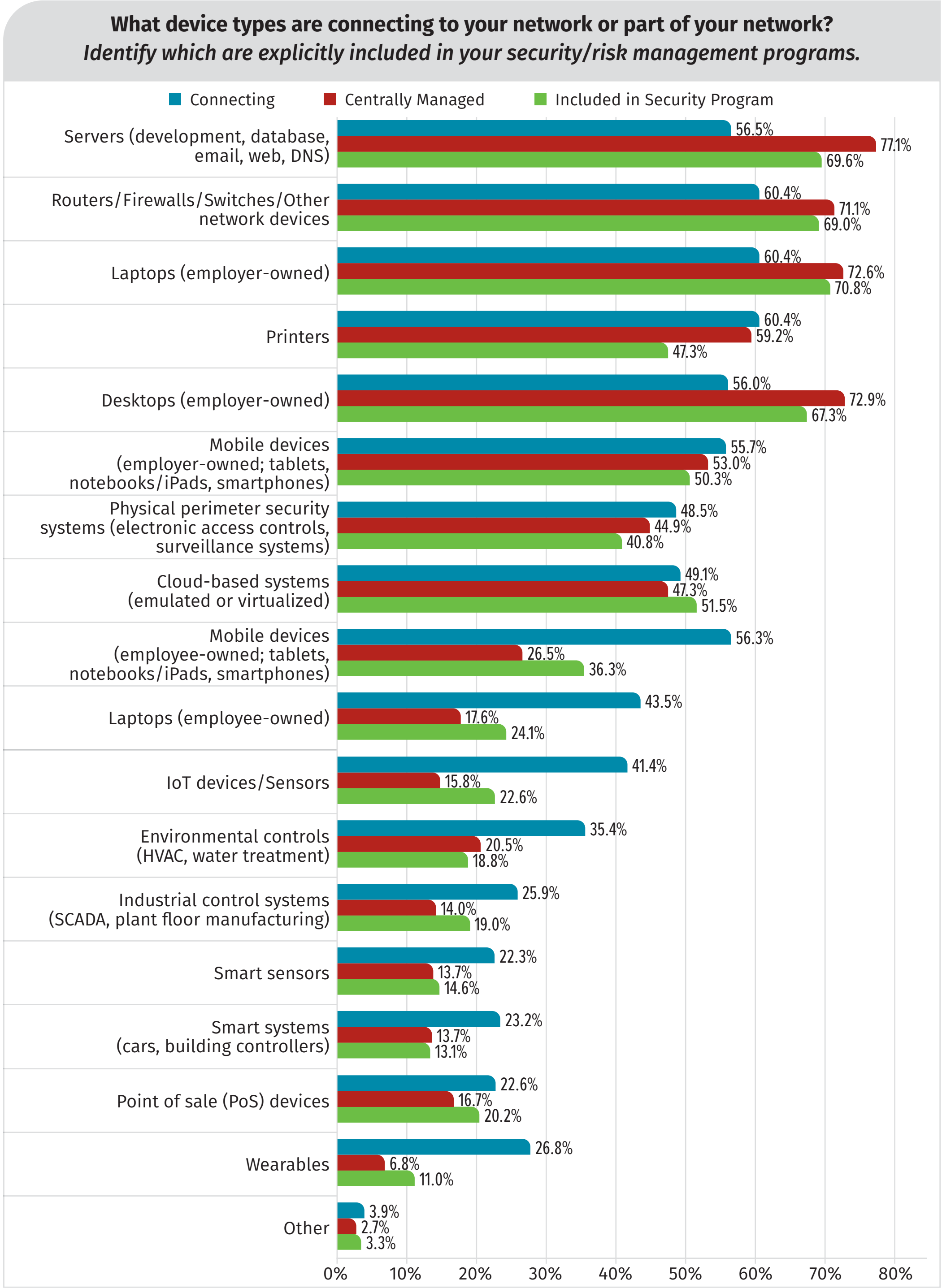


Figure 2. Centrally Managed Devices

Based on survey results, organizations are aware of the potential risks that employee-owned assets present; respondents indicated that, of devices not yet covered in a security management program, employee-owned mobile devices (39%) and laptops (34%) were of greatest concern. IoT devices posed a serious concern as well, according to respondents. See Table 2 on the next page.

In contrast, between 29% and 51% of respondents characterized specialty devices such as IoT, smart speakers, smart cars, industrial controls systems and wearables as not a concern. These percentages may be based on a lack of reported compromised devices in the media or due to proper segmentation and alternative controls limiting the damages from a potentially compromised device. Organizations need to proceed with care when handling non-standard operating systems and devices. Some of these devices are under review and scrutiny (such as smart cars falling under the US National Highway Traffic Safety Administration), while other devices (such as consumer-grade IoT devices) might have little or no cybersecurity standards or reviews.[2]

Table 2. Endpoint Concerns Covered by Security Programs

	Of Concern and Covered	Of Concern and Not Covered	Not of Concern
Mobile devices (employee-owned; tablets, notebooks/iPads, smartphones)	63.9%	39.1%	16.4%
IoT devices/Sensors	18.8%	34.2%	29.4%
Laptops (employee-owned)	32.4%	33.9%	22.1%
Printers	50.6%	28.2%	12.1%
Environmental controls (HVAC, water treatment)	22.7%	27.0%	32.1%
Cloud-based applications (SaaS)	51.2%	26.7%	10.0%
Smart sensors	15.2%	25.2%	38.2%
Mobile devices (employer-owned; tablets, notebooks/iPads, smartphones)	60.3%	24.8%	7.6%
Physical perimeter security systems (electronic access controls, surveillance systems)	47.6%	24.2%	15.5%
Cloud-based servers (platform-as-a-service [PaaS], emulated or virtualized)	53.6%	23.9%	11.2%
Smart speakers (Amazon, Google, Echo)	7.9%	23.6%	49.4%
Smart systems (cars, building controllers)	15.2%	21.5%	41.2%
Wearables	9.1%	20.3%	51.2%
Industrial control systems (SCADA, plant floor manufacturing)	21.8%	17.3%	40.6%
Point of sale (PoS) devices	21.8%	12.4%	43.9%
Desktops (employer-owned)	77.3%	10.3%	4.8%
Servers (line of business applications, legacy)	78.5%	10.0%	4.8%
Laptops (employer-owned)	79.7%	9.4%	5.2%
Servers (development, database, email, web, DNS)	83.3%	7.9%	4.2%
Routers/Firewalls/Switches/Other network devices	80.6%	6.1%	6.7%
Other	3.3%	4.5%	15.2%

[2] www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

Control Capabilities

Fortunately, organizations are showing an increase in the use of next-generation endpoint controls. For example, the 2019 survey results show a consistent increase in technologies implemented compared with 2018. Anomaly detection increased by 10% and machine learning solutions increased by 12%. Even tools such as automation tools and vulnerability scanners increased in implementation by 5% year-over-year. Based on these increases, there is a positive trend in organizations investing in security solutions. Holistically, there is a large increase in analyst-driven technologies focused on identifying potentially compromised assets or aiding analysts in investigations. Technologies such as EDR, threat hunting and machine learning have increased by close to 10%. See Table 3.[3]

As a technology that respondents consider important but have not yet implemented, automation (at 59%) is comparable with last year's respondents (58%), as shown in Figure 3 on the next page. Automation is critical to minimizing false positives, speeding investigations and remediation tasks, and providing a more efficient analyst workflow. Unfortunately, purchasing automation tools is not the same as implementing such tools. Initially, experienced staff needs to assess and evaluate what can and should be automated. While this ultimately takes personnel away from other tasks during initial setup and implementation, organizations will greatly benefit after automation is in place.

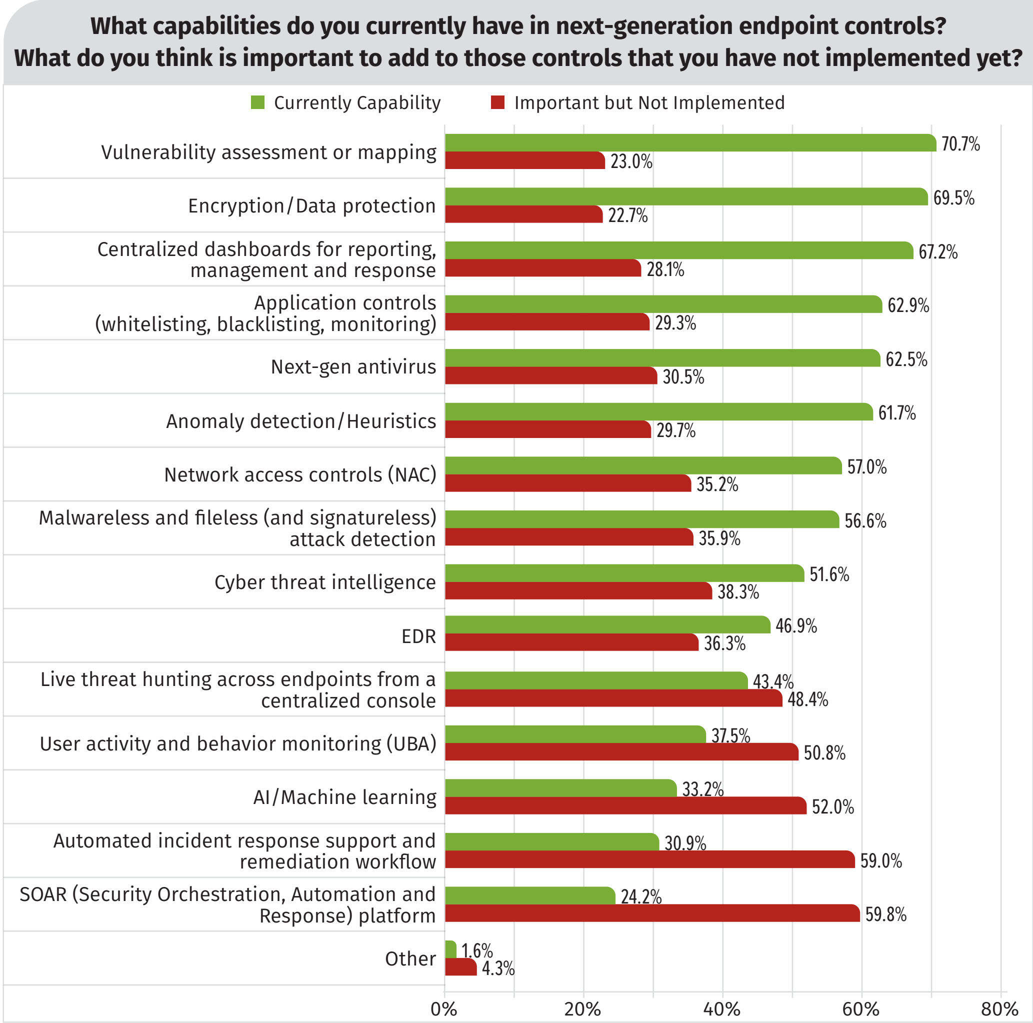
Table 3. Next-Generation Endpoint Control Capabilities (2018 vs. 2019)

	2018	2019	% Change Where Applicable
AI/Machine learning	21.1%	33.2%	12.1%
Anomaly detection/Heuristics	52.0%	61.7%	9.8%
Anti-ransomware	52.5%		
Application controls (whitelisting, blacklisting, monitoring)	63.2%	62.9%	-0.3%
Automated incident response support and remediation workflow	25.5%	30.9%	5.4%
Centralized dashboards for reporting, management and response	59.3%	67.2%	7.9%
Cross-correlation to reduce false positives	32.4%		
Cyber threat intelligence	54.4%	51.6%	-2.8%
EDR	35.8%	46.9%	11.1%
Encryption/Data protection	65.2%	69.5%	4.3%
Malwareless and fileless (and signatureless) attack detection	49.0%	43.4%	-5.7%
Network access controls (NAC)	52.9%	56.6%	3.7%
Next-gen antivirus	50.0%	62.5%	12.5%
Other	6.9%	1.6%	-5.3%
Threat hunting	38.7%		
SOAR (Security Orchestration, Automation and Response) platform		24.2%	
User activity and behavior monitoring	46.1%	37.5%	-8.6%
User behavior modeling and analytics	29.4%		
Vulnerability assessment or mapping	63.2%	70.7%	7.5%
Vulnerability remediation automation	29.4%		

[3] Note: In this table, SOAR is a new addition in the 2019 survey. SOAR is an extension of the SIEM platform, which is related to centralized dashboards and data analysis.

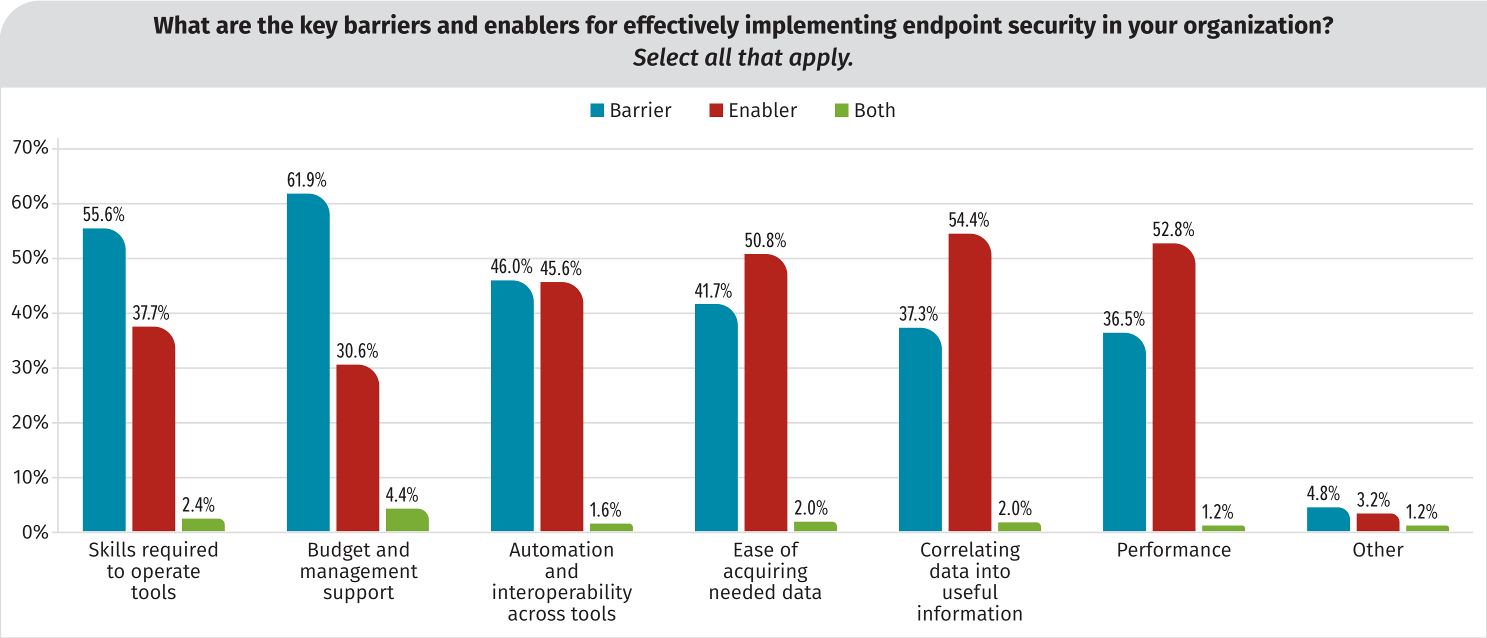
Challenges to Managing Endpoints

To implement an effective security program, organizations need to identify potential barriers as well as key success criteria. While 54% stated that the ability to correlate data into useful information was a key enabler, 51% also selected ease of acquiring data. These percentages again reflect the need for visibility into and context of an organization. However, the most-highly reported barriers make it difficult to execute these critical success areas: 62% stated budget and management support were lacking, and 56% lacked skilled staff to operate tools. See Figure 4.



What capabilities do you currently have in next-generation endpoint controls? What do you think is important to add to those controls that you have not implemented yet?

Figure 3. Importance of Next-Generation Endpoint Control Capabilities



What are the key barriers and enablers for effectively implementing endpoint security in your organization? *Select all that apply.*

Figure 4. Barriers to and Enablers of Effective Endpoint Security

There will continue to be a struggle to acquire and use tools. The solution to this is either acquiring easy-to-use tools or hiring and training staff to a higher level of competence.

Takeaway

Organizations need to achieve a balance between purchasing simplified tools that lack flexibility in mapping to business requirements and optional automation and maintaining expert-level staff.

Data Collection for Attack Detection

This year, we put extra focus on the type of data collected (or not collected) and whether or not that information was viewed as important. We believe that understanding the multitude of Windows event channels and network service logs that can be collected is of utmost importance to cyber defense; yet many organizations anecdotally seem to report not collecting some of the most basic and crucial log sources. To this end, many new questions were included in the survey to better understand what data was collected by the average organization and why, given that this can be one of the defining factors between spotting an attack immediately or completely missing it.

When asked about what type of network-related logs are considered necessary, access logs and user data was most frequently reported (collected by 90%), followed by network security data from IPS, firewall, UTM (at 80%). While this indeed is some of the most important data, it might not be sufficient to catch all attack types. System access logs are very useful in helping organizations determine who is logging into a system and from where. Many common SIEM use cases revolve around authentication data and logs, which likely lead to their No. 1 spot. This is a great place to start. However, network security data is often focused on known types of attacks and might miss zero-day exploits or protocol-compliant yet malicious use of "good" protocols such as HTTP/S, a technique often utilized by advanced malware to blend in with normal traffic. To identify these types of attacks, collecting *all* network events in at least a simple transaction record of some sort might be necessary. That kind of data is collected in the next four categories: DNS data, network traffic analysis, network flow data and metadata collection, with use by respondents reported as being between 50% and 73%. See Figure 5.

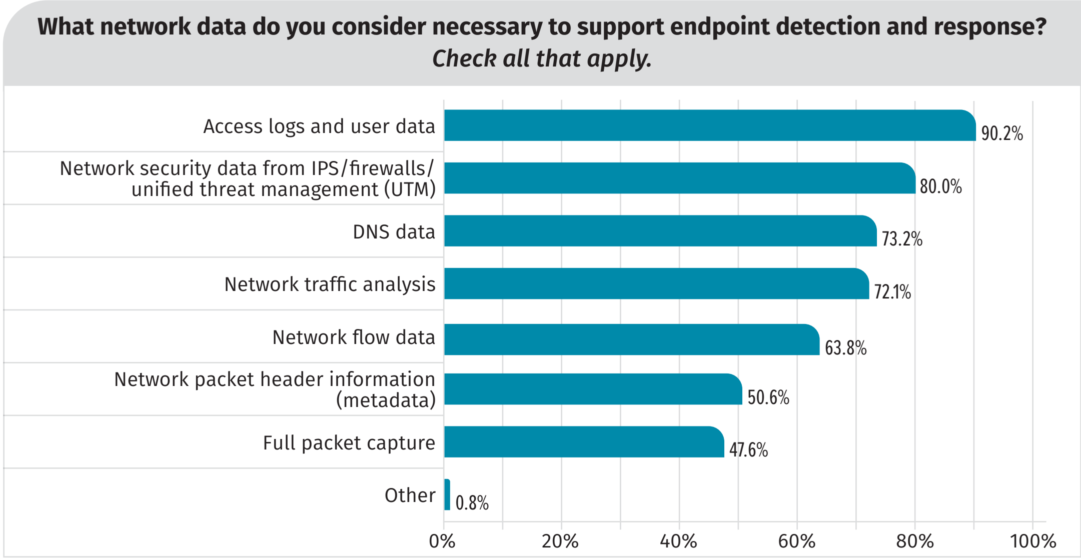

What network data do you consider necessary to support endpoint detection and response?
Check all that apply.

Figure 5. Network Data Needed for EDR

Full packet capture was considered necessary by only 48% of respondents. It is true that, in many cases, full packet capture is not needed to detect malicious traffic, protocol-compliant command and control used by malware may slip by if security personnel cannot see the full content of the transaction. Free and open source tools such as Security Onion and Moloch have lowered the cost of full packet capture solutions, in some cases, to the price of the hardware needed to capture and record the packets.

Takeaway

We encourage organizations that have not assessed full packet capture solutions to do so to help supplement their ability to detect tricky endpoint compromises.

Windows Logs

When it comes to Windows logs, we were curious to examine what logs are collected by organizations. Many modern and common attacks used against Windows might not be identified via the most basic of log collection (in-memory only PowerShell-based attacks, for example).

The survey shows that, as expected, the Windows Security and System logs are the most popular sources to collect and centralize. This is a rational place to start, but it isn't enough to catch advanced attacks. PowerShell, Sysmon, Windows Defender, WMI and AppLocker logs (from a 42% to a 15% collection rate) represent some of the most often overlooked log sources in a Windows system—and are often the location where evidence of an advanced attack may appear. See Figure 6.

Barriers to collection of non-centralized logs were reported to be too much volume (36%), lack of an audit policy that records those events (24%) and the perception that the expense to collect them is too high (19%). While these reasons might be justified in some cases, highly filtered tactical log collection of key events can help overcome these hurdles.

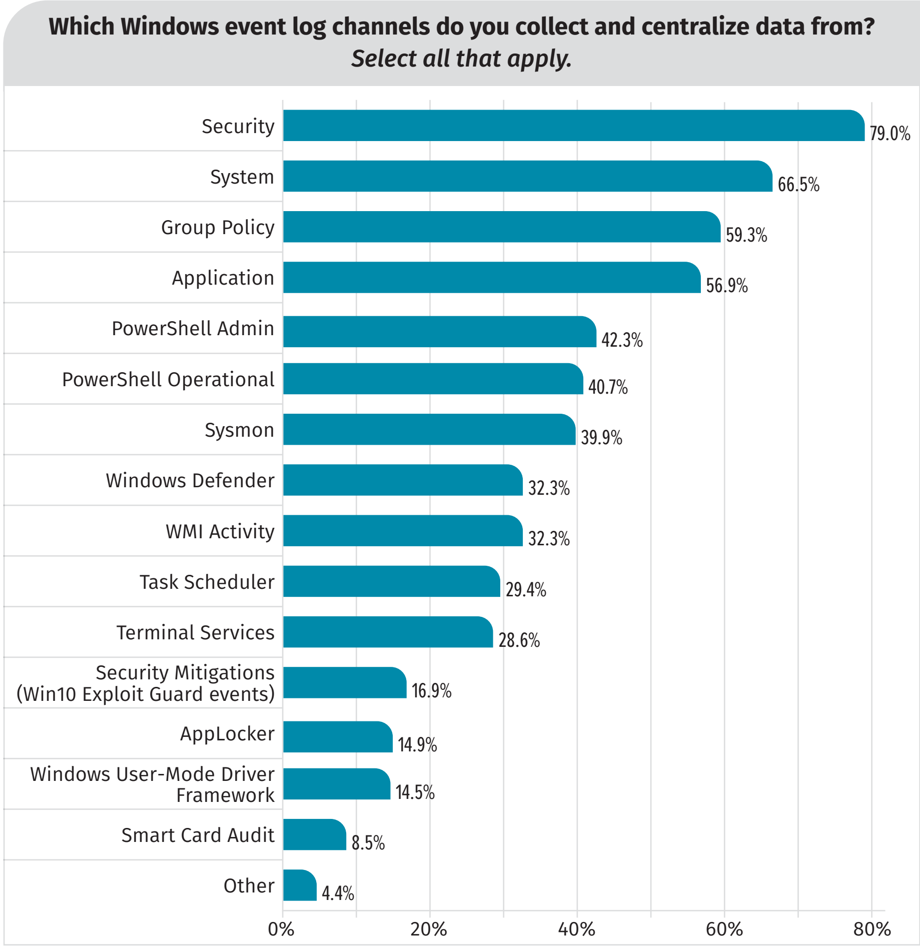


Figure 6. Log Channels Collected

Volume and Cost of Logging

One of the common pain points, as previously noted, is the perceived volume and cost of collecting logs from all desktops and servers. Faced with this challenge, many organizations choose to collect logs only from a portion of the devices in their environment, prioritizing the server or desktop estate and collecting only local logs for other devices. In the survey, only 18% of respondents said they collect logs from nearly all types of endpoints. Most others took a different approach; 37% said they collected both types of logs, but more logs from servers; 16% collected *only* server logs; and 8% said they collect both servers and desktops, but more from desktops. Additionally, a full 15% said they "collect very minimal logs"—a difficult position from which to defend your network. See Figure 7.

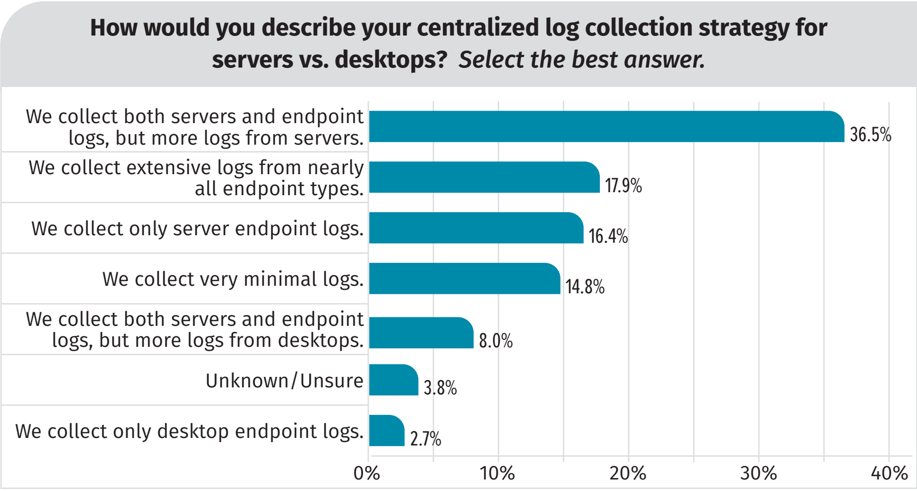


Figure 7. Server vs. Desktop Log Collection Strategies

Because visibility of endpoint activity is a key piece of endpoint attack detection, organizations that find themselves lacking log collection might find themselves at a disadvantage for stopping attacks in their early stages. If organizations collect logs only from servers, for example, they might find themselves only able to detect an attack once the adversary has pivoted through multiple user machines and made his or her way deep into the environment. Organizations in this situation might find that a better strategy is to collect logs from *all* device types—but to be more tactical and selective in terms of what exactly is collected from each device. This allows for an early warning of attacks while keeping the log-collection price minimized.

Takeaway

All organizations should explore collecting logs from additional Windows log channels. Modern attack techniques are likely to continue to find new and innovative ways to stay out of traditionally collected log areas. Consider collecting logs from all device types and be tactical—if volume must be reduced, be more selective in what you collect from each device as opposed to eliminating full classes of devices.

Analysis and Consolidation

As for *how* that log data is being analyzed and consolidated, 62% of organizations report using a SIEM solution, 37% use a centralized log management platform, and 33% also search manually through logs using disparate tools (e.g., the command line). While SIEM is the most common method of analyzing logs (as expected), it's worth noting that 32% report utilizing EDR as well, as shown in Figure 8.

EDRs are a relatively new product in the security market space and focus specifically on endpoint visibility, allowing organizations to capture endpoint activity that might otherwise fall under the realm of "too much volume" or "too expensive to collect" without them. We suspect this will continue to be a driving force in the market for supplementing visibility and enabling quick response.

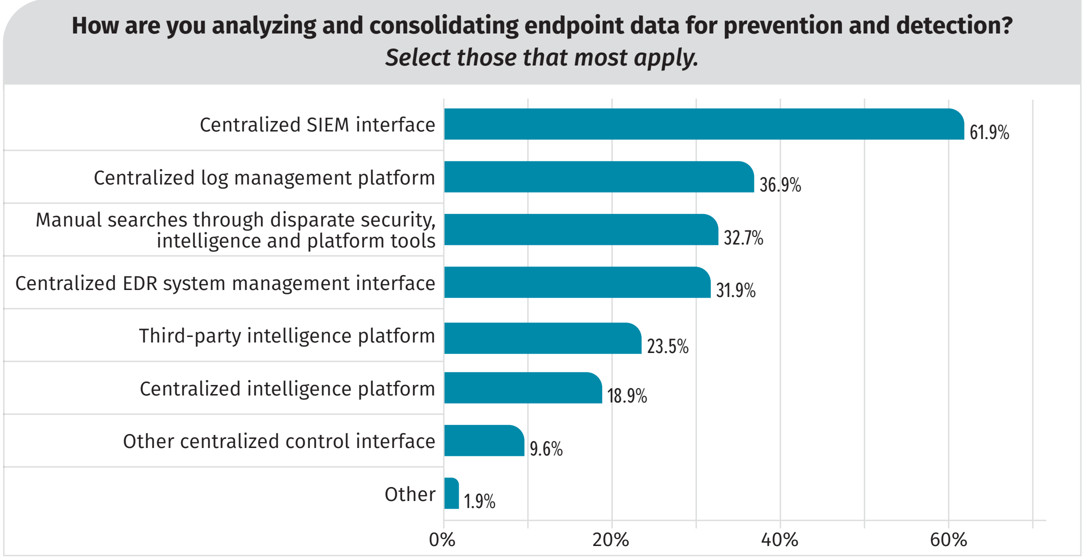


Figure 8. Analysis and Consolidation of Endpoint Data

SIEMs make log collection and interpretation much easier by normalizing and categorizing all the information they take in, but that's not all. SIEMs have the capability to take normal logs and make them much better through the process of enrichment. While enrichment can be a huge boon for those who know how to utilize it effectively, not all companies do. Our survey asked which types of log enrichment were the most common to try to understand what the industry is using to bolster detection capabilities.

Log Enrichment

The three most common enrichment techniques are DNS request enrichment (51%), user identification and role lookups (50%) and GeoIP information (48%), as shown in Figure 9.

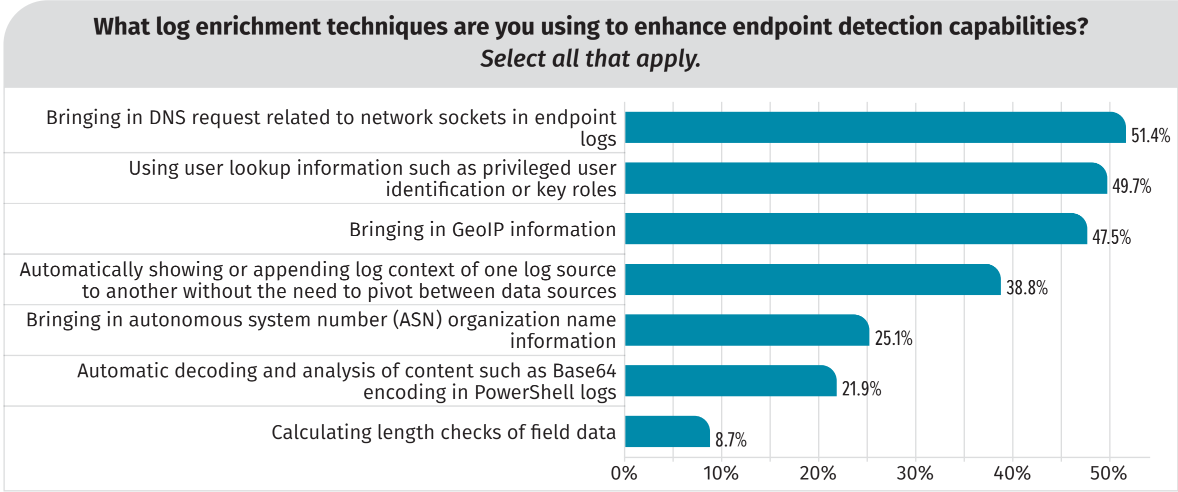


Figure 9. Log Enrichment Techniques

These responses come as no surprise; DNS enrichment, user and role lookups, and GeoIP resolution are common features in many of the products in the SIEM space. But why are only half of our respondents utilizing them? The other techniques are more niche approaches, and while their benefits are clear, we theorize they are used less frequently because SIEMs do not commonly have these enrichment features built in. For all SIEM users and SIEM vendors, we suggest log enrichment as an area for improvement, as these features can help bring much needed fidelity to the torrent of alerts and events that security teams receive on a daily basis. Gaining even minor additional context can be the difference between fast, accurate triage of the most important events and fumbling to understand which data is truly the most important.

Takeaway

Make log enrichment a priority. Better context can be the difference between directing swift attention to the most important events and spending extra time trying to figure out which data and events are the most important to pursue.

Off-network Log Collection

One final piece of the log collection puzzle that we theorized might add difficulty to log collection is the effect of endpoints that leave the physical network. Collecting logs from off-network devices is as important as—if not more important than—collecting logs from on-network devices, given that machines out in the world must defend themselves. Unless VPN connections are enforced at all times, these machines are beyond the reach of the corporate firewall, proxy and other network-based protections that would normally add to their ability to repel attacks.

This year's survey indicates that there is indeed a lack of visibility into device logs for off-network endpoints, with 28% of respondents saying they cannot collect logs from off-network assets at all, while 26% said they could collect logs only while the user was connected to a VPN. Only 19% of organizations are able to collect endpoint logs without a VPN connection via a cloud-based or DMZ server, as shown in Figure 10.

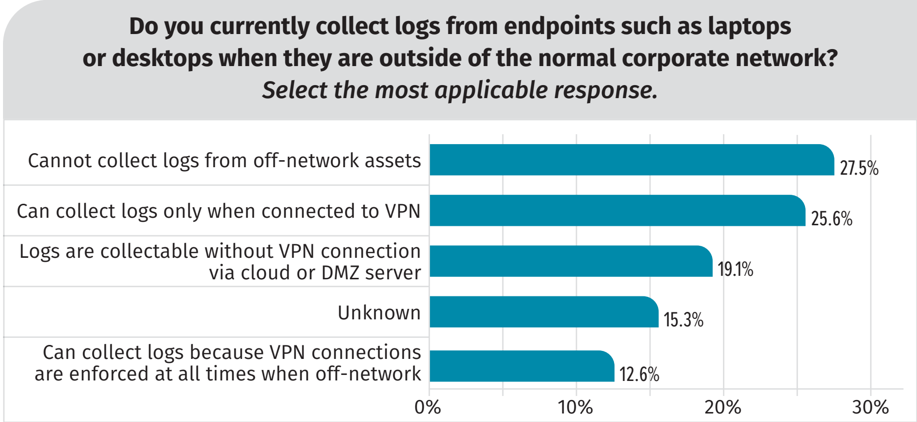


Figure 10. Off-network Endpoint Log Collection

This means more than half of organizations have no visibility into off-network endpoints. For organizations with many employees working remotely or on the road, this poses a significant risk because all detection and response to attack activity on those devices will be delayed until the traveling worker returns to the network or connects via the VPN. To partially mitigate difficulties in off-network visibility, 13% of organizations enforce using a VPN when employees are off-network.

Takeaway

Organizations should make their best efforts to enable log collection for off-network devices. Those that are unable to collect logs unless the user is on-network or VPN-connected should double down on endpoint-based protection to prevent attacks in the wild and consider investing in always-reachable collection servers to ensure compromises don't have a chance to linger on the machine longer than necessary.

Detection of Endpoint Attacks

This year's survey made it clear that traditional antivirus still is a key player in protecting organizations, but next-generation antivirus (NGAV) shows a higher installation footprint and a sharp increase in detection of attacks. NGAV tools detected the compromise for 44% of respondents, more than double that of last year's respondents, which was 14%. Also, SIEM technologies—both automated alerts at 39% and manual searches of SIEM data at 28%—caught more compromises than in the 2018 survey (32% and 16% respectively). EDR technologies also rose from approximately 26% in 2018 to 35%. Overall, detection of compromised assets is occurring more frequently in threat-centric technologies such as SIEM, EDR and NGAV as opposed to general network data analysis. See Figure 11.

This year, organizations reported that their detection capabilities are mostly reactive, with 29% of respondents indicating they successfully detected only 10% or fewer potential threats through proactive discovery. Proactive discovery involves actively querying endpoints or using automatic discovery techniques on the endpoint before centralization of the data. Tools such as threat intelligence, threat hunting, active EDR and scripting all are examples of proactive discovery tools that allow mass investigations at scale for identifying attacker behaviors.

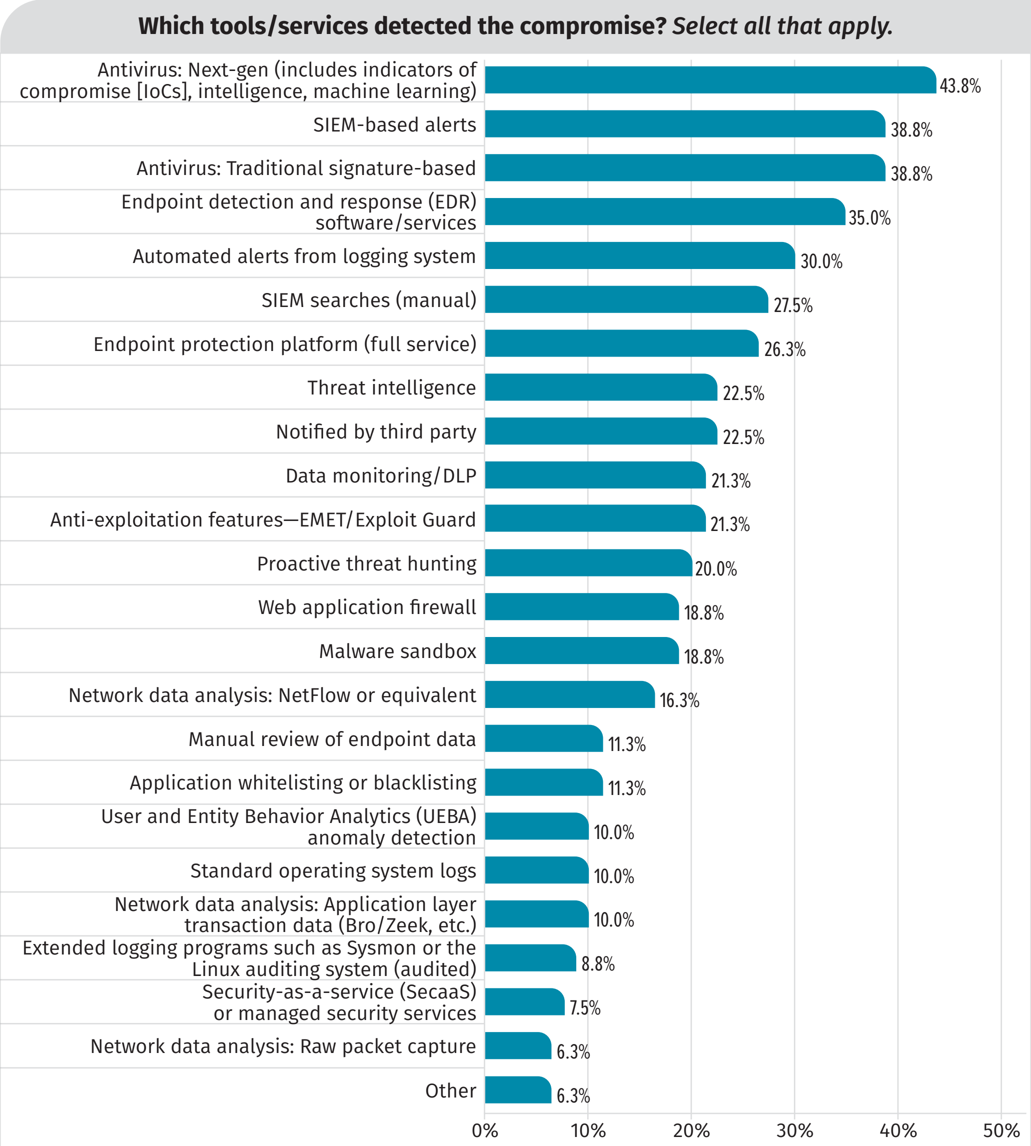


Figure 11. Tools/Services Detecting Compromise

Data Analytics

A critical aspect of detection is the centralization of data and subsequent data analytics. Often, organizations find ad hoc analysis to be ineffective and costly. Thus it comes as no surprise that respondents heavily centralize endpoint data. Table 4 shows a breakdown of the top seven data types and the percentage of organizations that centralize it.

Table 4. Endpoint Data Centralization

Data Type	Percent of Centralization
OS and version	76.9%
Type of endpoint	68.3%
Installed software and version	66.0%
Version of endpoint	66.0%
User logins, including date, time and location	65.3%
Computer object association in Active Directory	63.8%
Vulnerability scan data	62.3%

While visibility into software inventory and configuration and user logins is important, many additional data sources continue to go unchecked. Default data sources such as Windows application, system and security channel events are insufficient on their own, and additional data sources must be considered. However, identifying, collecting and operationalizing new data sources is difficult:

- 21% of respondents report no capability to acquire memory artifacts. With modern capability to run fileless malware, memory analysis is more important than ever. Memory artifact analysis is necessary on multiple fronts, such as for forensics investigations, hunt teaming or automatic detection capabilities. 38.1% of respondents do collect memory-based artifacts, but in a disparate fashion—only 25% report the ability to centrally collect memory artifacts.
- 12% of respondents report no capability to collect browser history and disk-based artifacts (16%).
- 35% report the inability to collect network connection data such as route tables, ARP cache, DNS cache and other network-related data points.

Overall, there is an ongoing issue with centralized visibility into what happens on an endpoint. Organizations must focus on the acquisition of data analytic solutions and move past default configurations and the collection of standard data sources. Log sources need to include the removal of low-value logs and focus on collecting data that identifies threats or abnormal behaviors. By eliminating noise, organizations can afford to collect additional data sources or hold onto data with higher retention rates.

Time to Detect

When choosing data sources to collect, organizations must let their threat model and use cases drive the strategy. Collecting what matters most aids in analysis or detection rule sets. Failure to do so leads to increased costs and a decrease in detection. Respondents report that 62% of the time, an exploit detected on an endpoint is found within the 24 hours, with 10% needing between eight and 365 days, as shown in Figure 12. The range in detection times might reflect the difference between signature-based solutions compared with threat or behavioral solutions.

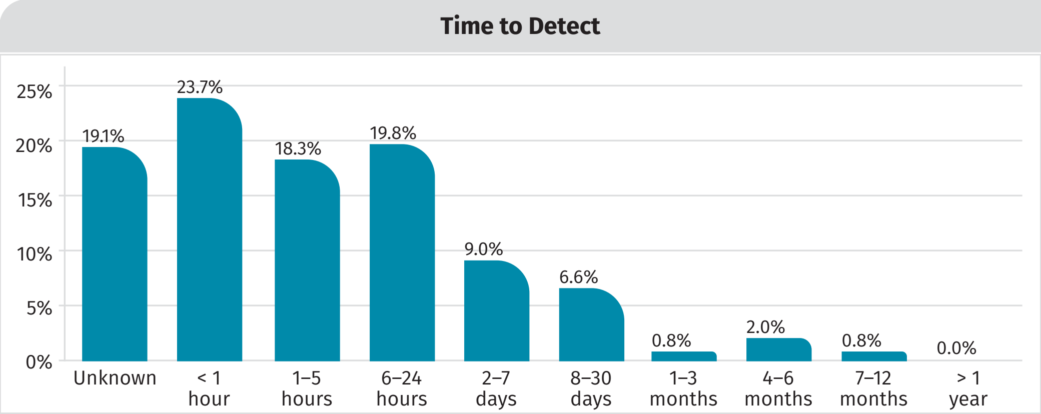


Figure 12. Time to Detect

Respondents report that 74% of the time they are able to kick off incident response within 24 hours of detecting an endpoint exploit. Last year, respondents responded within 24 hours only 76% of the time, evidence that organizations might be responding more quickly to alerts. A possible explanation for this is a rise in both processes and technologies that focus on removing alert fatigue by emphasizing false-positive reduction and building additional context into alerts.

Endpoint Attack Details

This year's survey showed a large downward shift in the number of endpoints that have been attacked, a trend moving in the right direction for the past three years of this survey. In 2017,[4] 53% of respondents reported endpoints attacks, followed by 42% in 2018. This year, only 28% of survey respondents confirmed that endpoints had been accessed by attackers, a decrease of 14%, as shown in Figure 13.

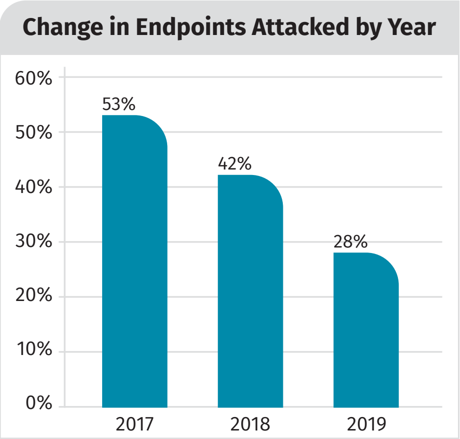


Figure 13. Number of Endpoints Attacked Year over Year

Additionally, 48% of respondents this year claimed that attackers had accessed no endpoints, compared with 38% in 2018 and 37% in 2017.

While this statistic may seem like a win, we must be cautious. There are a couple of ways the result could be interpreted: Either defense teams are truly getting better at stopping endpoint attacks or attacks are getting stealthier and teams are not seeing them. Unfortunately, this survey does not contain the data necessary to tell which is the case, but a further examination of this topic would be an interesting road for further exploration.

Just over 49% of this year's respondents report fewer than 10 incidents in the past year involving exploited endpoints—a fantastic number. Another 28% of respondents claimed to have fewer than 100 incidents per year, with only 16% reporting more than 100. The remaining 7% didn't know how many incidents their organization faced. See Figure 14.

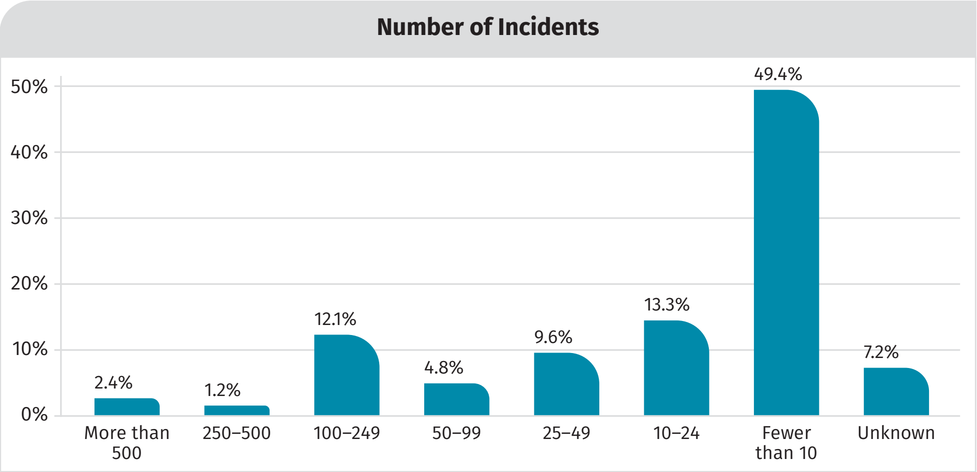


Figure 14. Number of Incidents

When asked about the number of endpoints impacted during each incident reported, most respondents (67%) said that fewer than 100 endpoints were impacted, as shown in Figure 15 on the next page. This makes sense because most incidents are likely to involve a small number of carefully selected endpoints. For incidents where large numbers of endpoints were impacted, organizations might have faced destructive attacks, ransomware or worm-like malware designed to cause widespread damage.

[4] "Next-Gen Endpoint Risks and Protections: A SANS Survey," March 2017, www.sans.org/reading-room/whitepapers/analyst/next-gen-endpoint-risks-protections-survey-37652 [Registration required.]

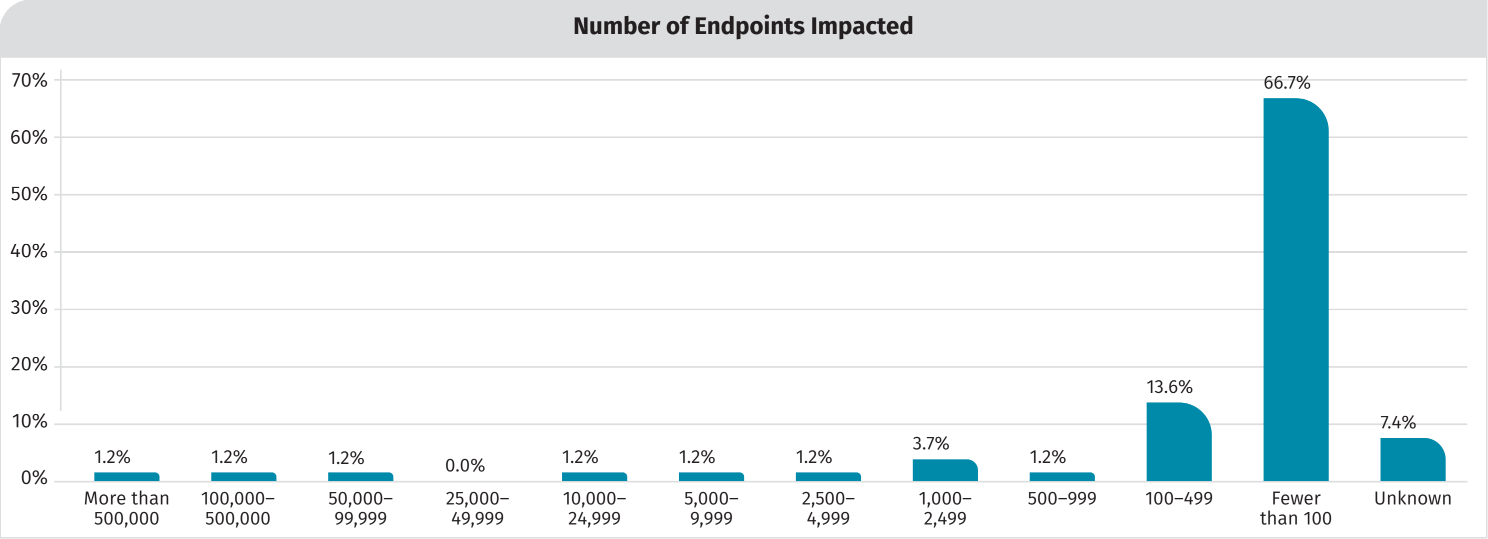


Figure 15. Number of Endpoints Impacted

Fortunately, the data shows that relatively few organizations were subjected to such attacks. We speculate that this may be due to continued progress in prevention measures (network segmentation, host hardening and removal of shared passwords from highly privileged accounts).

Endpoints Compromised

The types of endpoints reported to be compromised are as we might expect and are very similar to the 2018 survey results—employer-owned desktops (69% total) and laptops (67%) top the list of most frequently impacted followed by servers (51% for dev, database, email, web, DNS, etc. and 47% for line of business/legacy servers), employer-owned mobile devices (36%), employee-owned laptops (35%) and cloud servers (29%)/applications (28%), as shown in Figure 16.

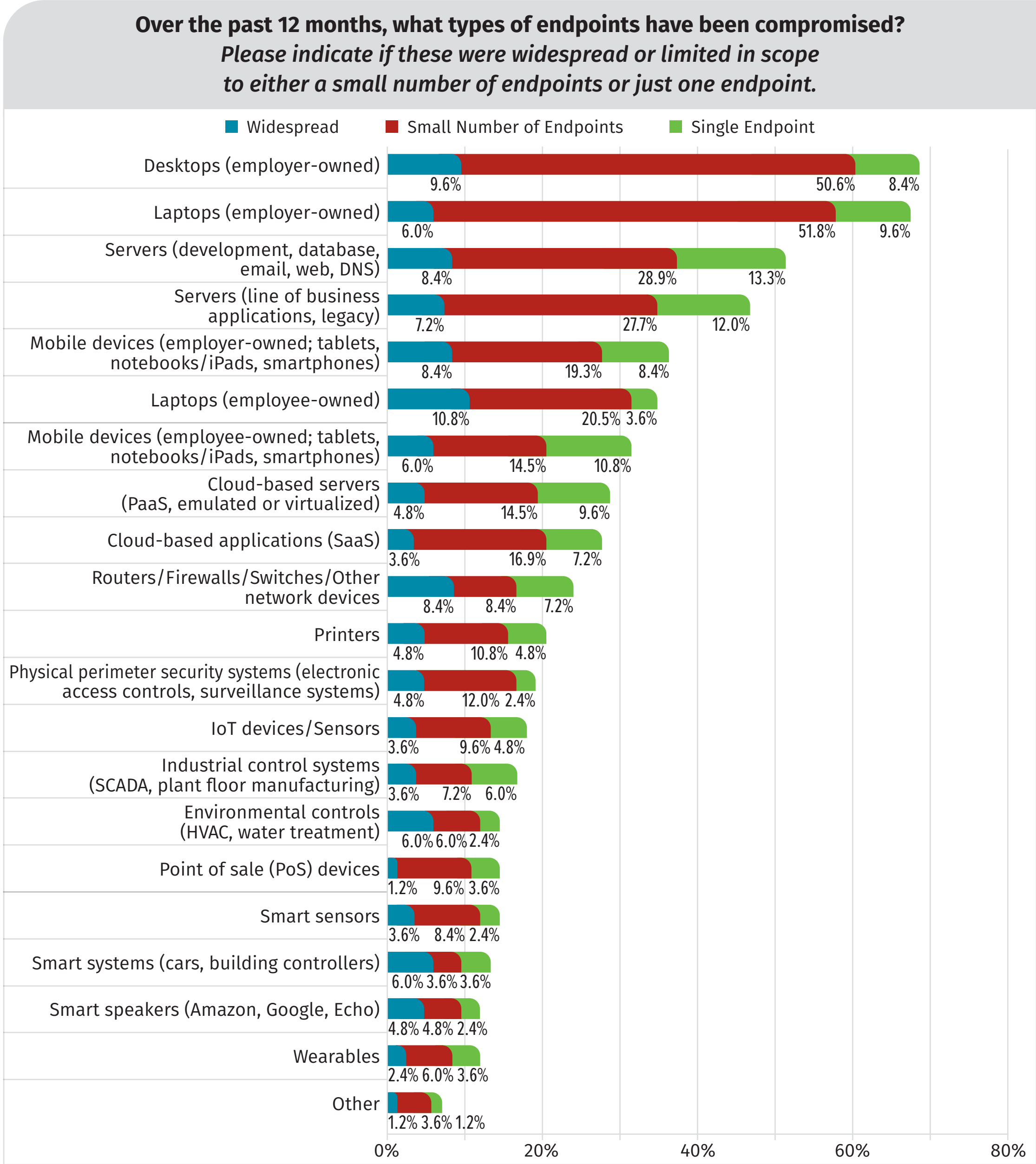


Figure 16. Types of Endpoints Compromised

Given that these endpoints tend to hold the data and credentials that attackers need, it is no surprise that these are the most targeted endpoints. That's not to say other devices are safe, however. At least some respondents experienced compromise in all areas, showing that nontraditional devices can be attacked as well, including network appliances, printers, physical security systems, IoT, smart devices, ICSes, environmental control systems, point-of-sale systems and even wearables. Although these systems might not be your main focus, your organization must still cover them in a well-rounded defense strategy—especially considering incident response, forensics and recovery procedures for these types of devices might be underdeveloped.

Attack Vectors

Through analysis of the most common types of attack delivery vectors, defensive teams can optimize their use of budgets and focus on blocking attacks early in the kill-chain, where exploitation hasn't yet occurred, and remediation is often the simplest and cheapest. It will likely come as no surprise that data from this year's survey shows you can get the best bang for your security buck by doubling down on efforts to prevent phishing, browser-based drive-by downloads and exploits, as well as credential theft. These three categories, plus ransomware (which was not included in this year's survey), took the top spots in the 2018 endpoint survey. As noted in Table 5, phishing and browser-based attacks switched spots in 2019, making phishing the top delivery vector this year.

Table 5. Top Three Attack Vectors

Attack Vector	2018	2019
Social engineering/phishing	53.1%	57.8%
Browser-based (drive-by downloads)	63.3%	51.8%
Credential theft or compromise	39.8%	48.2%

The security industry has focused on these categories for years due to the continued threat of phishing, drive-by downloads and credential theft. Solutions such as whitelisting, Windows Credential Guard, strict filtering proxies and next-gen firewalls and email attachment/URL sandboxing can make a *significant* dent in the likelihood of compromise via these methods. Of course, the fourth most-popular response—exploitation of a known vulnerability—continues to show that quick endpoint patch deployment and verification continues to be a pain point for many organizations as well.

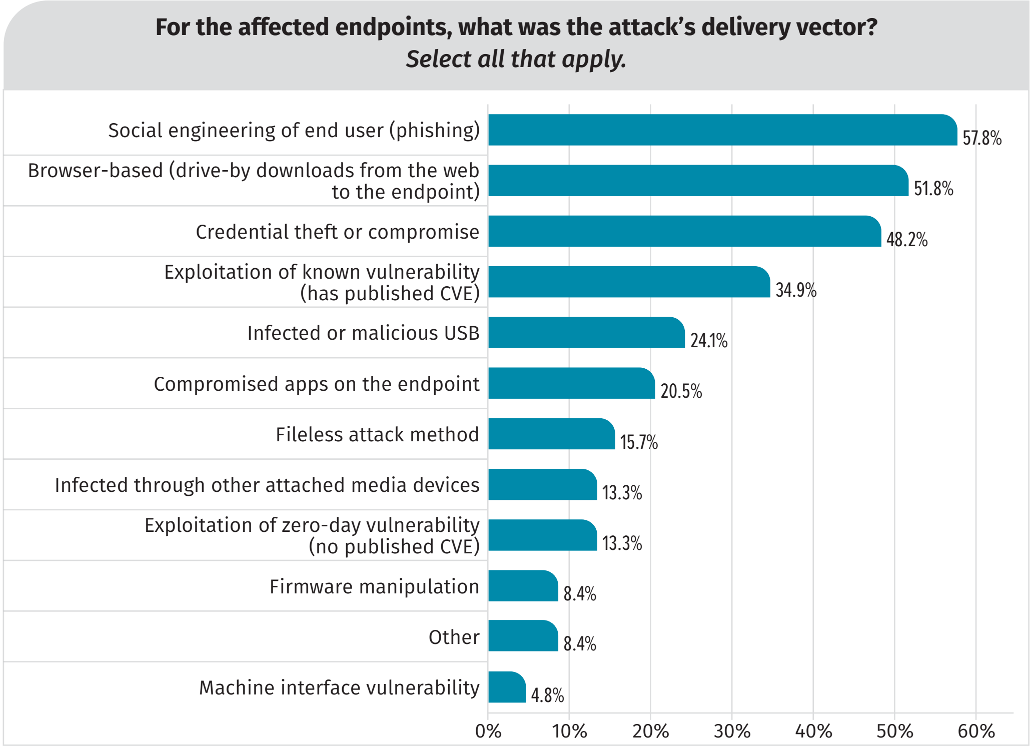


Figure 17. Attack Delivery Vector

An interesting finding in 2019's results is that 13% of organizations claim to have been victims of exploitation of a zero-day vulnerability, as shown in Figure 17.

If representative of the industry at large, this number shows that blacklist-based prevention and detection techniques are not enough. To stop these sorts of unknown attack vectors, solutions such as whitelisting of executable applications, scripts, PowerShell—and even web traffic via solutions like web-application firewalls—must become the norm. Unfortunately, the management burden of increased complexity and time required to implement whitelisting techniques often drives organizations away, opening them up to these types of attacks.

Takeaway

Where possible, organizations should evaluate the benefits of using free whitelisting solutions such as Windows AppLocker. In lieu of the ability to implement full whitelisting with blocking enforced, organizations should consider falling back to at least detect-only mode whitelisting (such as AppLocker's "audit-only" mode), giving them the ability to at least detect attacks, even if they can't outright prevent them.

Remediation and Recovery

When it comes to remediation, different organizations take different approaches. In terms of efficacy, 97% of respondents said that they trusted the wipe and reimage process as very effective or effective. As opposed to wiping the machine, which causes disruption for the user, some organizations preferred to surgically remove the problem. There was a significant difference in the reported confidence of this method—only 16% rated this option very effective, and 45% called it effective, leaving 39% not trusting surgical removal to fix issues fully. Given the complicated nature of many infections (not to mention kernel-level malware and rootkits that can hide from the operating system itself), it's no wonder teams seem to prefer the wipe-and-reimage process. Sometimes it's the only way to be sure.

Outside of surgical removal and wiping, a number of respondents suggested they also like to try other routes such as leveraging endpoint security agents or using system restore points, these approaches can work as well. As one respondent put it, their effectiveness could "depend on the malware trajectory and TTP of the incident."

With so many organizations preferring the wipe and reimage route of remediation, this brings up the question of how easy this process is for them to complete. According to the respondents, only 9% have a fully automated wipe and rebuild process, while 44% categorized their abilities as partly automated. Another 44% of organizations reported their remediation process as involving manual cleaning having to be done on-premises, as illustrated in Figure 18. For employees out in the field, this significantly complicates the matter and may slow down response time on critical issues. Organizations leveraging security automation, orchestration and response (SOAR) tools should ensure that they develop response workflows and use their solutions their full potential. Having an automated process for remote virus removal or even a full rebuild can be a fantastic tool in the SOC arsenal.

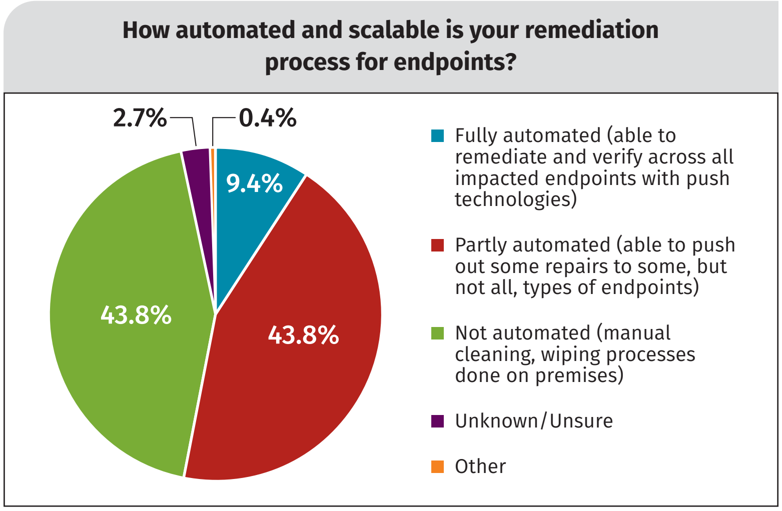

How automated and scalable is your remediation process for endpoints?

Figure 18. Remediation Process Scalability and Automation Level

Just because remediation is automated does not apparently mean it's viewed as being easy. The survey results show a clear pattern that many companies find remediation activities of nearly all varieties difficult. Table 6 organizes the data into the three categories and shows the top three items in each category.

Table 6. Remediation Levels of Difficulty

Impossible		**Difficult**		**Easy**	
1. Hunting for compromised endpoints without known IoCs	14.4%	1. Identifying what data has been impacted on breached endpoints	66.1%	1. Scanning for compromised endpoints with known IoCs	53.3%
2. Identifying what data has been impacted on breached endpoints	11.3%	2. Ensuring full remediation across all impacted endpoints	65.8%	2. Preventing inadvertent data loss during the wipe	36.2%
3. Detecting and remediating compromised endpoints in the cloud	11.3%	3. Determining the scope of a threat across multiple endpoints	63.8%	3. Removing all malicious artifacts on endpoints	31.1%

Given these findings, and the fact that the percentages across most categories in the "difficult" response were over 50%, the general conclusion is that organizations are still not fully happy with the ease of many activities involved in remediation, especially when it comes to finding data that has been impacted, ensuring remediation across multiple endpoints and determining the scope of an attack. Admittedly, these are very complex activities, and it is not surprising to see them at the top of this list. A combination of file access auditing, DLP and EDR solutions may help organizations that struggle with these activities.

The "Easy" section is also interesting in that there are some higher responses for categories that seem to align with the capabilities of EDR, namely scanning for compromised endpoints with known IOCs and removing all malicious artifacts on endpoints. This could be an indication that those that have EDR are able to use it for fast and accurate remediation activities of these types. Unfortunately, we do not have enough data to show whether these responses came from those with EDR or not, and additional research would have to be done to identify that is truly what is behind these responses.

Finally, in the "Very Difficult" section, the highest response category was hunting for compromised endpoints without known IoCs. This makes intuitive sense as hunting for compromise with nothing to go on typically requires analysts that have high levels of experience, know what attacks may look like and have the tools to search at scale. Cloud remediation also makes an appearance here, likely due to the fact that as a newer capability, many organizations do not know or have the tools to do forensics and remediation on cloud-based endpoints.

Takeaway

When it comes to scoping and intrusion, visibility tools such as EDR and proper log centralization will play a key role in both the speed and capability with which an incident can be investigated and remediated. On the investigation front, these tools give analysts the fast answers they need in order to respond quickly. On the remediation front, having options for either a clean wipe or surgical removal give teams the ability to choose the most appropriate response. Some infections can certainly be fixed through automated means or through fully automated reimaging, and that's a great option to have when appropriate. This shouldn't, however, be the only tool in the toolbox. Analysts confident in their scoping of an infection and familiarity with a virus may choose to wield the capability to surgically remove a virus, returning an endpoint to service with minimal to zero disruption to the user.

Progress Made?

In comparison with last year's survey, respondents are reporting an improvement in some areas while also reporting a decrease in others. Overall, technology adoption to aid in detection and prevention controls is on the rise. Organizations are investing more in solutions that provide enterprise-grade controls as well as offer centralized visibility and decision-making power. However, mapping technologies to the business continues to be an arduous task. Table 7 represents a few data points from the 2018 SANS Survey compared with 2019.

Table 7. Endpoint Security Report Card

Criterion	2018	2019	Grade	
Overall average of devices included in security program	41.4%	36.1%	D	for substantial decrease in devices covered in security program and processes
Increase in AI/machine learning and anomaly detection	36.6%	47.5%	B+	for adoption of new technologies to provide more detection and insight
Conducting manual searches trying to find adversary activities	16.0%	28.0%	A	for substantial increase in manual threat hunting searches
Percentage of organizations reporting endpoint compromise	42.0%	28.0%	B+	for substantial decrease in endpoints compromised
Ability to tie a user to a compromised endpoint (based on ability to do so at least 50% of the time)	79.0%	59.5%	F	for a massive decrease in the ability to associate a user to a compromised asset

Conclusion

Attacks continue to utilize phishing, malicious processes, command and control, pivoting and many other endpoint-enabled threats. The definition of endpoints is now broad and includes devices ranging from Windows operating systems to IoT devices and cloud containers. As such, organizations must place great emphasis on central visibility and control of all endpoints, not just servers. Throughout this report multiple areas of concern have been identified such as:

- Lack of central management of assets
- Inability to tie users to compromised assets
- Increase in IoT, wearables and other smart endpoints
- Limited data collected for analysis
- Increase in social engineering attacks

Security must focus on maximum visibility for detection and prevention logic—while at the same time, accepting that inspecting everything is impractical. The standard approach of analysis of traditional data sources is no longer enough, and organizations must apply new methodologies to collect and enrich tactical data sources for better decision-making power. To do this, technologies that allow data collection or central analysis of decentralized data are necessary and should include an emphasis on filtering out noise.

Takeaway

An increase in visibility is critical to informed decision making, as well as identifying compromised assets. To aid in this endeavor, centralized data analytic tools such as SIEM, EDR or event automated scripts should be implemented as a continuous improvement loop. Tools are important, but emphasis should also be placed on automating mundane tasks as well as sophisticated prevention and analytics via machine learning or behavior heuristics. Ultimately, such tools are helpful but only if trained staff are putting them to maximum use.

About the Authors

Justin Henderson is a certified SANS instructor who authored the SEC555: SIEM with Tactical Analytics course and co-authored SEC455: SIEM Design and Implementation and SEC530: Defensible Security Architecture and Engineering. He is a member of the SANS Cyber Guardian Blue Team who is passionate about making defense fun and engaging. Justin specializes in threat hunting via SIEM, network security monitoring and ad hoc scripting.

John Hubbard is a certified SANS instructor who authored the new SEC450: Blue Team Fundamentals: Security Operations and Analysis and co-authored SEC455: SIEM Design and Implementation. As an active security operations center lead and dedicated blue team member, he has firsthand knowledge of what it takes to defend an organization against advanced cyberattacks. John specializes in threat hunting, tactical SIEM design and optimization, and tailoring security operations to enable organizations to protect their most sensitive data.

Sponsor

SANS would like to thank this survey's sponsor:

opentext™