SANS

A SANS Survey

Endpoint Protection and Response:

A SANS Survey

Written by **Lee Neely**
Advisor: **Alissa Torres**

June 2018

Sponsored by:
Malwarebytes

SANS Analyst Program

Executive Summary

Automating endpoint detection and response solutions is the top priority for IT professionals trying to put actionable controls around their endpoints, according to the SANS 2018 Survey on Endpoint Protection and Response.

Automating and integrating workload across the detection and response cycle are critical, as endpoint systems of every type, including Industrial IoT (IIoT) devices, are under constant attack. As in our past surveys, user endpoints in particular continue to be a persistent problem for organizations.[1] Most successful endpoint compromises still leverage human factors, such as social engineering/phishing, web drive-bys and ransomware. This year's survey results also show a slight increase in USB-based infections as the initial attack vector.

Although antivirus was the tool most commonly used to detect the initial vector of attack, only 47% of attacks were detected this way. Other attacks (32%) were detected through automated SIEM alerts and network analysis, and 26% were detected through EDR (endpoint detection and response) platforms.

Yet, detection technologies that look at user and system behavior or provide context awareness were much less involved in detecting breaches. Only 23% of respondents' compromises were detected through attack behavior modeling and only 11% of compromises with behavior analytics. Because user and machine behaviors are the cause of most endpoint breaches, these technologies are critical for endpoint detection and response.

The lower rate of usage aligns with the types of technologies organizations have installed and are fully using. Funding isn't being directed toward predictive technologies and automated response, while respondents report having next-gen capabilities they have not yet implemented. For example, only 50% have acquired next-gen antivirus, but 37% have not implemented the capabilities. Additionally, 49% have malware-less attack detection, but 38% have not implemented the capabilities. In some cases, it appears that while respondent organizations were able to procure these types of newer technologies, they lacked the resources to implement them.

This gap in implementation indicates incomplete strategies, a leadership shortfall or a failure in project management related to tools and processes. Security teams are likely suffering from "shiny object syndrome," where their security operations center (SOC) is inundated with so many of the latest tools that the promise of reducing the functions of cyber analysts to enable them to perform analyses has instead limited their ability to implement or leverage available features in depth.

Predictive Technologies

Technologies that leverage machine learning and move the bar from searching for known bad elements to focusing on identification of abnormal behavior

Automated Responses

Use machine learning and analytics to speed remediation, restrict or block disallowed behaviors, and consistently orchestrate and update response plans

Key Findings

of respondents report their endpoints have been breached; **20%** don't know

of breaches involved 10–24 endpoints; **11%** involved 100–249 endpoints; and **9%** involved 25–49 endpoints

of respondents manage ICS systems, and **28%** manage IOT systems in their security programs, yet approximately **20%** (21% and 18%, respectively) of respondents suffered a compromise of one of these system types over the past year

of respondents report remediation of a single endpoint takes an average of 24 hours or less, and **67%** remediate an entire incident in under 7 days, yet only **45%** use fully automated response processes

[1] "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

"Can We Say Next-Gen Yet? State of Endpoint Security," March 2016, www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827

Respondents have a vested interest in improving visibility, detection and response through more automated, integrated endpoint protection, detection and response technologies. In this survey, 84% of endpoint breaches included more than one endpoint. And, while desktops and laptops are still the top endpoint types to be breached, their server endpoints, endpoints in the cloud, SCADA and other IIoT devices are also being caught in the dragnet of multi-endpoint breaches. These and other results, along with best practices and advice, are covered in the following pages.

Endpoints Everywhere

Whether at the managerial or hands-on analyst level, the 277 IT professionals who took this survey voiced concerns about their endpoints and shared their best practices by answering our 30-question survey held during March and April 2018. Security analysts/security administrators made up 29% of our survey base, while IT security and operations managers and executives constituted 29% of our sample. Overall, 55% of the respondents were part of their entity's security organization, while 22% came from the IT organization.

Organizations represented in this survey are primarily headquartered in the United States, but they have endpoints around the globe and in multiple locations, the top three regions being:

- U.S.— 65%
- Europe—47%
- Asia—41%

Number of Endpoints

Of the companies represented, 40% have 1,000 or less employees—and 27% had 15,000 to more than 100,000 employees. Those employees use a large number of endpoints. In the survey, 44% of respondents say their IT teams are managing between 5,000 and 500,000 endpoints. Nearly 10% of those are managing networks of 100,000–500,000 endpoints. See Figure 1.

A variety of industry segments were represented in this survey including banking and finance, technology, government, healthcare, manufacturing and telecom agencies.

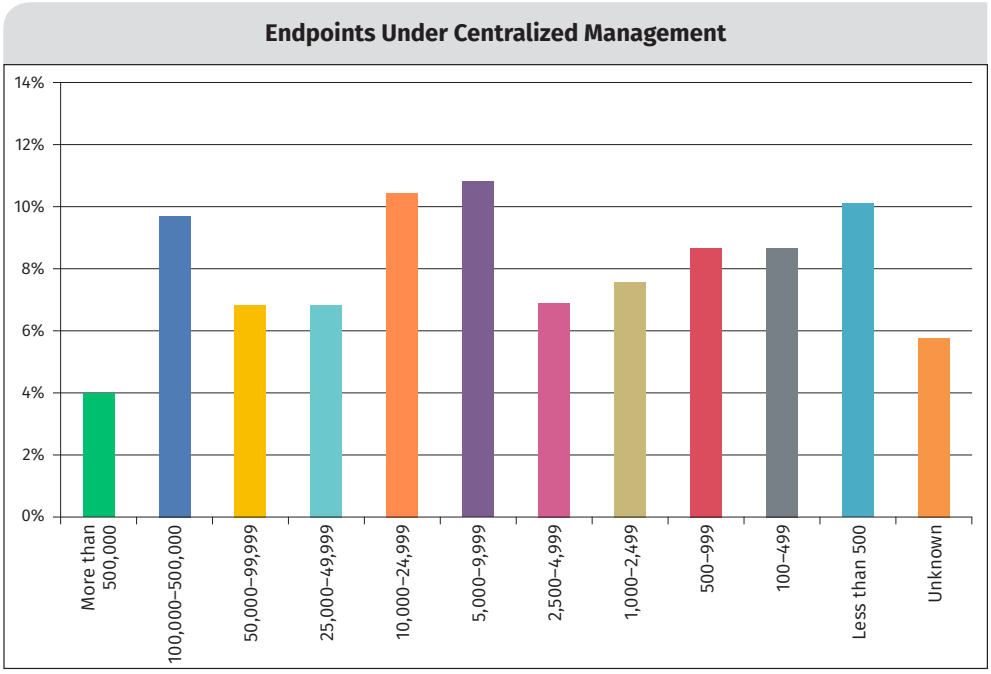

Figure 1. Endpoints Under Central Management

Variety of Endpoints

Many device types are connecting to networks: desktop computers, followed by employer-owned laptops, network devices and servers, mobile devices, even cloud-based systems, IoT devices, mobile and network devices, and wearables, as illustrated in Figure 2.

With the exception of cloud-based endpoints, which rose from just over 40% in 2017 to 60% in 2018, these results are similar to our 2017 endpoint security survey.[2] The rise in cloud-based endpoints not only challenges the standard remediation model, but introduces the need to secure those endpoints in a nontraditional setting.

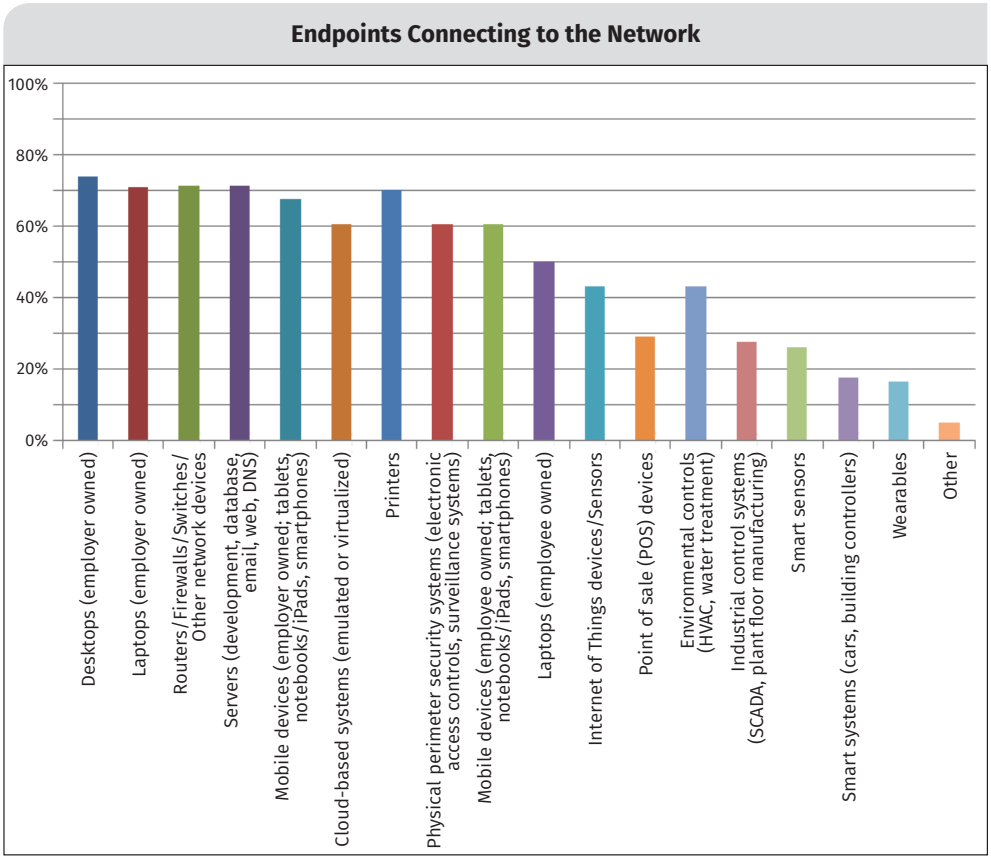

Figure 2. Endpoints Accessing the Network

Protecting Endpoints in the Cloud: Key Steps

1. Discover
   - Make sure cloud services are known and approved. Use a cloud access security broker (CASB).
   - Know what data types are being stored and processed in the cloud.
   - Determine who else may access the data on the nodes, such as the cloud service provider (CSP).
2. Inventory
   - Cloud-based endpoint nodes need to be part of your configuration management. Automation needs to include creation and disposition of endpoints, as well as updating your configuration management (CM) system.
   - Scan to detect new devices as well as existing, vulnerable devices and services.
3. Monitor
   - Make sure that logs are forwarded to your SIEM or centralized log management system, just as traditional nodes are.
   - Monitor traffic to/from cloud endpoints, including noting restrictions on sites and content types.
4. Protect
   - Cloud-based endpoints need approved configurations, just as traditional endpoints do.
     - New service offerings need to be analyzed and approved prior to use.
     - EDR solutions need to be included in the configuration.
     - Include additional steps, such as encryption of data at rest, to protect access to your data.
   - Ensure that data backup and recovery includes cloud endpoints.
   - Ensure that cloud storage is accessible only to authorized nodes/networks.

[2] "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, p. 5, Figure 4.

Traditional corporate IT services, servers, desktops, etc., whether delivered conventionally (insourced) or via cloud services (outsourced), remain well-entrenched in security programs. The drive for anytime/anyplace/any device computing, including the growing use of BYOD (employee-owned handhelds, smartphones, etc.) opens new windows of vulnerability, yet such devices are less frequently included in organizations' management programs. See Figure 3.

What device types are connecting to your network or part of your network?
Identify which are explicitly included in your security/risk management programs.

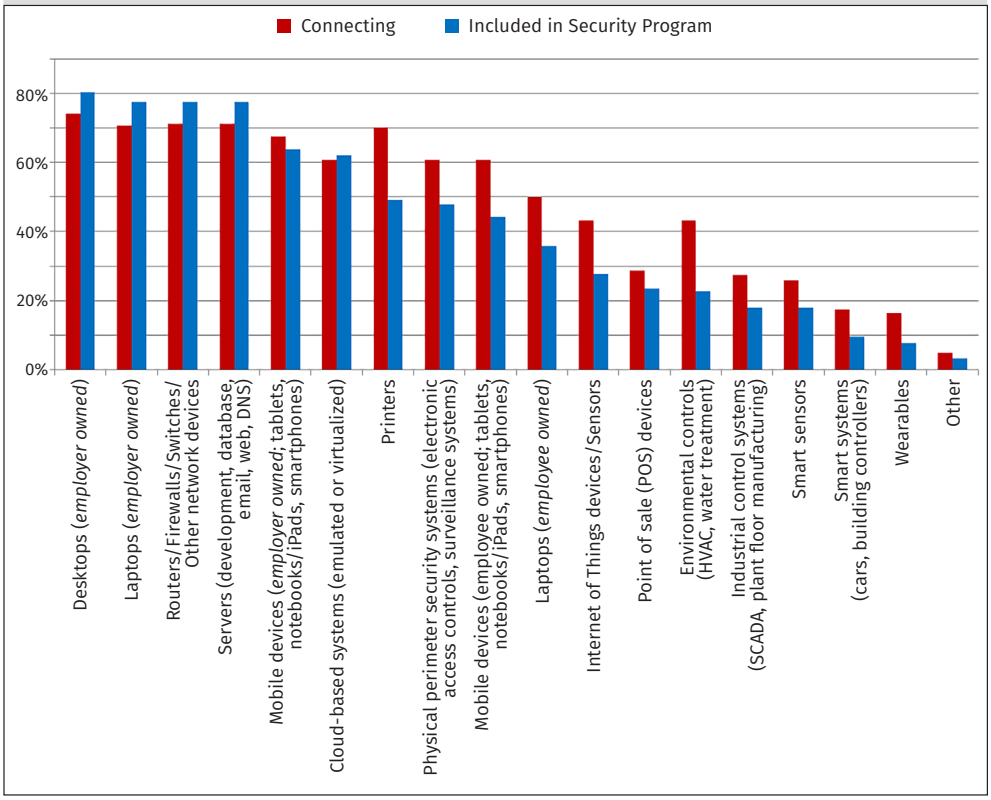

Figure 3. Management Most Mature for Traditional, Employer-Owned Endpoints

Organizations are focusing on the known attacks rather than worrying about the unknown—including shadow IT or IoT. Yet, recent studies have found that systems remain vulnerable to WannaCry.[3] Lack of patching and security updating is most prevalent in vendor-managed devices or appliances, including IoT and purpose-built systems, where IT and security teams tend to "set it and forget it." Such an approach to these endpoints contributes to a weaker overall security posture and provides attackers with additional entry points to leverage. These devices are often behind on patches and OS versions because the devices don't support updates or will no longer function with updates due to legacy software requirements. Active discovery and containment of unauthorized or insecure devices have to be standard operating procedures.

TAKEAWAY

While focusing on the needs for new endpoints, such as IIoT, cloud and BYOD, don't overlook existing possible points of attack, such as printers.

Know Your Users

When asked whether they could tie a user to the endpoints and servers they were accessing, 79% reported they can make the association at least half of the time (34% always, 45% at least half the time). This is key, since it adds a dimension of identity to making decisions about anomalous behavior.

TAKEAWAY

Just as traditional endpoints need protections and secure configurations, so do newer classes of endpoints such as IIoT, mobile and cloud. Diversity of endpoints, location, type and security requires increased awareness and inclusion in the security program. Automation is key for discovering, monitoring and securing these nodes.

[3] "State of play: One year on from WannaCry ransomware outbreak," Digital Journal, April 2018. www.digitaljournal.com/business/state-of-play-one-year-on-from-wannacry-ransomware-outbreak/article/519129

Caught in the Crossfire

Pretty much all endpoints house sensitive data. Yet, we've just shown that some are managed more frequently than others, based on an organization's perception of the risk to which each device exposes the organization. Table 1 shows that organizations are most concerned about their corporate-owned laptops (32%), servers (32%) and desktops (29%)—which are the same devices that respondents report are most under attack.

Traditional servers running line-of-business (LOB) and legacy applications are of lower concern (14%) as compared to other types of noncloud servers (32%). This lower level of concern is more likely due to other types of services having more front-of-mind weaknesses, as illustrated by Wired Magazine's report that the mobile phone is the most vulnerable gadget,[4] rather than these services themselves being secure.

Table 1. Types of Endpoints Most at Risk

Device of Concern	Percent
Laptops (employer owned)	32.2%
Servers (development, database, email, web, DNS)	31.8%
Desktops (employer owned)	28.8%
Cloud-based servers (PaaS, emulated or virtualized)	26.2%
Mobile devices (employee owned; tablets, notebooks/iPads, smartphones)	26.2%
Laptops (employee owned)	25.1%
Cloud-based applications (SaaS)	22.8%
Internet of Things devices/Sensors	13.9%
Servers (line-of-business applications, legacy)	13.5%
Mobile devices (employer owned; tablets, notebooks/iPads, smartphones)	12.4%
Routers/Firewalls/Switches/Other network devices	12.4%
Industrial control systems (SCADA, plant floor manufacturing)	11.6%
Environmental controls (HVAC, water treatment)	5.2%
Physical perimeter security systems (electronic access controls, surveillance systems)	4.9%
Point of sale (POS) devices	4.1%
Printers	1.9%
Smart systems (cars, building controllers)	1.9%
Smart speakers (Amazon, Google, Echo)	1.5%
Wearables	1.5%
Smart sensors	1.1%

Managed Devices

Configured and maintained devices operating in accordance with security policies and centralized regulation

Unmanaged Devices

Devices that have no standard configuration and are not controlled or monitored by security policies or monitoring/detection implementations

TAKEAWAY

Patching LOB, legacy applications and their supporting services can be tricky due to interdependencies and the mixture of technologies involved in delivering those services, particularly for legacy applications, which may not work on updated technology stacks. The challenge here is reaching the right balance between keeping the applications secure/updated and minimizing the business impact.

[4] "Your Phone Is Your Most Vulnerable Gadget. Protect It Now.," Wired Magazine, July 2017, www.wired.com/story/your-phone-is-your-most-vulnerable-gadget-protect-it-now

Under Attack

In this year's survey, 42% of respondents report having had their endpoints exploited (see Figure 4), which is nearly 10 percentage points lower than the 53% of respondents reporting such breaches in 2017.[5]

However, those who didn't know whether they'd been breached rose the same amount from 10% in 2017 to 20% in 2018, indicating things may actually be getting worse or that organizations may be getting more realistic about what they do and do not know is occurring on their endpoints.

Important Distinctions[6]

Threat—Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm

Threat vector—Method a threat uses to get to the target

Incident—Adverse network event in an information system or network or the threat of the occurrence of such an event

Data breach—A confirmed incident in which sensitive, protected or confidential data (e.g., personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property) has been potentially viewed, stolen or used by an individual unauthorized to do so [7]

Have any of your endpoint systems been exploited (involving unauthorized access, malicious files/ processes, APTs or other malicious activities resulting in data exposure, exfiltration or business disruption) in the past 12 months?

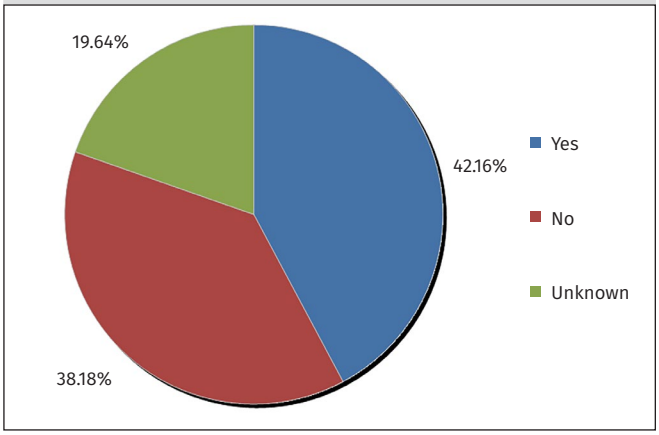

Figure 4. Breaches at the Endpoint

Concerns Mirror Detected Exploits

The systems of increasing concern are those respondents believe are the most involved in actual exploits. In the survey, 82% of respondents said their actual breaches involved desktops, while 69% also involved corporate laptops. Another 42% involved employee-owned laptops, which are not as well-covered in security programs (as shown previously in Figure 3). Servers (LOB 38%, other types 37%) round out the top five most frequently compromised endpoints. See Figure 5 on the next page.

Ultimately, compromises most often affect the resources that comprise the user's traditional workspace. Note that in most cases more than one endpoint is involved, indicating that once an attacker gains a foothold, compromise of other assets is likely to follow due to lateral movement.

> *Unmanaged devices were infected through an unpatched browser vulnerability at the endpoint. The exploit was able to offer lateral movement capabilities to the attacker ….*
>
> —Survey Respondent

[5] "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, p. 10, Figure 8.

[6] Definitions from the Internet Storm Center, https://isc.sans.edu/glossary.html, unless otherwise indicated.

[7] https://searchsecurity.techtarget.com/definition/data-breach

Successful Threat Vectors

As in our previous surveys, the top threat vectors for these exploited endpoints take advantage of the hapless user: web drive-by (63%), social engineering/phishing (53%) and ransomware (50%). Credential theft was used in 40% of compromises detected by respondents. See Figure 6.

TAKEAWAY

Attacks align with areas of concern. Know your weaknesses, and have full coverage of your assets. Consider using the MITRE ATT&CK™ matrix,[8] an open source tool that provides a comprehensive scope of attacker techniques and technologies or another framework to guide your actions.

Research shows that 90% of unknown, undetected malware is delivered via the web. Organizations need to ask whether lax proxy settings and lack of stringent file download restrictions are failing them.

Perhaps more importantly, these top three vectors leverage human actions taken on the endpoint to achieve success. Is the security program missing a key element for success? Or, is it simply not mature enough to properly incorporate human risk factors and the accompanying mitigations? Because these top compromises rely on human actions, it suggests that human actions taken at the endpoint should be monitored and contained, along with providing user education whenever possible. A variety of tools, including next-gen antivirus (to detect malware-less and file-less attacks) and automated EDR (with next-generation antivirus [NGAV], user/behavior analytics included) should assist in this mission.

Over the past 12 months, what types of endpoints have been compromised? *Please indicate if these were widespread or limited in scope to either a small number of endpoints or just one endpoint. Leave blank all types that were not compromised.*

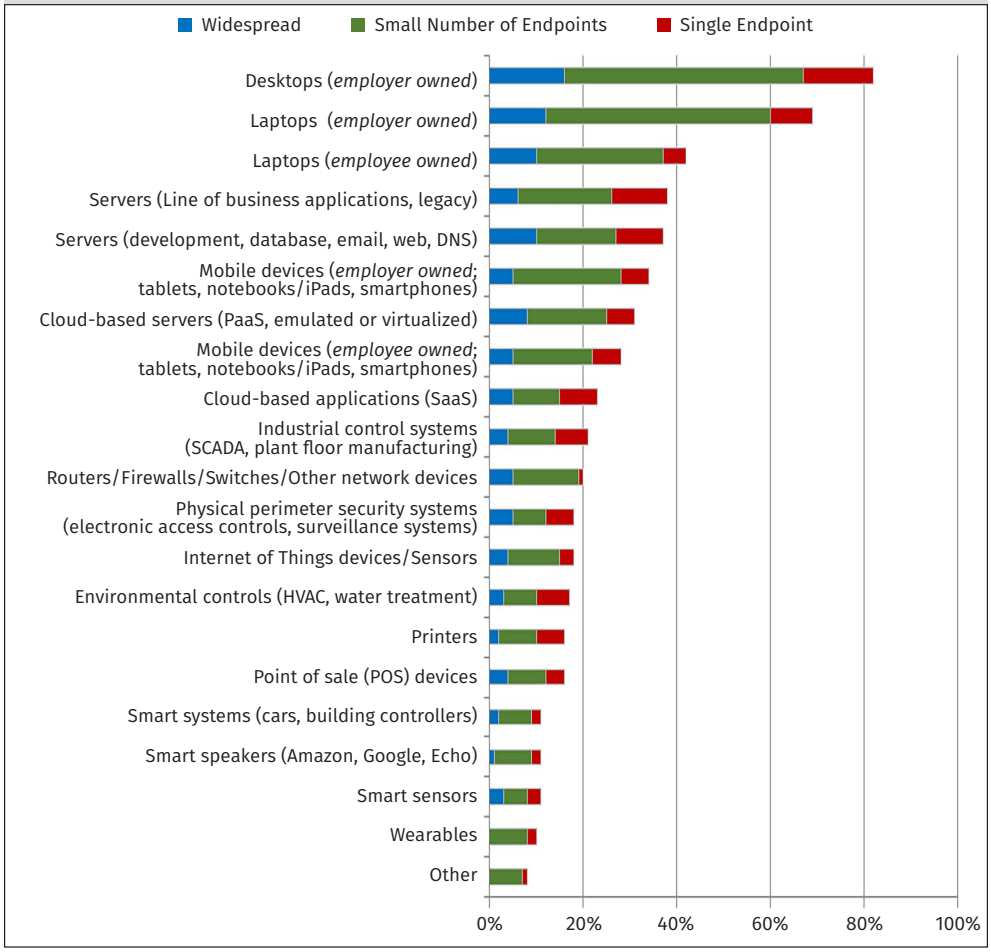

Figure 5. Endpoints and Exploits

How were these endpoints exploited? *Select all that apply.*

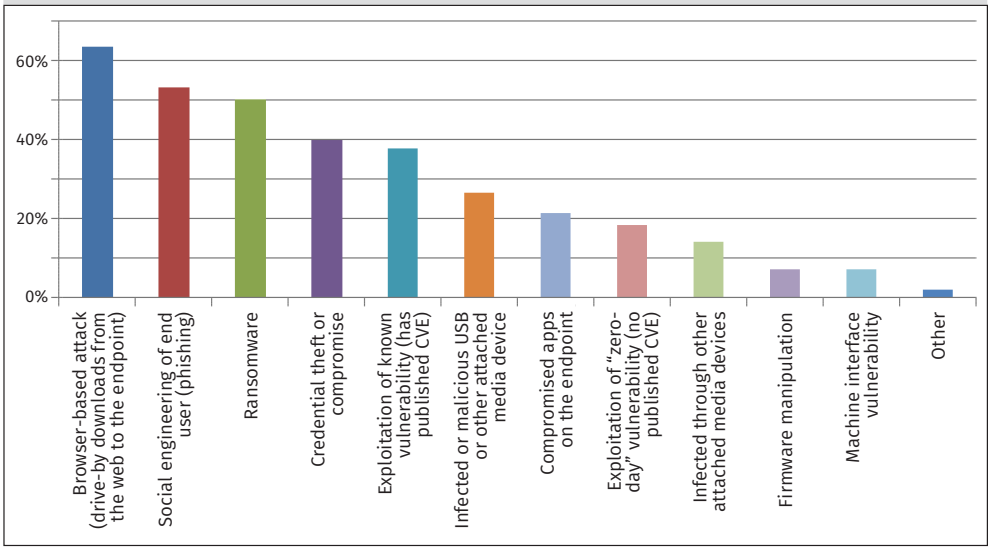

Figure 6. Successful Vectors of Attack

[8] https://attack.mitre.org/wiki/Main_Page

[9] "90% of unknown malware is delivered via the web." Infosecurity Magazine, March 2013, www.infosecurity-magazine.com/news/90-of-unknown-malware-is-delivered-via-the-web

Typical Exploits Described

When asked to describe exploits in the enterprise, respondents contributed interesting stories that involved traditional endpoints and mobile devices, often citing the users as the initial point of exploit. As one wrote:

> *Most of what we deal with is commodity, opportunistic attacks against our users. [They receive an] email asking them to click on a link, they go to an infected site, get malware, etc. So, we wipe & reimage their machine.*

And another wrote:

> *[A user received a] phish with [a] link to* **`maldoc`** *[and] forward[ed it] to IT person as suspicious. IT person with overly promiscuous admin access hit link and detonated it, and we ended up with* **`emotet`** *and* **`qakbot`**.

A similar number of respondents cited unpatched vulnerabilities and zero days as the cause of their breaches. Respondents described a resurgence of WannaCry or Petya (further indicating prevention/patching shortfalls), and DocuSign® credential theft (indicating successful phishing for credential compromise). Other examples include successful exploitation of zero-day threats, where mitigations include limiting network access ports, protocol enforcement and restriction of access to bad sites—or, better still, whitelisting. Additionally, one respondent indicated: "A firewall in one of the datacenters [sic] was compromised leading to an attack on the monitoring system," which speaks to the router/network device being an attack vector, as mentioned previously in Table 1.

Protect the Browser

Use remote browser isolation (RBI) technologies along with EDR configurations to restrict access to inappropriate sites. Limit the security vulnerabilities of outdated browsers, and improve scanning endpoints for malicious artifacts.

Detection and Response

Antivirus caught endpoint compromises 47% of the time—which is still less than 50%—showing that signature-based antivirus, while still useful, is not enough. Automated SIEM alerts detected compromises 32% of the time. See Figure 7.

Results show that organizations are utilizing a number of technologies and likely centralizing their searches through their SIEMS. In these cases, the SIEM is collecting the endpoint and network data organizations are utilizing to find endpoint-related events, analyzing it with endpoint analytics, and providing correlation against data elements from the EDR systems and beyond.

How were the compromises detected? *Select all that apply.*

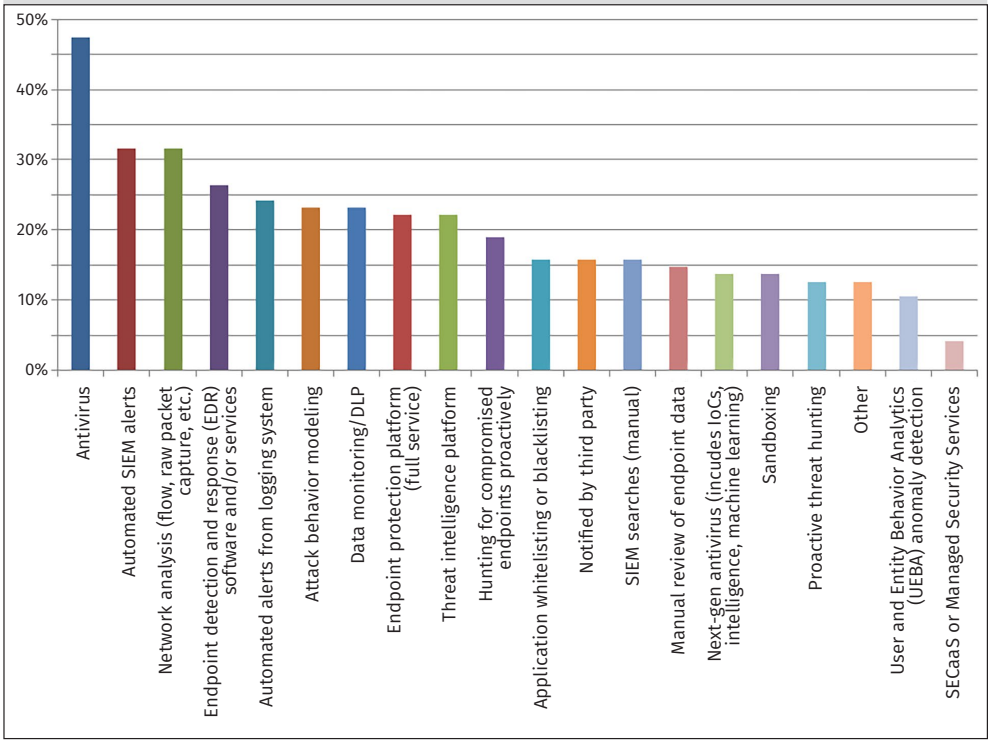

Figure 7. How Compromises on Endpoints Were Detected

Unfortunately, 32% of respondents reported that proactive discovery, involving active endpoint inquiry, detected compromises only 10% or less of the time, meaning that discovery is dependent on alerts from the endpoint or network tool. This is another area where automation and integration with EDR and other orchestration platforms would make great improvements in endpoint detection and response capabilities.

Examples of proactive discovery include behavior modeling, threat intelligence and hunting platforms. Learning to discover attack behaviors rather than simple indicators of compromise is key to becoming proactive. Using red teaming, internal penetration testing and learning behaviors of threat actors all aid in building behavior models.

TAKEAWAY

The number of respondents still conducting manual searches through disparate tools and sources demonstrates that organizations are not automating these menial tasks, even though vendor products contain mature capabilities to accomplish these functions.

Seeing What Isn't There

When it comes to tracking down artifacts to investigate compromises, centralized data collection covers many of the key items, such as software inventory and configuration, but there are gaps:

- The largest gap lies in discovery of memory-resident objects where antivirus and traditional security mechanisms fail. Detecting memory objects is key for the detection of and response to file-less malware. Respondents from prior surveys also voiced concerns over lack of these artifacts, which are themselves an effective, if not strongly preferred, way to perform postinfection analysis.[10]
- Identification of sensitive data usage and lack of radius accounting information are key to understanding gaps in coverage. Such types of information provide insight into where information is processed, which may be of concern when the data has been exfiltrated. Moreover, *when* users are accessing systems is key to correlating user and threat actions.
- Respondents tell us they are missing network data (machine-to-machine connections and Address Resolution Protocol [ARP] data) to correlate with the endpoint artifacts. Such information is necessary to obtain a full understanding of malware and how it is leveraging or coopting the network.
- They are also missing user-behavior data, which in some cases simply doesn't exist. Organizations need such data for correlation and proper baselining. With the advent of cloud services, organizations need to ensure that similar data collection services are in place and verify that the data is incorporated into centralized data collection.

When asked what data they needed better access to, 84% of respondents want more network access and user data, 74% want more network security data from the firewall/IPS/unified threat management (UTM) systems, and 69% need better network traffic analysis, demonstrating a clear understanding of the need to correlate such information. This information is necessary both when an event is happening and after the fact—when analysts need to conduct forensic investigations and answer questions about what happened and whether the threat was completely remediated (one of the most difficult questions to answer).

[10] "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, p. 8, Figure 7.

Predicting the Unknown

Automation and predictive technologies should be included in the corporate acquisition and implementation road map. These technologies enable analysts to more readily separate and categorize events and actions, facilitate threat hunting, detect malware-less and memory attacks, and reduce the number of tools and data sources analysts need to examine. The inability to process massive amounts of security data directly affects the analyst's ability to detect attacks.[11]

Harden Your Endpoints

To turn the tide, organizations must identify, install and configure effective solutions, as well as establish baseline readings. Key success factors indicated by respondents are ease of data collection (49%), correlation of data into usable information (47%), skilled operators (46%) and automation/tool interoperability (43%). See Figure 8.

The top barrier is budget and management support (47%), followed by lack of automation/tool interoperability (43%) and finding the skills required to operate tools (40%). From these results, it is clear that, beyond procuring tools that feature automation and interoperability, organizations must address the staffing needed to operate and use their tools, either by resourcing up or reducing the complexity of the toolsets analysts must directly interact with.

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

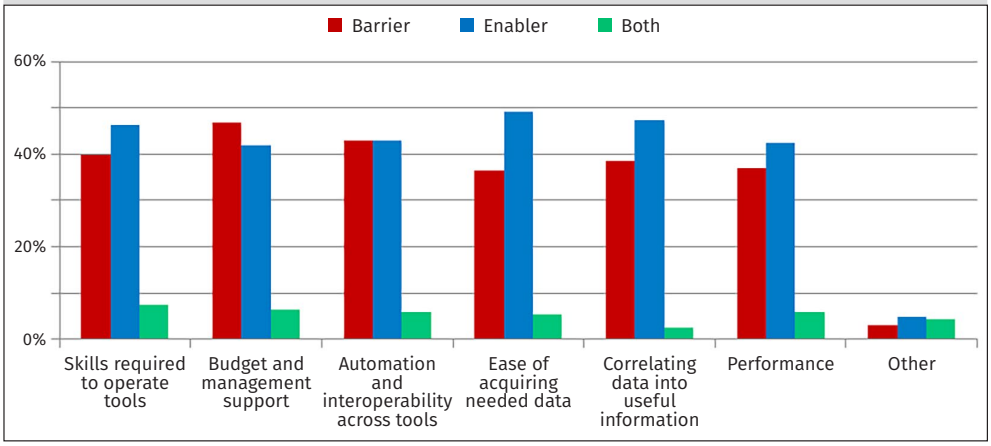

Figure 8. Barriers and Enablers to Successful Endpoint Controls

Analysis and Consolidation

When it comes to analyzing and consolidating endpoint data, 63% of respondents say that their main tool is the SIEM, followed by 46% who favor a centralized log management platform. See Table 2.

Sadly, 33% of data analysis and consolidation still involves manual searching through disparate security, intelligence and platform tools. Use of a centralized EDR system management interface follows at 32%. Therefore, it is important that EDR solutions provide robust bidirectional API integrations into SIEM applications so that analysts can leverage a single-pane-of-glass user experience in their preferred application.

Table 2. Means of Analyzing and Consolidating Endpoint Data

Tools for Analysis and Consolidation	% of Respondents
Centralized SIEM interface	62.68%
Centralized log management platform	45.93%
Manual searches through disparate security, intelligence and platform tools	33.49%
Centralized EDR system management interface	32.06%
Centralized intelligence platform	27.27%
Third-party intelligence platform	20.10%
Other centralized control interface	12.92%
Other	2.87%

[11] "Are you buried under your security data?" CSO Online, May 2016, www.csoonline.com/article/3075001/security/are-you-buried-under-your-security-data.html

Improving Detection and Response

Endpoint threat intelligence is also critical and should be able to feed into the detection and response systems automatically. This should reduce the time to detect, respond and ultimately remediate the threat/vulnerability the attacker was trying to exploit.

A typical endpoint response scenario starts with an alert to the SOC from an automated detection source indicating unusual behaviors or actions, or with a call from the user saying something "odd" is happening (detection). The analyst can then immediately scan the target endpoint to search for any unusual processes, connections or other artifacts for early triage. If it's not a false positive and a true threat exists, the analyst would quarantine the endpoint from accessing other endpoints to prevent the spread of the attack, as well as to make sure access to related Internet sources is restricted by the threat response system (response). While the security analyst identifies the sources and attack vectors, the system and any additional compromised nodes are remediated to restore operation. The SOC initiates measures to block the sources of infection if possible, and user training is scheduled if appropriate (remediation).

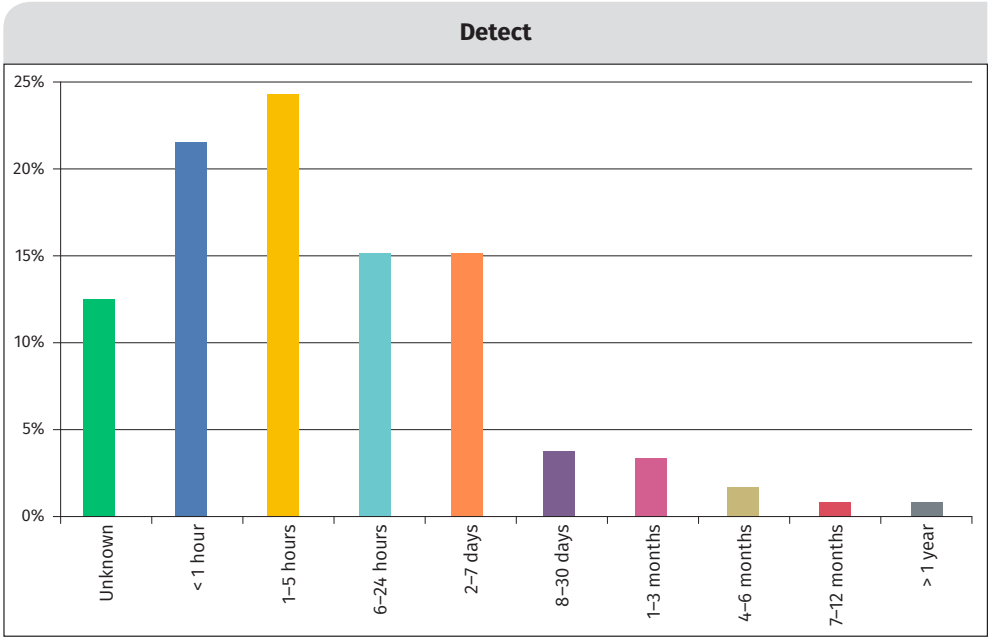

Figure 9. Reported Time to Detection

In this year's survey, 61% of respondents report being able to detect a threat in under 24 hours, with 46% needing under 5 hours. See Figure 9.

Time to respond takes a little longer, but the majority of respondents (53%) were able to respond in five hours or less, as shown in Figure 10.

However, given that 62% took up to 24 hours and another 19% took 2–7 days to remediate a single endpoint, the opportunity still exists to reduce these intervals further with auto-response and predictive systems. With infections spreading across endpoints in minutes, this is a lengthy window for attackers.

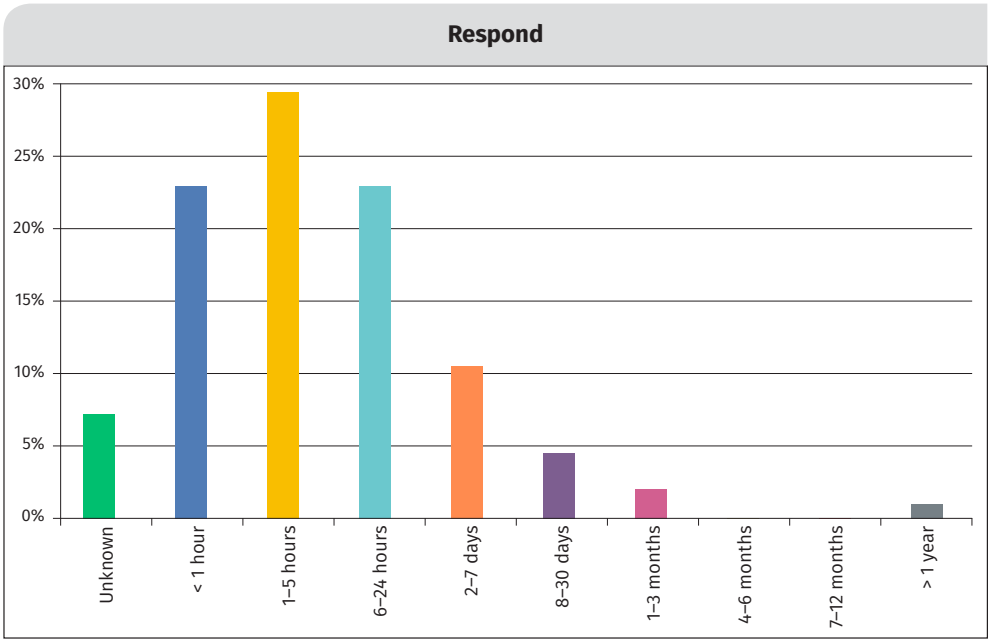

Figure 10. Reported Response Times

Remediation Challenges

Once a threat is identified, remediation is still a looming challenge—not only cleaning up the incident, but also determining how to prevent recurrence of a similar threat. Complete remediation takes two to seven days, chosen by 33% of respondents. Given the choice between surgical remediation (without reimaging) and wiping and reimaging, 92% feel the most effective solution overall is reimaging, while 55% identified surgical repair as effective overall.[12] While a wipe-and-reimage remediation may be perceived as more effective, depending on the confidence level of the incident responder, it requires more time and higher costs than surgical remote remediation; also, some servers that undergo a wipe-and-reimage can potentially cost millions in downtime. Write-in responses remind us that flashing the BIOS may also be part of the necessary remediation plan.

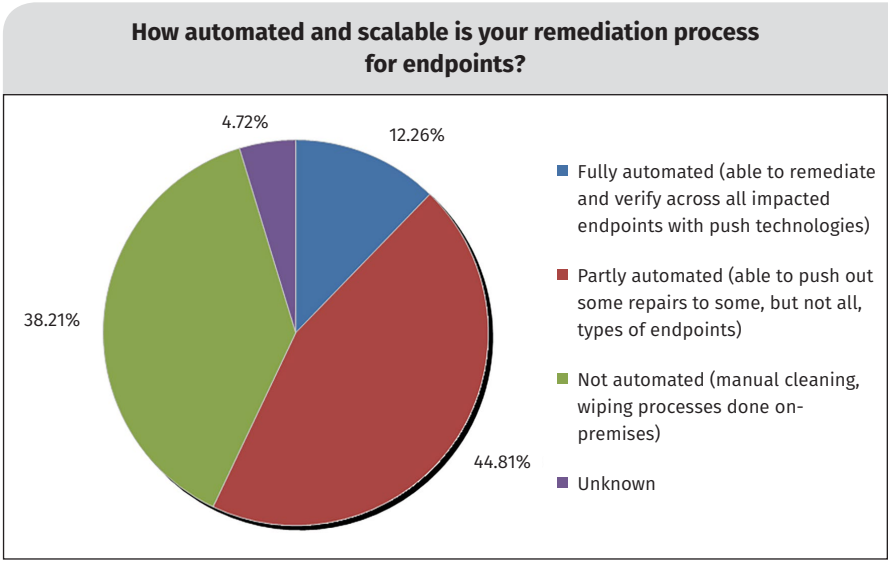

Figure 11. Few Accomplish Full Remediation with Verification

When it comes to how remediation tasks are orchestrated and completed, full automation is elusive, according to respondents. In our survey, only 12% of respondents have fully automated remediation and verification processes, as shown in Figure 11.

Overall, 57% have achieved some level of automation; up from 52% in 2017, whereas 38% still rely on manual processes. Automation represents a path to improve response time as well as getting users back online more quickly. It also aids consistency of response and frees up resources needed to deal with the increased diversity and quantity of devices in the corporate ecosystem.

TAKEAWAY

Automate the process of reimaging systems, reloading standard applications and setting approved security standards.

Validating Remediation

Of all the remediation steps, finding breaches using known indicators of compromise is the least difficult for responders (58%), followed by removing all malicious artifacts on endpoints (which emphasizes the call to wipe and reimage as indicated previously). The most difficult remediation tasks were identifying what data has been affected on the breached endpoints, selected by 71%, followed by determining the scope of a threat across multiple endpoints, chosen by 68%. See Figure 12.

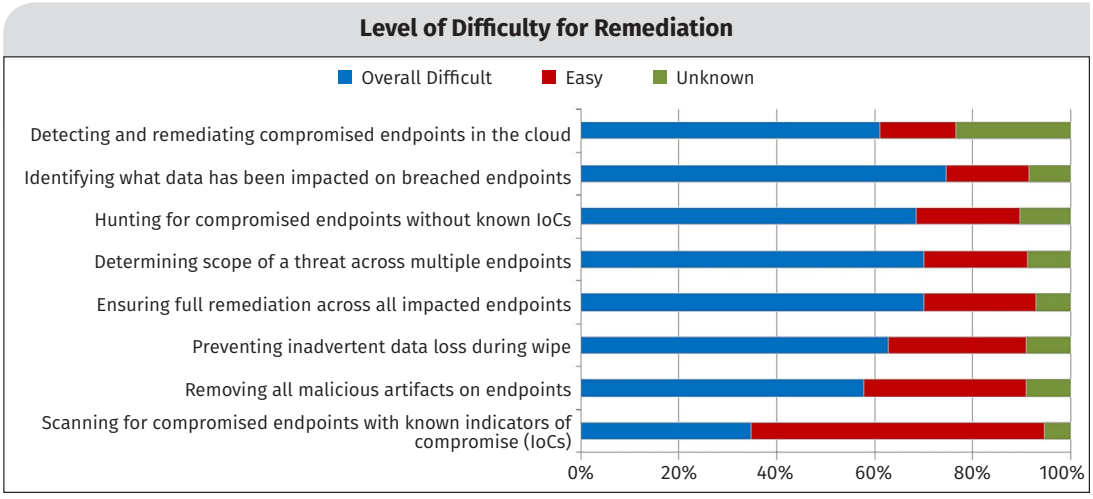

Figure 12. Difficulty of Remediation

[12] Results total more than 100% because respondents could make multiple evaluations.

The relatively high incidence of ransomware attacks, as shown previously in Figure 6, highlights the need to remediate affected data. This requires being able to detect the modified data and having known good copies of that data that are recent enough to have minimal business impact when installed.

Restoring Compromised Data

Restoring user data, including profiles and documents, must include identification of a known good restore point. Leverage real-time or continuous differential backups to reduce the data loss interval for data restoration. Be sure to back up to sources that are not directly connected to endpoints, such as file shares or disks, and use services not accessible by built-in OS file I/O libraries.

Enterprise file synchronization and storage services such as OneDrive, Box, Google Drive, etc. can replicate corrupted content to multiple nodes. Select services that allow files to be restored to specific point-in-time versions so the known good copies can replace the replicated contaminated content.

Next-Gen Practices and Capabilities

It is encouraging to note that 65% of respondents are using data protection and encryption technologies, which are key enablers for effective restoration. Vulnerability assessment and application controls are utilized in 63% of organizations, with 59% implementing centralized management dashboards and 54% utilizing cyber threat intelligence (CTI). Where respondents seem to fall short is on workflow automation and artificial intelligence (AI)/machine learning—which are key enablers to improve detection, remediation and response—but are used by only 25% and 21%, respectively. See Figure 13.

Overall, 58% indicated that automated incident response/remediation workflows and AI/Machine learning are important, but that they have not yet implemented those technologies. As previously mentioned, having automated responses along with automatic invocation of workflow is key to an effective and timely response to incidents. Further, without leveraging automation to identify trends and build models, the already overworked analysts have to manually perform those duties rather than just refining the results and minimizing or eliminating false positives or negatives. Finally, when analysts have to spread their attention

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?

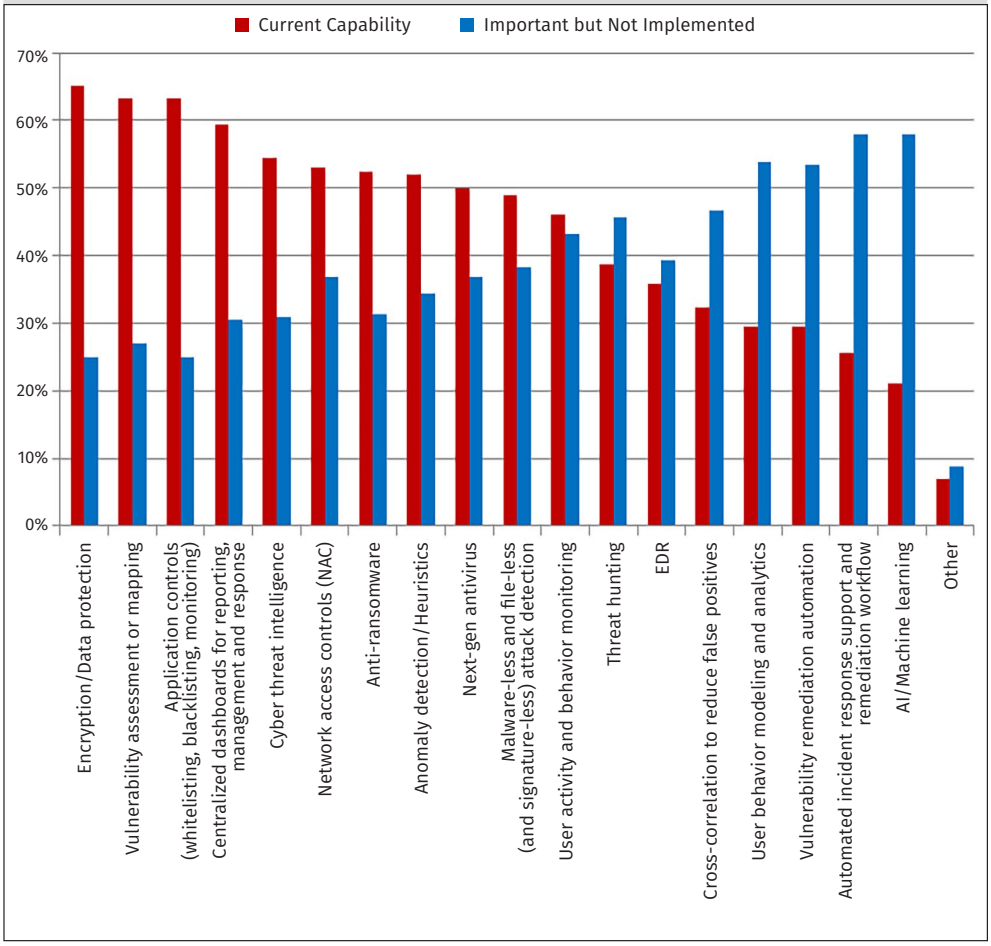

Figure 13. Next-Gen Controls

over large numbers of alerts, the related lack of analysis time means that root cause analysis cannot be successfully completed. Without in-depth information on how the organization was compromised, corporate knowledge and/or intelligence about threat actor tactics, techniques and procedures (TTPs) cannot be gained.

Organizations need to create a master plan or road map to integrate the tools they already have in place and prioritize spending to fill in the gaps. They must prioritize spending for modern detection and response capabilities that leverage machine learning, all while being careful not to tip the balance and add to the drain on security analysts' abilities to secure the organization by adding too many disparate tools that dilute their focus on actionable data.

TAKEAWAY

Invest in solutions that provide comprehensive coverage of the attacker landscape and make it easy for analysts of any skill level to stop advanced threats.

Conclusion

The top threats to organizations still include web-based malware, social engineering and ransomware, all of which are focused on user endpoints.

Organizations must augment their abilities to more proactively defend their systems and detect threats earlier in the cyber kill chain. They also need a clearly central location to administer endpoint security—even for endpoints in the cloud. Results show some confusion about whether or not SIEM, EDR or even log management systems represent that centralized capability. Without a central point to analyze endpoint-related activity (including network-related data), automation will take a back seat.

Ultimately, the goal of endpoint protection is to shorten the mean time to detect, to respond and to contain malware. Meeting that goal helps keep organizations moving toward business goals at appropriate resource levels rather than having to take time out to wipe and reimage endpoints or take other actions that negatively affect business viability.

TAKEAWAY

Improved analysis and automation tools are key to discovery and remediation. Next-generation tools bring not only machine learning, but also the automation needed to model normal behavior and highlight unexpected behavior. Such automation enables validation that an attack has been fully remediated, which requires resources to perform root cause analysis and provide both corporate knowledge and the information needed for successful hunting. Having tools that provide ease of use for the analysts can reduce the skills gap challenge.

About the Authoring Team

Lee Neely, a SANS analyst and mentor instructor, teaches cyber security courses for SANS and serves as a NewsBites editor and OnDemand quality control tester. He worked with the SCORE (Security Consensus Operational Readiness Evaluation) project to develop the iOS Step-by-Step Configuration Guide and the Mobile Device Configuration Checklist included in the SEC575 course. Lee holds the GMOB, GPEN, GWAPT, GAWN, CISSP, CISA, CISM and CRISC certifications. He leads the cyber security new technology group at the Lawrence Livermore National Laboratory, working to develop secure implementations of new technology, including developing the secure configurations, risk assessments and policy updates required for its corporate and bring-your-own-device mobile devices.

Alissa Torres (advisor) is a SANS analyst and certified SANS instructor specializing in advanced computer forensics and incident response (IR). She teaches internationally for SANS, educating security professionals on digital forensics and IR techniques, with special interest in increasing workforce diversity in the digital forensics and incident response (DFIR) community. Alissa currently leads the cyber security IR team at a global manufacturing and agriculture company. With extensive experience in information security in government, academic and corporate environments, she has served as an incident handler and digital forensic investigator. A GIAC Certified Forensic Analyst (GCFA), Alissa holds the GCFE, GPEN, GSEC, GCIA, GCIH, CISSP, EnCE, CFCE, MCT and CTT+ certifications.

Sponsor

SANS would like to thank this survey's sponsor:

Malwarebytes