WHITE PAPER

SECURITY THREATS DEMAND NEXT-GENERATION ENDPOINT PROTECTION

Capabilities such as threat hunting, behavioral monitoring and endpoint detection and response contribute to an effective security posture.

EXECUTIVE SUMMARY

The world of cybersecurity never stops evolving. Attackers continue to become more sophisticated and well-funded, developing new tools and techniques that threaten the security of their targets. The business environment also evolves as organizations adopt new practices and supporting technologies, which can introduce new avenues for attacks. Security technology also marches on, rising to meet the challenges of new technologies to defend and new threats to defend against.

Endpoint protection technology plays an important role in this changing landscape, defending some of the most exposed components of an organization's technology infrastructure from increasingly sophisticated attacks. Organizations that find themselves relying on outdated endpoint protection strategies expose themselves to significant risk when they operate in the modern threat environment. Next-generation endpoint protection technologies reach beyond the simplistic signature detection techniques of years past to incorporate many advanced features that help detect novel attacks, manage endpoint security proactively and identify the root causes of security compromises.

Organizations that incorporate next-generation endpoint protection solutions into their cybersecurity programs will find themselves not only well positioned against the threats posed by today's landscape but also prepared to respond to the novel threats that will arise in the future.

The Evolution of Endpoint Protection

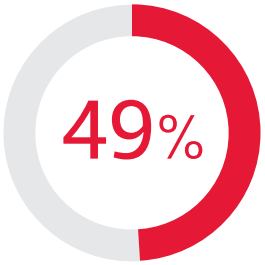
Endpoint protection isn't new. The discipline of protecting workstations, servers and mobile devices against malware and other threats is as old as the cybersecurity profession itself. Most organizations purchased anti-virus software subscriptions long before they hired a single cybersecurity professional. Those original purchases often drove cybersecurity investments for years afterward and became the first components of a broader cybersecurity program that embraced a defense-in-depth approach to protect systems and information from threats to their confidentiality, integrity and availability. Those broader strategies evolved to include email security, web application security, intrusion detection and prevention, and other supporting technologies.

The earliest approaches to endpoint protection focused on signature detection strategies. Malware authors would develop new viruses, worms, Trojan horses and other software threats and release them into the wild. After spreading to systems around the world, samples of the malware would wind up in the hands of security researchers at anti-virus firms. Those researchers would analyze the malware and develop unique fingerprints in the code that endpoint protection tools could use to identify future infections. They would then release those signatures to their customers in anti-virus updates, protecting systems against future infections by the same strain. The cycle would then begin anew, as malware authors modified their code to evade detection.

The signature detection approach is reliable and consistent. When anti-virus software encounters a known threat, it can easily recognize and eradicate it. This technology remains a foundational element of endpoint protection strategies today because it works. However, while signature detection remains a necessary component of endpoint protection strategies, it is no longer sufficient to provide robust protection. The signature detection approach leaves enterprises wide open to zero-day attacks that use new malware strains to exploit previously unknown vulnerabilities. Modern threats require a modern response.

New Targets and Shifting Strategies

The threat landscape isn't the only source of change, either. Enterprise computing is also shifting significantly. With more data and workloads moving to the cloud, the challenge of protecting assets spread across multiple locations becomes more complex. Something will eventually slip through the cracks if organizations don't take steps to carefully manage their deployed computing base and defend it against attacks.



The percentage of organizations that do not think their endpoint protection solution provides sufficient protection against the newest attacks[1]

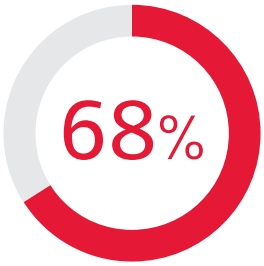
Adversaries understand the complexity facing enterprise security teams and seek to exploit the weak links in the chain by using a diverse set of tools to compromise security. They realize that end users are often the soft spot in enterprise security, and they deploy attacks that target those users through spear-phishing emails and other focused attacks.

Endpoint protection strategies have evolved to provide a strong defense in this new environment. Modern endpoint security tools still incorporate reliable signature detection technology but now supplement it with newer techniques, including behavioral analysis, sandboxing, predictive analytics and threat intelligence. While different vendors

Source: [1]AT&T, "2019 Endpoint Security Survey Report," 2019

adopt different tactics for combating modern endpoint threats, the common theme is that they all deploy a multipronged defensive strategy to increase the likelihood of rapid detection, blocking and eradication of attacks.

Threat hunting plays a crucial role in enterprise security strategies. This approach, built on the presumption of compromise, seeks to identify existing and future intrusions into an organization's networks and systems. Threat hunters analyze the approaches attackers have historically used and complement this knowledge with current threat intelligence to better understand adversary tactics and identify the use of those tactics within their environments. During their initial efforts, threat hunting programs generally uncover one or more existing compromises on a network that went undetected with traditional security controls. Attackers who are able to persist in this manner increase their dwell time, the amount of time after a compromise that they are able to retain access to the organization's systems.



The percentage of organizations that experienced an endpoint attack in 2019 that compromised data or infrastructure assets[2]

Reducing the Time to Detect an Attack

Many organizations are choosing to deploy managed threat hunting services that operate 24/7, seeking to immediately identify anomalous network behavior and spot compromises before they can cause significant damage. Cybersecurity leaders are accepting the fact that their systems will eventually be the victim of an attack and are seeking to reduce the dwell time of attackers from weeks or days down to hours or minutes. Time is of the essence during a security incident, and the faster a cybersecurity team can react and remediate a problem, the better an organization can protect the valuable data on its network.

Another common feature of next-generation endpoint protection solutions is their incorporation of endpoint detection and response (EDR) technology. This technology moves beyond simple detection of a security compromise and manages an active response that contains the damage, isolates affected systems and recovers normal operations as quickly as possible. EDR approaches minimize requirements for human interaction, facilitating a rapid and effective response. EDR tools also provide root cause analysis of threats and incidents, allowing organizations not only to recover from a security incident but also to learn from the experience and improve their security controls. Although EDR tools are highly effective, they do require the supervision of highly skilled security professionals. For this reason, many organizations opt for managed EDR services that include professional monitoring and analysis.

The COVID-19 pandemic has rapidly changed the ways many organizations think about work styles in general, and computing in particular. Before the pandemic, organizations were already shifting toward telecommuting models that allowed many employees to work from remote locations and at unusual hours. The pandemic accelerated this change, pushing organizations toward greater adoption of telework-friendly cloud applications and forcing cybersecurity teams to rapidly adapt their controls to protect confidentiality, integrity and availability in this shifting environment. For example, email is still a primary attack vector for many adversaries. Shifting to a remote work model means that endpoints now may often fall outside of the protection afforded by network-based controls. In this new world, the combination of cloud-based solutions and next-generation endpoint protection provides robust control, wherever the end user is located.

Developing a Threat Hunting Program

In a cybersecurity landscape dominated by advanced persistent threats, organizations are shifting philosophies: Instead of seeking to achieve the impractical goal of protecting themselves against all possible attacks, they now presume that compromises might occur. Threat hunting takes this presumption seriously and analyzes an organization's operating environment to search for signs of a compromise, under the assumption that one has already taken place. This approach seeks to identify successful incursions, eradicate them and strengthen controls to prevent similar attacks.

Next-generation endpoint platforms include sophisticated threat hunting capabilities, but it's also important to understand that threat hunting is about more than just endpoints. Threat hunting is an inherently human activity, similar to penetration testing, that requires the creative insight of skilled cybersecurity professionals. Working with the data provided by next-generation endpoint protection solutions and other cybersecurity tools, these analysts adopt the attacker mindset, seeking out the digital breadcrumbs left behind after an attack. Organizations wanting to develop threat hunting programs should include their most skilled analysts in the effort and provide them with the time, tools and data that they need to perform this important work.

The Elements of Effective Endpoint Protection

Effective endpoint protection solutions take a defense-in-depth approach to securing systems. Rather than relying on a single security technology, they leverage multiple, overlapping controls that provide a layered defense against sophisticated adversaries. Security professionals may think of this approach by using the analogy of the layered defenses built around medieval castles. Long-range archers were the first line of defense for these castles, attempting to disable adversaries before they approached the building. As enemies drew closer, they encountered catapults, spears, a moat and boiling oil. If one defense didn't stop them, chances are that another would. Next-generation endpoint protection technologies layer defenses in a

Source: [2]Ponemon Institute, "The Third Annual Study on the State of Endpoint Security Risk," January 2020

similar manner. If basic signature detection doesn't stop a threat, behavioral analysis, application control or EDR might do the trick.

Let's take a look at two categories of next-generation endpoint protection technology: the core features that should exist in any NGEP platform and the advanced capabilities that might serve as differentiators.

Core Features of Next-Generation Endpoint Protection Platforms

Signature detection technology remains the staple of endpoint protection. Although it is not capable of identifying advanced, novel threats, signature detection is a proven technique for identifying and blocking known threats. Every NGEP platform should include this core capability, and administrators should ensure that the platform receives daily signature updates from the vendor to protect systems against newly identified threats.

Behavioral monitoring approaches move beyond signature detection to analyze system behavior. If users start taking unusual actions, or if software behaves in an unexpected way, this may indicate a threat that managed to evade signature detection capabilities and gain a foothold in a system. Behavioral monitoring may detect these advanced threats and automatically quarantine them or flag them for further investigation.

Machine learning technology allows endpoint protection platforms to learn from past activity, creating new cybersecurity knowledge that can feed behavioral monitoring approaches. NGEP platforms that incorporate machine learning and artificial intelligence develop models of both user and system behavior over time and refine those models as behavior evolves. This active learning approach improves the accuracy of behavioral monitoring and accommodates natural changes that occur within an organization.

Centralized management is an important core component of NGEP platforms. Endpoint protection provides security at the endpoints distributed throughout an organization, but these distributed endpoints must be centrally managed. Centralized management lets administrators control the configuration of NGEP deployments, push security policies to endpoints and receive alerts generated from agents that reside on endpoints around the world. Centralized management facilitates reporting that can quickly spot trends and help administrators adapt and refine security controls.

Device control capabilities allow administrators to move beyond configuring the NGEP platform itself and use the platform to modify the security configuration of endpoint operating systems and hardware. For example, many threats enter an organization through malware that resides on USB sticks and other removable media. Device control technology can disable USB ports on endpoints, prohibiting users from accessing removable media without first seeking administrator intervention.

Application control technology brings administrative control to the software running on endpoints. This may be through a simple blacklisting approach that uses signatures of known malicious (or unwanted) software and prevents users from launching blacklisted applications. Whitelisting, in which users are prevented from launching any software that does not appear on a list of approved applications, is a more effective approach, but it places an extra burden on administrators and may impose unacceptable constraints on user behavior.

Vulnerability protection seeks to supplement enterprise vulnerability management programs by proactively identifying missing patches, misconfigurations and other issues on Windows, Mac and Linux endpoints that attackers might exploit. In many cases, NGEP platforms may also trigger automated remediation of detected vulnerabilities, quickly correcting a problem before it leads to a security incident.

Threat intelligence provides NGEP platforms with access to real-time threat information. NGEP vendors are uniquely positioned to receive reports of malicious activity from thousands of clients across industries and around the world. Threat intelligence capabilities automatically analyze this information and deploy immediate updates to a vendor's client base, allowing organizations to block IP addresses, update malware signatures and identify new adversary tactics quickly, providing rapid detection of evolving threats.

Advanced Capabilities of Next-Generation Endpoint Protection Platforms

Endpoint detection and response capabilities allow organizations to automate significant portions of their incident response efforts, automatically redeploying defenses to protect systems and providing enhanced threat information to security professionals responding to an incident. EDR capabilities often

Machine Learning: Beyond the Hype

Machine learning is among the hottest buzzwords in cybersecurity, with virtually every security tool on the market hyping new artificial intelligence capabilities. Technologists should take the time to understand what these features really do and determine whether they represent true machine learning capabilities or are simply dressing up old technology in new language.

The core feature of true machine learning technology is the ability of the system to absorb new information and learn from it. For example, a behavioral analysis system might monitor user behavior on a network and then use that information to develop a model of each system's normal activity. Once that model is in place, the platform uses it to detect deviations from that normal behavior and flag them for further investigation. That's a great example of machine learning approaches applied to cybersecurity.

Pattern recognition, on the other hand, is not machine learning. Systems deploying signature detection for malware detection, threat hunting and similar tasks are not actually developing new knowledge themselves. They're simply accepting instructions from the vendor and monitoring the local environment for activity matching those signatures. Machine learning approaches differ in that they can customize the performance of the system based on locally observed activity.

integrate with security orchestration, automation and response platforms as a component of a well-rounded automatic response strategy.

Root cause analysis and reporting features allow analysts to go beyond a basic response and drill down into the root causes of an incident. This capability is particularly important during the remediation and lessons-learned phases of an incident. After the immediate damage is contained, responders can perform a deep dive into the conditions that allowed an incident to occur and use this information in two ways. First, they can remediate the direct issues that contributed to the incident, preventing another attacker from following the same path to compromise. Second, they can extract generalized lessons from that experience, search for related pathways that an attacker might exploit in the future and remediate those proactively, blocking compromise attempts before they take place.

Threat hunting plays a crucial role in the toolkit of forward-thinking organizations that wish to ferret out the presence of sophisticated attackers on their networks. Some NGEP platforms offer advanced threat hunting capabilities, giving cybersecurity teams real-time access to endpoint information that provides vital clues during threat hunting exercises. Automation capabilities also allow the rapid notification of threat hunting teams when suspicious activity occurs on any endpoint in the organization, reducing the dwell time of attackers on compromised systems.

Endpoint Protection in the New Normal

Traditional endpoint protection technology served organizations well for many years, but the time has come to replace it with more effective tools. The key challenges to using existing technology include:

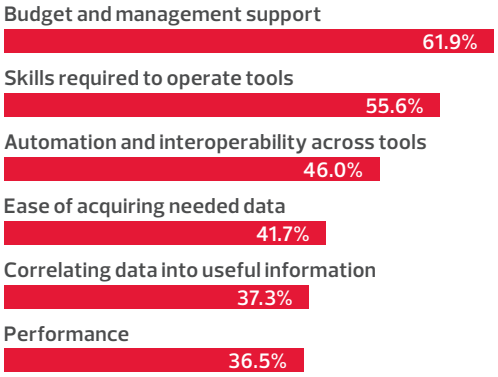
- The inability of existing technology to correlate security data into useful information
- The lack of skilled staff who can operate diverse tools
- The lack of support for automation and integration with other security tools
- The inability of existing tools to tie users to compromised assets

The bottom line is that the previous standard — straightforward analysis techniques applied to traditional data sources — is no longer enough. Organizations must apply new methodologies to collect and enrich tactical data sources for better decision-making. Effective endpoint security strategies should focus on these newer approaches to enable maximum visibility for detection and prevention while accepting the fact that inspecting every tidbit of security data is impractical. They must either enable remote data collection or facilitate the central analysis of decentralized information while offering tuning capabilities that filter out the signal from the noise before presenting results to analysts.

This enhanced visibility not only informs security decision-making but also helps analysts quickly pinpoint and isolate compromised assets. Organizations may choose different approaches to this automation, ranging from centralized security information and event management solutions to EDR technology or even automated scripts that are triggered in response to security events. Whatever approach an organization chooses, the essential task is combining automation and continuous improvement to drive security programs to the next level.

Although tools play an important role, these enhancement efforts also require the skillful involvement of IT and security professionals. Expert users can take advantage of these tools to implement sophisticated prevention and analytic techniques, but it's equally important that they leverage them to automate the mundane tasks of cybersecurity. This, in turn, frees staff from duties that are important but also time-consuming and

Key Barriers to Effective Endpoint Security[3]



Developing Endpoint Protection Talent

The effective management of an endpoint protection program requires a talented team of cybersecurity professionals who are attuned to changes in the threat environment and can rapidly adapt controls to meet evolving threats. The automation capabilities of next-generation endpoint protection solutions alleviate the need for hiring large teams of analysts to pore over raw data in search of anomalies. Modern tools offer rapid and automated detection of these anomalies. They require smaller teams of analysts, but those professionals need more advanced knowledge to get to the root cause of a possible security incident.

Organizations seeking to modernize their endpoint protection programs should begin with investments in their teams. Leadership teams should seek out curious people who want to learn more and provide them with the time and resources necessary to develop that knowledge. In addition to traditional training and certification programs, organizations may invest in threat intelligence subscriptions that provide team members with access to the latest threat analysis and research, allowing the team to protect against new threats proactively rather than waiting until disaster strikes.

Source: [3]SANS Institute, "2019 SANS Survey on Next-Generation Endpoint Risks and Protections," December 2019

undesirable, so they can focus on work that delivers more value to the organization.

Coordinated Security via the Cloud

As organizations evolve their security strategies, they should do so in close synchronization with their cloud strategies. Cloud delivery is an important emerging capability of effective NGEP solutions, and most customers now demand cloud-based platforms to leverage the cloud's cost efficiencies, flexibility, scalability, manageability and configurability.

Products deployed and managed in the cloud provide valuable automation capabilities, including automated patching of endpoints, but in cases where this automation isn't sufficient to reduce the demands on staff, organizations may turn to managed security services to gain expert assistance in the design, deployment and monitoring of their NGEP platforms.

The future of endpoint security is here. With modern NGEP solutions, we can move beyond the reactive detection of the past and use proactive tools to rapidly detect and respond to security incidents. With a strong NGEP strategy in place, organizations can quickly detect threatening activity, evaluate it against the most recent threat intelligence, quarantine affected systems and automatically remediate vulnerabilities to prevent recurrences of that threat.

The beauty of NGEP solutions is that all of this activity can occur without the intervention of cybersecurity teams. Instead, they can review reports that automatically land in their inboxes and discover that their automated systems were actively engaged in protecting enterprise data and resources. The endpoint incident response strategies that they developed were executed automatically to protect the organization from a sophisticated threat.

The type of response that might have consumed several analysts' time over the course of a week now takes place without anyone lifting a finger. That's the next generation of endpoint security.

CDW: We Get Endpoint Security

CDW's team of account executives and solution architects can assist any organization with its endpoint security needs. Our team routinely works with organizations of all sizes and across industries to design, implement and modernize their endpoint protection strategies.

Our extensive and experienced staff of security and industry experts can help you find the right solutions and services to build a robust and secure endpoint computing environment and manage that environment more effectively. CDW's subject matter experts assist organizations with a variety of endpoint security efforts that meet their security requirements, accommodate their business needs and fit within the constraints of their budgets and teams.

CDW's comprehensive set of security services includes:

- Penetration testing
- Compliance assessment
- Framework assessment
- Professional services
- Consultation services

CDW AMPLIFIED™ Services

CDW Amplified™ Security services are composed of both information security and network security practices, offer an objective look at your current security posture and provide continuous defense against, detection of and response to growing threats.

DESIGN for the Future

All CDW Amplified Security services provide a comprehensive approach to prevent data breaches and proactively respond to cyberattacks.

ORCHESTRATE Progress

CDW Amplified Security engineers can assist with installation and deployment of advanced security techniques and ensure technologies are optimized for your needs.

MANAGE Operations

We can manage security solutions for you, helping you stay vigilant and maintain compliance while easing the burden on your IT staff.

Sponsors

TREND MICRO™ paloalto® NETWORKS McAfee™ Together is power. Malwarebytes

Learn more about how CDW can help you secure your endpoints.

CDW PEOPLE WHO GET IT®