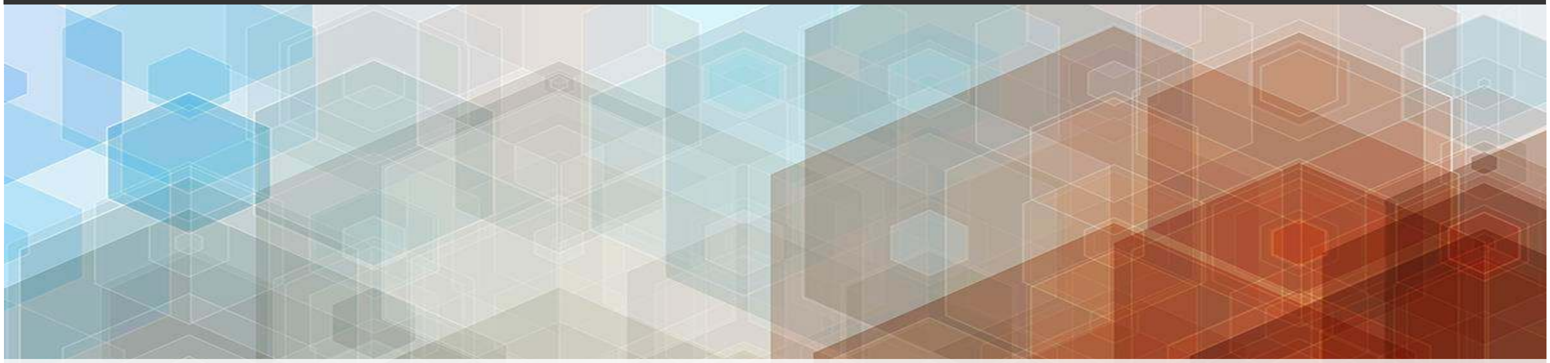
Enterprise Strategy Group | Getting to the bigger truth.™



Market Landscape Report

Enterprise Adoption of Next-generation Endpoint Security

How Enterprises Are Evaluating, Testing, and Deploying Next-generation Endpoint Security Products

By Jon Oltsik, Senior Principal Analyst; Doug Cahill, Senior Analyst; and Kyle Prigmore, Research Analyst

May 2016

Contents

Overview

In early 2016, ESG interviewed dozens of cybersecurity professionals about their organization's endpoint security challenges, requirements, and strategies. Most of these cybersecurity professionals worked at enterprise organizations (i.e., more than 1,000 employees) though a few worked for slightly smaller firms. Interviewees worked at North American organizations across a variety of industries.

For the purposes of this market landscape report (MLR), ESG defines endpoint security as follows:

"The policies, processes, and technology controls used to protect the confidentiality, integrity, and availability of an endpoint system."

While the term "endpoint security" is often equated with antivirus software, true endpoint security extends well beyond AV alone (see Table 1). In an enterprise organization, endpoint security is actually a lifecycle discipline that includes things like:

- **Configuration management.** Endpoints are often deployed in "hardened" configurations, according to guidelines from organizations such as Microsoft, NSA, or NIST. For example, endpoints can be configured so that users are limited to "user" rather than "administrator" privileges, limiting the types of configuration changes users are permitted to make. Some organizations modify these guidelines to create customized endpoint security configurations that meet their compliance and governance requirements. Once endpoints are deployed, operating system configurations are monitored and adjusted accordingly for risk mitigation.

- **Data security.** To protect sensitive data, many regulated organizations outfit PC endpoints with hardware or software used for full-disk encryption. Some firms supplement full-disk encryption with additional software for file-level encryption to protect the confidentiality and integrity of file system elements like directories, folders, and documents. Endpoint data security controls can include specialized software such as data loss prevention (DLP) or enterprise rights management. This type of software can enforce security policies guiding the data users can access and what they are allowed to do with this data.

- **Host-based firewalls and IDS/IPS.** Many endpoint security software suites include host-based firewalls for filtering or blocking specific network traffic. Host-based IDS/IPS (HIDS/HIPS) software is also utilized to detect and block suspicious/malicious system-level activities based upon signatures of known attack patterns or behavior-based heuristics. In general terms, HIDS/HIPS systems are designed to safeguard the integrity of individual systems by examining any programs or services that seek to change a system's configuration.

- **Integrity monitoring.** Deviations and unauthorized change can sometimes be indicative of a compromise. File integrity monitoring (FIM), along with the monitoring of changes to the Microsoft Windows registry, are functional capabilities which look for changes on specific areas of the file system and in the registry which should either not be changed or should only be altered by specified trusted entities whether they are users or application processes. FIM is also a requirement for certain industry regulations, including PCI DSS.

- **Add-on controls.** Endpoint systems can also be instrumented with additional controls to limit what users can and cannot do. Port and device controls can be used to limit what types of peripheral devices are allowed to connect to systems, or what these peripheral devices can do once connected. Application controls (i.e., white listing/black listing) can regulate which applications can run (white list) and which are prohibited from doing so (black list). Add-on controls are used for regulatory compliance, corporate governance, or as a security best practice to decrease the "attack surface" of endpoint systems. For certain types of fixed-function endpoints, such as point-of-sales systems, some organizations employ a lockdown approach with a combination of device and application controls in lieu of the aforementioned controls.

Table 1. Components of Endpoint Security

Category	Examples	Purpose
Endpoint provisioning	"Hardened configurations" (i.e., following secure deployment guidelines, removing all unnecessary services, etc.)	Establish a security baseline, decrease the attack surface, reduce risk.
System controls	Port controls, application controls, HIDS/HIPS, FIM, etc.	Policy enforcement, decrease attack surface, regulatory compliance, etc.
Network controls	Device firewalls, network access controls, network segmentation, etc.	Policy enforcement, decrease attack surface by limiting network activity, regulatory compliance, etc.
System authentication	802.1X supplicant, X.509 certificates, etc.	Provide strong credentials for device authentication.
Data security controls	Full-disk encryption, file-level encryption, DLP, ERM, file integrity monitoring, etc.	Policy enforcement around file access and entitlements. Decrease attack surface by preventing the leakage of sensitive endpoint data.
Vulnerability management	Vulnerability scanners and patch management.	Discover and fix system and application vulnerabilities in a timely manner to protect systems for exploitation.
Anti-malware	Antivirus software, advanced prevention software.	Detect and block malware and exploits.
System monitoring	Endpoint forensic software, Windows logging, FIM, advanced detection and response tools.	Monitor system behavior and changes in order to detect and remediate suspicious/malicious activities.

Source: Enterprise Strategy Group, 2016

Endpoint security should include all-encompassing policies, processes, and technologies used to protect endpoint devices. Given this, what is "next-generation endpoint security?" This seemingly simple question isn't easy to answer. "Next-generation endpoint security" has become an industry marketing term, usually highlighted with ample hyperbole. Cybersecurity professionals are often confused by this type of marketing rhetoric.

For the purposes of this MLR, the term "next-generation endpoint security" is defined as:

Endpoint security software controls designed to prevent, detect, and respond to previously unseen exploits and malware.

With this definition established, this report focuses on next-generation endpoint security products in two specific areas:

- **Advanced prevention technologies**. This type of software could actually be characterized as "next-generation antivirus software," as it is designed to block exploits and malware while delivering a higher and more accurate detection rate than traditional AV products. Stated another way, AV is designed to block known malware variants and families while advanced prevention technologies are designed to block unknown malware and 0-day exploits. Next-generation advanced prevention tools leverage a multitude of technology underpinnings (see Table 2).

- **Advanced detection and response technologies.** Sometimes referred to as endpoint forensics or endpoint detection and response (EDR) tools, advanced detection and response technologies are designed to monitor and report on system-level endpoint activities (i.e., in-memory activities, registry setting activities, file system activities, processes running, NetFlow, etc.). Typically, these tools also offer components like central reporting, endpoint analytics, and threat intelligence integration to help security analysts detect anomalous endpoint behavior, provide visibility to detailed system-level data elements, and give security operations staff a way to remediate problems without reimaging systems.

Table 2. Examples of Next-generation Endpoint Security Technologies Used for Advanced Prevention

Technology Category	Description	Use Case
Executable inspection and analysis	Deep analysis of hundreds of executable properties before permitting system access. Note that this technique does not actually execute the code itself.	Look at multiple properties of malware to calculate a risk score. Block executable if risk score exceeds a certain threshold.
Machine learning	Create a statistical model to predict normal system behavior.	Systems can be configured to block or alert on anomalous activities that deviate from normal behavior.
Containerization	Sandboxed environment for code execution.	Adds an extraction layer that prevents exploits and malware from direct access to system resources.
Static/dynamic malware analysis	Deep file analysis, can be done on the system itself or integrated with network- or cloud-based analysis capabilities. Code is executed to monitor post-execution behavior.	Code inspection and execution in a contained environment for malware detection/prevention.
Threat intelligence integration	Proactive and continuous updates based upon indicators of compromise (IoCs) and the tactics, techniques, and procedures (TTPs) used by cyber-adversaries.	Block exploits and malware based upon real-time intelligence on attack sources, methodologies, or patterns associated with threat actors.

Source: Enterprise Strategy Group, 2016

What Is an Endpoint?

Just what is an "endpoint" within the context of endpoint security? This definition can vary by organization. As part of this research project, ESG found that next-generation endpoint security projects:

- **Are anchored by Windows PCs.** Next-generation endpoint security tools are applied to Windows PCs in almost all cases. Occasionally an organization may have a discrete project for Mac security (i.e., Mac only), but this was usually done as a pilot project to be followed by a broader Windows deployment.

- **Include all types of PCs.** Many organizations are deploying next-generation endpoint security technologies on Macs and Windows PCs simultaneously. It is worth noting that the cybersecurity professionals interviewed for this project often commented about the growth of their Mac population and were actively applying security controls to these systems. It seems apparent that enterprise organizations now believe that risks associated with Apple Macs warrant proactive security policies and controls.

- **Extend to servers.** In a few instances, next-generation endpoint security technologies are deployed to servers as well as endpoints. Typically, these are Windows servers but some next-generation endpoint security projects also extend to Linux servers. Many organizations are also looking to apply next-generation security controls on virtual desktops, virtual servers, and cloud-based workloads, but this seems to be a strategic initiative rather than a component of near-term next-generation endpoint projects.

- **Rarely include mobile devices.** Mobile devices like smartphones and tablet computers are end-user devices and also considered alternative endpoints to PCs. Nevertheless, ESG did not speak with a single organization that included mobile devices as part of its initial next-generation endpoint security projects. Several mentioned the need to improve mobile device security, but this was viewed as a long-term strategic consideration rather than a short-term priority. It is worth noting that most next-generation endpoint security products don't offer support for mobile devices today. This lack of availability likely impacts a scope of next-generation endpoint security projects today.

While different organizations were engaged in different projects, ESG learned that next-generation endpoint security projects tend to start with a finite population of Windows PCs and sometimes Macs during the initial pilot phase. These projects tended to be extended over long periods of time as organizations took ample time—typically a year—to test, scale, and gain experience with products.

Antivirus Software and Next-generation Endpoint Security

According to a 2014 ESG research survey of enterprise IT and security professionals, 89% of organizations report that they always install AV software on Windows-based desktops and laptops.[1] Most of the organizations participating in this project purchase thousands of antivirus software licenses from a single vendor, renew their subscription on an annual basis, and have generally stuck with the same AV vendors for several years.

Given this ubiquity, enterprise organizations have lots of experience and opinions about antivirus software. ESG learned that:

- AV is viewed as a commodity technology, not a commodity product. Many security professionals are familiar with multiple AV product suites and tend to choose those that provide the best combination of product features, performance, and manageability for their organizations. Alternatively, signature-based AV for threat prevention and detection is generally viewed as commodity functionality with little difference in efficacy among products.

- Day-to-day administration of traditional AV software is often delegated to IT operations groups. While CISOs may drive endpoint security policy, policy enforcement, and product decisions, IT operations teams are most often tasked with maintaining and operating all aspects of endpoint management including AV. The security professionals interviewed for this project admit that delegating AV management can lead to issues in areas such as configuration management, timely updates of AV signatures, and upgrading to current software revisions, but these have traditionally been considered acceptable risks.

> "You'd think we would have used, or at least tested, advanced AV features before deciding to go in a completely different direction with next-generation endpoint security but we didn't. It was kind of an 'out with the old, in with the new' decision, I guess."
>
> --Cybersecurity professional, financial services company

- AV advanced features are often ignored. Antivirus software has evolved over the years to include a number of advanced features like reputation lists, threat intelligence integration, and system-level heuristics for exploit and malware prevention/detection beyond signatures alone. These features aren't usually turned on in default configurations; rather users (or administrators) must manually configure AV to enable advanced settings. About half of the organizations participating in this research

[1] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.

project said that they regularly use AV advanced settings. Of this group, about 50% claim that while AV advanced settings may improve prevention and detection efficacy, they tend to consume extensive system resources and thus impose an unacceptable performance penalty that may disrupt user productivity. Some participants also noted an unacceptable rate of false positives and an associated cost to triage erroneous alerts. Business managers often step in and ask IT personnel to disable advanced AV features when this happens. As for the rest of the organizations, they admit that they continue to rely on basic protection settings in AV software and haven't tested or used any of the advanced settings. Many confessed that there was no good reason why they weren't using or hadn't tested AV advanced protection features, they simply hadn't gotten around to it.

From a market perspective, all leading AV vendors are adding next-generation endpoint security capabilities into their existing products as quickly as they can. Given this trend, ESG asked each cybersecurity professional interviewed for this project whether they considered evaluating their current AV vendor's next-generation endpoint security offering. The majority hadn't done so. Why? Most were inclined to seek out innovative new products designed as countermeasures for sophisticated threats rather than what they perceived as incremental product updates in AV.

Some enterprise organizations did open the next-generation endpoint security door to incumbent AV vendors and readily admitted that they were greatly disappointed by their responses. Cybersecurity professionals complained that their incumbent AV vendors couldn't articulate a cogent next-generation endpoint security strategy or had trouble getting participation from the right technical resources. One infosec professional mentioned that a frustrated account manager working for his AV vendor told him that his company hadn't "gotten its act together yet" with next-generation endpoint security and advised him to look elsewhere.

While ESG's interviews represent a small sample size, they hint at a threatening trend in the lucrative AV market. Many large organizations are investing in next-generation endpoint security strategies without stopping to consider whether existing AV products can address new requirements. When AV vendors are considered, they often seem exceedingly unprepared, lacking the right resources or strategies. Antivirus vendors must address the reality of a next-generation endpoint security market transition quickly or they could lose significant business in the enterprise market over the next few years.

The Transition from AV Product Suites to Next-generation Endpoint Security

Does the transition to next-generation endpoint security sound a death knell for AV software? No. It is worth noting that while all of the organizations participating in this research project were moving forward with a next-generation endpoint security project, these firms are really on the leading edge of an overall endpoint security transition. In fact, the majority of midmarket and enterprise firms continue to rely on antivirus software exclusively for exploit and malware prevention and detection. According to a 2014 ESG research survey of IT and cybersecurity professionals, 49% said that the AV product(s) used at their organization were very effective at preventing/detecting security events (i.e., exploits, malware attacks, anomalous/suspicious behavior, etc.) while another 39% claimed that AV was somewhat effective with prevention and detection.[2]

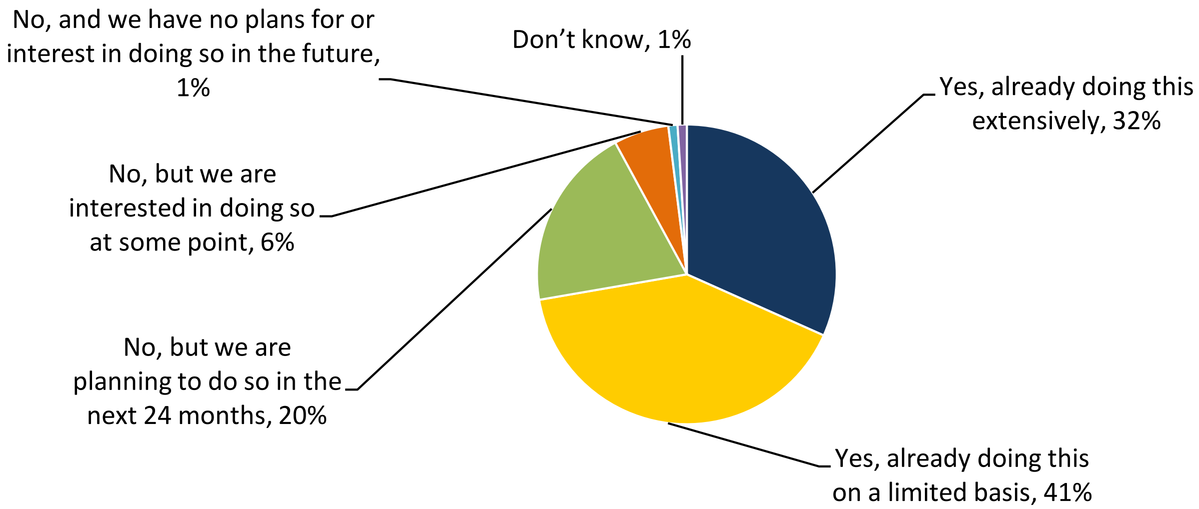
While many organizations continue to anchor their endpoint security strategies in AV, ESG believes that these interviews reveal a harbinger of things to come. This thesis is also supported by ESG's 2014 research. At that time, nearly one-third (32%) of organizations were already deploying advanced malware prevention/detection (in addition to traditional AV) extensively, while another 41% were deploying advanced malware prevention/detection (in addition to traditional AV) on a limited basis (see Figure 1).[3]

[2] Source: ibid.
[3] Source: ibid.

Many organizations tend to be risk-averse in nature as they continue to rely on AV and monitor next-generation endpoint security product and vendor maturity. Nevertheless, even these conservative organizations will likely adopt next-generation endpoint security capabilities over the next few years. Some will wait for their AV vendors to add these capabilities while others will actively seek out next-generation endpoint security on their own as the market develops. ESG believes that by 2019, the majority of midmarket and enterprise organizations will adopt next-generation endpoint security capabilities in one form or another.

Figure 1. Trend Toward Next-generation Endpoint Security

Has your organization deployed or is it considering deploying this type of advanced malware detection/prevention software (in addition to traditional AV)? (Percent of respondents, N=329)



Source: Enterprise Strategy Group, 2016

On to Next-generation Endpoint Security

As previously mentioned, all of the enterprise organizations interviewed for this project are actively deploying next-generation endpoint security tools. What’s behind this decision? The cybersecurity professionals ESG spoke with cited several common reasons:

- **Their organization (or industry) experienced a devastating security breach.** Several firms suffered a security breach where cyber-adversaries had circumvented traditional security controls (i.e., firewalls, IDS/IPS, AV software, SIEM, etc.), and compromised endpoint systems. These breaches clearly exposed weaknesses associated with existing endpoint security strategies, leading organizations to explore other options. In a few cases, next-generation security initiatives were driven

> “Everything changed after the Anthem breach. Business and IT executives wanted to know if the organization was vulnerable to a similar type of attack. Our endpoint security project became a high priority at that point.”
>
> --Cybersecurity professional, health care organization

indirectly by a highly visible security breach within an organization's industry. This was especially true with regards to the health care industry reacting to data breaches at Anthem, CareFirst (BlueCross BlueShield), and Premera (BlueCross BlueShield).

- **Other security analytics tools pointed to endpoint threats and vulnerabilities.** Several of the organizations interviewed claim that the next-generation endpoint security project derived from earlier deployments of anti-malware sandboxing appliances on their networks. Cybersecurity professionals commented that once these tools were implemented, they detected lots of malicious traffic (i.e., botnet traffic, command-and-control traffic, network scanning, etc.) emanating from endpoint systems. Armed with this new information, many security professionals had factual evidence that their current AV did not offer adequate protection, prompting them to adopt additional layers of endpoint security defense.

> "Once we started seeing malicious traffic on the network, we realized that AV can't keep up with APTs."
>
> --Cybersecurity professional, business services organization

- **They were overwhelmed by a constant cycle of system reimaging.** A number of cybersecurity professionals told ESG that they were seeking next-generation endpoint security tools to help them alleviate the time and effort associated with reimaging PCs every week. One organization estimated that it spent ten hours or more reimaging systems on a weekly basis. These organizations seek out endpoint security tools that can decrease the number of system compromises, thus reducing their system reimaging burden. Many also want advanced incident detection and response capabilities that provide detailed reporting on all system changes and automated features for rolling back system configurations to a known good state, obviating the need for manual reimaging.

- **Improving endpoint security was a part of a more comprehensive strategy.** Several security professionals mentioned that improving endpoint security was one of several pressing security initiatives in process. It is worth noting that this flurry of activity often coincided with the hiring of a new CISO or other senior cybersecurity manager or the creation of new cybersecurity teams tasked with an overall objective for upgrading security protection across the organization. Enhancing endpoint security was often grouped with other projects such as automating incident response tasks, tightening network access controls, adding new security analytics tools, or strengthening security controls and auditing for privileged accounts. These organizations consider next-generation endpoint security as a contributing component of a bigger cybersecurity strategy.

Of all of these factors, ESG found that security breaches tended to motivate organizations into immediate actions. In other words, enterprises with no plans for next-generation endpoint security were quick to fund new initiatives, dedicate project teams, and prioritize endpoint security plans once a serious security breach was uncovered (note: This was also true of health care organizations in response to the data breaches at organizations like Anthem). Many reported that once business executives understood the gravity of particular security incidents, they demanded immediate action and became actively involved in project oversight.

Alternatively, ESG believes that firms that did not experience a security breach viewed endpoint security improvements as part of an overall enterprise security transition. Since sophisticated cyber-adversaries could easily circumvent traditional security tools (i.e., firewalls, IDS/IPS, web threat gateways, AV software/gateways, etc.), these organizations were intent on building new defenses across the network. Next-generation endpoint security was viewed as an essential component of this strategy.

Once organizations decide to pursue some type of next-generation endpoint security project, cybersecurity teams assume responsibility for defining requirements, researching options, and developing a project plan. What about IT operations teams with responsibilities for day-to-day AV software management and oversight? This group is often asked to provide input in the requirements definition phase of the project, and is certainly involved in next-generation endpoint security pilots and enterprise deployments in areas such as software agent installation, configuration, and administration. Nevertheless, next-generation endpoint security projects tend to be high-priority, high-visibility efforts where cybersecurity teams are considered project "owners," responsible for project management and accountable for meeting goals and objectives. All others assume supporting roles.

> "At my previous job, I was responsible for security architecture, and I had a dedicated team evaluating products to the magnitude of $100 million year over year focusing on 50 engineers evaluating products. So, you can just see the scale of what we were doing."
>
> --Cybersecurity professional, health care industry

The Endpoint Security Continuum

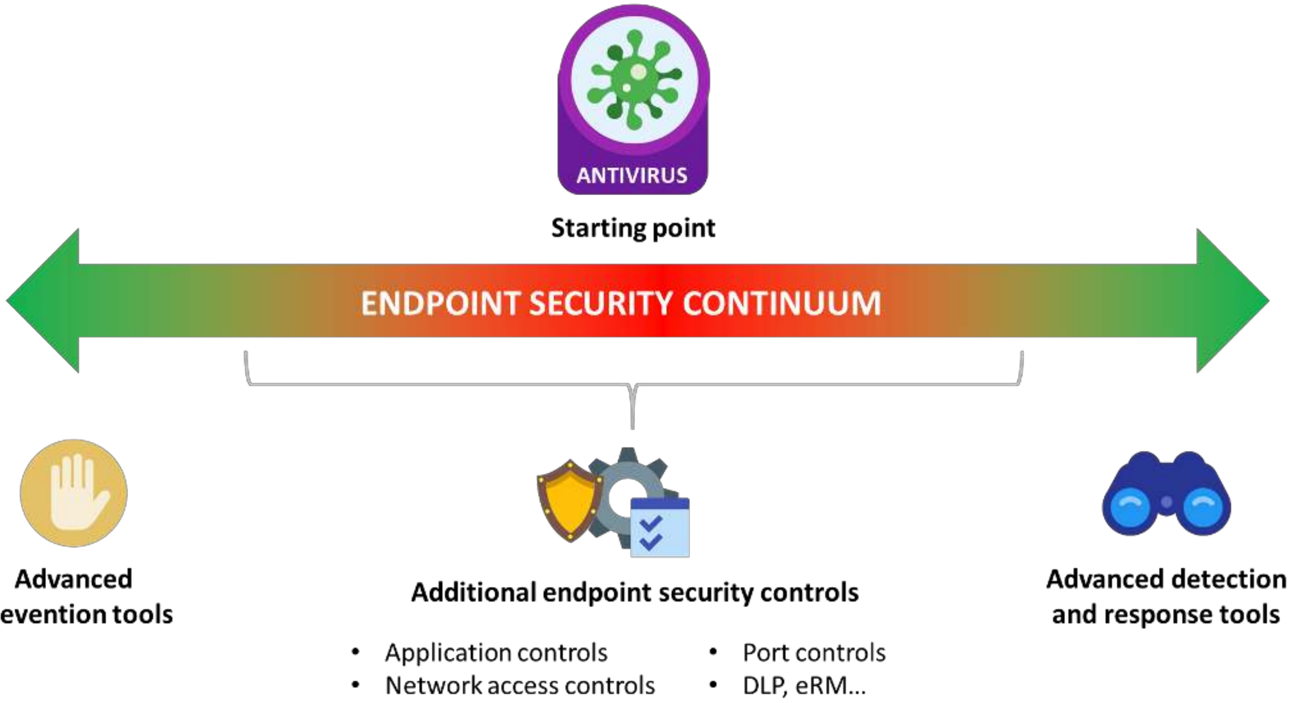
As previously mentioned, next-generation endpoint security products tend to fall into one of two categories:

1. Advanced prevention technologies designed to block exploits and malware with much greater accuracy than traditional AV products. The real objective here is blocking sophisticated cyber-adversaries and targeted attacks using previously unknown malware and/or 0-day exploits.

2. Advanced detection and response technologies designed to monitor and report on all endpoint system activities while using a variety of technologies (i.e., algorithms, static/dynamic analysis, threat intelligence correlation, etc.) to detect anomalous/suspicious behavior (Note: Tools in this category are sometimes referred to as endpoint detection and response solutions, or ETDR). These tools also tend to provide various methods for incident response and system remediation (i.e., terminating a network connection, halting a process, wiping a file, etc.).

In spite of this dichotomy, ESG believes that next-generation endpoint security should really include both sets of capabilities across an overall endpoint security continuum (see Figure 2). At one end, advanced prevention technologies should offer superior efficacy for malware and exploit prevention when compared to traditional AV products. In this way, next-generation endpoint security can block all but the most sophisticated cyber-attacks, greatly reducing the amount of malicious traffic on the network and system reimaging burden placed on IT operations. At the same time, however, CISOs must assume that sophisticated cyber-criminals and nation-states will discover and exploit advanced prevention technology vulnerabilities over time so they will also need the right tools for efficient detection and remediation of malicious endpoint activities.

Figure 2. The Endpoint Security Continuum


ANTIVIRUS
Starting point
ENDPOINT SECURITY CONTINUUM
Advanced prevention tools
Additional endpoint security controls
Application controls
Network access controls
Port controls
DLP, eRM…
Advanced detection and response tools

Source: Enterprise Strategy Group, 2016

As part of the continuum, next-generation endpoint security is also supported with additional types of security controls—some basic and some advanced (see Table 3). These controls are intended to decrease the endpoint and network attack surface, making network penetration and system compromises more difficult for cyber-adversaries.

An example of a "basic" security control might be removing system administrator privileges for the majority of employees. While this has long been considered a security best practice, ESG's interviews revealed that many organizations haven't done so in the past, usually because of some historical dispute between the security team and IT operations or business managers who wanted users to have the freedom to make changes to their systems. Given the dangerous threat landscape, however, many firms are rethinking this policy and configuring endpoints with "user" privileges only. Other basic endpoint security controls could include things like enforcing port controls, creating endpoint firewall rule sets, and encrypting files and disk drives resident on endpoints.

More advanced endpoint security controls could include things like application controls (i.e., whitelisting/blacklisting applications resident on endpoints), granular network access controls (i.e., enforcing access controls for who gets access to what IT assets and under what conditions), and even micro-segmentation (i.e., setting up more granular virtual network segments by user, group, or asset types).

> "We use application controls on servers but not on endpoints yet. There's value there but we know that it won't be easy to classify applications, associate applications with roles, and build the right rules to lower risk. I'm sure we'll break some eggs in the process."
>
> --Cybersecurity professional, manufacturing organization

While decreasing the attack surface can certainly help reduce IT risk, it should be noted that endpoint security controls don't come for free. For example, cybersecurity and IT operations teams may need business buy-in before removing administrator privileges from users' systems and approval and implementation could take months before completion. Similarly, before deploying granular network access controls, cybersecurity teams need to institute access policies, determine which data sources need to be collected, processed, and acted upon for policy oversight, and create a series of enforcement rules based upon real-time data analysis. Once again, this could take months to implement.

ESG found that the large organizations interviewed were certainly moving toward additional endpoint security controls but were doing so methodically over time. CISOs understand the goals of endpoint security controls but need to balance potential benefits against things like disrupting status quo business operations and committing scarce resources. Given this tradeoff, ESG expects enterprise organizations to deploy next-generation endpoint security products in the short term while adding more granular and hardened endpoint security controls over time.

Table 3. Examples of Endpoint Security Controls Being Deployed by Enterprise Organizations

Endpoint security control	Details	Use case	Potential issues
Removing system administration privileges for end-users	Change OS configuration settings	Limit users’ ability to install software or change system configurations and prevent malicious software from using administrative privileges.	Need buy-in from business managers and IT. May disrupt some business processes.
Port and system controls	Change OS configuration settings and/or install additional software	Limit peripheral device connections to systems, limit system capabilities (ex., save to DVD)	Need buy-in from business managers and IT. May disrupt some business processes.
Application controls	Change OS configuration settings and/or install additional software	Limit the type and number of applications running on each system.	Need buy-in from business managers and IT. May disrupt some business processes. Works best with servers and fix-function PCs. Can be difficult to manage for general-purpose PCs.
Full-disk and/or file encryption	Encrypt content of individual file system entities or entire HDD	Protect the confidentiality and integrity of endpoint data, especially useful for lost/stolen devices.	Can degrade system performance. May require supporting services like key management and password reset.
Network access controls	Enforce network access policies based upon device type, user role, network location, etc.	Enforce rule of least privileges. Can adapt to real-time risk factors.	Demands coordination between business, IT, and security management. Demands real-time data analysis. Can be difficult to implement and manage.

Source: Enterprise Strategy Group, 2016

Enterprise Organizations Are Making Next-generation Endpoint Security Choices

Based upon the interviews conducted for this project, ESG sees enterprise organizations rallying around one of the two poles within the endpoint security continuum. Over the next few years, ESG believes this will play out as follows:

- About 75% to 80% of midmarket and enterprise organizations will begin their transition to next-generation endpoint security by evaluating, testing, purchasing, and deploying advanced prevention technologies.

- The remaining 20% to 25% will enter the endpoint security continuum from the opposite side as they start by evaluating, testing, purchasing, and deploying next-generation endpoint security products focused on advanced detection and response.

It's likely that both camps will progress across the entire endpoint security continuum over time. In other words, organizations that start with prevention will supplement these tools with additional security controls and advanced detection and response technologies. Likewise, firms that start with detection and response will add advanced prevention and response tools as well as incremental controls.

Next-generation Endpoint Security: Advanced Prevention

Most enterprise organizations are choosing advanced prevention tools designed to block sophisticated exploits and malware that would typically bypass traditional AV. Enterprise security professionals who prioritize advanced prevention tools do so:

- **In reaction to a security breach.** As previously mentioned, large organizations tend to find time and money for next-generation endpoint security projects soon after experiencing a damaging security breach. In these situations, business executives push the security team to address process weaknesses and mitigate risk as quickly as possible, making endpoint security a high-priority project with senior management oversight. ESG found the pressure to "do something soon" drives the cybersecurity team to look for turnkey endpoint solutions that have the potential to deliver near-term benefits without creating a lot of additional work. In theory, advanced prevention tools seem like an ideal solution, promising much higher out-of-box efficacy than traditional AV software.

- **As a single component of a bigger strategy.** CISOs often have a lot of security projects happening simultaneously so they have to pick and choose where they apply their scarce resources. This was certainly true of the organizations interviewed for this project. Security professionals claimed that while they were addressing endpoint security, they were also doing things like bolstering network security controls, consolidating security analytics tools within a security operations center (SOC), and automating their incident response (IR) processes. With all of these projects in process, CISOs chose advanced prevention tools with the hope of reducing endpoint "noise" and achieving rapid ROI benefits, while pointing security resources at other projects.

> "I was hired to improve security and so we've engaged in a number of projects since I started. Endpoint security is one of these. We had to find a way to use our resources in the right areas and this certainly influenced our endpoint security decisions."
>
> --Cybersecurity professional, transportation organization

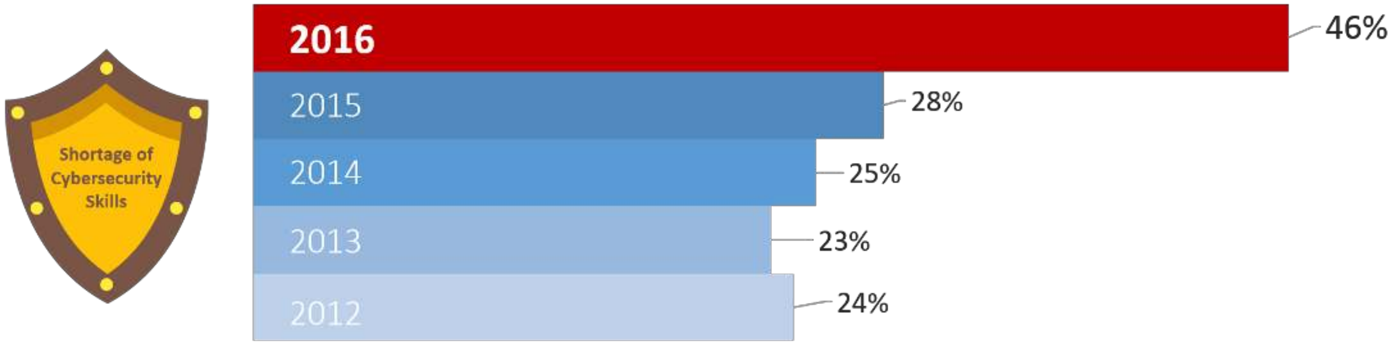
- **Because they lack the right skills or resources for advanced detection and response.** The organizations interviewed by ESG recognized the need to monitor endpoint activities to "hunt" for suspicious activities, detect malicious behavior, and respond to problems in a timely fashion. Unfortunately, many enterprises simply lack the right level of security analytics skills or staff to perform these tasks effectually, leading them to lean toward advanced prevention solutions. ESG believes this is a pragmatic decision. Monitoring endpoint behavior and correlating this with threat intelligence, network forensics, and other security data sources is hard work that demands a highly experienced team of security analysts and SOC personnel. Lacking these resources, smart CISOs realize that advanced prevention tools are the best short-term choice for next-generation endpoint security.

It is not surprising that even enterprise-class organizations find themselves lacking in security analytics skills, as this is symptomatic of a bigger problem—the global cybersecurity skills shortage. According to ESG research, 46% of organizations claim to have a problematic shortage of cybersecurity skills—the biggest skills gap of all types of IT skills. Furthermore, this gap seems to be getting worse, as the percentage of organizations with a problematic shortage of cybersecurity skills grew 18% from 2015 to 2016 (see Figure 3).[4]

With no end in sight for the cybersecurity skills shortage, most organizations will have little choice but to approach next-generation endpoint security from the advanced prevention side of the continuum. This is precisely why ESG believes that 75% to 80% of midmarket and enterprise organizations will proceed in this manner.

> "We looked at endpoint threat detection and response tools (ETDR). Oh, we understand the value they can provide but you really need a team of security analysts who know how to use them. We just don't have those skills."
>
> --Cybersecurity professional, health care organization

Figure 3. Organizations Claiming to Have a Problematic Shortage of Cybersecurity Skills



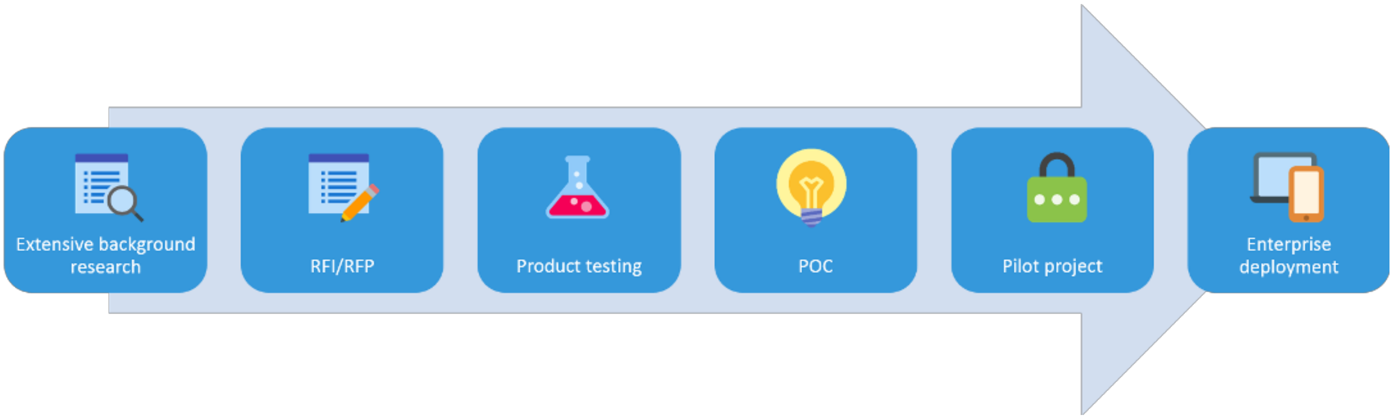
Source: Enterprise Strategy Group, 2016

Advanced Prevention Projects

Once organizations decide to pursue the endpoint security continuum from the advanced prevention side, they tend to initiate thorough projects that proceed through six phases (see Figure 4).

[4] Source: ESG Brief, *Cybersecurity Skills Shortage*, February 2016.

Figure 4. Project Phases for Evaluating, Testing, and Deploying Advanced Prevention Tools



Source: Enterprise Strategy Group, 2016

- **Extensive background research.** Cybersecurity professionals often commented about their confusion around next-generation endpoint security technologies and struggled to figure out how advanced prevention tools really differed from traditional AV software. This is certainly understandable since many next-generation endpoint security vendors make bold marketing claims or provide cryptic technical descriptions about what their products do and how they do it. To overcome this knowledge deficit, large organizations put a lot of work into the upfront background research phase of their next-generation endpoint projects. This involved several steps including:

    - Reading product reviews, analyst papers, and third-party testing reports.
    - Attending cybersecurity events and local seminars.
    - Reaching out to cybersecurity professional organizations and local networks.

  The goal was to cut through the rhetoric and delineate a list of tools that best met their technical requirements while adhering to their resource constraints. Organizations tended to spend four to six weeks on background research before moving forward.

- **RFI/RFP.** Upon completion of the background research phase, leading infosec teams codify their requirements into request-for-information (RFI) or request-for-proposal (RFP) documents and send them to vendors for responses. The number of RFI/RFP documents sent out varied widely based upon an organization's overall endpoint security knowledge and experience. Out of those organizations that employed a formal RFI/RFP process, some view it as an extension of their background research so they "cast a wide net," sending RFI/RFPs to around a dozen vendors. Others took a different approach, using RFIs/RFPs as a method to start to winnow down their lists. Efficient organizations reduced the list of potential suitors, directing RFIs/RFPs to a maximum of five vendors. The RFI/RFP phase of the project took about one month in total on average.

> "We use a methodology we call 5-3-1. We send an RFP to 5 vendors, test 3, and ultimately select one. This helps us structure the project and helps us learn a lot along the way."
>
> --Cybersecurity professional, health care organization

- **Product testing.** Organizations used a thorough RFI/RFP review process to further reduce the number of products in consideration. One cybersecurity professional described his firm's "5-3-1" process: Send an RFI/RFP document to five vendors, review RFIs/RFPs with the goal of reducing the list to three products for product testing, and then choose the one product that excels in the test phase and provides the best fit for all business, operational, and technical requirements. Based upon this project, ESG believes that the product testing phase is a critical milestone toward ultimate success. Product testing best practices include:

  - **Testing ownership and control.** While vendors were encouraged to provide help with product configurations and support, cybersecurity teams demanded ultimate control of the testing process in order to avoid testing bias.

  - **Participation by the most experienced staff.** CISOs tended to draft a testing "dream team," enlisting the help of senior penetration testers, risk and vulnerability specialists, threat analysts, and forensic investigators. In some cases, they hired third-party experts to help design strong test plans. This group was tasked with gathering an assortment of exploits and malware samples capable of bypassing traditional AV products to test the efficacy of advanced prevention solutions.

  - **Product efficacy metrics.** Product efficacy metrics were collected, tracked, and evaluated in minute detail. In some cases, vendors were presented with final test results and asked for feedback but it should be noted that this was more of a technical "request for comment" (RFC) than part of a sales process.

  - **Testing focus.** The testing phase of these projects was heavily skewed toward product efficacy—the ability to detect and block exploits and malware variants with a high degree of accuracy and low rate of false positive alerts out of the box. Product integration was also considered during the product testing phase, but other product capabilities like manageability and scalability were given cursory attention and are assessed more thoroughly during POCs.

  - **Further requirements definition.** While organizations are heads-down testing product efficacy, they also tend to invest time into project requirements definitions. This was especially true for requirements beyond security, so many firms used this phase to recruit key business and IT stakeholders into this process.

  Product testing phases lasted anywhere from one to three months depending upon test development, the number of products tested, test evaluations, and vendor follow-up discussions.

- **Proof-of-concept (POC).** For some organizations, the POC phase comes down to a single product while others will use the POC phase as a final contest between two or three tools. At this stage, all products had proven their ability to detect and block sophisticated exploits and malware in a lab setting. POCs were designed to supplement this testing in a more real-world setting. Organizations used POCs to evaluate other types of product attributes beyond detection and blocking rates. Can the product be easily installed? Does it impact system performance? How much training will security and IT operations staff need to become proficient with the product? Some organizations also used the POC phase to integrate next-generation endpoint security products with other cybersecurity systems. At this point, cybersecurity professionals were fairly familiar with remaining products, so this phase tended to take a month to six weeks.

> "We emphasized security efficacy in the product testing phase and then focused on product operations during the POC. We found some weaknesses—we'll live with them for now since our vendor promises to address them in the next rev."
>
> --Cybersecurity professional, technology products organization

- **Pilot project.** In most cases, POCs were used to select the next-generation endpoint security product that best addresses an organization's requirement. Pilot projects then act as a stepping-stone phase where organizations deployed advanced prevention tools to a subset of employee systems—typically, a few hundred at most. Product pilots were used to verify the conclusions of product testing and POCs in a true real-world setting with an emphasis on product integration, manageability, and scale. Enterprises also used product pilots to develop an integration fabric between next-generation endpoint security products and various other security systems like network anti-malware gateways, threat intelligence portals, and SIEM. Finally, CISOs used product pilots to fine-tune operational processes. Pilot project duration varied widely from a few to several months depending upon things like the size of the pilot, organizational and technical objectives, and the review cycle for pilot completion.

- **Enterprise deployment.** During this final phase, advanced prevention tools were often deployed on thousands of end-user systems. Once again, the length of this phase fluctuates. Some organizations took their time with enterprise deployment of next-generation endpoint security tools, continually evaluating their progress and next steps as they proceeded. Others simply needed ample time to deploy and configure endpoint security agents on thousands of systems or train the IT operations team on day-to-day management of advanced prevention tools. While many of the organizations interviewed for this project were proceeding with enterprise deployments of next-generation endpoint security products, it should be noted that few had actually completed this process.

Several CISOs noted that advanced prevention products and vendors are extremely immature today. As a result, organizations are asking a lot of their new vendors by:

- Demanding lots of hands-on product support.
- Regularly pushing vendors for product enhancements.
- Conducting regular meetings with the executive team of next-generation endpoint security vendors to monitor progress and evaluate product roadmaps.

Many CISOs also commented that they are using operational budgets (rather than capital budgets) to purchase next-generation endpoint security tools. This provides next-generation endpoint security as an annual subscription, giving them the opportunity to evaluate products and even opt for replacements if their advanced prevention initiatives don't progress as expected.

Advanced Prevention as an AV Replacement

As previously mentioned, advanced prevention software tools can be thought of as "next-generation AV," as these products apply modern technical designs to an old problem—detecting and blocking exploits and malware from endpoint systems. While enterprise organizations understand this function, many continue to run traditional AV in parallel with advanced prevention tools at present. It should be noted, however, that this appears to be a short-term "holding pattern" rather than a long-term strategy. The vast majority of interviewees plan on removing, or no longer paying for, AV software from systems within a 12 to 18 month timeframe, once they have had sufficient time to gain confidence in next-generation endpoint security tools and modify endpoint security processes accordingly. The annual renewal for the incumbent AV product was cited as a checkpoint at which the role of signature-based AV will be reassessed. Of those planning to maintain AV AND advanced prevention tools, many plan to replace commercial AV with some type of no-cost alternative (i.e., freeware or Microsoft AV for those organizations with a Microsoft Enterprise Client Access License [ECAL]).

> "We plan to get rid of AV but we're in no hurry to do so. We want to see how things play out over the next year or so, and when we make this move, we'll need to use the Windows firewalls and replace other types of controls from AV software. This transition will take some work."
>
> --Cybersecurity professional, higher education organization

This points to a major transition in the endpoint security market over the next few years. ESG believes that the majority of midmarket and enterprise organizations will approach the endpoint security continuum by starting with advanced prevention tools. All indications are that these organizations will then wait for their AV vendors to catch up, deploy next-generation endpoint security tools, and eliminate AV altogether, or implement next-generation endpoint security tools and then replace commercial AV with free alternatives within 24 to 36 months at most. In order to remain relevant, traditional AV vendors will need to add advanced prevention features AND convince customers that their products are just as effective as new types of "next-generation" alternatives. Given these market trends, traditional AV vendors face numerous market and technical challenges moving forward.

Next-generation Endpoint Security: Advanced Detection and Response

On the other side of the endpoint security continuum, ESG believes that between 20% and 25% of midmarket and large organizations will eschew advanced prevention technologies and focus instead on advanced detection and response. Based upon the interviews conducted by ESG, enterprises starting with advanced detection and response tend to have large cybersecurity organizations and progressive skills in areas like computer forensics, malware analysis, and penetration testing. Given the global cybersecurity skills shortage, a small percentage of organizations match this description.

As part of possessing leading cybersecurity skills, organizations choosing advanced detection and response tended to be extremely cynical about the notion of advanced prevention in general. Infosec professionals in this camp were pessimistic about product efficacy and felt that sophisticated cyber-adversaries would discover product weaknesses and easily circumvent leading advanced prevention tools over time, just as they have with AV software and various anti-malware gateways today. These organizations believe that the only true way to prevent security incidents is to invest in tools, skills, and processes for collecting, processing, and analyzing massive quantities of internal security data and external threat intelligence.

Organizations prioritizing advanced detection and response had other common characteristics, including:

> "We realize that our AV vendor won't detect or block targeted attacks in real time but they usually develop signatures pretty quickly, I'd say within a week's time. Besides, they've always been there for us with threat intelligence and incident response. This project will improve our detection and response capabilities but AV isn't going anywhere."
>
> --Cybersecurity professional, manufacturing organization

- A skeptical attitude toward all prevention controls. A number of cybersecurity professionals agree that advanced prevention products are superior to signature-based AV but they also believe that it is only a matter of time until skillful hackers find and exploit product vulnerabilities and bypass advanced prevention controls with aplomb. This viewpoint is certainly understandable as sophisticated cyber-adversaries have readily succeeded with this type of "cat and mouse" game in the past. Given this inevitable cycle, cybersecurity professionals in this camp believe that they may as well stick with traditional AV software and invest valuable time and resources into a more intelligence-driven security strategy. Next-generation endpoint security for advanced detection and response represents an integral component of a broader commitment to security analytics.

- A willingness to install multiple agents per endpoint. Organizations in this camp live by the old adage, "the right tool for the right job." In other words, they are willing to install multiple agents on each endpoint to get best-of-breed functionality rather than settle for a consolidated but subpar single agent.

- An enterprise security strategy. Even the term "endpoint security" is misaligned in these organizations as they view prevention, detection, and response as holistic activities that span endpoints, networks, threat intelligence, and a wide variety of open source and commercial security tools. To be considered at all, acceptable endpoint security tools must plug into a broader security architecture rather than operate in an endpoint security vacuum. This means that product integration capabilities are a key purchasing consideration.

- A focus on security analytics. These firms collect, process, and analyze terabytes of security data, and invest heavily in security analytics skills and tools. To some extent, endpoint advanced detection and response tools are viewed as data input, so security professionals place a high priority on the types of data collected, the frequency of data collection, and the underlying data management infrastructure. Do tools poll endpoints occasionally or collect all data? Is the data stored locally or centrally? Is the data stored in a relational database or some other type of repository? How long does it take to run queries? All of these questions are critical considerations.

- A focus on incident response automation and orchestration. As part of these organizations' do-it-yourself approach to cybersecurity, they also handle detection and response on a systemic basis. ESG found that many organizations leaning toward advanced detection and response were also engaged in projects to integrate technologies, automate data collection, and orchestrate IR workflow for tasks like security investigations and system remediation. Once again, next-generation endpoint security is treated as a means to an end (i.e., enterprise incident response) rather than an end in itself.

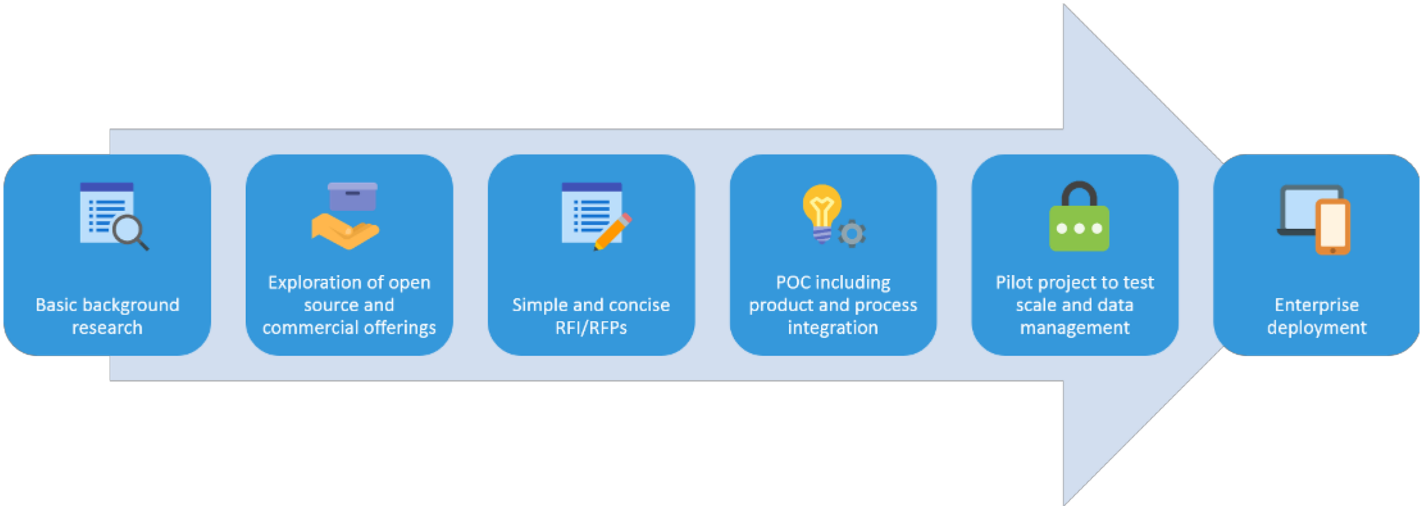
- Scalability is a critical success factor. There are a number of functional factors that contribute to the scalability requirement for these products. Because most advanced detection and response solutions employ continuous monitoring to collect data from protected endpoints, a significant amount of events are generated from each system. Given largely enterprise adoption, these products are typically deployed on thousands of endpoints. To enable the response use case, the recording of system activities must be retained for a notable amount of time, usually a few months at a minimum. The organizations interviewed noted that these factors of periodicity and scope are such that advanced detection and response offerings must be highly scalable, which has led to some companies switching vendors in order to meet their scale requirements.

Since advanced detection and response tools are brought in as part of a broader security analytics architecture, some organizations will place little value on things like a product's management GUI or onboard analytics. In cases like this, these features are deemed as lower priorities when compared with things like product integration or data collection, distribution, and management.

Advanced Detection and Response Projects

Organizations focused on advanced detection and response follow a much different project plan than those starting from the opposite side of the endpoint security continuum with advanced prevention (see Figure 5).

Figure 5. Project Phases for Evaluating, Testing, and Deploying Advanced Detection and Response Tools


Basic background research
Exploration of open source and commercial offerings
Simple and concise RFI/RFPs
POC including product and process integration
Pilot project to test scale and data management
Enterprise deployment

Source: Enterprise Strategy Group, 2016

- Basic background research. While organizations seeking advanced prevention tools remain confused by industry rhetoric and hype, enterprises adopting advanced detection and response for endpoint security tend to know just what they want. ESG found that organizations conducted some perfunctory product research to gain an understanding of the current market, but this phase of the project didn't require much of a time commitment. Basic background research took no more than a month's time and was usually performed on the side by a knowledgeable security analyst with direct involvement in the project.

- Exploration of open source and commercial offerings. Rather than reviewing analyst reports and third-party tests, cybersecurity professionals used the research period to get hands-on experience with commercial and open source tools by downloading evaluation software, playing with open source, and seeking out the opinions of other experts in the cybersecurity community. In this way, CISOs use all available resources in order to winnow down the list of potential products in order to focus the selection process on their own specific IR processes, use cases, integration needs, and security analytics requirements. This process is also fairly abbreviated, taking a month or two to complete.

> "We've played with open source tools and we know the commercial EDR vendors well. We knew we could create a short-list of products to look at fairly quickly"
>
> --Cybersecurity professional, financial services organization

- Simple and concise RFIs/RFPs. While there are dozens of products claiming to provide advanced detection and response capabilities, the security professionals ESG spoke with consistently look to a handful of market leaders and visible innovators. Based upon this behavior, it may be difficult for other vendors to gain traction in this space. ESG found that the RFI/RFP differed greatly from firms moving toward advanced prevention. Rather than seeking out generic information, organizations pursuing advanced detection and response products crafted very specific RFIs/RFPs to gauge how well each product would fit into their security analytics processes and data management requirements. Once again, this phase took a month or two at most.

- POCs. Note the lack of a dedicated product testing phase. Organizations adopting advanced endpoint detection and response products were able to condense project phases because of their strong security analytics capabilities, previous experience with these types of products, and succinct evaluation process. This is not to say that products weren't tested. Rather, proficient security staff was interested in testing products' capabilities as they related to their networks and explicit security requirements. This included all-encompassing process and technical integration, as well as in-depth testing around data collection and management. While previous project phases occurred quickly, enterprise organizations slowed way down during POCs, which ranged from 6 to 12 months.

- **Pilot projects.** Like those for advanced prevention, pilot projects for advanced detection and response tended to focus on manageability and scalability—especially with regard to data collection and management. In other words, this is where security analysts decide whether advanced detection and response products could actually collect and analyze the right data, deliver data to the right security personnel and analytics tools, retain the data for the appropriate timeframes, and respond to data queries in a timely fashion. Assessing these characteristics can require a lot of vendor support as they adjust product configurations and design a distributed data management architecture. Similarly, organizations spend a fair amount of time creating custom prevention and remediation rules which can take a while to work through. ESG witnessed a few projects where approved advanced detection and response products actually failed to meet enterprise scale, manageability, and performance requirements during this phase, forcing organizations to begin anew. To truly understand product functionality and data management capabilities It is not unusual for advanced detection and response project pilots to take 6 months or more.

> "We had to make sure that our vendors understood that this was going to be a partnership and not just a sale."
>
> --Cybersecurity professional, construction company

- **Enterprise deployment.** By the time organizations get to this phase, the bulk of the hard work is already done. Since the security team will maintain oversight of advanced detection and response products, IT operations is only needed for software distribution and agent installation. This phase is often completed in less than 6 months.

It's clear to ESG that advanced detection and response projects demand an unwavering commitment and strong technical skills from organizations seeking to deploy products AND vendors developing products in this space. Indeed, the experienced cybersecurity professionals driving these projects have high standards and numerous detailed requirements so product vendors must be willing to dedicate ample time and resources for hands-on support, features enhancement, and product customization as they help customers configure and integrate products, build a data management architecture, and create custom rule sets.

This is certainly a resource-intensive sales process but hard-working vendors will be rewarded with lucrative enterprise contracts. And, unlike advanced prevention tools, technical and process integration make advanced detection and response products much more difficult to replace. This means that leading advanced detection and response tools could become foundational security technologies in enterprise organizations for years to come.

Final Observations on Next-generation Endpoint Security

Based upon the interviews conducted for this project, ESG reached several conclusions about next-generation endpoint security products and the overall endpoint security market:

- **The endpoint security continuum represents a disconnect between supply and demand.** ESG's concept of an endpoint security continuum represents a bifurcated model where organizations tend to choose one pole or the other. This raises an obvious question: Is this behavior a function of an immature market that will consolidate over time? If so, it would be safe to assume that future innovation will lead to endpoint continuum product suites that span across advanced prevention, endpoint security controls, and advanced detection and response. This aggregation is actually already happening as several established vendors and startups alike offer one-stop-shop endpoint security products.

Over the next few years, ESG believes that the next-generation endpoint security market will proceed as follows:

- **All-in-one suites will appeal to midmarket and small enterprise organizations**. Many firms will start with advanced prevention products and then ease their way into detection and response. These organizations are most likely to opt for comprehensive next-generation endpoint security suites but this is far from a certainty. Given the resources and skills necessary for advanced detection and response activities, many cybersecurity professionals will outsource these processes to qualified service providers.

- **Large enterprises will continue with a best-of-breed approach**. Progressive global enterprise organizations are approaching next-generation endpoint security projects with very specific requirements, strong opinions, and explicit objectives. Next-generation endpoint security projects are also highly influenced by cybersecurity resources—organizations with resource constraints opt for advanced prevention while those with ample resources and strong security analytics skills lean toward advanced detection and response. Each of these characteristics pushes enterprises toward short-term, focused next-generation endpoint security projects rather than long-term endpoint security strategy.

- **AV products may catch up**. Traditional AV vendors are adding new security functionality to existing products and/or buying startups to add innovative software capabilities to their products. If these vendors can survive the onslaught of next-generation endpoint security startups and bolster their sales, service, and support accordingly, they may have an opportunity to usurp new functionality, just as they did with functionality like port controls, application controls, and anti-spyware. This second chance opportunity is most likely in the midmarket and small enterprise segments. Some organizations noted important criteria for judging AV vendors such as how regularly they provided product roadmap updates and how well they engaged in non-sales-related discussions. These and other factors could determine which AV vendors remain and which get replaced.

> **"I don't see us making long-term endpoint security product decisions anymore. The threat landscape and technology innovation happen too quickly these days, so we'll have to be more open to making changes when necessary."**
>
> **--Cybersecurity professional, financial services organization**

The market dynamics here really call for next-generation endpoint security product vendors to adopt an endpoint continuum go-to-market strategy. How? By offering independent next-generation endpoint security products (i.e., advanced prevention AND advanced detection and response products) that can stand on their own or be combined to form integrated solutions with common command-and-control (i.e., configuration management, policy management, reporting, etc.). Smart vendors will back these suites with well-crafted professional services to help customers evolve across the endpoint security continuum through phased projects supported by clear metrics of success. Finally, next-generation endpoint security vendors should create MSSP offerings on their own or with partners to meet the needs of a large percentage of organizations lacking the skills and resources necessary for more rigorous endpoint security controls and oversight.

- **Next-generation endpoint security is a "rip-and-replace" domain**. Many large organizations have used the same AV software products year after year without a thought about replacement. This type of market stability will disappear over the next few years with the transition to next-generation endpoint security tools for several reasons:

- **Enterprises are buying next-generation endpoint security products with operating budgets.** As previously mentioned, large organizations are choosing to use operating rather than capital budgets, purchasing next-generation endpoint security products as annual subscriptions. This gives CISOs the opportunity to evaluate endpoint security products and vendors each year, continually research competitive offerings, and replace incumbent products based upon poor product performance or attractive newly available alternatives. This is not to suggest that next-generation endpoint security products are disposable, but rather that CISOs are making sure that they remain flexible as the market and products mature.

- **Market churn will necessitate change.** As of this writing there are dozens of venture-backed next-generation endpoint startups vying for the same enterprise customers. Over the next few years, some of these companies will IPO, some will be acquired, and the majority will go out of business. CISOs are keenly aware of these inevitable market dynamics and will be willing to seek substitute solutions as circumstances change. On the vendor side, ESG noticed that the most successful next-generation endpoint security product vendors were investing heavily in customer relationships by getting to know their customers, providing hands-on technical support, customizing products to meet customer needs, etc. ESG also believes that most endpoint security vendors will work to address the respective preventative and EDR gaps in their portfolio in order to capture business from customers who start their journey on either end of the next-generation endpoint security continuum. This type of vendor commitment will determine which of the dozens of startups will survive and thrive over the longer-term.

> "It seemed like anytime we tried to turn an advanced control on, it broke something else. Even [incumbent AV vendor] support was telling me 'really, you want to rebuild this whole system.' Which were the worst words to say to me because if I'm rebuilding, I might as well start from scratch; I might as well look at other vendors at that point. That was the calling to me to look at something else. And I'm glad we did, because [new AV vendor] doesn't have these back-end issues."
>
> --Cybersecurity professional, health care, discussing his experience with antivirus software

- **New benevolent and malicious innovation will continue.** Venture capitalists realize that the multi-billion-dollar endpoint security market is in transition and will continue to invest with the hope of creating the next McAfee, Symantec, or Trend Micro. This will continue to drive endpoint security innovation and a revolving door of new startups. At the other end of the security spectrum, sophisticated hackers will pool their skills in order to discover and exploit next-generation endpoint security product weaknesses. Today's highly effective endpoint security prevention tools could suffer an AV-like decline in detection/prevention efficacy as this happens, forcing CISOs to reassess their product choices.

- **Data security and insider threats represent the next hurdles.** Several of the organizations interviewed for this project were bullish about the potential for next-generation security as a countermeasure against sophisticated cyber-criminals, nation state hackers, and hacktivists. In spite of these improvements, however, they believe these tools provide little help against security incidents and data breaches emanating from knowledgeable insiders (i.e., Edward Snowden, Bradley Manning, etc.). This will likely become the next frontier for next-generation endpoint security. Today's advanced prevention and advanced detection and response tools will likely gain DLP functionality or become tightly integrated with security analytics for insider attack detection over the next few years.

> "We believe we've really improved our ability to detect malicious endpoint activities but a skilled insider could still fly under the radar. Our next step is to integrate detection and response tools with DLP and user behavior monitoring."
>
> --Cybersecurity professional, government agency

- **Resistance aside, cloud-based control planes are here to stay.** Several next-generation endpoint security products are built around a cloud-based control plane (i.e., for configuration management, change management, reporting, etc.), with no option for on-site management servers whatsoever. The cybersecurity professionals interviewed had mixed feelings about this design. On the positive side, they were pleased that they could install and test products quickly while avoiding the need to purchase, install, configure, and manage dedicated server hardware. Nevertheless, infosec professionals are paranoid by nature and used to full control of all hardware and software. Furthermore, cloud-based control planes may not conform to certain regulations (i.e., FISMA), keeping innovative products out of some industries altogether. Cloud-based control planes may be uncomfortable and somewhat controversial in the cybersecurity community today, but this model isn't going away and may become the de-facto standard for software management in the future. Rather than continue to fight a losing battle, CISOs should abandon historical biases and modify policies and processes so they can take advantage, rather than avoid, this burgeoning software model.

- **Advanced detection and response will be dominated by managed services.** Organizations considering advanced detection and response should spend extra time assessing whether they have the right skills and an adequately sized SOC staff to deploy and take advantage of this type of next-generation endpoint security software. Based upon this project, ESG believes that a small percentage of organizations actually fit this profile. Those enterprises lacking adequate resources and skills still need advanced detection and response capabilities, so they will likely turn to service providers to fill this void. This means that the MSSP market for advanced detection and response should experience rapid and persistent growth since only 20% to 25% of organizations are capable of addressing these needs on their own.

The Bigger Truth

As part of each interview, ESG asked cybersecurity professionals what advice they would provide to other organizations beginning to consider next-generation endpoint security options. There were a number of consistent "lessons learned" suggestions:

> "It's critical to clearly define what you want to achieve. And not just from a security perspective—you need to set specific business and IT goals as well."
>
> --Cybersecurity professional, manufacturing organization

- **Get to know your AV.** As previously described, about half of the organizations interviewed never considered, much less tested, the advanced in-memory prevention/detection features within their existing AV software. When pressed on this, most admitted that this was an oversight and certainly would have been worth investigating. Aside from current advanced security functionality, large organizations with good relationships with their AV vendors should also push for a broader discussion with executive management on product roadmaps and corporate strategies. There may even be an opportunity to work collectively as a beta site for upcoming product releases. To be clear, this doesn't mean that enterprises should simply default to AV alone but it is certainly worth including an AV assessment during the research phase, so organizations can learn more about endpoint security functionality they already own but don't know or use.

- **Spend adequate time on requirements definition.** CISOs made an explicit point about the requirements definition phase of next-generation endpoint security products. More specifically, they recommended participation from a wide assortment of groups including business managers, IT operations, security analysts, network administrators, etc. While the focus on next-generation endpoint security projects is on preventing, detecting, and responding to security incidents, lots of groups and individuals are involved with desktop computing. Consequently, next-generation endpoint security projects have the opportunity to address other issues (i.e., operational issues, process issues, performance issues, etc.) and must avoid any new types of business disruption.

- **Seek out innovative vendors and technologies.** The colloquial expression "cast a wide net" is appropriate here once again. Given the abundance of both market confusion AND innovation, cybersecurity professionals should be willing to research and even evaluate new products and unknown vendors. While next-generation endpoint security companies may be new, many of the founders have long histories in this space and know well what works and what doesn't. At the very least, organizations can learn more about the threat landscape and creative countermeasures as part of this process.

- **Perform blind testing during the initial product testing phase.** One organization pursued a novel methodology by anonymizing all products and vendors during the product testing phase. This can be difficult from a political perspective but it will eliminate any testing biases based upon personal relationships and vendor participation. This can help ensure that products are judged purely on their ability to prevent, detect, or respond to real security events.

- **Create a plan for endpoint security controls.** While organizations approach the endpoint security continuum from the advanced prevention or advanced detection and response side, leading organizations also consider endpoint security controls as part of their long-term strategy. Smart CISOs also recognize that all endpoints are not created equally, and therefore create specific security controls for sub-segments of the overall endpoint population. For example, Windows PCs configured as point-of-sales (POS) systems can be outfitted with application controls and firewall rules much more easily than mobile laptops. The overall goal should be reducing the attack surface while avoiding resource-intensive projects or any type of business or productivity disruptions.

- **AV replacement strategies may require extra work.** Organizations replacing AV software mentioned that this decision doesn't come entirely for free as they often use some AV features like port controls, network firewalls, or password vaults. Some even commented that they didn't know that users were using these features until they'd made the decision to abandon AV. CISOs should assess how and where their organizations are using AV and consider the time, technology replacements, and money that should be put into overall endpoint security strategies.

- **Think in terms of the endpoint continuum for long-term strategy.** Whether organizations start with advanced prevention or advanced detection and response, they will ultimately need processes, skills, and tools in both areas—as well as additional endpoint security controls in between. Savvy companies make sure that next-generation endpoint security projects are phased in over time. Furthermore, each phase has its own objectives and metrics while future phases are adjusted based upon near-term results. These projects ultimately cover the entire endpoint security continuum with a combination of new processes, projects, services, and tools.

Vendor Participation

To facilitate this project, ESG contacted numerous endpoint security vendors and solicited their participation. Each vendor was asked to provide the names and contact information of customers. ESG then contacted these companies on its own, scheduled meetings, and conducted hour-long interviews with each. To maintain research integrity, vendors were prohibited from participating on these calls and had no input into the questions ESG posed to participating enterprise cybersecurity professionals. Additionally, interviewees were not limited to discussing only the vendor that referred them to ESG. Rather, ESG was able to ask questions on a multitude of other cybersecurity topics across people, process, and technology. While each interview was unique, ESG tried to ask the following questions of each cybersecurity professional:

1. What type of endpoint security tools did your organization have in place previous to next-generation endpoint security product deployment? Which groups/individuals owned and operated these technologies?

2. Please describe the factors that drove your organization to consider new types of endpoint security technologies.

3. Please describe your evaluation process (research, testing, POC, individuals involved, etc.).

4. Which products were considered? What prompted you to choose the endpoint security product you chose?

5. How are endpoint security products integrated into other types of controls and security monitoring systems? What are your plans in this area?

6. Please describe how you are using any new endpoint security tools (or functionality) today. How will your use of this product/functionality change in the future?

7. What additional plans does your organization have for endpoint security moving forward?

ESG would like to recognize all participating endpoint security vendors and express our sincere appreciation for their help. The following vendors were gracious enough to partake in this research project:

- Bromium
- Carbon Black (formerly Bit9 + Carbon Black)
- CounterTack
- Cisco Systems
- CrowdStrike
- Cylance
- FireEye
- Hexis Cyber Solutions
- Intel Security (McAfee)
- Invincea
- Kaspersky Lab
- SentinelOne
- Sophos
- Symantec
- Trend Micro
- Triumfant
- Webroot
- Ziften

ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

www.esg-global.com contact@esg-global.com P. 508.482.0188