Next-generation Endpoint Security

An Integrated and Automated Approach to Defending Today's Advanced Threats

In the past, antivirus was the de facto endpoint protection. Today, it has quickly become a commodity technology that has proven ineffective when dealing with advanced malware. Antivirus has evolved to include additional endpoint security controls but is unprepared to meet today's sophisticated threats. This has forced organizations and the industry as a whole to search for an alternative.

In the endpoint security spectrum, organizations can choose between endpoint detection and response (EDR) and endpoint protection platform (EPP). Due to the lack of IT security talent, most organizations choose to start with EPP, as it can prevent threats from the onset when a right approach is applied to known and unknown threats, thus requiring less human intervention when compared to EDR. In addition, automating remediation at the endpoint is a must with these scarce resources.

After a security breach or a sandbox project evaluation occurs, EPP is a typical consideration to building a cohesive security strategy, which requires that endpoint protection not work in a vacuum. Instead, it should seamlessly integrate and work cooperatively with other elements in the security architecture to respond to advanced threats quickly and effectively.

Unified Next-generation Endpoint Security

Unlike traditional endpoint protection, the Fortinet FortiClient is a unified endpoint protection platform that integrates into the overall security architecture, automates threat protection, and provides secure remote access (i.e., VPN) in a small, lightweight package supporting a multitude of devices (PC, Mac, Linux, Apple, and Android) either on- or off-premises.

Integrating Endpoint within a Security Architecture

Fortinet Security Fabric is built to combat today's sophisticated threats, with a scalable, aware, secure, actionable, and open solution. This is extended to the endpoint through FortiClient and is achieved by sharing endpoint telemetry that enables security operators to enforce endpoint security compliance for a user segment or organization as a whole and quarantine a compromised endpoint with a single click (see Figure 1).

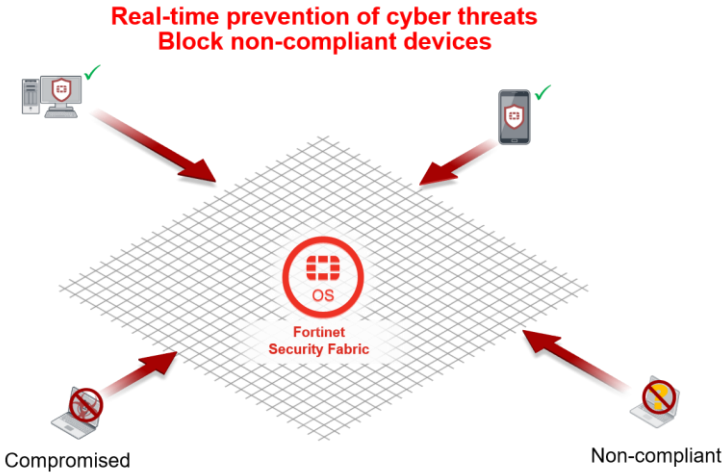


Figure 1. FortiClient integrates and works cooperatively with Fortinet Security Fabric

For example, when an endpoint attempts to join the network and is unpatched at the application or OS level, it will not be allowed access based on the security-administered compliance check. Consequently, the user can choose to remediate via manual patching or via an administered policy to perform auto-patching as a method to automate remediation.

Benefits

- Full endpoint visibility for user segments or an organization as a whole
- Simplified enforcement of non-compliant endpoints
- Effective threat containment with a single-click endpoint quarantine

Automating Prevent-Detect-Mitigate Threat Protection Lifecycle

FortiClient protects against known threats through its built-in security stack that includes dynamic AV engine, application firewall, vulnerability scanner with auto-patching, and web filter, all working in concert to reduce the attack surface and prevent polymorphic and common malware, as well as known exploits, from various attack vectors at the endpoint.

FortiClient protects against unknown threats by automating the submission of unknown objects to the highly rated Fortinet FortiSandbox. In turn, FortiSandbox provides detection through validation of an unknown file's hash, or performs dynamic analysis to determine malicious behavior. Advanced malware or zero-day threats are mitigated through the sharing of intelligence with FortiClient to automatically quarantine that object as well as immunize all other endpoints and, with FortiGuard intelligence, to extend protection to the global community.

Benefits

- Fully automated threat protection
- Top marks for effectiveness from NSS Labs, AV Bulletin, and AV Comparatives
- Powered by Fortinet's global threat intelligence
- Fully integrated with various security elements for an effective response

Conclusion: Defining the Next-generation Endpoint Security

Organizations expect next-generation endpoint security to protect against known and unknown threats in an automated fashion that can seamlessly integrate with other elements in the security architecture as part of a cohesive security strategy. This allows organizations to reduce management complexity yet respond to sophisticated threats effectively with a leaner security team.

Excerpt from ESG Market Landscape Report

Enterprise Adoption of Next-generation Endpoint Security

Date: May 2016 **Author**: Jon Oltsik, Senior Principal Analyst; Doug Cahill, Senior Analyst; and Kyle Prigmore, Research Analyst

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. 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.

Next-generation endpoint security can be further divided into two main categories- advanced prevention technologies, and advanced detection/response technologies.

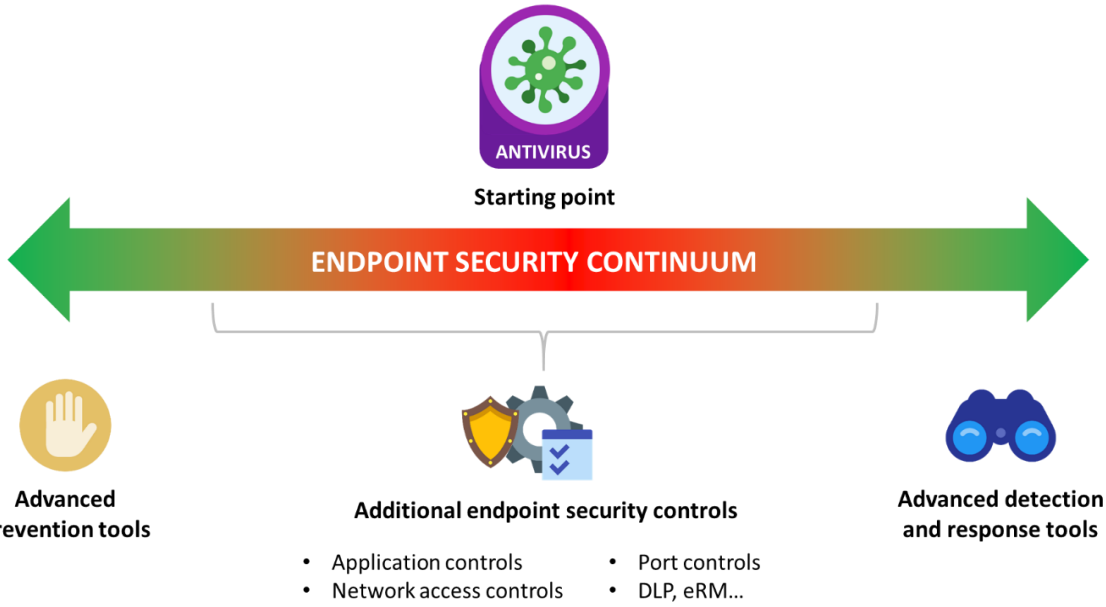
- Advanced prevention technologies. This type of software could actually be characterized as "next-generation antivirus software," as it is designed to block exploits and malware while delivering a higher and more accurate detection rate than traditional AV products. Stated another way, AV is designed 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 such as executable inspection and analysis, machine learning, containerization, static/dynamic malware analysis and/or threat intelligence integration.

- 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.

ESG believes that next-generation endpoint security should really include both sets of capabilities across an overall endpoint security continuum (see Figure 1). 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 1. The Endpoint Security Continuum



Source: Enterprise Strategy Group, 2016

The full ESG Market Landscape report explores both ends of the spectrum in equal measure. However, in the interest of time and relevance, this customized version of the report focuses exclusively on advanced prevention.

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.

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.

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

- **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.

- **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 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.

  "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

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.

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 indirectly by a highly visible security breach within an organization's industry.

> "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

- **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.

- **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.

A Closer Look at Advanced Prevention

Organizations are deploying advanced endpoint security products, but why are many choosing advanced prevention products as opposed to an EDR tool? Security professionals describe a variety of factors that lead them to advanced prevention:

- **Advanced prevention after 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 and a much faster time-to-value than most EDR products.

> **"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

- **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.

- **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 2).[2]

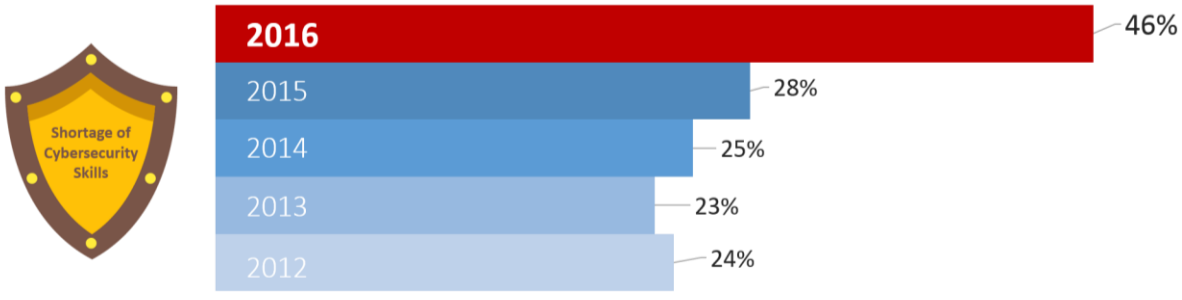
With no end in sight for the cybersecurity skills shortage, most organizations will have little choice but to approach next-generation endpoint security from the advanced prevention side of the continuum. This is precisely why ESG believes that 75% to 80% of midmarket and enterprise organizations will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

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

Figure 2. Organizations Claiming to Have a Problematic Shortage of Cybersecurity Skills



Source: Enterprise Strategy Group, 2016

The Bigger Truth

The evolving threat landscape and the ineffectiveness of traditional signature-based antivirus technology to cope with today's dynamic attacks, which often target end-users, and thus endpoints, has created a strategic imperative to improve prevention efficacy without adversely impacting operational efficiency. ESG's research indicates that most organizations opt to start at one end of the Endpoint Security Continuum with larger companies investing the time and resources to leverage advanced detection and response capabilities while the significant majority of companies opt to deploy advanced prevention controls. ESG believes that, as vendors deliver converged next-generation endpoint security platforms over time, these options will not be mutually exclusive but, in the interim, most organizations will continue to start their journey to an improved endpoint security posture with advanced preventative controls. The drivers include both external and internal factors with respect to an increasing awareness of the endpoint's central role as the entry point for many of today's threats and the fact that many organizations need to address this reality with limited resources. These considerations and more combine to make advanced prevention technologies a next-generation endpoint security approach that should be explored.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. More than 270,000 customers worldwide trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com.

US Headquarters
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel: +1-408-235-7700
Fax: +1-408-235-7737

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