Solution Showcase

Redefining Next-generation Endpoint Security Solutions

Date: October 2016 **Author:** Jon Oltsik, Senior Principal Analyst

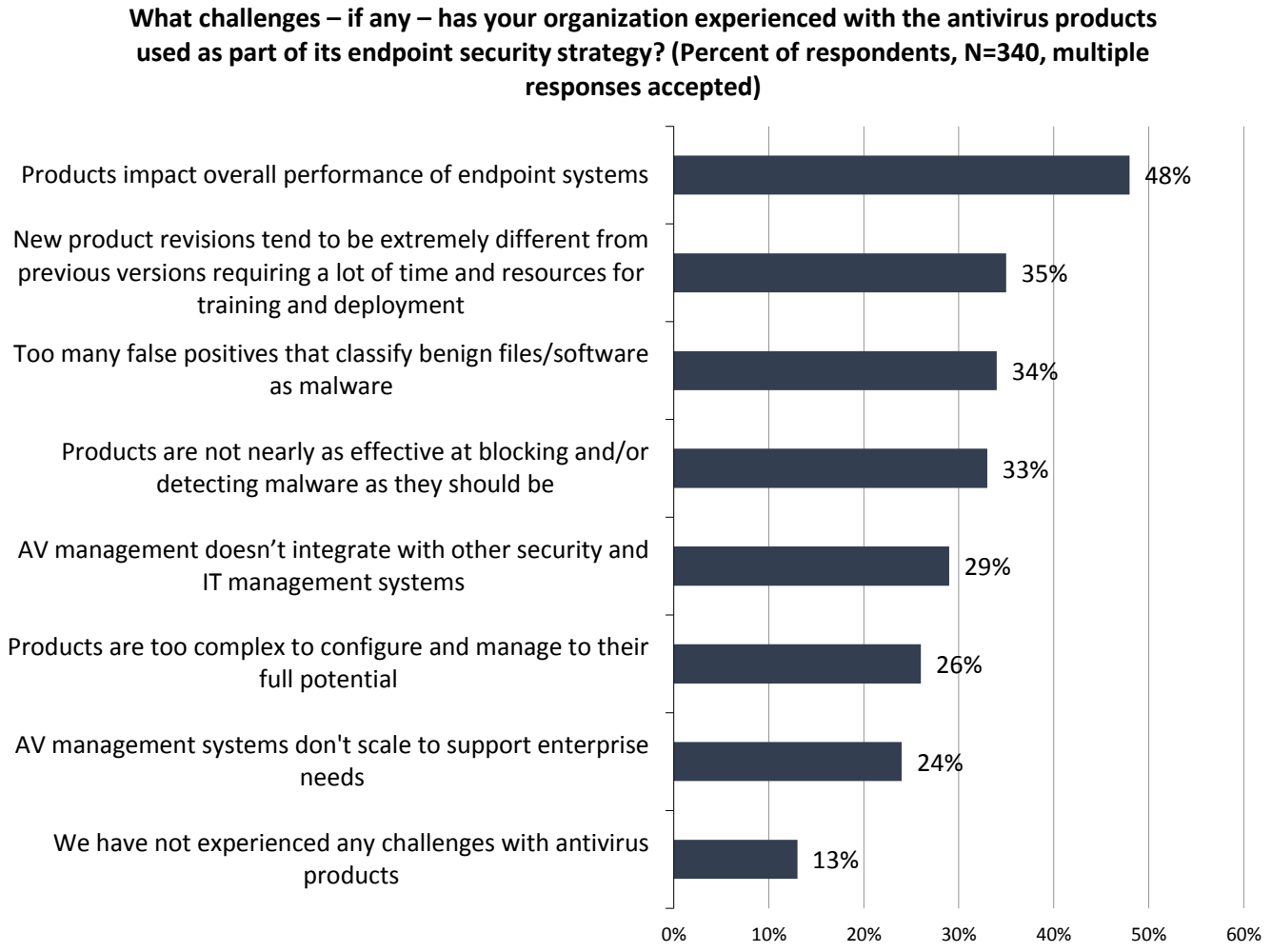
Abstract: Enterprise organizations face a difficult situation. Many current endpoint security tools can't prevent or detect sophisticated exploits or zero-day malware, forcing CISOs to implement an assortment of next-generation endpoint security tools. Unfortunately, this strategy can increase cost and complexity while introducing the potential for resource contention and performance issues on the endpoints themselves. Is there any alternative to this Faustian compromise? Yes—next-generation endpoint security solutions built for centralization, consolidation, and integration that offer functionality for prevention, detection, and response. McAfee's recently announced Dynamic Endpoint Threat Defense is a next-generation endpoint security solution that can improve security efficacy while streamlining security operations.

Overview

When it comes to endpoint security, ESG research paints a disheartening picture. Last year, while more than two-thirds (67%) of cybersecurity professionals believed the threat landscape had grown worse than it was in the previous two years,[1] 80% of respondents to another ESG survey cited that endpoint security (processes and technology management) had become more difficult than it was two years previously.[2] Of course, enterprise organizations have endpoint security technologies in place to help address some of these issues, but many report numerous challenges with current antivirus products, including performance requirements, upgrade processes, the number of false positive alerts, and overall product efficacy in preventing/detecting exploits and malware (see Figure 1).[3]

[1] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.
[2] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.
[3] ibid.

Figure 1. Antivirus Product Challenges



Source: Enterprise Strategy Group, 2016

Endpoint security challenges are also exacerbated by the global cybersecurity skills shortage. According to research published earlier this year, 46% of organizations report a problematic shortage of cybersecurity skills.[4] This cybersecurity shortage is compounded by the use of tools that work in isolation and require manual coordination. In many cases, organizations are understaffed *and* lack the right skills to employ strong endpoint security best practices. Instead, security administrators are relegated to "firefighting" an overwhelming amount of security alerts and using precious time to address risks and update protection through manual processes.

The Endpoint Security Continuum

New endpoint security requirements have created a flurry of technology innovation and industry buzz around "next-generation endpoint security (NGEPS)" products. This has only led to market confusion as infosec professionals try to sort through an avalanche of vendor marketing hype.

ESG believes it shouldn't be this difficult. In its 2016 market landscape report titled, *Enterprise Adoption of Next-generation Endpoint Security,* ESG defined endpoint security as:

[4] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

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

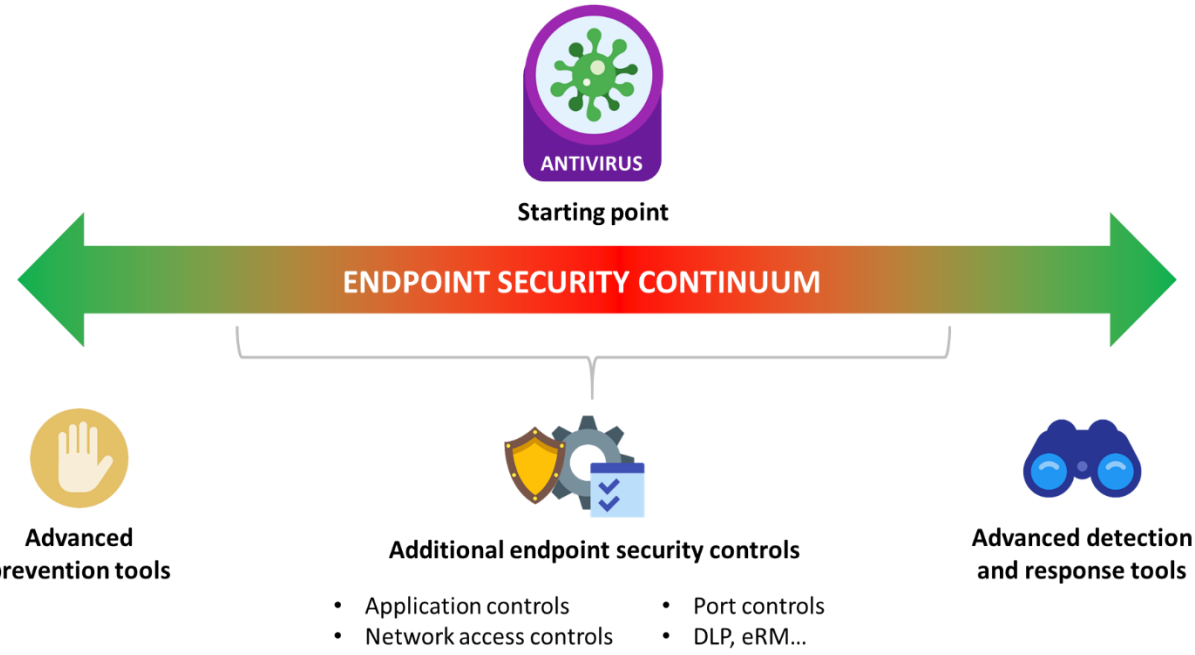
Furthermore, NGEPS was defined as:

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

ESG believes that next-generation endpoint security should include 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 with traditional AV products. This functionality should include the ability to "learn" from every attack for stronger response, faster performance, and improved efficacy. 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



Source: Enterprise Strategy Group, 2016

As part of the continuum, next-generation endpoint security is supported with additional types of security controls (i.e., port controls, application controls, DLP/eRM, etc.). These controls are intended to decrease the endpoint and network attack surface, making network penetration and system compromises more difficult for cyber-adversaries. This can improve security, but can also carry costs because of:

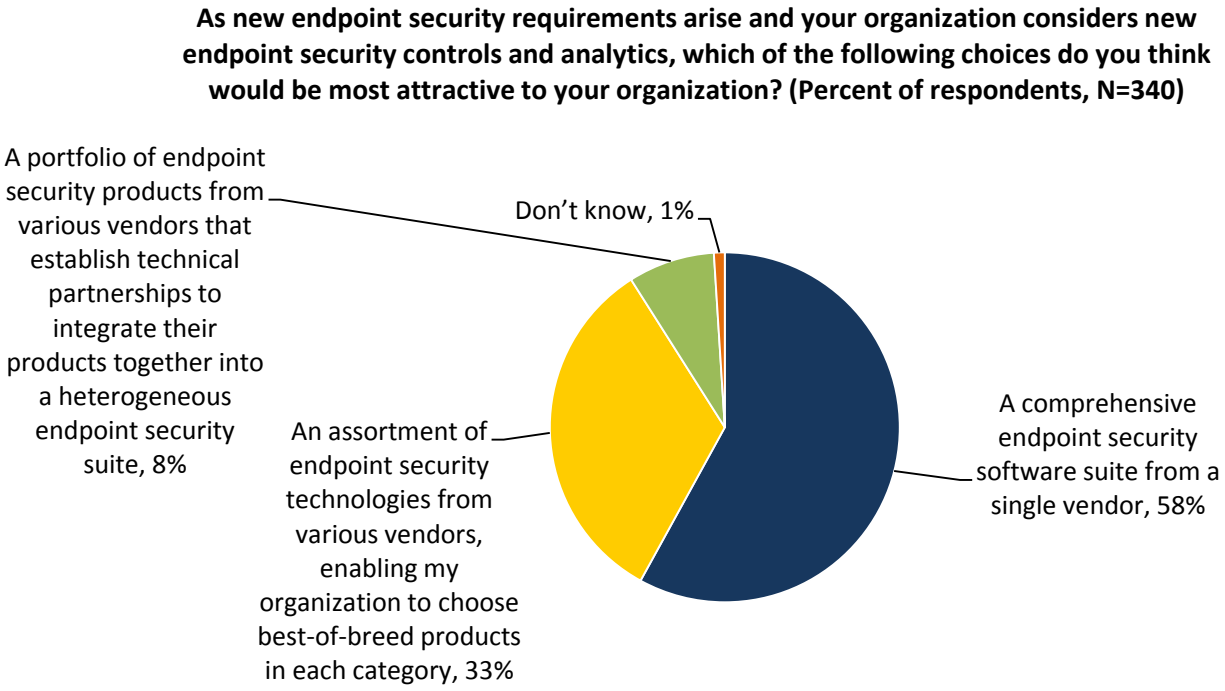
- Multiple products working in isolation. Security and IT operations teams may be forced to install and manage multiple, isolated products on their endpoints. This introduces an operational burden and can cause contention and performance issues on the endpoint systems.

- **Multiple management planes.** New endpoint software tools for prevention, detection, and response come with their own management consoles for policy management, configuration management, and reporting. Once again, this adds more work for an already overwhelmed security and IT operations staff.

Toward Next-generation Endpoint Security Solutions

Clearly, large organizations want to improve security efficacy without adding operational overhead or disrupting business processes or user productivity. This is likely why the majority of cybersecurity professionals (58%) claim that their organization would prefer to buy a comprehensive endpoint security solution from a single vendor rather than cobble together a solution out of assorted endpoint security point tools (see Figure 3).[5]

Figure 3. Most Attractive Choice of Endpoint Security Controls and Analytics Delivery



Source: Enterprise Strategy Group, 2016

A comprehensive endpoint security software solution from a single vendor would need to have all of the elements of the ESG endpoint security continuum, spanning from advanced prevention to advanced detection and response. This would include:

- **A defense-in-depth architecture for threat and exploit prevention**. Strong network security is built using layered security with each security control supporting and complementing others. In this way, packets must pass through an assortment of filters (i.e., firewalls, web threat gateways, AV gateways, etc.) before they reach their ultimate destination. Similarly, next-generation endpoint security tools should contain several pre- and post-execution filters in order to prevent and detect exploits and malware. These filters will range from tried-and-true AV signatures to an assortment of other technologies including behavioral heuristics, machine learning algorithms, threat intelligence

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

correlation engines, and isolation technologies that execute files in virtual containers blocking access to real system resources.

- **Competitive EDR capabilities.** In addition to a defense-in-depth endpoint security architecture, next-generation endpoint security tools must be able to monitor and capture system behavior as well as standalone EDR solutions do today. To fulfill this requirement, NGEPS solutions must be able to collect, process, analyze, and present active endpoint behavior data in ways that support organizations' security analysis processes. The best tools will include tight integration with threat intelligence and offer closed-loop processes that take newly discovered exploits, malware, and vulnerabilities and translate them into remediation rules for blocking future similar attacks.

- **An architecture designed for consolidation, centralization, and integration.** NGEPS solutions can provide real value in a few of the most important areas for enterprise organizations. First, next-generation endpoint security solutions can be built on an integrated infrastructure, creating a single coordinated system and minimizing management overhead. Second, NGEPS solutions offer a consolidated management plane with integrated functionality for policy management, configuration management, and reporting. These solutions should also feature role-based access control to support division of labor and separation of duties between security and IT operations personnel. Finally, enterprise organizations often integrate endpoint security solutions with network security tools, security analytics systems, incident response platforms, and third-party threat intelligence feeds. NGEPS solutions should be designed around industry standards, open APIs, a common language, and an ecosystem of partners that support these requirements.

Of course, NGEPS solutions must also be built for business and user productivity. To meet this requirement, these solutions must offer strong security while remaining transparent and non-disruptive to users.

McAfee Dynamic Endpoint Threat Defense

Next-generation endpoint security is a security category highlighting signature-less defenses and dominated by startup vendors and point tools. As this market matures however, traditional endpoint security vendors are catching up, offering the first true next-generation endpoint security solutions. One example of this is the recently announced McAfee Dynamic Endpoint Threat Defense featuring:

- **Adaptive threat defenses.** McAfee's solution is built on a shared ecosystem of other McAfee and third-party partner technologies. Shared threat intelligence and endpoint context can help solutions learn from every encounter to evolve security. This enables coordinated defenses that can share insights and work as a common system across multiple layers of security filters to automatically adapt defenses across all components.

- **Advanced prevention capabilities**. McAfee's solution takes the observations from different technologies and vantage points, which by themselves may not provide enough to convict malware, and combines them to offer enough insight to catch the latest threats. For example, McAfee has extended its existing endpoint security offerings with static and dynamic behavioral analysis informed by machine learning and dynamic reputation scoring with shared threat intelligence. In this way, McAfee has significantly improved its efficacy in preventing and detecting greyware and zero-day malware to secure "patient zero."

- **Integrated EDR.** McAfee has also bolstered its endpoint security solution with EDR capabilities, providing unified visibility for security investigations, hunting activities, and remediation actions—including an emphasis on efficiency with single-click correction and setting triggers to automate responses against future attacks.

The Bigger Truth

Endpoints are often used as a beachhead for sophisticated cyber-attacks like APTs. Cyber-adversaries compromise Windows PCs and then use them as staging grounds for extended offensive campaigns that ultimately lead to costly data breaches. Given this, enterprise CISOs must do everything possible to improve endpoint security efficacy, but today's next-generation endpoint security tools often come at the cost of operational overhead. Given the global cybersecurity skills shortage, this is an unacceptable tradeoff.

To enhance security without the excess operational baggage, many CISOs want integrated next-generation endpoint security solutions built for consolidation, centralization, and integration. Fortunately, next-generation endpoint security solutions, like McAfee Dynamic Endpoint Threat Defense, have the potential to improve security efficacy while streamlining security operations.