White Paper

Beyond Next-gen:

Defining Future-ready Endpoint Security

By Doug Cahill, ESG Senior Analyst

October 2016

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

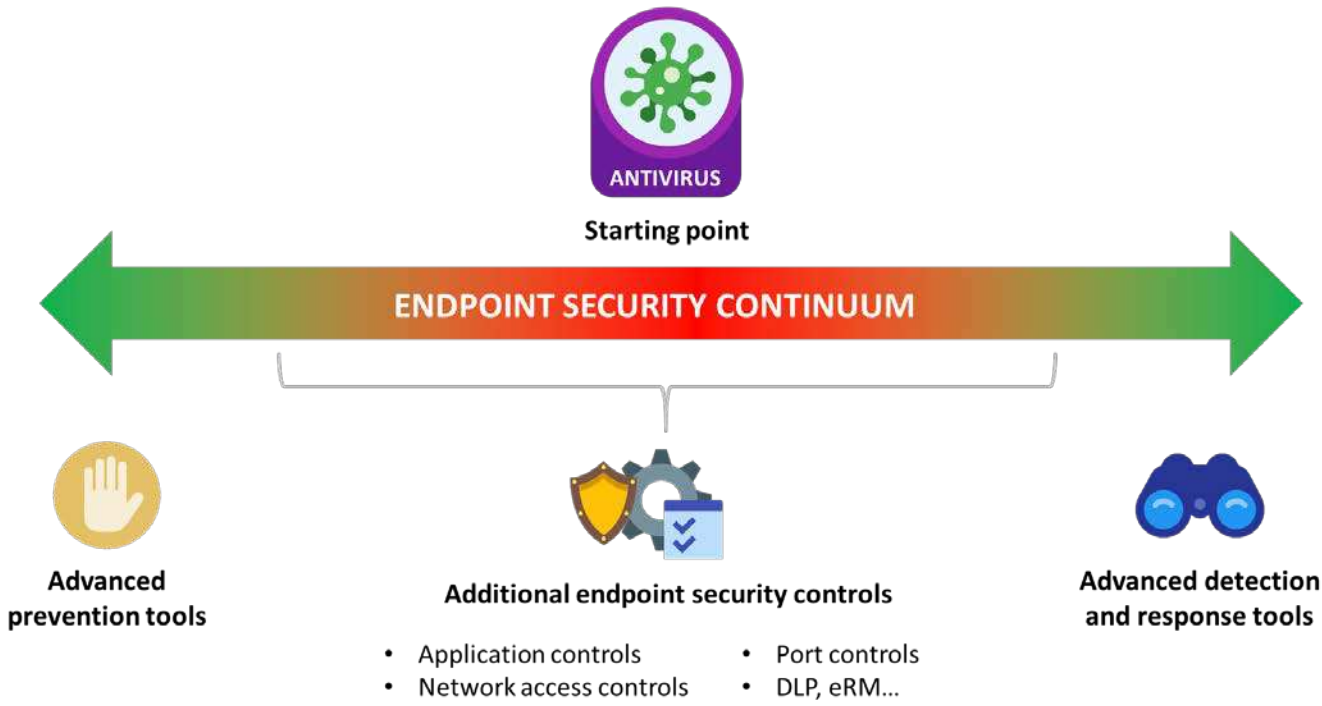
Contents

Executive Summary

The term "next-gen" is commonly cited by technology vendors to position a product as being innovative based on new and differentiated capabilities. Notable next-gen cybersecurity products include next-gen firewalls, the state of the art of which now represents the standard, current-generation firewall technology. The notion of "next-gen" is now promoted by some providers of endpoint security software as a way to improve the efficacy of protecting endpoints from compromise, given the prominent role endpoints play in cybersecurity attacks, the ways in which mobility and cloud apps have expanded the attack surface area, and the multitude of threats that circumvent signature-based antivirus. Because next-gen products become current-gen and, eventually, last-gen, organizations should think strategically about their next endpoint security investment as one that can transcend generations by keeping pace with the shifting threat landscape across a broadening attack surface area.

ESG conducted market research to explore how organizations employ advanced endpoint security controls. This research revealed that a continuum is at play, with most organizations that ESG interviewed starting with advanced preventative controls to augment their antivirus technology and a smaller number of companies, typically those that are well resourced, employing advanced detection and response capabilities (see Figure 1).[1] While the use of advanced preventative controls and advanced detection and response controls are not mutually exclusive over time, the weighting toward the former was due in large part to the need to balance the efficacy of better protecting endpoints from compromise with the operational cost of doing so.

Figure 1. The Endpoint Security Continuum



Source: Enterprise Strategy Group, 2016.

[1] Source: ESG Market Landscape Report, *Enterprise Adoption of Next-generation Endpoint Security*, May 2016.

As next-gen endpoint security technology becomes the current generation, the definition of next-gen endpoint security as "those controls that can detect and prevent *new and unknown* malware and exploits" needs to be expanded. ESG defines endpoint security as "*the policies, processes, and technology controls used to protect the confidentiality, integrity, and availability of an endpoint system and the applications and data assets accessed by endpoints."* This definition implies endpoint security solutions must deal with both the more pedestrian set of known threats (i.e., viruses) as well as the new and unknown zero-day threats, irrespective of type and vector. Out of necessity, many organizations are deploying multiple point tools to address this variety, but incurring an operational tax in doing so, as realized by the need to deploy additional agents and management consoles, configure overlapping policy settings, and establish a familiarity and expertise with multiple new technologies.

ESG defines endpoint security as "*the policies, processes, and technology controls used to protect the confidentiality, integrity, and availability of an endpoint system and the applications and data assets accessed by endpoints."*

As endpoint technologies converge once again into suites, as was the case in the first generation of endpoint protection platforms that consolidated antivirus, anti-spyware, personal firewalls, device control, and more, customers will be able to more efficiently defend against the multitude of threats that put their endpoints at risk. Newer such endpoint security suites will enable customers to move along the continuum to employ prevention, detection, and response capabilities to protect endpoints from compromise. This paper explores the central role of the endpoint in the cybersecurity kill chain to frame the requirements of endpoint security solutions that are both contemporary and based on technology that remains relevant over time.

The Endpoint Vulnerability

To explore what is both immediately next and future-ready for endpoint security technology, we need to consider how the endpoint itself has changed and how its weaknesses are exploited to perpetrate attacks.

The Entry Point

The endpoint is very often the entry point, the virtual front door, via which malware and exploits are introduced during an attack campaign. The cybersecurity kill chain illustrates the central role of the endpoint in an attack lifecycle during which endpoints are especially prominent in the middle of the kill chain, from the delivery of the threat, the exploitation of a vulnerability, whether that is software or human gullibility, the installation of malware, through the contacting of command and control and taking action on the target. Organizations can no longer lean on a network-centric "catch it on the wire" orientation to cybersecurity and must include future-ready endpoint security controls as part of a holistic strategy to improve one's security posture.

Mobility, Cloud Apps, and the Expanded Attack Surface Area

Remote and mobile employees regularly access corporate assets via cloud services outside of the network perimeter secured by their employer. Such cloud services include "shadow IT" apps that are used outside of the purview of corporate IT and security teams, resulting in a lack of security controls being applied to such usage. As a result, the cloud has opened up a new attack vector for the introduction of malware including the fan-out effect of malware that is synched from a cloud storage service to multiple devices.

While Windows-based PCs are still the most prevalent endpoint platform, there has been a notable increase in MacOS in corporate environments. Multi-device knowledge workers have broadened the scope of endpoints to include mobile devices and a wide variety of IoT devices are expanding the set of fixed function machines that need to be secured. And if we further broaden the definition to more generically include all hosts, servers can also be consider endpoints. In total, such device sprawl and an increasingly mobile workforce represent an appreciably expanded attack surface area.

Diversified Threat Types and Attack Vectors

It's important to establish a baseline of the types of threats and introduction vectors that put endpoints at risk to understand how different detection techniques help mitigate each, respectively.

Exploitable Weaknesses

The multiple exploitable weaknesses in the typical endpoint include:

- ***Known software vulnerabilities*** in the form unpatched apps, browsers, and operating systems.
- ***Human gullibility,*** an oft-exploited vulnerability via techniques such as spear phishing, email impersonation, and drive-by downloads.
- ***Weak passwords and stolen credentials,*** *which* provide authenticated access to authorized resources.
- ***Open device ports,*** via which contaminated portable storage devices can introduce malware.

And while some zero days exploits never see the light of day thanks to responsible disclosure and bug bounty programs, many do and are especially difficult to detect due to their lack of provenance.

File and File-less Threats

Once such a weakness is exploited, most malware will establish a foothold on disk and begin to interact with system services such as the registry, or, in the case of ransomware, network services, to retrieve an encryption key and then the file system to encrypt data. However, some malware is file-less in that it executes in memory only, making it especially difficult to detect. Weaponized content is another type of malicious payload employed by adversaries to disguise malware as a macro in order to evade detection techniques limited to binary executables.

This combination of vulnerabilities, vectors, methods, and threat types makes for a multi-dimensional matrix, requiring a correlating set of non-mutually exclusive detection techniques.

Spotlight: Ransomware

Prevalent across industries, organizational size, and geographies, ransomware is putting endpoint security controls to the test. Ransomware is often introduced via spear phishing as well as drive-by downloads and increasingly via compromised cloud applications, including enterprise file synch and share (EFSS) services. Attack methods are manifested as both malware and exploits, highlighting the need for multiple detection techniques. These attack methods and vectors employed by cybercriminals and the introduction of new ransomware variants and strains circumvent solutions limited to one detection approach, representing a case-in-point for the application of multiple techniques. In addition to being extorted to pay a ransom, the impact to end-user productivity has, in fact, been a catalyst for many companies to revisit the endpoint security solution.

Minding the Gap with Point Tools

To date, out of necessity, many organizations have deployed additional endpoint security controls to fill the gap created by their current technology not keeping pace with the threat landscape. While traditional signature-based antivirus (AV) is widely understood to be ineffective against new threats, for most organizations it serves as a baseline level of defense against known viruses that can be detected via pattern matching. Additional discrete solutions being layered on top of AV include:

- ***Software reputation*** to augment signatures by identifying known good and bad software based on a trust rating calculated by prevalence and usage.

- *Machine learning* to detect new and unknown malware.
- *Behavior analysis* for exploit detection.
- *Application control* to only allow whitelisted applications for a default-deny approach to secure fixed function systems and some knowledge-worker operated endpoints.

While all are good techniques, disparate controls add to the cost and complexity of endpoint security, a significant consideration punctuated by the acute shortage of cybersecurity skills that makes it difficult for many organizations to resource establishing a core competency in multiple security tools.

Integrated Detection Techniques for Filtering the Threat Spectrum

In order to convey a set of requirements for an endpoint security solution that can address these vulnerabilities, some constructs to do so are in order. The notion of known and unknown threats helps illustrate the techniques and controls that can mitigate these threats, respectively. But trust is amorphous, such that techniques also need to account for a certain level of ambiguity, in the form of files that may initially be deemed trusted, but warrant further investigation. The concept of breadth and depth will help lay out the need for coverage and a layered set of detection techniques. Finally, a prevent-detect-respond methodology offers an actionable framework within which endpoints and corporate assets can be protected via a closed loop approach.

Breadth: Coverage Across Devices, Threat Types, and Attack Vectors

There are multiple aspects to the scope of coverage that a modern endpoint security solution should provide, including:

- *Device coverage* means both operating systems and form factor, encompassing Windows, MacOS, IoS, Android, and Linux across laptops, desktops, mobile devices, and fixed function machines.
- *File-based threats* are payloads delivered as binary executables malicious in nature—or "malware"—certain types of exploits, and weaponized content.
- *File-less threats* include other types of exploits as well as code that will attempt to evade detection by compromising an active program and then staying memory-resident.
- As for *vectors*, most threats are delivered via the applications end-users interact with most often—email, web browsers, and, cloud applications.

A modern endpoint security solution must be able to detect in-bound threats via all noted vectors, inspect both disk and memory-resident entities, and detect and prevent both file and file-less threats.

Depth: Detection Techniques

Triaging the spectrum of possible threats requires the use of non-mutually exclusive techniques that serve as a series of filters which, cumulatively, create a sieve via which threats are detected and prevented. Such an approach starts by arbitrating between the known-good and the known-bad, the white and black, leaving a set of files that require further inspection, the

> The use of multiple detection techniques not only improves efficacy, but also the efficiency with which endpoints are protected. Less compute-intensive and more deterministic checks are applied initially with more sophisticated controls used for evaluating the gray list to separate those entities into black or white.

gray. The gray or unknown files, for which there is not a clear initial verdict, require the use of stage-appropriate detection techniques.

The use of multiple detection techniques not only improves efficacy, but also the efficiency with which endpoints are protected. Less compute-intensive and more deterministic checks are applied initially with more sophisticated controls used for evaluating the gray list to separate those entities into black or white. With less files evaluated at a latter stage by more subjective techniques such as behavioral analysis, the likelihood of false positive is reduced. As such, neither the set of detection techniques nor the desired outcomes of improved efficacy and efficiency are mutually exclusive.

Detecting Threats of Known Provenance

Reducing the attack surface area starts, but does not end, with filtering out the known threats while allowing the known-good, whether they are applications to be run, emails to be read, or websites to be visited. A reputation service that is tightly integrated into one's endpoint security product will cover the following entities:

- *Email (IP) reputation* services will catalog the IP addresses for legitimate email servers, reducing the introduction of threats and spam.
- *Website (URL) reputation* services will prevent users from visiting websites known to be used to disseminate threats.
- *File reputation*, based on provenance with respect to the maturity of a file (the period of time for which a file has been known) and frequency (how often the file has been executed and thus trusted by others), can identify those files that are clearly trustworthy by virtue of scoring high on both accounts, and those that are new and unknown and thus require additional vetting. Software reputation also identifies and discards to an exit ramp files known to be malicious.

Such reputation services are not a static list since reputation can change over time. For example, a file obfuscated by being included in a compressed ZIP file will need to have its reputation checked once its true identity has been revealed. And signatures still have a role by matching patterns based on portable executable PE headers with a list of known bad files. Long plagued by expensive scanning, modern endpoint security solutions that employ signatures will have implemented optimizations that only evaluate newly introduced files.

In total these techniques to filter in or out the known good and bad, respectively, reduce the scope of the unknown for improved fidelity.

Detecting Threats of Unknown Provenance

A future-ready endpoint security product will employ machine learning and behavioral analysis as non-mutually exclusive techniques to vet new and unknown files and code before and during execution.

Pre-Execution

Machine learning, based on algorithms trained against massive corpuses of both known good and malicious binaries, learns the attributes, over time, that make an executable trustworthy or not. As such, machine learning is predictive in that it can detect unknown malware by detecting whether a file shares attributes with other pieces of malware, thus thwarting malicious binaries that evade detection by signatures and reputation services. Machine learning is also adaptive—as the algorithm inspects more executables, it literally gets smarter.

During Execution:

To then detect the set of threats which have thus far evaded the aforementioned checkpoints, machine learning and behavioral analysis work in concert as the next set of filters to vet files during runtime. Behavioral analysis evaluates files for more generalized behavior associated with other known threats such as the rapid encryption of files, as is seen with ransomware. Other activities associated with malware and exploits include:

- System changes (e.g., registry, file system, new processes).
- Scripts that inject malicious code.
- Weaponized content that exploits an application vulnerability.
- Memory inspection for malware fragments and corruption of memory spaces utilized by legitimate programs.
- Network connections to/from IPs associated with command and control servers.

While some of these behaviors will evade machine learning, machine learning can also be used for runtime analysis, by watching for lower level behaviors, including the use of system calls and the ways in which such interactions with system APIs are sequenced together. Monitoring these "micro behaviors" detects new and unknown malware based on how a set of binary features are known to have worked together in other pieces of malware.

The complementary nature of behavioral analysis and machine learning to evaluate macro and micro behaviors represents additional layers of filters. While these capabilities have been associated with a high incident rate of false positives due to the difficulty in determining what constitutes malicious behavior, threat research and machine learning have resulted in greater accuracy.

Default Deny with Application Control

In contrast to the aforementioned detection techniques, application control operates on the basis of denying all software by default unless it meets a policy that constitutes a basis of trust. A contemporary endpoint security solution will have a flexible policy lexicon from which trust can be established, including reputation, source, and code signing. Often applied on systems where there is a known and finite set of trusted software and systems that change infrequently, if at all, application control provides a highly deterministic, lockdown approach to protect fixed function systems and servers from intrusion and compromise. Application control can also be appropriate for knowledge worker endpoints allowing end-users to run the applications they want by employing a dynamic whitelist of trusted applications based on the aforementioned policy settings.

Visibility with Detection and Response

While this paper has focused on the preventative controls of a future-ready endpoint security solution, one should assume some threats will continue to evade even the most sophisticated set of layered detection techniques. Indeed, as highlighted in ESG's research, preventative controls do not obviate the need for instrumenting and capturing system activity for post-execution response measures including:

- ***Expediting incident response*** to reduce dwell time and loss of data assets.
- ***Decomposing the attack chain*** including identifying patient zero, the infection point, and understanding attacker methods to fortify defenses against future attacks.

- *Proactively hunting for threats* already present in organizations' environments based on known indicators of compromise (IOCs) and other forms of threat intelligence, using forensics and leveraging endpoint detection and response (EDR).

As such, enterprise-class endpoint security suites will offer optional detection and response capabilities for those organizations appropriately resourced to execute these use cases.

Other Considerations for Modern Endpoint Security

In addition to the concerns already outlined, organizations should also consider the following attributes of a future-ready endpoint security offering:

- *A centralized management console* to reduce the operation cost by providing visibility across an enterprise's entire footprint of endpoints
- *Resource-friendly host agents,* which impose no discernable impact on system performance
- *A judicious use of the cloud* for the dissemination of threat intelligence, entity reputation ratings, and dynamic analysis
- *The incorporation of threat intelligence* to improve an organization's situational awareness as it relates to external events
- *Integrations with complementary security controls* such as network sensors and SIEMs to help security teams coordinate and expedite threat detection and response to thwart attacks and reduce dwell time
- *Foundational best practices* to address common vulnerabilities, including:
  - *Cybersecurity awareness training* to reduce the risk associated with the human vulnerability, which should be conducted regularly to educate all employees, including executives and knowledge, on common attack methods such as spear and whale phishing and email impersonations
  - *Regular application of security updates* to help organization prioritize what systems are updated and protect their critical systems from the most severe operating system and application vulnerabilities.

The Bigger Truth

The rate of innovation across consumer goods such as 4K televisions and smartphones as well as corporate IT solutions has conditioned buyers to seek "next-generation" products. But when it comes to cybersecurity products, the evolving threat landscape and cost of ownership begs for solutions that are more than one generation away from becoming obsolete. As the entry point for many attacks, the endpoint is the front door that must be better secured using modern techniques for today's and tomorrow's threats. The combination of the sophistication of the threat landscape, the expanding attack surface area, the new attack vector opened up by the cloud, and the rate of innovation in detection techniques all contribute to the definition of what comes next for endpoint security.

What comes next for endpoint security should embody a design that is multi-generational by virtue of being based on an architecture that can transcend technology, threats, and end-user computing behaviors for greater efficacy and sustained operational efficiency.

For most organizations, the central role that endpoints play in cybersecurity attacks has led to the evaluation, procurement, and deployment of advanced preventative controls that are often referred to as next-gen antivirus (NGAV). To achieve the desired level of high fidelity, preventative controls should employ multiple detection techniques as a coordinated series of filters. And as endpoint detection and response (EDR) functionality becomes more actionable, prevention, detection, and response controls will be less mutually exclusive over time, allowing more companies to augment prevention with a greater level of visibility. As such, what comes next for endpoint security should embody a design that is multi-generational by virtue of being based on an architecture that can transcend technology, threats, and end-user computing behaviors for greater efficacy and sustained operational efficiency.

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