Solution Showcase

Next-generation Endpoint Security and Cybereason

Date: March 2018 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Since the early days of Internet connectivity, organizations have installed antivirus software on endpoint PCs to protect them against malware. Unfortunately, malware volume and sophistication has increased to the point where AV vendors can't keep up with the latest threats and this has opened many organizations to cyber-attacks and data breaches. Over the past few years, the cybersecurity industry responded with a wide variety of innovative security tools across a continuum of threat prevention, detection, and response. Individual tools are now coalescing into next-generation endpoint security suites for comprehensive protection. In this solution showcase, ESG outlines necessary and optional functionality for consideration in next-generation endpoint security suites and assesses how Cybereason aligns with these requirements.

Overview

Since organizations first deployed browsers on employee PCs and connected corporate networks to the Internet, endpoint security has been synonymous with antivirus software from a handful of vendors. Over the past few years, this direct association has changed, however. Security managers believe that traditional signature-based AV can no longer provide adequate protection because of:

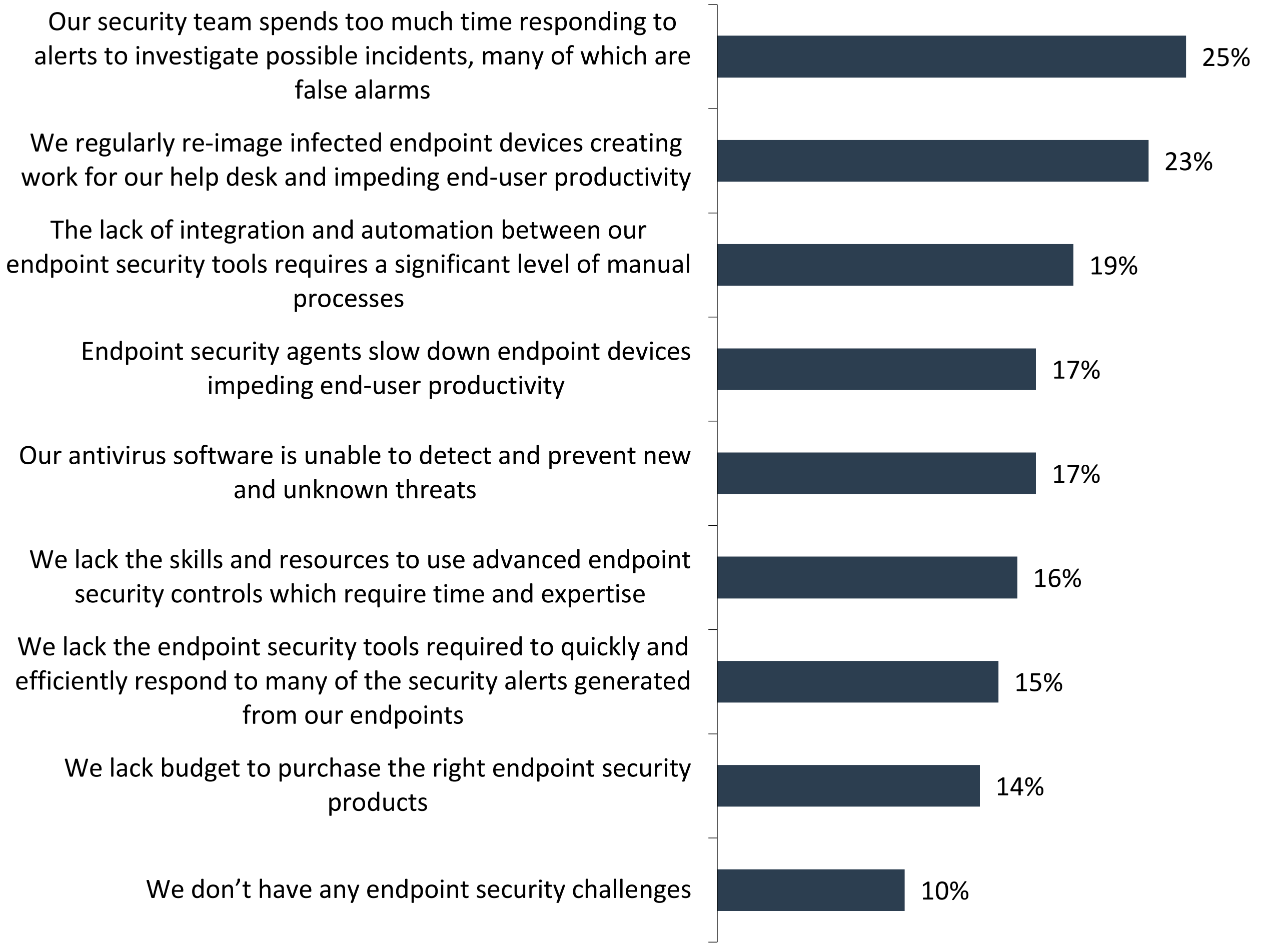
- **Unacceptably low malware detection rates.** As far back as 2014, security research noticed that new types of malware variants often bypassed traditional AV detection technologies. Overall malware detection rates ranged from 50% to 60% in many industry tests. Alarmingly, this means that CISOs could anticipate that 40% to 50% of new sophisticated malware attacks could evade endpoint AV, compromise PCs, and act as a beachhead for advanced cyber-attacks. This was and still is an intolerable situation.

- **Insufficient analytics for incident response.** In the past, AV management provided a map of all nodes under management, signature distribution, and policy management tools for configuring firewalls, port controls, etc. Reporting functions were somewhat limited, however, focused on the number of viruses discovered, deleted, and quarantined. CISOs realize today that, regardless of the controls they deploy, some malware will sneak through, so they need continuous monitoring and visibility of endpoint behavior to identify suspicious behavior and malicious operations (i.e., malops) indicating a compromised system and/or a multi-staged attack in progress. Traditional AV does not provide this type of oversight.

These product shortcomings tend to result in numerous endpoint security challenges (see Figure 1). For example, cybersecurity professionals point to endpoint security challenges such as prioritizing and investigating a tsunami of security alerts, constantly reimaging infected systems, and figuring out how to manage an army of disconnected endpoint security point tools.[1]

Figure 1. Endpoint Security Challenges

In your opinion, which of the following presents the most significant endpoint security challenges to your organization? (Percent of respondents, N=385, two responses accepted)



Source: Enterprise Strategy Group

The Endpoint Security Continuum

Given the shortcomings of traditional AV, the security industry responded with new "next-generation" endpoint security point tools in two primary areas:

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 zero-day exploits.

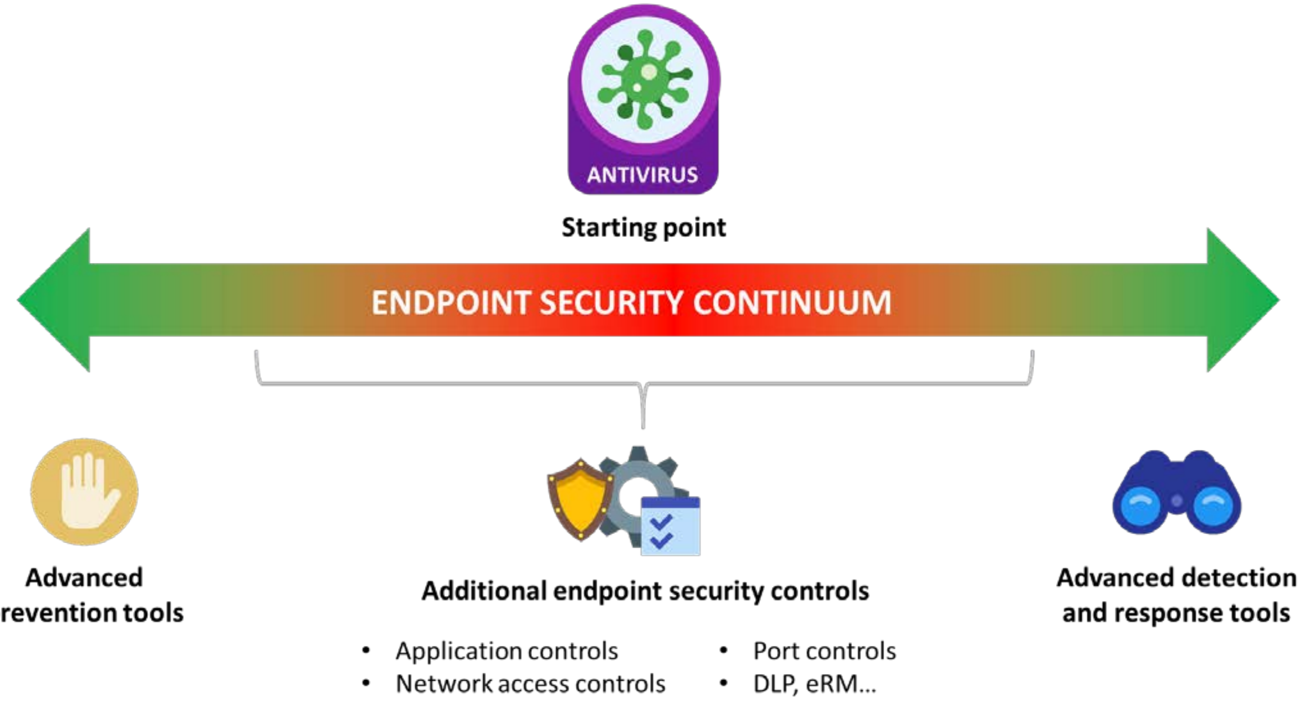
2. **Advanced detection and response technologies** designed to monitor and report on all endpoint system activities while using a variety of technologies (i.e., algorithms, static/dynamic analysis, threat intelligence correlation, etc.) to detect anomalous/suspicious behavior (Note: Tools in this category are sometimes referred to as endpoint

[1] Source: ESG Master Survey Results, *The Evolution of Endpoint Security Controls and Suites*, November 2017.

detection and response solutions, or EDR). These tools provide various methods for incident response and system remediation (i.e., terminating a network connection, halting a process, wiping a file, etc.).

ESG believes that next-generation endpoint security should include both sets of capabilities across an overall endpoint security continuum, including advanced prevention, EDR, and other types of endpoint security controls and capabilities (see Figure 2). According to ESG research, enterprise organizations agree—87% of organizations said that they consider a comprehensive endpoint security suite from either a single next-generation vendor or a single established vendor the most attractive choices when they consider new endpoint security controls for their organizations.[2] Of course, these suites are intended to replace traditional AV software (and any other endpoint security point tools) with a comprehensive endpoint security solution designed for threat prevention, detection, and response.

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

Next-generation Endpoint Security Suite Priorities

Since the endpoint security market is composed of a mix of veteran and startup vendors, next-generation endpoint security suites offer different features and functionality. This can make it confusing to understand which capabilities are most important and which are secondary. Based upon years of qualitative and quantitative research on endpoint security, ESG suggests that organizations break down next-generation endpoint security suite functionality into two categories: required and optional functionality.

Required Functionality for Next-generation Endpoint Security Suites

Organizations want better endpoint security protection and analytics but they also need next-generation endpoint security technologies to be easy to deploy and operate. Based upon these criteria, cybersecurity professionals should demand the following next-generation endpoint security functionality regardless of their choice of vendor:

[2] ibid.

1. **High-efficacy malware prevention everywhere.** This can be based upon layered endpoint security technologies (i.e., AV signatures, heuristics, IoC comparisons, etc.) or solely on machine learning algorithms or other types of new defenses. Regardless of the technologies used, leading solutions can detect and block nearly 100% of known malware and 90%+ of zero-day file and fileless malware while maintaining low false positive rates. Leading tools will also provide capabilities for real-time and on-demand scanning.

2. **EDR capabilities.** CISOs should choose carefully here as there is a lot of product variation in EDR tools. EDR tools should collect, process, analyze, and retain endpoint security data for a variety of activities including security analysis, forensic investigations, threat hunting, etc. Beyond analytics and data queries, leading tools should also offer built-in analytics to identify suspicious/malicious behavior that may evade human analysts. Finally, EDR tools should be able to monitor behavior across systems to detect malicious "kill chain" activities like network reconnaissance, lateral movement, escalation of privileges, etc.

3. **Anti-exploit technologies.** Anti-exploit technology can be thought of as a modern version of host-based intrusion prevention (HIPS) used to block in-memory and common application-layer attacks. Blocking ransomware comes to mind here. Note that anti-exploit technologies can be fairly geeky so CISOs should look for options that are easy to configure and operate.

4. **A single endpoint agent.** Leading products should be based upon a single, easy-to-deploy and -operate agent. This can help security and IT operations teams balance security, desktop administration, and system performance.

5. **Centralized management.** All endpoint security functionality should be controlled by a centralized management system. For separation of duties, centralized management must support multi-factor authentication, customized views/dashboards, and role-based access control.

6. **Hybrid deployment options.** Organizations should be able to pick and choose whether the endpoint security management plane lives on-premises or in the cloud, or is made up of a combination of both.

7. **Remediation capabilities.** When an endpoint gets infected, security and IT operations need the ability to quarantine the system, delete registry keys, or terminate malicious processes. This should help security teams accelerate incident response and greatly decrease the number of systems requiring a full reimaging.

Next-generation endpoint security tools must also integrate with other types of security controls and analytics. For example, EDR tools often interoperate with SIEMs for security operations and/or network behavioral analytics systems for threat detection. Many firms also align endpoint security technologies with cyber threat intelligence (CTI) for blocking malicious indicators of compromise (IoCs) and comparing suspicious endpoint behavior with what's happening with the threat landscape "in the wild."

To gain an objective measurement of product efficacy, it may also be worthwhile to demand that next-generation endpoint security vendors participate in third-party tests. Note that these tests should be used as input for decision making and not as a substitute for rigorous in-house product testing and proof-of-concept projects.

Optional Functionality

Aside from the list above, organizations will have their own requirements based upon size, industry, skill sets, etc. Furthermore, different vendors will pad next-generation endpoint security suites with additional functionality to differentiate their products from competitors. CISOs should align organizational requirements with optional endpoint security functionality including:

1. **System and application controls.** Some organizations have adopted things like port controls to prevent data exfiltration via thumb drives while others have implemented application white listing/black listing to block the installation or execution of rogue programs. These types of controls may be an attractive option for decreasing the attack surface.

2. **Asset and configuration management features.** Some endpoint security tools can report on the applications/ versions and operating system configurations on endpoint systems. This information can be useful for improving the efficiency of vulnerability and patch management tasks.

3. **DLP.** A few endpoint security tools bundle in DLP capabilities. This may be an attractive package for security teams responsible for both endpoint and data security.

Note that this list does not include traditional endpoint security capabilities like network firewalls or hard disk encryption. This functionality is now offered as part of modern operating systems so add-on endpoint security suite functionality is no longer necessary.

Next-generation Endpoint Security from Cybereason

There are many new endpoint security options available so organizations must put in ample time to research, evaluate, and test products that can meet their unique requirements. As part of this process, CISOs may want to consider Cybereason when evaluating next-generation endpoint security suites. The Boston-based company has a growing customer base around the world. The company was founded by former members of the Israel Defense Forces' 8200 unit, an elite group that specializes in cybersecurity with strong knowledge of hacking operations, and has added similar expertise from many nations over the years with offices today in the USA, UK, Japan, and Israel.

Over the last few years, Cybereason used its knowledge of the threat landscape as well as effective cybersecurity operations to build a next-generation endpoint security suite.

While Cybereason may not be as well recognized as other vendors, its platform provides all required functionality (defined by ESG) as follows.

1. **Layered defenses for high-efficacy malware detection/blocking.** Cybereason uses a layered approach for malware prevention. First, pedestrian malware is blocked by antivirus signatures. Sophisticated malware that bypasses this layer is then pushed through pre- and post-execution inspection. Pre-execution inspection extracts file features and then examines them against proprietary machine learning algorithms to detect files that fit a malware profile. Files that move beyond this detection engine are then pushed through a dynamic behavioral analysis filter that looks for known malicious behavior like illicit changes to registry settings or file encryption operations. Dynamic behavioral analysis is especially effective for blocking fileless malware using PowerShell, WMI, and scripting languages and for blocking never-before-seen ransomware. Cybereason supports capabilities for real-time and on-demand scanning.

2. **Strong EDR capabilities designed to detect attacks in progress.** Cybereason started in the EDR space shortly after its founding in 2012. Rather than simply collect endpoint data, Cybereason EDR is designed to assess and detect behaviors associated with actual cyber-attacks. Furthermore, Cybereason EDR is anchored by a graph database to collect, analyze, and correlate millions of simultaneous events. This provides the capability to track malicious behavior across individual systems as attackers' progress through a kill chain for full attack lifecycle detection. As part of this process, Cybereason also integrates with threat intelligence feeds to correlate internal behavior with the tactics, techniques, and procedures (TTPs) used by cyber-adversaries. To keep up with sophisticated attacks,

Cybereason also provides pre-configured malicious activity models that can help security analysts detect sophisticated and stealthy attacks. Finally, Cybereason provides a feedback loop model from detection and response back to prevention rules. When malops are discovered, Cybereason can "tag" the malicious behavior and then use the tag to find or block similar behavior on other systems in the network.

3. **Anti-exploit technologies for in-memory and application layer attacks.** Cybereason provides behavior-based anti-exploit technologies for attacks on common applications like browsers, Office applications, Adobe applications, Java, etc. While the list is not exhaustive, it does cover the primary exploits used by cyber-attackers. Anti-exploit technology is also used for effective detection and blocking of ransomware.

4. **A single endpoint agent.** Cybereason next-generation endpoint security is based upon a single endpoint agent.

5. **Centralized management for multiple use cases.** Cybereason provides one user interface for all threat prevention, detection, and response operations. Management functionality also supports multi-factor authentication, customized views/dashboards, and role-based access control.

6. **Hybrid deployment options.** Cybereason can be deployed on-premises or in the cloud. For organizations needing staff/skills augmentation, Cybereason provides 7 by 24 managed detection/response (MDR) services on its own and works with MSSPs to supplement its services with MDR capabilities.

7. **Various and simple remediation capabilities.** Cybereason offers what it calls, "single click remediation," which can be used to quarantine a system, terminate processes running in memory, delete registry keys, etc. While this won't eliminate reimaging, it can significantly reduce the number of systems requiring reimaging.

Cybereason technology provides integration capabilities through its set of published APIs. Customers use these APIs to interoperate Cybereason with SIEM, SOAR, network behavioral analytics, etc.

In essence, Cybereason can act as a full system of records for endpoint systems across an organization, enabling visualization, investigations, and threat hunting by users and/or service providers. The goal? Preventing cyber-attacks, offering strong analytics, and providing remediation capabilities without disrupting business operations.

Caveats

While Cybereason offers all the required functionality for a next-generation endpoint security suite, it is important to note:

- Cybereason does not currently offer system controls, and/or traditional endpoint security controls like network firewalls or full-disk encryption.

- Cybereason can be configured to provide cursory application controls but should not be considered a full solution for application white listing/black listing.

- Endpoint asset and configuration management data can be accessed via the Cybereason API. While some customers use the API to query this information through other security and IT operations tools, Cybereason does not provide native capabilities for asset, configuration, vulnerability, or patch management.

- ESG did not perform any type of hands-on testing of Cybereason technologies. As previously stated, organizations in need of a next-generation endpoint security suite should thoroughly test the efficacy, functionality, and operational capabilities before purchasing or deploying any endpoint security solution.

The Bigger Truth

It’s clear that traditional endpoint security controls are no longer adequate safeguards against unique file-based and fileless malware or sophisticated cyber-attacks. Before turning to new types of endpoint security controls, however, organizations should understand what types of endpoint security functionality should be considered a requirement and which capabilities should be classified as optional.

These lists will vary based upon a number of factors including organizational size, industry, and location, as well as security resources and experience. In general, however, at the very least, ESG believes that next-generation endpoint security suites should offer high-efficacy malware detection/blocking, anti-exploit technology, EDR capabilities, a single endpoint agent, centralized management, hybrid deployment options, and remediation capabilities.

Based on these requirements, CISOs should consider Cybereason when evaluating next-generation endpoint security suites. Organizations should conduct in-depth testing to ensure that Cybereason (or any other next-generation endpoint security suite solution) can block the majority of malware threats, provide thorough EDR capabilities, scale to meet enterprise needs, and deliver a simple yet effective management model.

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