Enterprise Strategy Group | **Getting to the bigger truth.™**

White Paper

An Adaptive and Layered Approach to Endpoint Security

Requirements for the Next Generation of Endpoint Protection Platforms

By Doug Cahill, ESG Senior Analyst; and Jack Poller, ESG Analyst

June 2017

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

Contents

Executive Summary

The increased awareness around the need to fortify endpoint security is well-founded: Endpoints play a central role as the entry point through which many cybersecurity attacks are launched. The cybersecurity kill chain, which models the lifecycle of an attack, details how bad actors leverage endpoints to exploit human and software vulnerabilities, deliver and install threats, and eventually take further action to achieve their objectives.

With contemporary cloud-first strategies, endpoints are even further exposed by being frequently used outside the corporate network perimeter, accessing cloud and on-premises applications over insecure networks, creating a fluid perimeter. This expansion of the attack surface area highlights that a network-centric orientation of cybersecurity, one that is predisposed to catching threats "on the wire," is no longer sufficient. An adaptive and layered defense-in-depth approach to endpoint security to protect corporate assets is an essential element of a cybersecurity strategy and architecture.

The need to layer on additional controls has resulted in an endpoint security continuum via which organizations have added advanced preventative controls and/or advanced detection and response controls on top of their existing endpoint protection platform (EPP) suites. Many organizations have opted to start with additional preventative controls, including those which employ machine learning to detect and prevent the introduction of new and previously unknown threats.

Those who start by adding such preventative controls may very well also travel in the other direction along the continuum by employing endpoint detection and response (EDR) solutions to gain greater visibility. This dynamic of adding disparate controls that entail the deployment of separate agents and the use of multiple management consoles is born out of tactical necessity to improve endpoint security posture, but comes at the cost of adding operational complexity.

…history is repeating itself with newer prevention, detection, and response controls being aggregated into a new generation of endpoint protection platform (EPP) suites that deliver both improved efficacy and operational efficiency.

ESG believes history is repeating itself with newer prevention, detection, and response controls being aggregated into a new generation of endpoint protection platform (EPP) suites that deliver both improved efficacy and operational efficiency. This paper explores the conditions that necessitate such a solution as well as the requirements of new generation EPPs organizations should consider when evaluating endpoint security offerings.

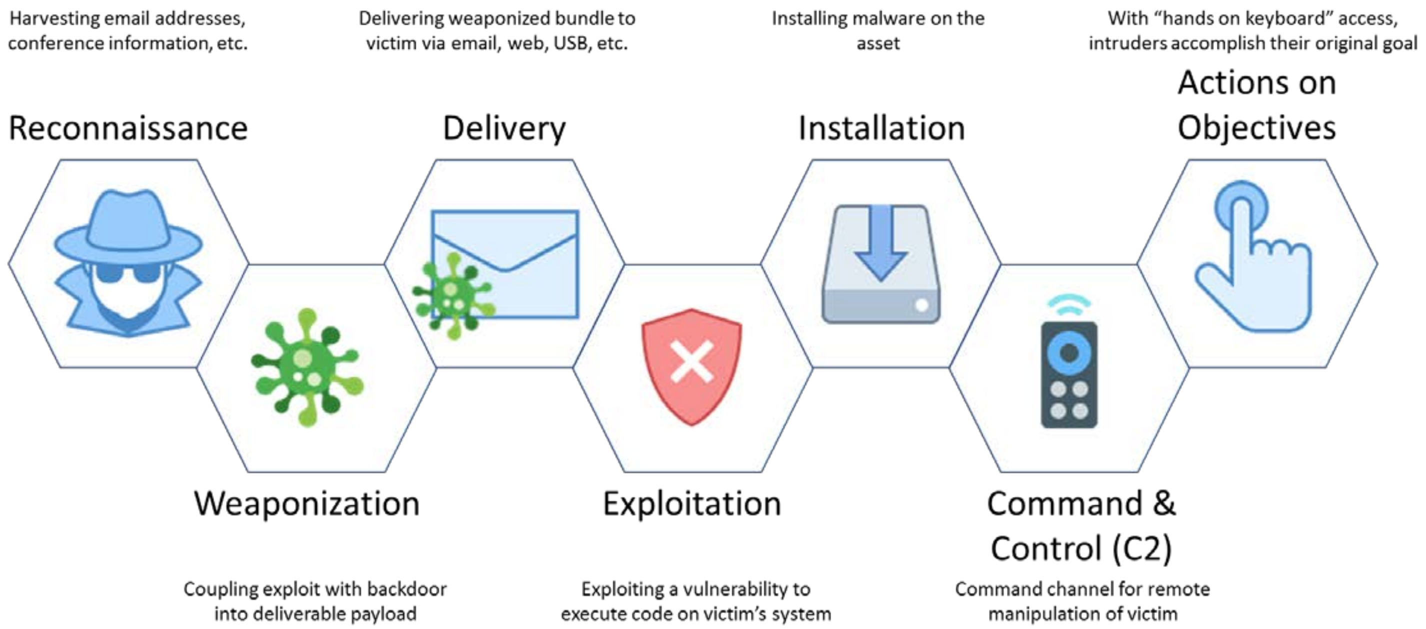
The Endpoint Security Imperative

Multiple factors contribute to making the principle of securing the endpoint an imperative for all organizations. Endpoints represent the prevalent entry point for infections, and with the rise of mobile-first and cloud-first initiatives, endpoints often operate outside of the secure confines of the protected corporate network. Simultaneously, malicious actors are improving their knowledge, their capabilities, and the diversity of their endpoint-targeted threats. Given the factors and dynamics discussed below, endpoint security has become a priority to achieve the desired outcome of protecting corporate assets from compromise.

The Endpoint's Starring Role in Cybersecurity Attacks

The endpoint plays a starring role in models that depict the behavior of typical cyber-attacks, such as Lockheed Martin's Cyber Kill Chain, which identifies the seven steps malicious actors must complete in order to achieve their objectives (see Figure 1). In the kill chain model, endpoints are involved in the last five steps: delivery, exploitation, installation, command and control, and actions on objectives.

Figure 1. Lockheed Martin's Cyber Kill Chain


Harvesting email addresses, conference information, etc.
Reconnaissance
Delivering weaponized bundle to victim via email, web, USB, etc.
Delivery
Installing malware on the asset
Installation
With "hands on keyboard" access, intruders accomplish their original goal
Actions on Objectives
Weaponization
Coupling exploit with backdoor into deliverable payload
Exploitation
Exploiting a vulnerability to execute code on victim's system
Command & Control (C2)
Command channel for remote manipulation of victim

Source: Enterprise Strategy Group, 2017

A common attack method is to exploit vulnerabilities in both endpoint operating systems and software commonly used by end-users. Adversaries also exploit human gullibility, which results in end-users falling prey to spear phishing, email impersonation, and drive-by downloads to set up the next step of the attack chain. In fact, 43% of breaches involved social attacks—pretexting, phishing, bribery, website, phone, in-person, and email.[1] Phishing—attempting to obtain sensitive information by masquerading as a trustworthy entity in electronic communications—was the top social attack tactic, found in 93% of breaches and other cybersecurity incidents. Proving the validity of the kill chain model, 95% of phishing attacks that led to a breach were followed by some form of software installation.[2] Even with organizations instituting end-user phishing awareness training and testing, phishing has surged in recent years. This suggests that cybercriminals are "living off the land," using proven successful and easy-to-exploit tactics targeting the endpoint and, specifically, the end-user.

Further complicating endpoint security are mobile-first and cloud-first initiatives that have fueled knowledge worker mobility and the prevalent use of cloud services that have made the perimeter amorphous. Users can access applications and data from anywhere in the world, using insecure Wi-Fi or cellular networks without the benefit of protection from the corporate firewall. Likewise, inter- and intra-cloud exchange of corporate data occurs outside of the physical corporate network. An approach is needed that fortifies the entities that access corporate data—i.e., endpoints and the users who operate them.

Diversified Threat Types

It is no surprise that bad actors tend to run the same play that has a track record of success. Why invest in new tactics when human gullibility causes so many users to click on attachments and links in emails? While attack methods and vectors such as spear phishing emails are commonly employed, the actual threat types they deliver can be file-based, file-less, or a combination of the two. Exploring the functional requirements of a next generation of endpoint protection platforms requires an understanding of the type of threats that put endpoints at risk.

[1] Source: *Verizon 2017 Data Breach Investigations Report, 10th Edition*, April 2017.
[2] Source: Ibid.

File-Based Attacks

File-based attacks, often referred to as malware, are self-executing binaries such as viruses, worms, spyware, and Trojan horses. These types of malware can take the following forms:

- **Common/mass malware.** File-based attacks that have been previously detected and for which signatures exist.
- **Targeted malware.** Malware engineered specifically for a single organization and for which a signature does not yet exist.
- **Mutated malware.** Malware that obfuscates changing its cryptographic hash value to avoid detection.

Fileless Attacks

Fileless attacks, often referred to as “living-off-the-land” attacks, use allowed and authorized applications to introduce an infection outside of the file system. Fileless attacks can take the following forms:

- **Memory-based.** Attacks which employ techniques to hijack the memory space used by a legitimate application to execute.
- **Weaponized-content.** Attacks which employ content specific to an application such as a macro or PDF file.
- **Script-based.** Attacks written in scripting language such as JavaScript or PowerShell.
- **Registry-based.** File-less threats which reside in the operating system’s registry.
- **Rootkits.** Kernel level attacks are disk-resident, but not located on the operating system’s file system.

Threat Type Spotlights

- **Multi-stage/component.** Threats are broken down into multiple components and delivered in multiple stages to evade detection. The components of such an attack type may include both file and fileless elements including, for example, fileless attacks which exploit a software vulnerability to install malware.
- **Ransomware.** The epidemic levels of ransomware incidents in 2016 and the scope of the Wannacry attack in May of 2017 have made ransomware a top-of-mind concern for all organizations. Ransomware attacks are becoming more sophisticated with file-based, fileless, and multi-stage/component variants being employed by cybercriminals.

Funded, Not Resourced

Increased awareness of the threat landscape and the impact on revenue loss, loss of IP, damage to brand reputation, and interruption of business operations has elevated cybersecurity to preeminence. Thus, it’s no surprise that, per ESG research, for the sixth year in a row, strengthening cybersecurity tools and processes has appeared at the top of the list of most important IT initiatives reported by respondents.[3]

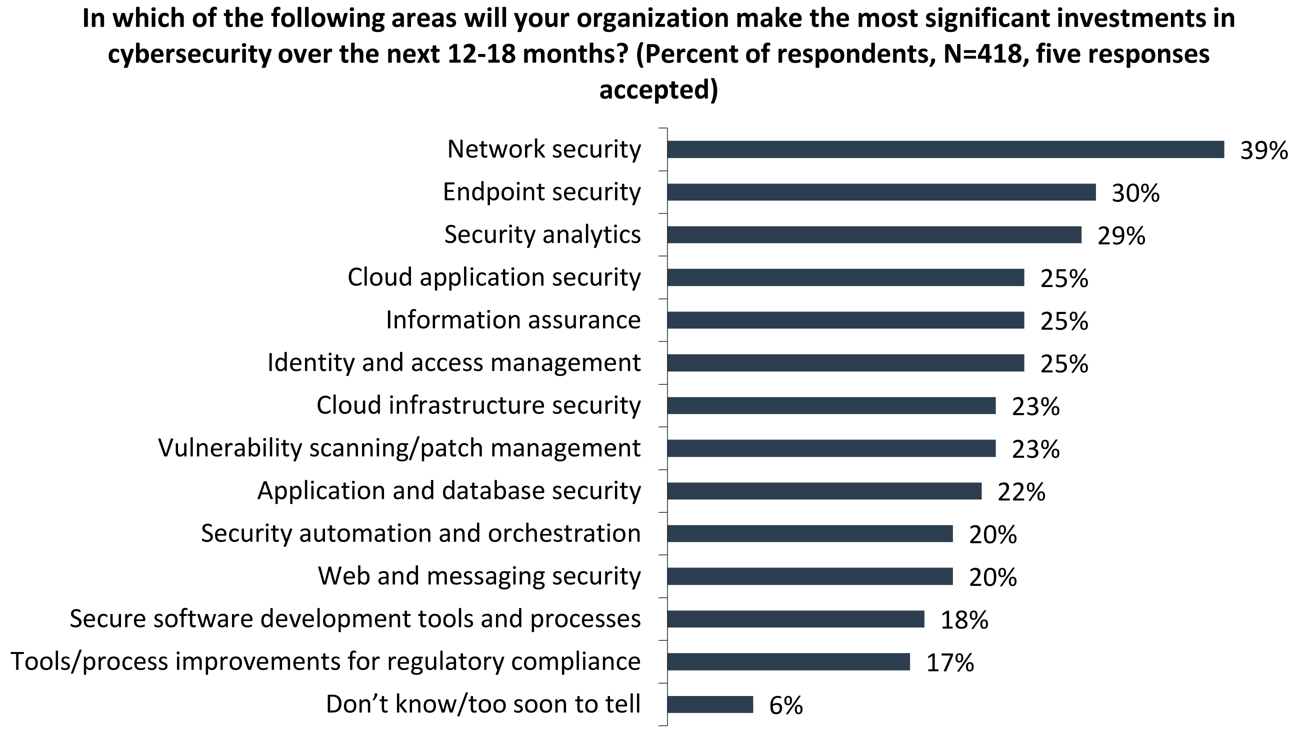
Organizations are acting on cybersecurity initiatives, with 69% of those surveyed by ESG indicating they are increasing their cybersecurity investments in 2017. Thirty-two percent of respondents said that increasing cybersecurity was the most

[3] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

important business initiative driving their organizations' technology investments in 2017, making it the most-cited response.

Within cybersecurity, endpoint security is one of the areas where many organizations have cited an intention to increase their investments. (see Figure 2).[4]

Figure 2. Plans for Cybersecurity Investment



Source: Enterprise Strategy Group, 2017

However, successfully executing on funded cybersecurity initiatives is often hampered by a lack of resources. 2017 continues the longstanding trend of global cybersecurity skill shortages. Per ESG research, 45% of organizations indicate that they have a problematic shortage of cybersecurity skills.[5] These results indicate that, in addition to effective threat detection and prevention, efficiency is a critical success factor for endpoint security initiatives.

Next-generation Endpoint Security Requirements

The ever-evolving threat landscape coupled with the lack of skilled cybersecurity resources highlight the need for next-generation endpoint protection platforms (EPPs) to provide "efficient efficacy." When it comes to efficiency, solutions need to be lightweight, minimizing their impact on endpoint performance with respect to CPU and memory consumption. Next-generation EPPs also need to be easy to implement across organizations spanning tens of thousands of users and hundreds of thousands of devices.

The efficacy charter of a next generation EPP is to prevent known and unknown threats while simultaneously minimizing the number and impact of false positives. To do so, next-generation EPPs will employ a range of technologies for advanced prevention (see Table 1).

[4] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.
[5] Source: Ibid.

Table 1. 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, 2017

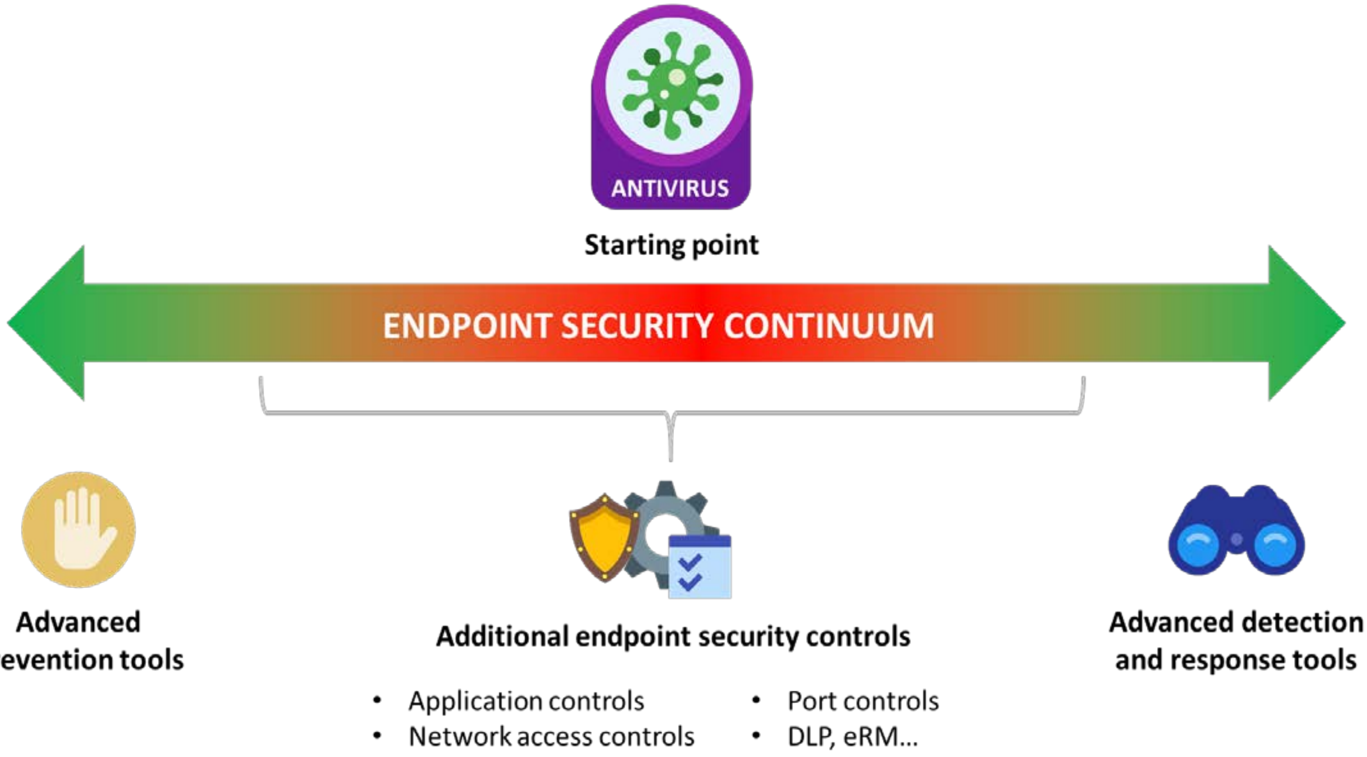
Smaller organizations as well as those with an acute shortage of resources will want to automate endpoint protection as much as possible. As time allows, cybersecurity personnel can review incident analysis reports for visibility into threat impact and behaviors. To do so requires multiple controls brought to bear in a modern implementation. Automated threat response and better context are essential attributes of next-generation endpoint security.

Automated threat response and better context are essential attributes of next-generation endpoint security.

The Continuum Leads Back to Suites

The new generation of EPPs marks the second time disparate endpoint security controls are being consolidated into suites. The first generation of EPPs brought together antivirus controls to detect and prevent known viruses from infecting desktops and laptops, anti-spyware to prevent spyware, anti-spam to filter spam from users' email, and personal firewalls to prevent unauthorized network communication. As threats became more sophisticated, additional discrete controls were developed to fill the void in traditional EPPs, such as application whitelisting to improve threat prevention by ensuring only known good applications are authorized. More recently, preventative controls have also been enhanced with machine learning algorithms to analyze files and predict the intent of potential threats. Along with other technologies, these are the controls on the prevention side of the endpoint security continuum (see Figure 3).

Figure 3. 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, 2017

Endpoint detection and response (EDR) tools that collect, store, and analyze endpoint telemetry data are often employed as part of a broader security analytics implementation and represent the other end of the endpoint security continuum. Heuristics, machine learning, and other advanced techniques are employed to analyze endpoint event data to detect anomalies and threats, and then generate alerts and mitigation responses based on specific behavior patterns and indications of compromise (IoCs).

These techniques and technologies build on top of each other, representing a defense-in-depth approach for endpoint security. Signatures, for example, still play an important role for the initial arbitration of files by matching cryptographic hash values with a database of both known good and bad software.

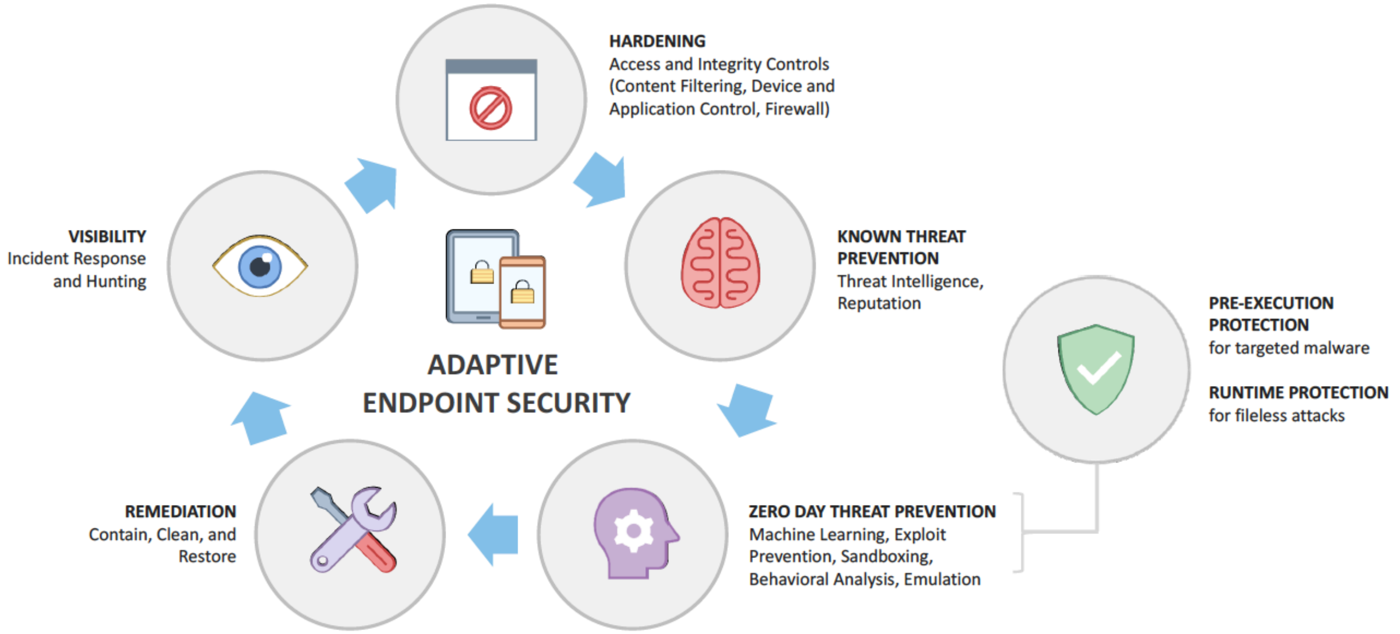
> ….endpoint security solutions are coming full circle with new EPP suites consolidating an updated set of controls into a single implementation.

This represents a technology adoption dynamic ESG refers to as the endpoint security continuum via which organizations employ additional, discrete preventative or EDR controls to augment their existing endpoint security tools and techniques. But the use of discreet tools has once again increased complexity. In response, endpoint security solutions are coming full circle with new EPP suites consolidating an updated set of controls into a single implementation. In addition to increasing comprehensiveness via feature aggregation, next-generation EPPs are characterized by contemporary, cloud-centric implementations.

Layered Controls

As discussed previously, inbound threats include malicious files (malware), a variety of fileless attacks, and hybrid threats that are both multi-stage and multi-component. Users can encounter threats in email, in file attachments, on websites, and elsewhere. As such, a layered approach employs the right control at the right time, relative to the stage of the attack chain and based on the threat vector and threat type, to maximize efficacy. Requisite controls include those that maintain system integrity via hardening, prevent both known and zero-day threats, automate remediation, and enable detection and response (see Figure 4).

Figure 4. Layered Controls for Adaptive Endpoint Security


HARDENING
Access and Integrity Controls (Content Filtering, Device and Application Control, Firewall)
KNOWN THREAT PREVENTION
Threat Intelligence, Reputation
PRE-EXECUTION PROTECTION
for targeted malware
RUNTIME PROTECTION
for fileless attacks
ZERO DAY THREAT PREVENTION
Machine Learning, Exploit Prevention, Sandboxing, Behavioral Analysis, Emulation
REMEDIATION
Contain, Clean, and Restore
VISIBILITY
Incident Response and Hunting
ADAPTIVE ENDPOINT SECURITY

Source: Enterprise Strategy Group, 2017

Hardening

System integrity controls and access filters harden endpoints by maintaining the integrity of the device, operating environment, and data to reduce the attack surface area. These controls include:

- Web filtering—preventing access to websites via which threats, malware and fileless, would be downloaded, mitigating drive-by downloads that may be part of a phishing campaign.
- Application control—deciding which applications are allowed or prevented from executing.
- Device control—dictating which actions are allowed or prevented on the device, including accessing USB ports, USB removable storage media, and data copy polices for data loss prevention.
- Personal firewall (PFW)—controlling what network ports can be accessed.
- File controls—maintaining the integrity of the file system.
- Data encryption—protecting data from unauthorized access and centralizing the management of native encryption controls (e.g., Windows BitLocker and MacOS FileVault) across heterogeneous endpoint operation systems.

Known Threat Prevention

While many are understandably concerned with the need to detect and prevent never-seen-before-in-the-wild threats (i.e., zero days), bad actors still “rinse and repeat” their use of threats that have been successful, are thus known, and can be thwarted provided the right set of controls are applied. A threat database containing known good and bad files, URLs, and IP addresses serves as an initial checkpoint to allow access to legitimate websites and IP addresses and the execution of benign executables, while blocking access to and the execution of those addresses and files, respectively, known to be malicious. However, with fast evolution of the threat landscape and attacker tactics, such signature-based techniques alone are insufficient to detect and prevent new and unknown threats, thus requiring additional controls.

Zero Day Threat Prevention

With known good files allowed to run and known malware prevented from doing so via the use of pattern matching, new and unknown objects, files, and content, travel down the funnel and need to be inspected by additional controls before execution, and then during runtime.

- **Machine learning**—analysis of binary attributes shared with a statistically significant set of known bad malware and known good software to predict and prevent zero day threats from executing.

- **Exploit-prevention**—protection of memory and vulnerable applications such as browsers, document readers (Adobe Acrobat), media files (e.g., Adobe Flash), and runtime environments (e.g., Java) from being compromised.

- **Sandbox**—runtime analysis of the behavior of new and unknown objects in a protected sandbox evaluating for malicious behavior. Sandboxes can be configured to run in blocking mode to prevent the execution of files determined to be malicious and in monitor mode to observe and capture runtime behavior.

- **Behavioral and process analysis**—Because known applications can be exploited and used for attacks, continuous process monitoring and behavior analysis is necessary to detect such attacks—for example, monitoring the Powershell process for attempts to modify protected system files or the system configuration. Such analysis of processes should be continuous in the event a seemingly common and benign file, script, or macro eventually exhibits malicious behavior.

Remediation

Remediation controls fix changes to the system caused by threats and exploits, especially those detected by sandboxing, behavioral and process analysis, and event analysis. Controls include:

- **Last known good state**—capturing and rolling back to the last known good state before modification by malicious actors.

- **Journaling**—capturing and rolling back unauthorized changes to file systems or configuration databases. This can also be used to determine the first change that compromised the system.

- **Alerting**—alerting cybersecurity and system administrators for manual remediation upon detection of unauthorized behavior.

- **Automated remediation**—automatically implementing measures to prevent malware from communicating, to remove malware, and to remove the artifacts of an attack.

Visibility

While some stealthy threats will bypass prevention, the continuous monitoring, recording, and analysis of endpoint activities can provide early visibility into compromises and enable response measures to prevent breaches. Controls include:

- Endpoint activity sensor—records events with enough detail to enable post-incident playback and analysis.
- Advanced threat detection and analysis—applies advanced analysis techniques, including behavioral analysis and machine learning, on suspicious and anomalous endpoint events to detect attack activities.
- Post-incident response analysis—analyzes incidents to foster an understanding of the behavior of threats, enabling organizations to further harden configurations and update policies and procedures, which improves endpoint security posture.

Cloud-centricity

The next generation of EPP suites will make judicious use of the cloud to provide the following substantial benefits:

- Security-as-a-service (SECaaS)—a security-as-a-service (SECaaS) implementation eliminates the need for on-premises resources, and automatically scales on demand, lowering operational costs, and reducing time to deployment.
- Cloud-based analytics—leverage cloud-based computational resources for advanced analytics to predict, detect, and prevent future attacks.
- Threat intelligence—centralized, cloud-based threat intelligence fosters expedited information sharing across all subscribers, reducing time to detection and prevention, and improving the security posture for all subscribers.

Truly Integrated

Comprehensive and complete integration is essential for operational efficiency. Next-generation EPPs will offer the following levels of integration:

- Endpoint integration—a high-performance single agent with a small footprint is needed to minimize end-user and device impact.
- Converged console—efficient operation with limited cybersecurity resources necessitates that next-generation EPP suites have visibility and control over all endpoints within the organization from a single converged console.

Bitdefender GravityZone Next-generation Endpoint Suites

Bitdefender GravityZone is a next-generation endpoint security suite that meets the requirements of a layered, adaptive endpoint protection platform by balancing security efficacy, manageability, and performance. GravityZone's capabilities and implementation can be summarized as follows:

Hardening to Reduce the Attack Surface

Bitdefender reduces the attack surface with a set of controls that protects against malicious websites and hardens the configuration of endpoints.

- **Web filtering**—GravityZone blocks access to malicious and fraudulent web pages by inspecting the URL, web traffic (http, https, and SSL), and web content to prevent malicious content from being downloaded to the endpoint.

- **Firewall with intrusion detection and prevention**—personal firewall that automatically detects and blocks attempts to infiltrate endpoints over the network.

- **Device control and USB scanning**—minimizing risks of infections and data loss by scanning USB mass storage devices before use, and preventing file transfers.

- **Application whitelisting**—policies that govern the use of approved and trusted applications.

- **Data security**—The ability to centrally manage native OS full-disk encryption technologies—Windows BitLocker and FileVault 2 for Mac.

Multi-Faceted Threat Prevention

GravityZone employs a rich set of techniques to detect and prevent known and unknown threats. Bitdefender's large threat intelligence database is the first line of defense to prevent access to malicious destinations and the execution of known malware. To detect and thus prevent zero day threats, GravityZone brings to bear a series of advanced controls that can be configured in adaptive manner. These technologies are applied pre-execution and during runtime as follows:

Pre-Execution Controls

In addition to the controls employed to reduce the attack surface area, including web filtering, GravityZone uses:

- **Machine learning**—By extracting and analyzing tens of thousands of static and dynamic features, GravityZone's machine learning algorithms enable the detection and prevention of new and unknown threats. Bitdefender employs both cloud-based and local machine learning models. It uses supervised machine learning algorithms trained against clean files to enhance accuracy and reduce false positives.

- **Hyper Detect**—A combination of machine learning models and behavioral analysis techniques trained to detect advanced, sophisticated attacks before execution including mutated malware, memory-based attacks, weaponized documents, Powershell scripts, and other hacking tools.

- **Endpoint integrated Sandbox**—This layer protects against advanced threats by automatically submitting suspicious files from the endpoint to a cloud-based sandbox for the analysis of malicious intent. Suspicious files are blocked from execution and removed upon conviction. Optionally, a monitor mode can provide insight into the malicious nature of a file to gather forensics and perform offline remediation.

Runtime Controls

- **Anti-Exploit**—protects against both unpatched and zero day vulnerabilities by detecting exploit techniques such as stack pivots and return-oriented-programming (ROP).

- **Process Inspector**—continuously monitors all running processes to detect anomalous behaviors such as attempts to disguise the type of process, execute code in another process's memory space, and more. This approach is applied to both the process(es) associated with new and unknown binary files as well as legitimate applications that may be exploited for a fileless attack. Process Inspector also allows for automated remediation.

As more multi-stage attacks are perpetrated by cyber adversaries, including those that include both malware and fileless threats, multiple runtime controls, such as those provided by the Bitdefender GravityZone offering, become more relevant to detect these stages and components and thwart such attacks.

Closed-loop Remediation

Bitdefender GravityZone can return an endpoint to its last known good configuration should malware make unauthorized system changes.

Bitdefender GravityZone provides remediation capabilities such as alerting, as well as advanced journaling and rollback functionality that works in concert with its Process Inspector runtime threat detection control. When a process has been determined to be malicious, GravityZone terminates the running process, rolls back any unauthorized system changes, and returns an endpoint to its last known good configuration. GravityZone can also quarantine, disinfect, and delete malicious files, preventing additional damage and halting the lateral spread of malware.

Threat Visibility and Post-incident Response

GravityZone's HyperDetect and Sandbox analysis provide early visibility into suspicious activities and the behavior of threats. Policies can be tuned to optimize threat detection based on an asset's risk profile. GravityZone records the system events necessary to enable cybersecurity analysts to understand how threats have infected a system. This expedites both the detection of the infection and the organizational response to current and future threats. The information can also be used to help cybersecurity analysts develop security policies and update endpoint control configurations to further prevent incidents.

Modern Implementation

GravityZone is a modern implementation of a next-generation EPP, and is comprised of:

- A single agent—providing comprehensive endpoint protection.
- One integrated management console—providing a single pane of glass for the management of GravityZone's abilities including policy management, alerting, and reporting.
- Broad platform coverage—providing support for physical, virtual, or cloud-resident workstations, servers, and embedded or mobile endpoints running Windows, Linux, or MacOS. GravityZone also supports multiple virtualization hypervisors including VMWare, Citrix, Hyper-V, and Oracle.
- Security-as-a-service—provided as an on-premises virtual appliance or cloud-delivered.
- Cloud-based analytics—offloading analytics to cloud resources.

The Bigger Truth

Malicious actors are relentless in their attacks against cyber-infrastructure, often targeting endpoints to achieve their objectives. This makes endpoint security a pillar of any organization's cybersecurity strategy and architecture. In addition to employing tried-and-true attack methods, especially those that prey on human gullibility and vulnerability, adversaries continue to innovate, developing ever-more complex methods to exploit software and people. Attackers are equally rigorous and ingenious in trying to hide from cybersecurity systems. These factors have resulted in the endpoint security continuum via which many organizations tactically employ prevention, detection, and response controls in addition to their existing endpoint protection platform (EPP), creating point tool fatigue. A new generation of EPP suites is required, ones that employ an adaptive approach based on layers of detection and prevention technology for defense in depth on the endpoint.

The next generation of endpoint protection platforms needs to meet a set of requirements covering multiple detection techniques, close the loop from detection through prevention to automated remediation, and make effective use of the cloud for simplicity, efficiency, and threat analytics. By doing so, the desired outcome of improved threat prevention efficacy and operational efficiency do not have to be mutually exclusive. Organizations seeking to improve their endpoint security postures should evaluate the next generation of endpoint protection platforms that meet the requirements discussed herein.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

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