

WHITE PAPER

# Advances in Endpoint Security

Adaptive Strategies Increase Efficacy and Efficiency

By Dave Gruber, Principal Analyst  
Enterprise Strategy Group

February 2024

# Contents

Introduction .....	3
Endpoint Security Challenges .....	3
Evolving Threat Landscape .....	3
Human-assisted Attacks Prevail .....	3
LOTL Attacks .....	4
Ransomware .....	4
Excessive Alerts .....	4
A Fundamental Misalignment in Prevention Strategy .....	4
New Approaches Are Needed .....	5
Introducing Symantec Adaptive Security .....	6
Adaptive Protection Actively Reduces the Attack Surface .....	7
Customizable Behavior Tuning .....	7
Principles of Symantec’s Adaptive Security Model .....	7
Symantec Adaptive Security Is Positively Affecting Security Outcomes .....	8
Adaptive Protection is Helping Healthcare Organizations .....	10
Conclusion .....	10

## Introduction

Endpoint security is a core security control protecting virtually every organization. While its capabilities have evolved dramatically since the early days of antivirus protection, innovation has slowed over the past few years as security vendors turned their attention to expanding offerings to address security challenges in other adjacent areas, including cloud, identity, IoT, extended detection and response (XDR), and more.

Endpoint device utilization patterns have also changed and expanded, as modern workers utilize, on average, five devices a day—including the regular use of unmanaged devices—to accomplish work-related tasks.<sup>1</sup> This diversity of device utilization increases both the attack surface and the complexity of endpoint security.

### Current Endpoint Security Solutions Are Struggling to Keep Up

Living off the land (LOTL) tools are helping attackers evade security controls by zeroing in on higher-value devices and users who are often granted higher levels of privileged access.

Attack techniques have also evolved, as more targeted attacks like spear phishing and ransomware utilize living off the land (LOTL) tools to zero in on higher-value devices and users who are often granted higher levels of privileged access.

As a consequence, many endpoint security solutions are misaligned to fundamental shifts in attacker strategies. A new, more adaptive approach that is customizable to each environment is needed.

## Endpoint Security Challenges

Although endpoint security has evolved to include sophisticated cloud- and AI-enabled strategies combining multiple detection mechanisms based on signatures; behavioral pattern analysis; decoys; tactics, techniques, and procedures (TTP) detection; and more. With this, the job of endpoint security has become increasingly difficult. Several factors, outlined below, have dramatically increased its complexity.

### Evolving Threat Landscape

The threat landscape continues to evolve as attackers automate their attack chains in an attempt to evade detection. Security vendors must work diligently to keep their security offerings up to date and flexible in order to keep pace with a continually morphing landscape. Although methods attackers use to gain access to an endpoint have not changed greatly, the mechanisms used to breach the endpoint have changed significantly.

### Human-assisted Attacks Prevail

The threat landscape has become increasingly sophisticated, capitalizing on “human-assisted” attack tactics to evade automated security controls:

- Attack techniques continue to leverage the human factor, with more targeted, human-assisted attack techniques zeroing in on higher-value devices and users, such as executives, finance personnel, and IT resources, who have higher levels of access and privileges.
- Credential theft is at an all-time high, providing attackers a fast path into all areas of the operating environment. Once compromised, identities are being leveraged to move laterally and escalate privileges in order to access “crown jewels” and core operating infrastructure.

<sup>1</sup> Source: Enterprise Strategy Group Research Report, [Managing the Endpoint Vulnerability Gap](#), May 2023.

## LOTL Attacks

As attackers strive to evade security controls and go unnoticed as long as possible, many popular attack techniques take advantage of known-good software and tools that natively exist on the endpoint and are used to support normal business activities. These LOTL attack strategies are used to carry out various phases of attacks that might not appear malicious or suspicious. Attacks leveraging LOTL tools are often difficult and time-consuming to identify and understand within the attack chain. This enables attacks, often including reconnaissance activities, to progress as adversaries prepare later phases of an attack.

## Ransomware

Ransomware continues to be one of the most lucrative forms of cybercrime as well as a critical threat for organizations of all sizes. The ransomware business model has evolved over time to include not only mass encryption of a company's data but also data theft prior to encryption, preventing organizations from recovering encrypted machines from backups. Even worse, some attackers are bypassing encryption altogether: The new trend is to steal data and threaten to expose the data publicly if the ransom is not paid.

### LOTL Tools Fueling Ransomware

Nearly 50% of ransomware attacks over the past three years have employed LOTL tools.

Recent Symantec analysis of ransomware attacks over the past three years (2021-2023) shows evidence that LOTL tools were used in nearly 50% of ransomware attacks.<sup>2</sup> LOTL tools are often risky to block, as they are also used for legitimate business purposes, so wholesale blocking their use without context could disrupt legitimate activities.

## Excessive Alerts

Fueled by the increasing number and types of security controls, large volumes of alerts are being generated by endpoint security solutions, leaving security operations analysts with the overwhelming task of triage, investigation, and human-assisted remediation actions—often post-execution. Research from TechTarget's Enterprise Strategy Group indicated that 70% of organizations reported having difficulty keeping up with the volume of security alerts generated by their security tools.<sup>3</sup>

# A Fundamental Misalignment in Prevention Strategy

### Misaligned Strategies Create Risk

A misalignment between attacker and defender strategies creates an ongoing opportunity for bad actors to successfully enter and execute attacks. A more dynamic, adaptive model is needed to align defensive controls.

Despite the dramatically expanded capabilities of endpoint security solutions in the past 10 years, most continue to depend on a model of monitoring attack patterns and responding to these activities. This reactive approach ignores the changing operating characteristics and dynamics of the devices being protected.

Meanwhile, bad actors are highly focused on looking for opportunities to exploit any vulnerable or unprotected part of the attack surface manifested by unrestricted LOTL

tools and applications which can be used to enter and execute various stages of an attack.

<sup>2</sup> Source: Broadcom-Symantec Independent Customer Data Analysis, 2021-2023.

<sup>3</sup> Source: Enterprise Strategy Group Research Report, [SOC Modernization and the Role of XDR](#), October 2022.

This fundamental misalignment between attacker and defender strategies creates an ongoing opportunity for bad actors to successfully enter and execute attacks. A more dynamic, adaptive model is needed to align defensive controls.

## New Approaches Are Needed

Security teams are falling behind, as dramatic changes in IT operating environments and a thriving, massive criminal attack economy have redefined the operating environment for most. More than half of security leaders (52%) reported to Enterprise Strategy Group (ESG) that security operations are more challenging than they were two years ago, fueled by a growing and changing attack surface alongside a rapidly changing threat landscape.<sup>4</sup> This includes an increased use of LOTL tools.

For example, of the tools most frequently used by ransomware attackers, 6 of the top 10 are LOTL tools, including PsExec, Powershell, WMI, VssAdmin, Reg.exe, and Net.exe (see Figure 1).<sup>5</sup>

Figure 1. Top 10 Tools Employed in Ransomware Attacks

### Top 10 Tools Employed in Ransomware Attacks

Tool	Tactics, Techniques, and Procedures	Frequency
PsExec*	A <b>Microsoft Sysinternals tool</b> for executing processes on other systems. The tool is primarily used by attackers to move laterally on victim networks.	27%
PowerShell*	A <b>Microsoft scripting tool</b> that can be used to run commands, download payloads, traverse compromised networks, and carry out reconnaissance.	20%
WMI*	Windows Management Instrumentation: a <b>Microsoft command-line tool</b> that can be used to execute commands on remote computers.	17%
VssAdmin*	A <b>Windows command-line tool</b> that is used to manage Volume Shadow Copies. It can be used by attackers to delete shadow copies and/or resize the storage allocation. Resizing may limit the space allocated for Volume Shadow Copies, potentially preventing more from being created.	16%
Netscan	SoftPerfect Network Scanner (netscan.exe), a <b>publicly available tool</b> used for discovery of host names and network services.	15%
Cobalt Strike	An off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files. It ostensibly has legitimate uses as a penetration-testing tool but is invariably exploited by malicious actors.	14%
Reg.exe*	A Windows <b>command-line tool</b> that can be used to edit the registry of local or remote computers.	13%
Net.exe*	A <b>Microsoft tool</b> that can be used to stop and start the IPv6 protocol.	11%
Mimikatz	A <b>publicly available credential-dumping tool</b> .	10%
AdFind	A <b>publicly available tool</b> that is used to query Active Directory. It has legitimate uses but is widely used by attackers to help map a network.	7%

\*Living off the Land Tools

Source: Symantec by Broadcom

<sup>4</sup> Source: Enterprise Strategy Group Research Report, [SOC Modernization and the Role of XDR](#), October 2022.

<sup>5</sup> Source: Broadcom-Symantec, [The 2024 Ransomware Threat Landscape](#), January 2024.

Often, system administrators use the majority of these tools to monitor and maintain their systems on a daily basis, making it impossible to outright block their usage. Even more difficult is that no two environments are alike in the way they employ each tool. An innovative approach is necessary to permit appropriate tool usage while still reducing the attack surface.

Despite incremental investments, core defensive security strategies remain fundamentally unchanged, leaving many security teams frustrated and overwhelmed by reactive security approaches. Preventive controls remain foundational, yet few preventive controls can dynamically adapt to the rapidly changing operating environment they are protecting. This leaves IT and security personnel with a constant burden of manually adapting security controls to align with a changing operating infrastructure.

## Introducing Symantec Adaptive Security

Adaptive Protection from Symantec, a division of Broadcom, is a customizable attack surface reduction capability that prevents the unused usage patterns of tools and applications often employed in LOTL attacks, while still enabling legitimate business usage to continue. Adaptive Protection continuously analyzes individual customer operating environments, providing guidance on unused behaviors of tools and applications that can be locked down to limit use by bad actors.

IT and security teams are often unaware of which tools within their environment are vulnerable to LOTL attacks. If the tools are running, attackers can take advantage of them to evade security controls and advance attack strategies. As a result, malicious activity can go undetected, providing bad actors more time to escalate attacks.

Businesses are unique and employ LOTL tools in various ways—often differently between business units—so a one-size-fits-all approach is inadequate. Understanding which LOTL tools are being used and the behaviors exhibited during use within individual environments is critical. Symantec Adaptive Protection provides granular behavioral analysis and corresponding controls, dramatically reducing the attack surface that stems from LOTL tools and applications. At the same time, normal business activities that may involve the use of these tools can continue uninterrupted.

Adaptive Protection caters to the unique behaviors in each organization, recommending a deny posture only for behaviors that are not active in each particular environment. Security administrators can easily pivot to deny the behaviors that have a zero prevalence. Symantec reports that most customers can set half of the behaviors to “deny” on day one.

Enriched with intelligence from the Symantec Global Intelligence Network, Adaptive Protection maps out the different attack methods used by attackers and displays this data in the form of a heatmap for quick reference. Incident responders can use this data to understand which LOTL tools are being employed within specific attacks, such as advanced persistent threats and ransomware. At the time of this writing, Adaptive Protection is tracking a total of 469 specific behaviors across 54 LOTL tools and applications. As new attack methods emerge, Symantec’s Global Intelligence Network feeds new data into Adaptive Protection to stay current.

### Symantec Adaptive Protection

Symantec released Adaptive Protection to provide custom attack surface reduction capabilities designed to close these attack routes otherwise available to attackers using LOTL methods.

## Adaptive Protection Actively Reduces the Attack Surface

Employing AI and machine learning, Adaptive Protection actively reduces the attack surface by:

- Identifying what the LOTL tools and behaviors that can be used by attackers and are in use within an organization (based on a look-back period of 90, 180, or 365-plus days).
- Automatically configuring or recommending a deny posture for the tools and behaviors that are not utilized in the normal course of business.
- Providing IT and security teams full control over how much is automated and where exceptions are applied as they utilize the available automation within Adaptive Protection.
- Supporting zero-trust initiatives with the custom exceptions creation wizard to generate exceptions for legitimate activities.

The threat landscape is constantly evolving as attackers test limits and look for opportunities to exploit weak spots. Because of the way Adaptive Protection tracks lineage, attackers are handcuffed in their abilities to successfully breach an organization, even if they alter their methods to do so. For example, using different tools to do the same behavior will be unsuccessful.

### Identify Emerging Risks

Adaptive Protection identifies emerging risks and makes blocking recommendations on specific application behaviors that are vulnerable to attack within individual customer operating environments.

Applying Symantec's global threat data, advanced analytics, and machine learning capabilities, Adaptive Protection identifies emerging risks and makes blocking recommendations on specific application behaviors that are vulnerable to attack within individual customer operating environments. By closing off application behaviors that are most vulnerable to LOTL attacks, Adaptive Protection greatly reduces the chances that an attacker will be able to move laterally and succeed in attack objectives.

## Customizable Behavior Tuning

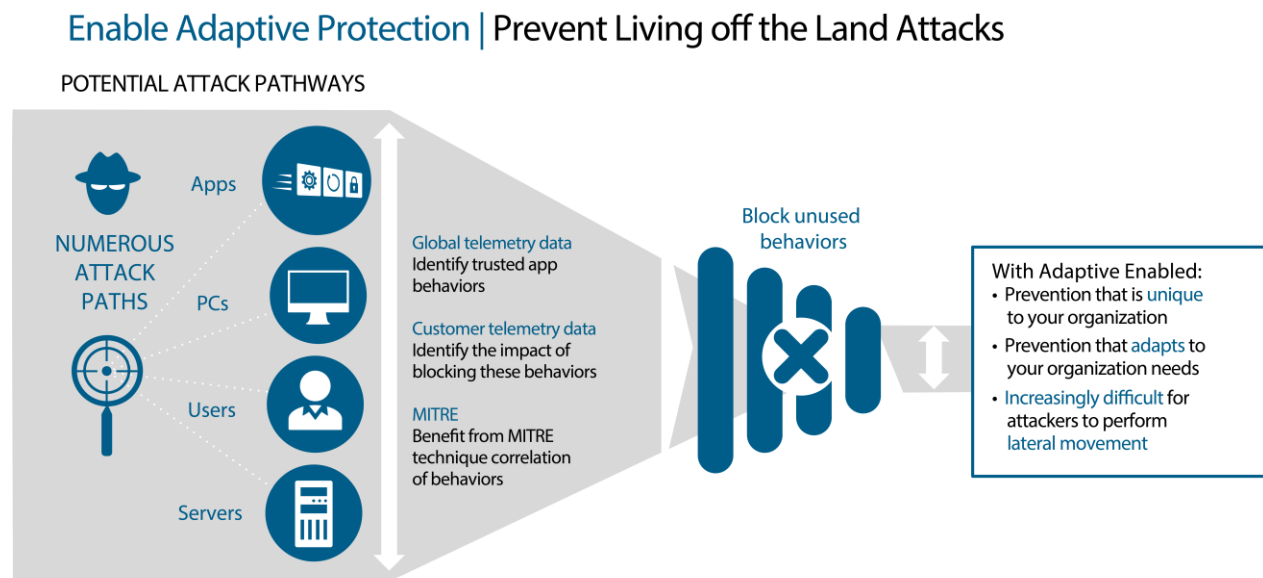
Relying on AI and machine learning, Adaptive Protection provides organizations with the ability to customize exceptions to allow legitimate behaviors. This LOTL customized behavioral tuning ensures businesses can continue legitimate operations, while simultaneously denying activity that could be suspicious or malicious.

Symantec Adaptive Protection provides an exception creation wizard that facilitates creating exceptions, as needed, to ensure continued business operations. IT and security teams have full control over how much is automated and where exceptions are applied as they leverage the available automation within Adaptive Protection.

## Principles of Symantec's Adaptive Security Model

This adaptive security model begins with a precise understanding of the operating characteristics of every device protected. Once expected patterns are chronicled, other patterns associated with potentially malicious activity can be restricted, effectively reducing the potential attack surface. This process must be dynamic and continuous to adapt to the changing characteristics of the endpoint operating environment (see Figure 2).

Figure 2. Symantec Adaptive Security Model



Source: Symantec by Broadcom

By restricting execution of activity patterns of known-good software capable of carrying out malicious activities, this adaptive security model can continuously adjust or adapt preventive controls based on a combination of evolving attacks techniques *and* the changing operating characteristics of an endpoint estate. To summarize, the defining characteristics of this adaptive security model are:

- Continuous monitoring and chronicling of the operating patterns of individual endpoint devices, cohorts of devices, and the many types of users who utilize them.
- Baselining the known-good software in use, what individuals and groups utilize it, how it is used, and the specific patterns of use associated with individual user cohorts.
- A comparison of this baseline of operating patterns to the many LOTL techniques attackers are utilizing to carry out malicious activities.
- The ability to restrict or prevent—by policy—potential attack patterns not used within specific groups of devices or users, effectively blocking execution of many attack patterns while reducing the potential attack surface.
- The capacity to continuously monitor every endpoint within the estate to detect new operating patterns in order to update the baseline. Concurrently monitoring these endpoints helps to detect malicious patterns of activity.
- Continuous visibility into changing operating patterns and suspicious or malicious activity.
- Giving security administrators the flexibility to adjust detection tolerances based on changing risk requirements.

### Symantec Adaptive Security Is Positively Affecting Security Outcomes

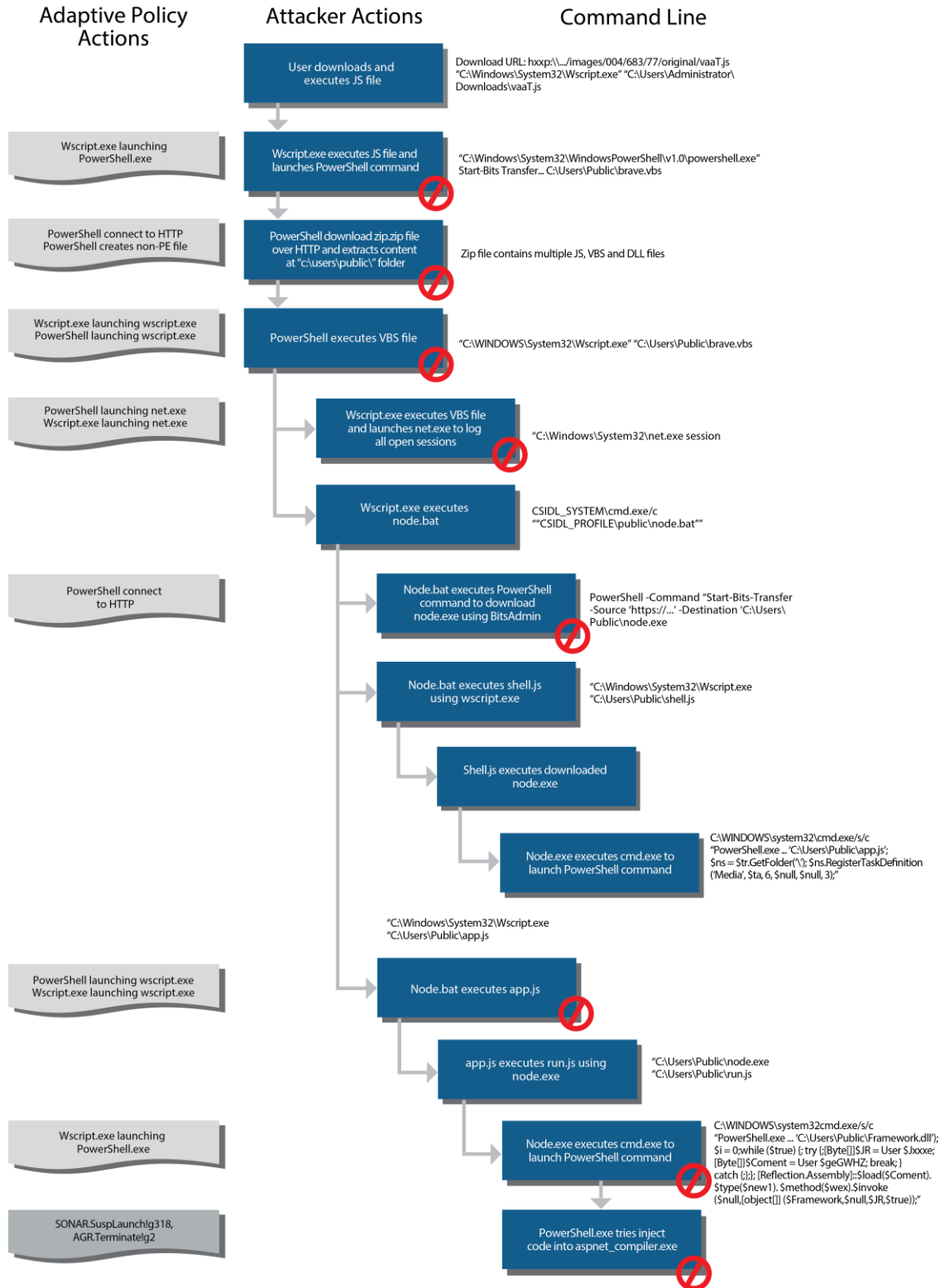
In an independent third-party test of the attack AsyncRAT, conducted by MRG Effitas, Symantec Adaptive Protection mitigation policies interrupted the attack at multiple levels (see Figure 3). Despite the attack's complexity, Symantec Adaptive Protection policies made it impossible for this threat to execute. Instead, the attack was restricted early in the process.<sup>6</sup>

<sup>6</sup> Source: MRG Effitas, *Independent Efficacy Test*, December 2023.



Figure 3. Attack Path Disruption

### Living Off the Land Attack Chain Disrupted By Adaptive Protection



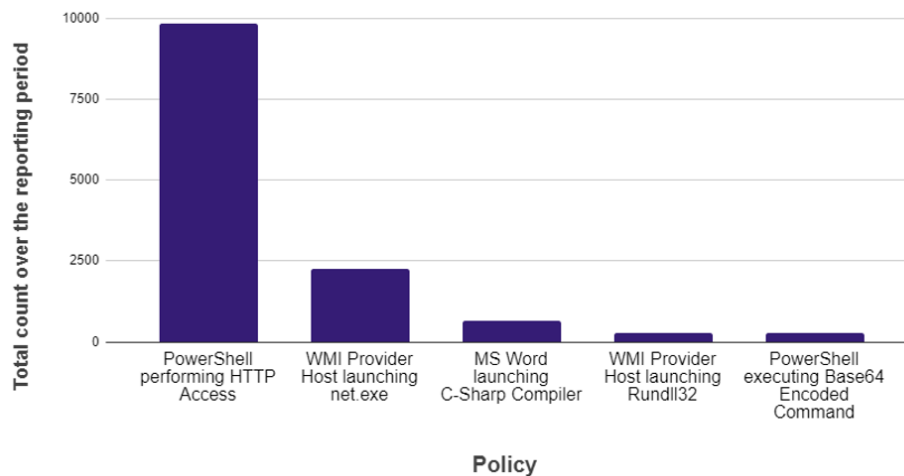
Source: Symantec by Broadcom

## Adaptive Protection is Helping Healthcare Organizations

A recent analysis completed by Symantec reported that Adaptive Protection is safeguarding healthcare organizations from potentially malicious activities preventing 14,000-plus policy violations across 1,300 devices. Top blocks by action include (see Figure 4):

- PowerShell performing HTTP Access (9,836).
- WMI Provider Host launching net.exe (2,253).
- MS Word launching C-Sharp Compiler (645).
- WMI Provider Host launching Rundll32 (284).
- PowerShell executing Base64 Encoded Command (3).

**Figure 4.** Top Policy Violations Blocked by Adaptive Protection



Source: Symantec by Broadcom

## Conclusion

The rapidly changing threat landscape, together with an increasingly diverse and distributed endpoint attack surface, is challenging even the most mature security teams to keep up. The same tools bad actors are leveraging in LOTL attacks play an important role in the administrator’s workflow. Simply limiting usage of these tools can negatively affect business and technical operations. New approaches are needed that can strengthen controls, while providing relief for security operations and endpoint security managers.

Symantec's new adaptive approach monitors operating patterns across the entire endpoint estate and tailors policy recommendations to restrict attacker access to vulnerable behaviors, while providing administrators complete customization and control of policies. This approach prevents lateral movement and the launch of full-blown attacks while allowing business to pursue normal operations.

Enterprise Strategy Group recommends that security leaders take the time to explore how Symantec Adaptive Protection can strengthen security posture by reducing the attack surface.

*Note: Current customers of Symantec Endpoint Protection Complete have immediate access to Adaptive Protection.*

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


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 TechTarget, 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 Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

#### About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 [contact@esg-global.com](mailto:contact@esg-global.com)

 [www.esg-global.com](http://www.esg-global.com)