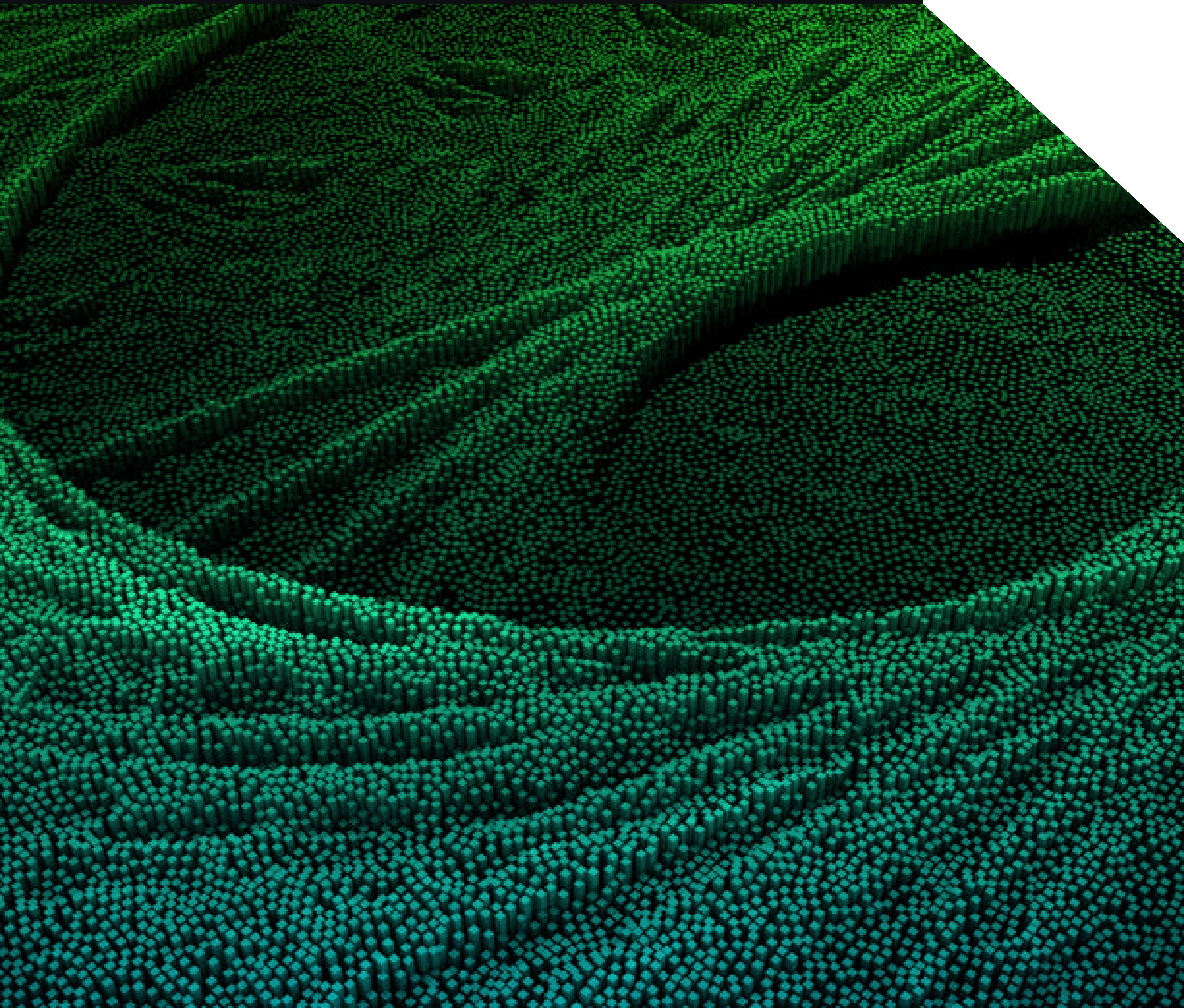
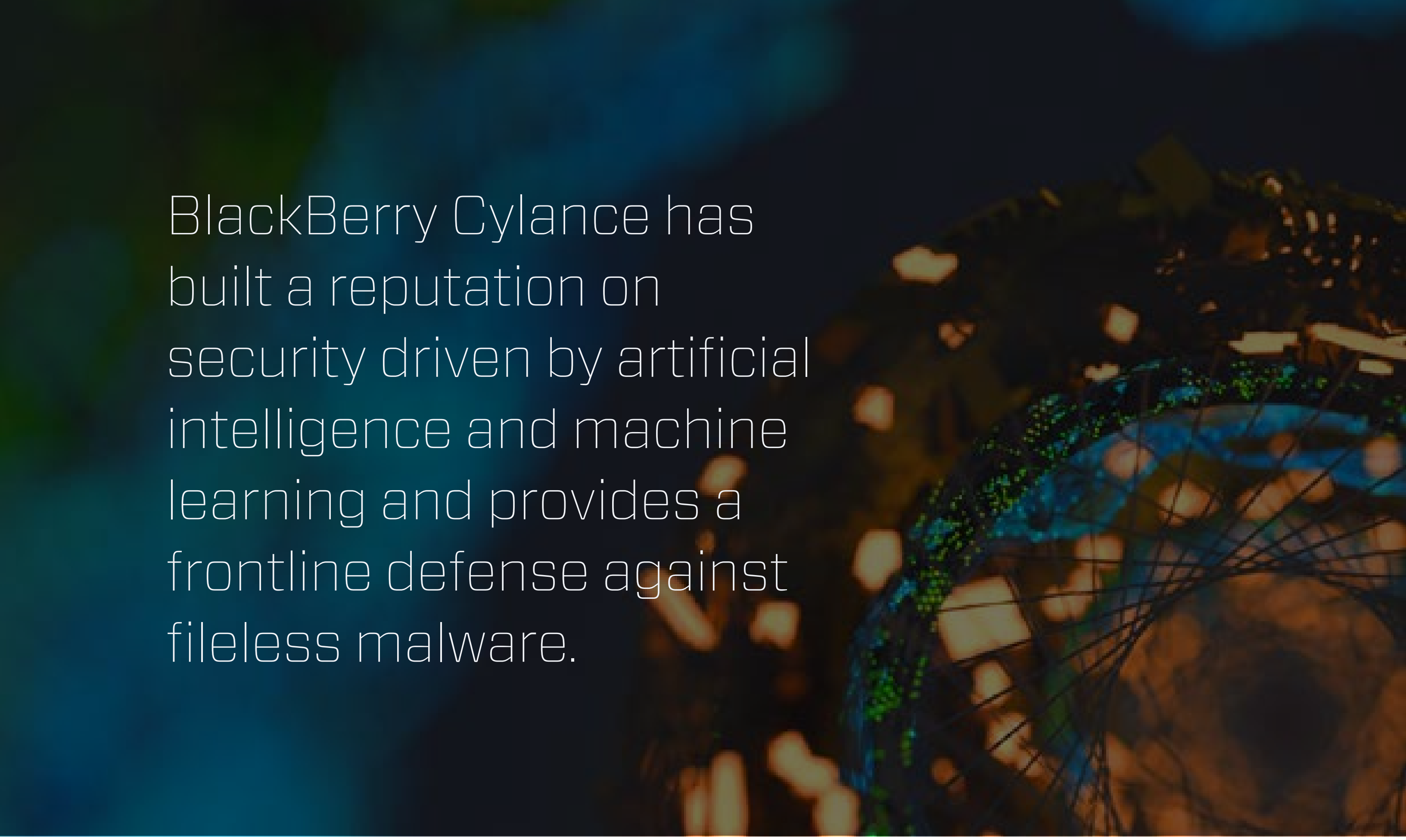
Combating the Scourge of Fileless Attacks

Providing a Frontline Defense Against Fileless Malware

WHITE PAPER





BlackBerry Cylance has built a reputation on security driven by artificial intelligence and machine learning and provides a frontline defense against fileless malware.

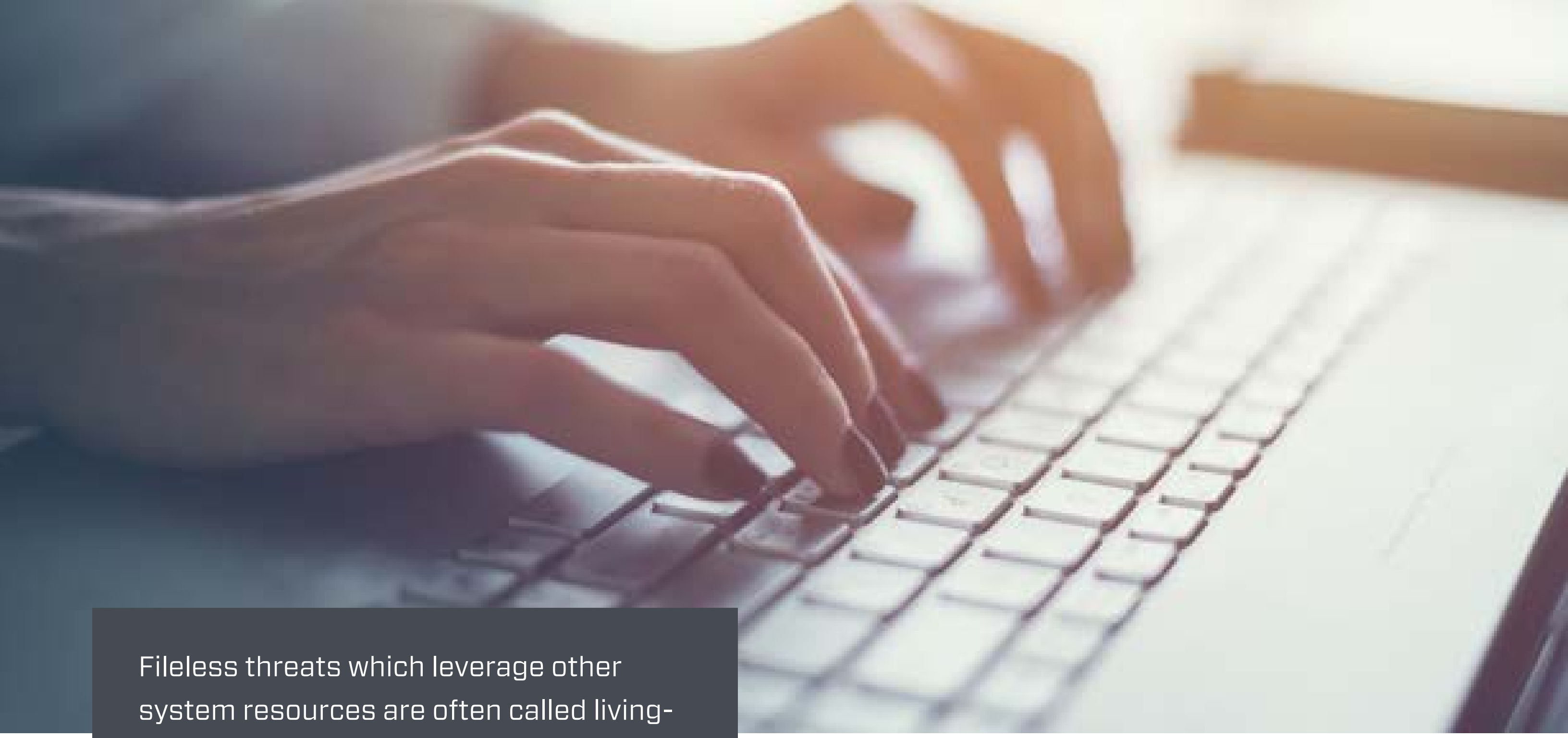
Abandoning files is a logical and tactical response to traditional AV solutions which have overcommitted to file-intensive, signature-based, blacklists. What can security solutions offer when there are no infected files to detect? How will a blacklist stop an aggressor that only uses legitimate system resources? The security landscape is changing and the divide between traditional AV products and next-generation security solutions is growing wider by the day.

BlackBerry Cylance has built a reputation on security driven by artificial intelligence and machine learning and provides a frontline defense against fileless malware. This document details how BlackBerry Cylance protects organizations.

What Is a Fileless Attack?

Fileless attacks originally described threats existing and operating exclusively in volatile memory. This tactic avoids triggering traditional antivirus file-scanning, leaves no on-disk forensic evidence, and requires experts to capture system memory to analyze the attack. Fileless threats commonly inject themselves into legitimate system processes, further frustrating efforts at detection.

The term fileless evolved to include threats that maliciously utilize legitimate system resources without writing new files on disk. Fileless threats which leverage other system resources are often called living-off-the-land (LOL) attacks. These threats can elevate privileges, achieve persistence, and spread across the network by using tools like PowerShell and WMI. They execute their payloads through running malicious scripts, executing DLLs, or running code stored at remote locations.



Fileless threats which leverage other system resources are often called living-off-the-land (LOL) attacks.

Threats like PowerSniff, which temporarily save a malicious DLL to the filesystem, have also been described as fileless. This expands the term fileless to include threats ranging from strictly memory-resident agents to malware which may store malicious files on disk.Given the multi-stage nature of cyber attacks, any attack using fileless elements within the attack chain may be described as fileless.

Blackberry Cylance recognizes three major types of fileless attack vectors affecting the endpoint:

1. Volatile and transient memory payloads
2. Script-based payloads
3. Living-off-the-land (LOL) binaries

Combating fileless attacks requires a departure from traditional, file-based, AV countermeasures. Fileless threats can be detected through contextual analysis of user and system behavior, like anomalous network connections, suspicious shell commands, process-level anomalies, and unusual file activity. Fileless attacks have been observed targeting Windows, macOS, and Linux systems.

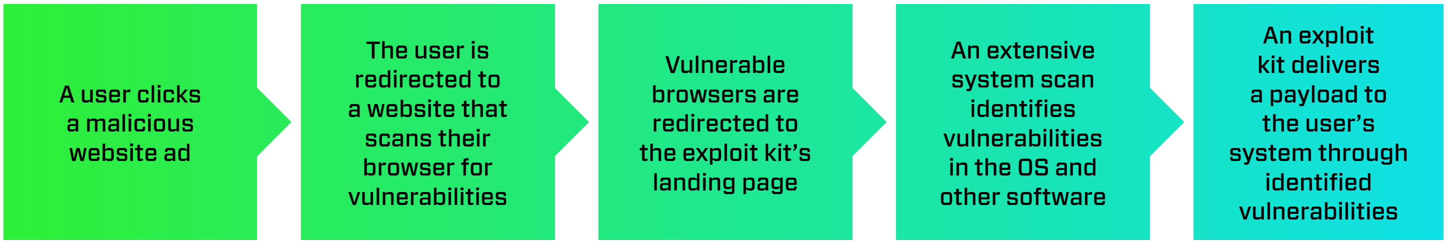
What Do Exploit Kits Have To Do With It?

Exploit kits are a critical component of fileless attacks because they package known software exploits with tools for system analysis and payload delivery. Often an exploit kit will use a malicious ad redirect to conduct a discreet scan of a user's browser. If security flaws are detected in the browser, the user is redirected to a landing page that conducts further scans of their system. Once system vulnerabilities are identified, the exploit kit can deliver malware to the system. This entire process is invisible to the end-user.

Fileless Example: Kovter

Kovter is a click-trojan that began leveraging fileless capabilities in 2016. The original version of Kovter created a folder under the active user profile. The payload, KB9162892.exe, was saved in this folder. Next, a registry key was created to run the file after every system restart. Traditional AV solutions could identify and disrupt Kovter malware using legacy measures like SHA signatures and blacklists targeting the KB9162892.exe file.

Kovter has since evolved to use a new fileless infection methodology. It invokes obfuscated Jscript/JavaScripting to download the Kovter executable to %TEMP% (Windows temp folder). Next, it writes entries in the Windows registry



A user clicks a malicious website ad

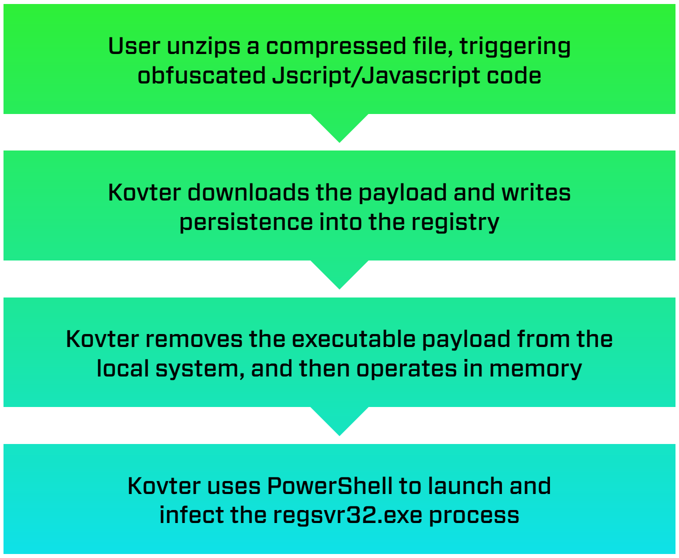
The user is redirected to a website that scans their browser for vulnerabilities

Vulnerable browsers are redirected to the exploit kit's landing page

An extensive system scan identifies vulnerabilities in the OS and other software

An exploit kit delivers a payload to the user's system through identified vulnerabilities to guarantee persistence after a reboot and to assist with the next stage of infection. Then, the malware uses PowerShell to launch and infect a regsvr32.exe process. Lastly, Kovter deletes its executable file from the %TEMP% directory leaving nothing behind for signature-based detection.

The new Kovter resides within a recognized system process operating in memory. Traditional AV detection methods are largely circumvented because there is no file to convict, and there are no rogue processes to detect.



User unzips a compressed file, triggering obfuscated Jscript/Javascript code

Kovter downloads the payload and writes persistence into the registry

Kovter removes the executable payload from the local system, and then operates in memory

Kovter uses PowerShell to launch and infect the regsvr32.exe process

The BlackBerry Cylance Approach

BlackBerry Cylance uses script control, memory protection, and the Context Analysis Engine (CAE) to stop fileless attacks before they cause damage.

Script Management

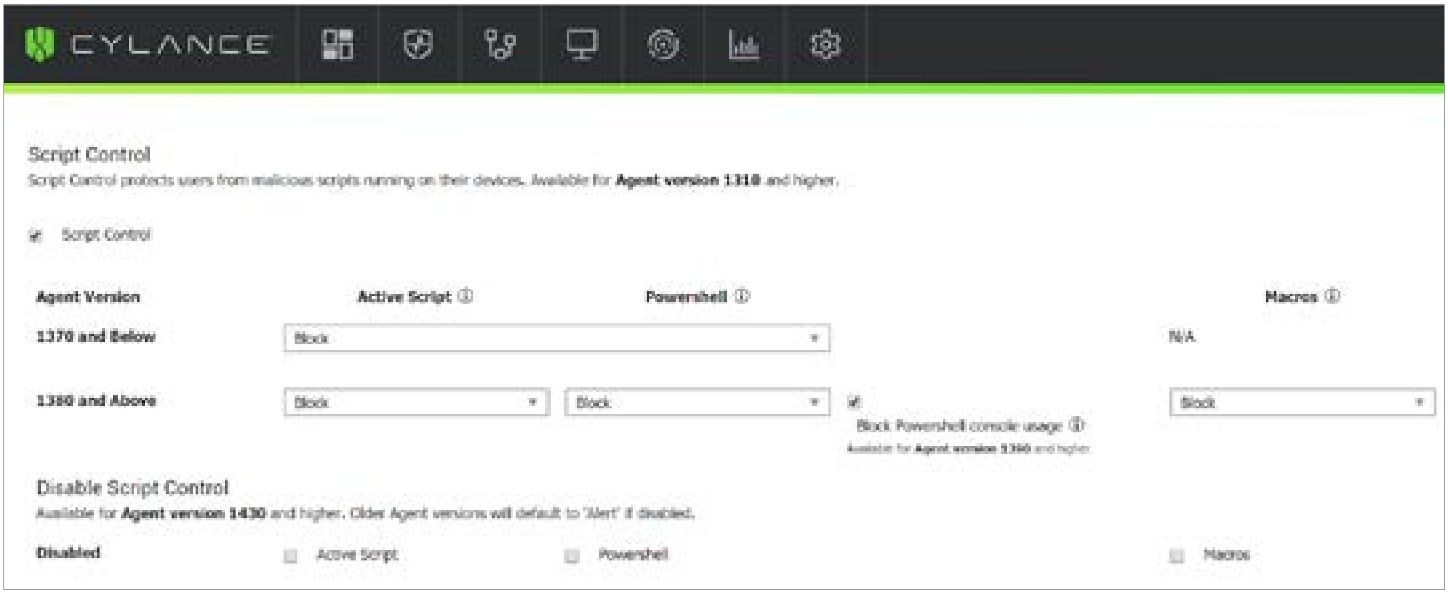
CylancePROTECT® Script Control gives system administrators the power to decide when, where, and how scripts are used in their environment. By injecting itself into the script interpreter, CylancePROTECT Script Control gains insight into both script activity and the script path before execution. Questionable script activity is either blocked or sends an alert to the system administrator.

BlackBerry Cylance offers script control and detection for PowerShell, Active Scripts (Jscript and VBScript), and Microsoft Office macros. Blocking PowerShell also prevents its console from launching. This protects a system from executing PowerShell one-liners. Explicitly approved scripts can still be run, even when PowerShell is blocked.

Memory Exploitation Detection and Prevention

CylancePROTECT Memory Protection denies fileless attacks a space in which to operate. The memory defense agent consists of a DLL that is loaded into each protected process and a service component that provides management capabilities. The agent hooks into user-mode API functions and monitors them for signs of compromise. When a detection occurs within an API, the suspected function is suspended and the agent offers a choice of proceeding via the following actions:

- Ignore the violation and let the process execute
- Alert on the violation, but let the process execute
- Block the violation and send an alert
- Terminate the process completely



Script Control

Script Control protects users from malicious scripts running on their devices. Available for **Agent version 1310** and higher.

☑ Script Control

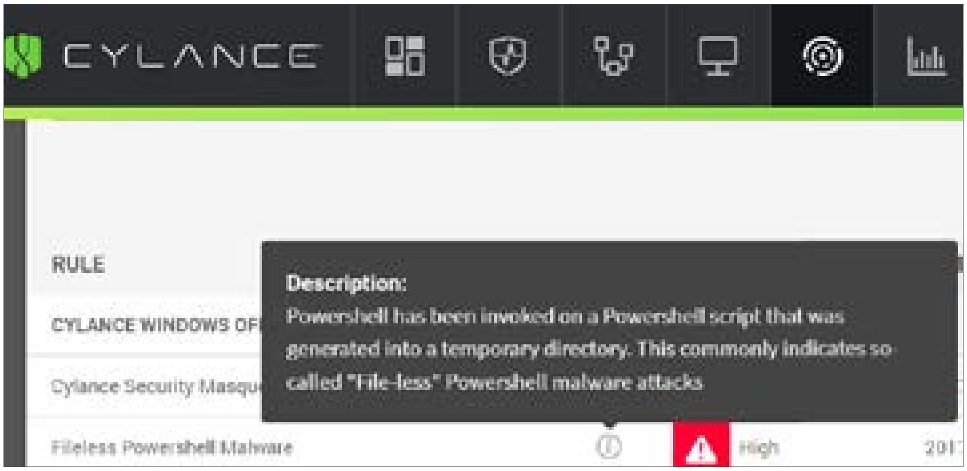
Agent Version	Active Script ⓘ	Powershell ⓘ		Macros ⓘ
1370 and Below	Block			N/A
1380 and Above	Block	Block	☑ Block Powershell console usage ⓘ Available for **Agent version 1380** and higher.	Block

Disable Script Control

Available for **Agent version 1430** and higher. Older Agent versions will default to 'Alert' if disabled.

Disabled □ Active Script □ Powershell □ Macros

CylancePROTECT Memory Protection operates on both 32- and 64-bit processes without heavily impacting system performance. CylancePROTECT® administrators can easily configure memory policies to offer the same protections as modern complex host intrusion prevention systems.



RULE

CYLANCE WINDOWS OF

Cylance Security Masqu

Fileless Powershell Malware High 201

Description:
Powershell has been invoked on a Powershell script that was generated into a temporary directory. This commonly indicates so called "File-less" Powershell malware attacks

Context Analysis Engine (CAE)

The CylanceOPTICS Context Analysis Engine empowers each endpoint with threat detection and response capabilities. This approach allows each endpoint to act as a virtual SOC, responding to threats with predetermined processes. In other words, it provides automated endpoint protection that functions 24x7 without placing demands on human operators. Time is saved in the form of reduced latency by the CAE conducting threat analysis on the endpoint instead of contacting the cloud.

CylanceOPTICS™ detects each atomic event that occurs on an endpoint in real time. Each event is evaluated using the Machine Learning Threat Detection Modules to determine if there is malicious intent. For instance, when a process is launched CylanceOPTICS analyzes the event and compares it with 'normal' process-launching behavior. A user invoking a PowerShell process on a script in a normal directory may not trigger an alert. An automated one-line shell command invoking PoweShell on a script in a temporary directory may.

The CAE provides a way to impose rules on a catalog of system behaviors. These behaviors include PowerShell, Javascript, and browser-specific actions that fileless attacks rely on to operate. Admins can also author custom rules to govern specific concerns in their environment. Denying fileless malware the resources it needs is a highly effective way to combat fileless attacks.

Conclusion

Fileless malware poses a serious threat to traditional AV solutions by using discrete methods often invisible to standard threat detection. By hijacking legitimate resources to attack a host system, fileless malware can camouflage its presence and operate unnoticed.

BlackBerry Cylance provides advanced tools that deprive fileless threats of the resources they need for survival. By controlling the execution of scripts, the memory space, and the manipulation of endpoints, BlackBerry Cylance products keep infrastructure safe from fileless attacks.

For more information about new cybersecurity technologies that can secure against fileless attacks, visit www.cylance.com.

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

BlackBerry
CYLANCE.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com