RevBits®

CYBER BRIEF

EDR Testing Found Leading Cybersecurity Solutions Missed the Mark.

The most effective EDR solutions inherently extend detection across multi-stage threats and balance the detection and alerting to minimize false positives.

Alerts are intended to help organizations quickly detect and mitigate advanced cyberattacks, providing security teams with timely information about vulnerabilities, active security events and exploits. However, when endpoint detection and response, or EDR, solutions alert on inconsequential events and/or false positives, security teams can become overwhelmed.

Identifying security incidents requires fine-tuned detection in order to avoid false positives. It's incumbent upon an EDR to converge on high-priority incidents, with an optimum balance and understanding that establishes normal behavior, eliminates false positives, and exposes real threats.

Detecting and alerting on cybersecurity events can be a Catch-22

Multi-stage malware attacks require a robust EDR design and architecture that enables finely-tuned detection.
It would be easy for an EDR to catch more unknown cybersecurity events, by opening up their detection thresholds. However, doing so can generate huge amounts of false positives. It becomes a careful balancing act of detecting as much malicious activity as possible, without inundating security teams with inconsequential alerts.

Security alerts are triggered by unusual activity on privileged accounts, anomalous external inbound traffic, suspicious port activity, abnormal security policy violations by internal users, and unexpected file changes. Security event response challenges not only come from the number of incidents, but also from myriad consoles, ticketing systems, emails, and phone calls that complicate and extend response and mitigation efforts. Organizations with mature security postures utilize automation within their EDR solutions, yet, they still face an increasing number of attacks.

The failure to include code that detects and checks what the control.EXE is loading, puts organizations that rely upon the EDR at great risk.

Research testing on leading EDRs reveals their faults

The University of Piraeus in Athens, Greece, recently conducted testing on 18 different EDR products from leading cybersecurity vendors. The testing of attacks against EDR software included Bitdefender, Carbon Black, Check Point, Cisco, Comodo, CrowdStrike, Elastic, ESET, F-Secure, Fortinet, Kaspersky, McAfee, Microsoft, Panda Security, Sentinel One, Sophos, Symantec, and Trend Micro.

The testing results were published in a report offered through Cornell University entitled, An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. Unfortunately, the results were less than stellar in almost all of the EDR products' ability to prevent and log the attacks.

The tests consisted of simulating common advanced persistent attack (APT) kill chains, and hosted four common attack files, including a Windows control panel shortcut file (CPL), a Microsoft Teams installer that loaded the malicious DLL, an unsigned portable executable file (EXE), and an HTML application file (HTA). When executed, the malicious files exploited legitimate functions to load an asset via network scan if they attempt to identify active devices.

and run Cobalt Strike Beacon backdoor. Cobalt Strike is a commercial, full-featured, remote access tool designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors.

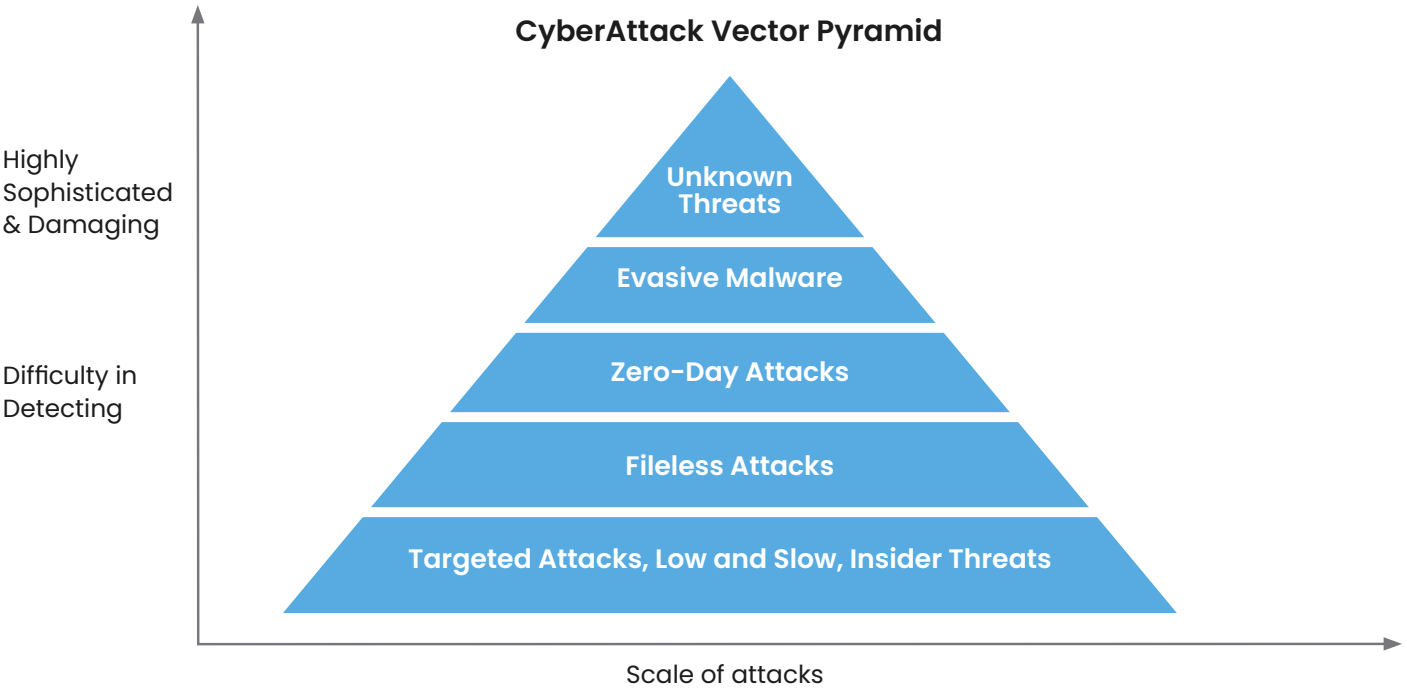
What is significant, and something organizations should be concerned about, is how these leading EDRs missed detecting the attack chain with the four files that enabled the Cobalt Strike Beacon backdoor, that are known regular payloads. These are typically sent as part of spear-phishing email campaigns that EDRs are expected to detect, block, and alert security teams, when deployed inside a corporate network.

Test Results Summary

The test results below show the majority of tested EDRs allowed would-be threat actors to slip through a company's defenses.

EDR	CPL	HTA	EXE	DLL
Bit.Defender GravityZone Plus	✘	✘	✔	✘
Carbon Black Response	●	✘	✔	✔
Check Point Harmony	✘	◆	✘	✔
Cisco AMP	✘	✘	✔	▼
Comodo OpenEDR	✘	✔	✘	✔
CrowdStrike Falcon	✔	✔	✘	✔
Elastic EDR	✘	✔	✔	✘
F-Secure Elements Endpoint Detection and Response	◆	†	✔	✘
FortiEDR	✘	✘	✘	✘
Microsoft Defender for Endpoints	✶	✘	✘	✔
Panda Adaptive Defense 360	✘	✔	✶	✔
Sentinel One (without test features)	✔	✔	✔	✘
Sentinel One (with test features)	✘	✘	✘	✘
Sophos Intercept X with EDR	✘	✘	✔	—
Trend micro Apex One	●	●	✔	✔
Endpoint Protection	**CPL**	**HTA**	**EXE**	**DLL**
EST PROTECT Enterprise	✘	✘	✔	✔
F-Secure Elements Endpoint Protection Platform	✔	✔	✔	✔
Kaspersky Endpoint Security	✘	✘	✘	✔
McAfee Endpoint Protection	✘	✘	✔	✔
Symantec Endpoint Protection	✔	✘	✔	✔

Table 1: Aggregated results of the attacks for each tested solution.
Notation: ✔: Successful attack, ◆: Successful attack, raised medium alert, ●: Successful attack, raised minor alert, ✶: Successful attack, alert was raised ❍: Unsuccessful attack, no alert raised, ✘: failed attack, alerts were raised. † In two experiments supplied by the vendor, in the first it was detected after five hours, in the second it was detected after 25 minutes. ▼ Initial test was blocked due to file signature, second one was successful with another application.



Short-sighted detection methods put organizations at risk

All of the EDR products tested have detection capabilities that the vendor can dial up or down. However, the higher the detection sensitivity is turned up, the greater the number of false positives. Another reason these EDRs failed the test is because they did not analyze the rundll32. exe properly, as CPL files can be weaponized to load an arbitrary malicious DLL via rundll32.exe.

In the test, the control file was loaded by rundll32.exe; a Windows core feature. The EDRs blindly trusted the CPL and rundll32.exe that loaded DLL via CPL. In doing so, they allowed the malicious Cobalt Strike Beacon to disguise the CPL, and run under the context of rundll32. exe. Because the EDRs didn't verify who started the rundll32.exe, and what rundll32.exe loaded, they couldn't know the source of the applet being loaded. In this case, the Microsoft Windows CPL applet was the Cobalt Strike malware, that turned into the applet.

In order to eliminate false positives, EDRs lower their scan detection capabilities by trusting core applications, like the Windows operating system rundll32.exe. The EDRs failed to include code that detects and checks what the control.exe loads. In this case, the rundll32.exe loaded a CPL that was not part of the Windows operating system. The malware could have been detected, if the EDRs had sandboxed the rundll32.exe for analysis, before being allowed to run.

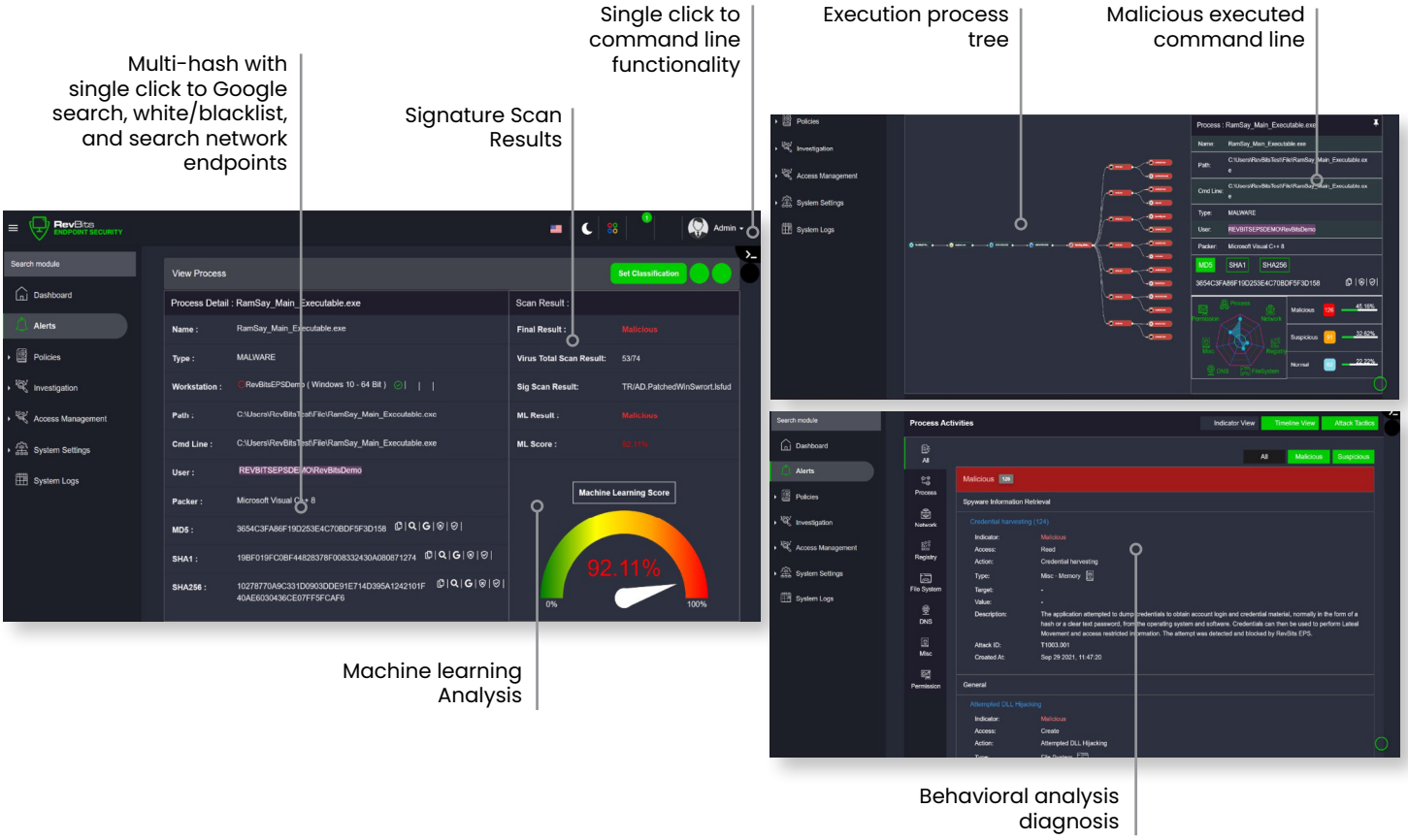
RevBits EPS unique architecture automatically extends detection across multi-stage attacks

RevBits EPS is built upon a unique architecture, with detection mechanisms that go far beyond other EDRs. RevBits' custom handlers, or proprietary application loading detection capabilities, find multi-stage malicious activities attempting to impersonate Windows applications, signing processes and trusted processes. RevBits EPS also has an accurate detection engine that prevents false positives and a distinctive architectural design for application whitelisting, sandboxing, spawning, and parent/child process analysis.

Installing Shell extensions is another way hackers load malicious DLLs and avoid detection. RevBits prevents this by requiring admin approval before allowing Shell extensions, the same way we require driver approvals. RevBits EPS also accurately scans DLLs with our machine learning model to detect unknown malware.

When a new executable is asked to run on a device, if it isn't already whitelisted, RevBits EPS automatically puts it into a sandbox for analysis. Regardless of what may have been added to obfuscate the malware, RevBits EPS evaluates the entire process, including executables, leaving no ability for malware to hide within legitimate programs and applications. This both mitigates malware and eliminates false positives.

The HTML application file (HTA) used in the test is a script that, when double clicked on, spawned mshta.exe and executed the custom HTML and Javascript codes inside, which had more privileges than typical HTML inside a browser. In the test example, HTA loaded mshta.exe, that loaded a VB Script, which in return loaded a .NET DLL. This was allowed because the EDRs trusted the process. The result was a malicious .NET DLL loaded that bypassed the EDR. RevBits' ability to analyze Microsoft applications and processes is fundamental in preventing malicious code from entering and launching these types of attacks.

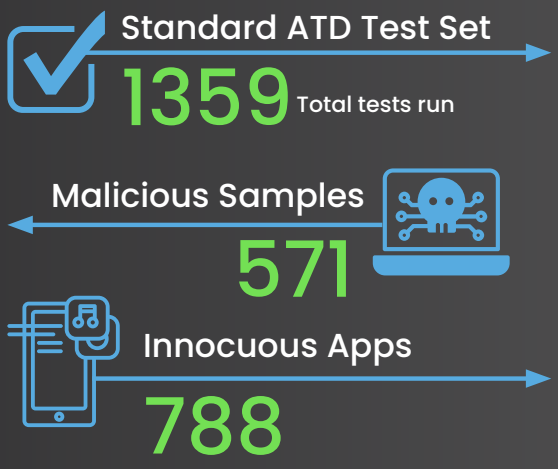


RevBits Endpoint Security's (RB-EPS) main alert dashboard for an individual workstation. RB-EPS provides a feature rich robust GUI.

RevBits EPS testing results conducted by ICSA

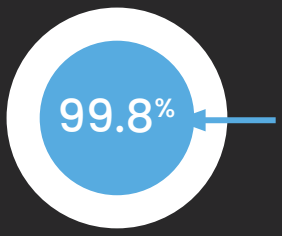
RevBits EPS was recently tested by ICSA Labs, an independent division of Verizon certification testing. According to Verizon's Data Breach Investigations Report (DBIR), in testing, ICSA Labs delivers malicious threats with the primary threat vectors that lead to enterprise breaches. Testing was performed under the Advanced Threat Detection protocol, which focuses on evaluating endpoint security products for protection against new and little-known threats across all malware types.

The process included over 1359 test runs containing 571 malicious samples and 788 innocuous applications, executed over thirty-two consecutive days. RevBits EPS had an overall detection rate of nearly 100% and zero false positives.



RevBits EPS was tested against threats missed by traditional security products, and not a single ransomware was able to cripple computers secured by RevBits Endpoint Security. For the detailed certification report, go to the Advanced Threat Test Report.

Effectiveness Details



RevBits Endpoint Security was nearly 100% effective during the Q4 2021 test cycle, detecting all but 1 of the new and little-known malicious samples in the test set

Standard ATD False Positives (FPs)

Zero innocuous apps were improperly categorized as malicious. Great!

ICSA Labs testing report found RevBits EPS had zero false positives.

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com

34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com