RevBits®

PRODUCT BRIEF

Endpoint Security

RevBit's Endpoint Security Identifies, Isolates, and Removes Endpoint Threats in Real-Time.

Endpoints are a primary target for cyberthreats. Protecting against malware, ransomware and fileless exploits requires NextGen advanced endpoint protection administered through a comprehensive security solution that detects and blocks known and unknown threats.

An endpoint security detection and response solution is an integral part of an enterprise's security posture. It should provide coverage for both cloud-based and on-premise infrastructure for managing endpoints with Windows, and non-Windows-based operating systems like Apple macOS and Linux. An organization's specific use cases will determine the factors for their endpoint security product decision, to align their security needs with the product's features and capabilities.

RevBits EPS solution covers security needs for today, and the future

Keep in mind that security requirements will evolve over time, as the threat landscape changes. Selecting the broadest detection and response coverage available will go a long way in meeting today's requirements, and the coverage needs for tomorrow.

RevBits Endpoint Security (EPS) includes EDR capabilities for centralized visibility and endpoint control.

Most anti-virus and Nextgen endpoint security solutions can't prevent exploits. Instead, they allow the exploit to enter, and rely upon their ability to detect and mitigate the injected malware. This is like allowing burglars into your house, and then trying to extricate them before they cause harm.

As evidenced by the number of breaches occurring on a daily basis, cyberattacks are increasingly more difficult to discover, and cyber threats should not be tolerated at any point in the attack chain. They must be eliminated at point zero (at the exploit), before they are allowed to drop their malware.

RevBits Endpoint Security (EPS) includes EDR capabilities for centralized visibility and endpoint control. RevBits EPS secure management is enabled by single sign-on to simplify access, and provides intuitive visibility to merged and correlated events, alerts and reports.

Protecting Windows-based endpoints from rootkit malware threats

Software drivers are becoming common target vectors. Drivers are a bridge between the hardware, software, and data on a computer or network. Cyberattacks using drivers are a strategic way for bad actors to gain system-level privileges, and remotely execute malicious code on otherwise inaccessible sections of the OS, like the kernel.

One approach to ensuring the security of the Windows operating system is to prevent drivers with malicious code from loading and accessing space in the Windows OS and kernel. Unfortunately, Windows doesn't provide a solution for this issue. The solution to this problem requires a system and method that selectively blocks unwanted drivers from being loaded and executed into the kernel.

When malicious Windows drivers are loaded and executed within the kernel, they can completely disarm anti-virus security products, rendering them useless. There is no inherent method in Windows to fully prevent

drivers, signed or not, from being loaded into the operating system kernel layer. Of course, this opens up opportunities for hackers to discover ways of bypassing driver signature enforcement. They can use stolen code signing certificates to sign malicious drivers, and find other ways of bypassing driver signing enforcement within the Windows OS kernel space.

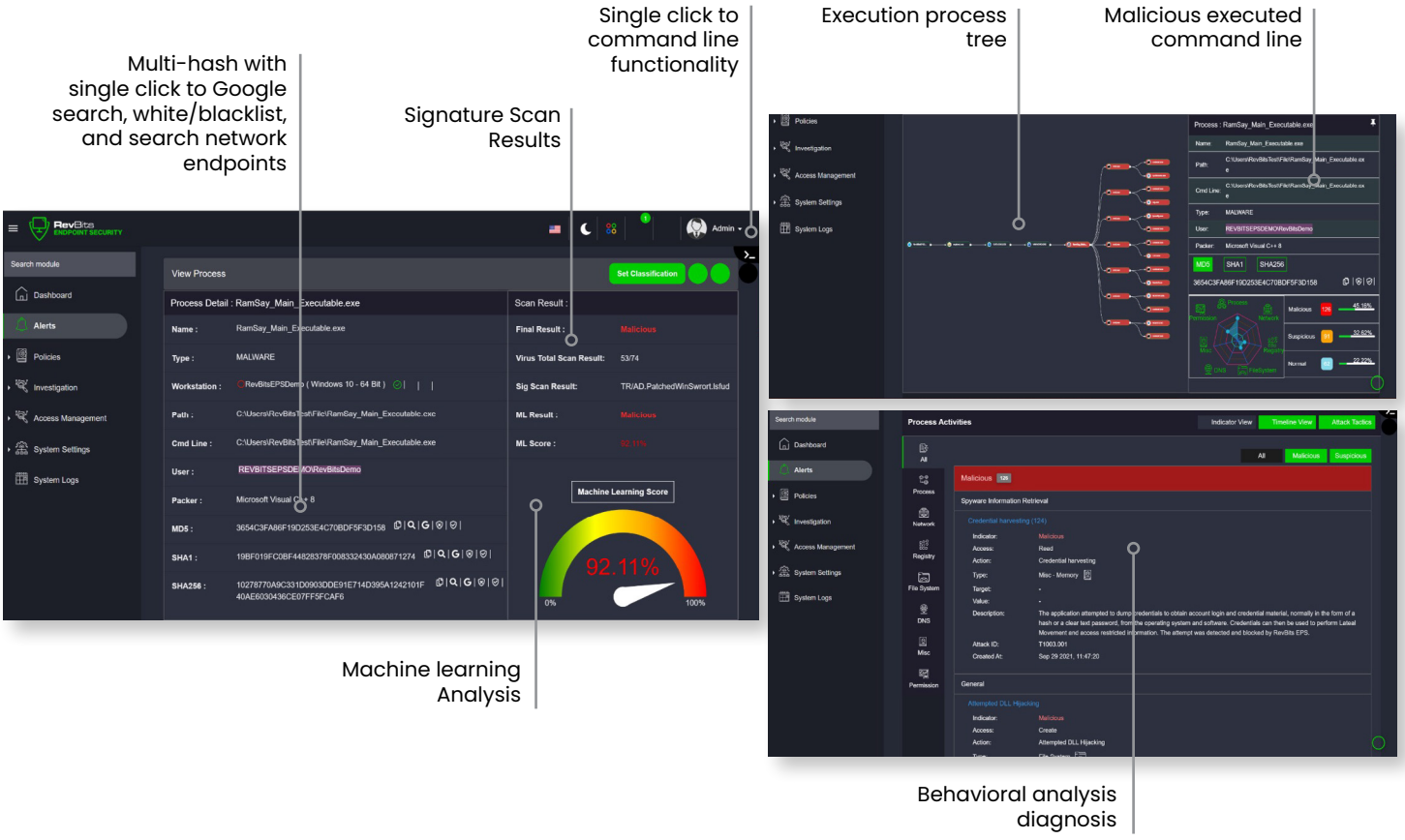
A rootkit is designed to protect against a malicious program delivered by a threat actor, using a sort of invisibility cloak. These attacks are some of the most destructive for organizations. Not only are they dangerous because of the damage they can inflict, they're also almost impossible to detect and remove. While remaining undetected, bad actors steal data and take over systems with nefarious intent.

These breaches almost always require IT to completely remove the malware by deleting the operating system and completely rebuilding the device. Protecting against rootkit malware requires specialized anti-rootkit software that detects, prevents and removes the malware.

RevBits endpoint security protects against rootkit threats

RevBits EPS includes patented anti-rootkit threat detection, prevention and removal capabilities. To remove known and unknown rootkit malware, RevBits EPS identifies suspicious callback processes, hooks, registry keys and modified files. RevBits EPS anti-rootkit capabilities protect computer systems and data by detecting, blocking and removing malicious drivers.

RevBits EPS patented anti-rootkit software is able to patch drivers in memory, before they access the kernel space. This allows administrators to decide which drivers are allowed, and which ones are denied access to the kernel space. RevBits EPS will detect and alert on known and unknown malicious rootkits using unique modeling techniques, and remove them through our callback capabilities, whether they are signed by Microsoft or any other certificate authority.



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

Not all endpoint behavioral analysis methods are equal

Behavioral analysis is the most advanced protection available within NextGen endpoint security. RevBits EPS includes behavioral analysis, machine learning and signature scanning capabilities. It also utilizes a scoring point system. Because everything is embedded within a single product, multiple data sources are aggregated together, and can be easily viewed collectively for fast mitigation response. This is important for not only detecting malware, but also for eliminating false positives.

RevBits EPS intelligence engine integrates its behavioral analysis with the MITRE Attack Framework. Critical detection points are implanted with sensors in system threads, registries, file systems, networks, etc. RevBits EPS has accumulated a massive list of abnormal activities that have been classified and scored for broad coverage of any process, including API calls and accessing of system resources.

In order to eliminate false positives, endpoint security products often lower their scan detection capabilities by trusting core applications within the Windows operating system. When normally trusted applications are not sandboxed for analysis before being allowed to run, malware can remain undetected. These attacks even get past Microsoft Defender for Endpoints, as evidenced in a recent report that tested over a dozen EDR solutions. The published results can be found in a report offered through Cornell University entitled, An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors.

Endpoint protection requires centralized visibility and management of policy setting, reporting and alerting. The pandemic-induced work from anywhere phenomenon has exacerbated many challenges for IT and security teams. Workers are buying and using myriad cloud apps that are unauthorized by IT. Employees are using their own smartphones, laptops and tablets. They attach USB and non-USB-connected devices, like printers, storage products and other digital equipment.

Shadow IT has become a top-of-mind problem, as unsanctioned products and services introduce new security risks and compliance violations. RevBits EPS gives IT and security teams assurance and confidence that no unknown code, apps and devices will be added to the network, without their approval. It provides them with centralized visibility and automatic detection of all shadow IT elements, with the control to whitelist or blacklist them through policy. This not only removes security risks from network scanning and unwanted elements, but also alleviates IT help desk and support calls.

RevBits EPS policies

- **USB Policy** – Built-in whitelisting and blacklisting USB device policies, including logging, recording and alerting.

- **Process Policy** – Prevents unwanted app, hash and certificate processes from running in your environment. Detects when an app, hash and certificate is being installed, and sends alerts to whitelist and blacklist. Hash values are useful for security analysts for shared Indicators of Compromise (IOCs). Threat-hunting reference malware samples shared through malware repositories can be easily integrated into the RevBits EPS Process Policy engine. Threat-hunting is made easy, by searching threats across the network using hash values managed within the RevBits EPS console. RevBits enables admins to upload IOCs to create blacklists to rapidly block new and emerging threats.

- **Exploit Detection Policy** - Detects and blocks known and unknown (0-day) exploits. Exploit threats are eliminated before their shellcode or payload can be executed to spread malware and steal credentials.

- **Script Logging Policy** – Enables/disables command prompt, terminal, Shell and PowerShell policies. Stores events in a database that is indexed for fast keyword searches. Enables/disables events through log script block invocation when a command, function or script, starts and stops. Records all sessions, including long-running background scripts.

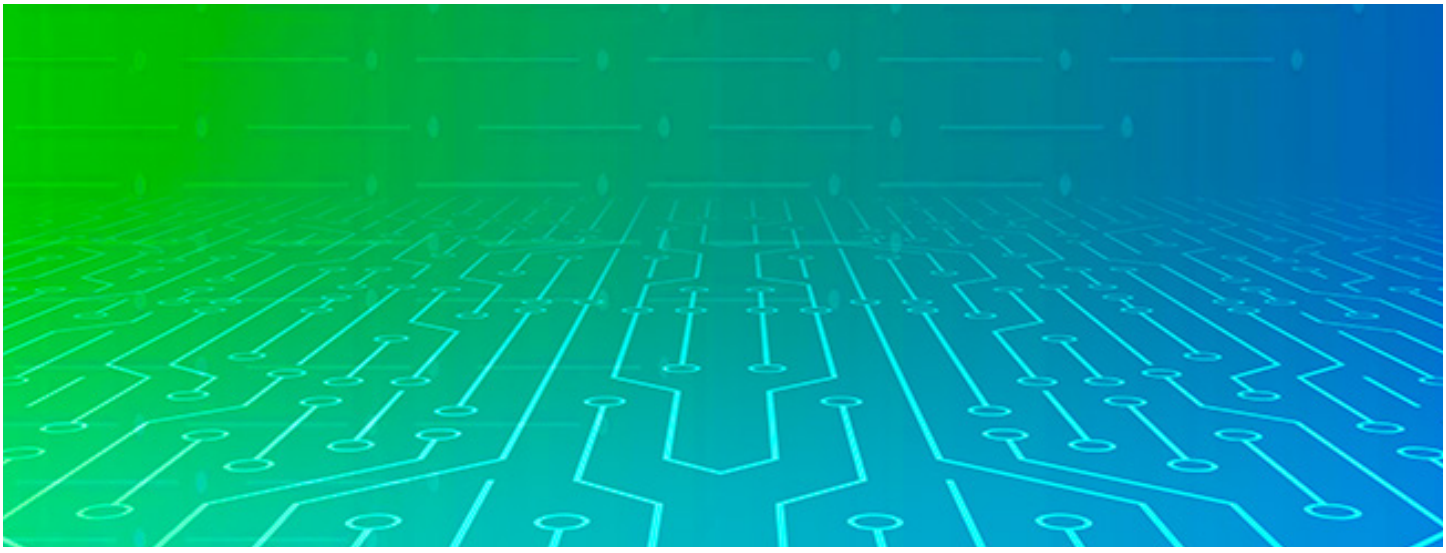
- **Network Policy** – Blocks sites, domains and IP addresses for internal and external networks. Host-level firewall policy enforcement provides granular protection of endpoints from viruses and malware, to control the spread of infections throughout the network. Blocks ports and IPs – incoming and outgoing.

RevBits EPS architecture extends protections across multi-stage attacks

Cyber criminals will always go after the most widely consumed software or applications. The most popular, and therefore, the most commonly exploited are Microsoft Office applications, like Word, Excel, PowerPoint and others; popular web browsers like Chrome, Firefox, Safari, Internet Explorer, Edge, and others; and Adobe Flash Player and Acrobat Reader.

An exploit can execute a custom shellcode directly from the vulnerable application. Shellcode is a small piece of code consisting of a list of assembly/machine instructions that is executed after exploiting a software vulnerability

Bad actors like to use exploits because they don't require users to tap, click or swipe anything. The exploit code can be inserted into a format that a vulnerable application will parse and read, such as a PDF file, a webpage or a document file. Once the innocent-looking file is opened or a web page is visited, a specially crafted exploit will trigger the code, exploit the vulnerability, and subsequently execute the shellcode that can lead to a full compromise of the system. When this occurs, it will be a challenging job for analysts to find a link between the dropped malware or executed shellcode, and the original source of the exploit.



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

RevBits EPS prevents the installation of hacker-created Shell extensions that can load malicious DLLs and avoid detection. It requires admin approval before allowing Shell extensions, the same way it requires driver approvals. RevBits EPS also accurately scans DLLs with a machine learning model that detects unknown malware.

When new executables try to run on a device, if they aren't already whitelisted, RevBits EPS automatically puts them into a sandbox for analysis. Regardless of what may have been added to obfuscate the malware, the entire process is evaluated, including executables. This makes it impossible for malware to hide within legitimate programs and applications.

PowerShell is a two-edged sword

Admins use PowerShell to find security holes in their IT systems, automate tasks and manage configurations. Threat actors take advantage of PowerShell, by running file-less malware through it, making it difficult for anti-virus solutions to detect. Hackers use PowerShell as a remote-control tool, capturing and retrieving user credentials, without leaving any evidence or trail. If they steal credentials by exploiting a Microsoft Office application or a browser or PDF file, the protections of a Privileged Account Management (PAM) solution can be undermined. This is just another reason why a multi-function security platform is so important.

When a hacker identifies an application vulnerability within an application, like Microsoft Word, they craft a special structure, packet, or field to overflow a buffer. Alternatively, they may create a heap overflow, leading vulnerable software to execute unintended code. They may overwrite the function return address with carefully crafted Return Oriented Programming (ROP) gadgets that can lead to arbitrary shellcode or machine code commands that Word is not supposed to run. This is an action that should never occur, because it allows hackers to run commands on the system, including code to download and execute remote malware, or open a backdoor shell access to steal credentials.

RevBits EPS is a highly effective, reliable, scalable solution

RevBits EPS has been comprehensively tested, and will not violate the stability of computer systems or applications. It is fully compatible with all Office applications, popular browsers and Adobe files. It is highly scalable, and will report every attack and every potential threat through the console and/or Cyber Intelligence Platform (CIP) dashboard. This provides comprehensive information about an infected web page, application or file, to localize the attack source and prevent further potentially unsafe actions. The solution works by monitoring endpoints, and collecting data into a centralized repository, where the data is analyzed and can be quickly acted upon.

RevBits EPS includes exploit and malware detection and response capabilities for processes that are commonly and constantly exploited in widely used applications, web browsers, and PDF files. RevBits EPS also protects legacy and custom applications. Any exploitation attempts will be thwarted, and no shellcode will ever be allowed to execute.

RevBits EPS has no hooks into the applications themselves, but monitors and analyzes memory allocations, code calls and function structures, and installs hooks into the APIs associated with the applications. This makes it extremely stable and reliable. It will detect all exploits without creating false positives, and will not crash the applications. It has been thoroughly tested on Microsoft Windows and all Office applications, popular web browsers, and on Adobe Flash Player, Acrobat Reader and PDF files. It has also had extensive exploit testing for Common Vulnerabilities and Exposures (CVEs).

RevBits EPS detects and responds to USB malware threats

All networks are vulnerable when data is passed through removable media, like a USB device or external hard drive. If an attacker gains access into a network through a USB device, they can move across the network laterally, acquiring elevated rights and privileges to access mission-critical resources and data.

USB devices are a growing cyberattack vector. There are many attack programs, like USBStealer, USBFerry, Fanny, USBCulprit, PlugX and others. To combat cyber breaches, RevBits EPS has policy controls that allow administrators to enforce whitelisting and blacklisting of any type of device, including USBs and external hard drives.

Before a USB is allowed to log into a computer within a network, the administrator must whitelist or blacklist the USB using the vendor ID (VID) and product ID (PID). These are 16-bit numbers that identify the USB. If a user brings any type of device into a network that is not whitelisted, it will not be granted access to the network.

When a USB is inserted, RevBits EPS will capture the event and the security log will automatically contact the admin. On the RevBits admin panel, the admin can whitelist or blacklist the device with a single click. If the device is whitelisted, it must be removed and re-inserted before it can be logged into the system.

Each time a USB is inserted or removed from a computer, whether allowed or not, RevBits EPS logs it and sends a notification to the admin panel. If a blacklisted or unlisted USB is inserted, it will be blocked, and a "Blocked Devices Log" alert will be sent to the admin panel.

RevBits EPS records historical information on all activity. If a malicious insider moves from one computer to another, inserting a USB and attempting to log into Microsoft Windows, RevBits EPS will alert the admin, and provide the historical information that identifies the times, the user, the USB, and all the computers they tried to log into.

Other endpoint security solutions might provide the ability to whitelist and blacklist USBs, but they fail to log the activity or send real-time notifications to the admin. They also require API integration with a SIEM in order to get an alert sent to the admin. This capability is often sold as a separate product or add-on, with additional cost and support required. These capabilities are included within RevBits EPS at no additional cost.

RevBits EPS testing results conducted by ICSA

RevBits EPS has been repeatedly 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 is 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 most recent test 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 EPS. For the detailed certification report, go to the Advanced Threat Test Report.

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