Endpoint Security

Intuitive, High-Performance Security Software That Blocks the Most Advanced Security Threats.

As an intuitive, high-performance security software, RevBits Endpoint Security blocks the most sophisticated attacks. RevBits Endpoint Security is the only solution available that conducts a three-phase analysis of threats. The feature-rich and comprehensive RevBits Endpoint Detection and Response (EDR) module provides complete control and access to the breached system from anywhere.

Analysis and Detection Features

Three-phase analysis of new executables
New executables are isolated and analyzed, before release, to protect the network. The analysis is conducted first with signature comparisons; second with machine learning verification, and third by behavioral analysis.

Advanced exploit detection
RevBits Endpoint Security's exploit detection is layered on top of vulnerable applications and processes, including, but not limited to, web browsers, desktop publishing software (such as Microsoft Office or Adobe Reader) and others.

Process recording
RevBits Endpoint Security records all process execution and termination information, including their hashes (MD5, SHA 1 and SHA2), workstation, username and timestamp for six months.

Effective anti-ransomware module
Through its sophisticated filesystem sandboxing feature, RevBits Endpoint Security can detect and block all types of simple and sophisticated ransomware.

Control USB devices
System administrators can establish extensive USB device policy through the built in USB manager environment.

> **Endpoint security with the power to detect and block the most sophisticated malware and fully support endpoint investigations and analysis through real EDR.**

Host-based firewall
System administrators can fine tune network and firewall rules for both individual workstations, as well as groups of workstations.

Immediate host isolation
Automatically or manually protect the network by confining hosts that are potentially infected.

Automatic forensic evidence extraction
On-demand or automatic pre-shutdown forensic evidence extraction to assist in fast incident response.

Advanced notification system
RevBits Endpoint Security integrates seamlessly with all SIEM solutions. Additionally, administrators will receive SMS and email notification when an incident occurs.

Endpoint Investigation Capabilities

Truly inventive
Two US Patents for a unique technological advancement to detect and block signed and unsigned drivers from accessing the kernel.

Command line capable
Powershell and command line prompt terminal to interact with all remote endpoints.

Complete EDR menu
Interact with remote endpoints to include: Process, File Explorer, Registry Explorer, Command Console, Services, Drivers, Anti-root Kit, Startup and Tools.

GUI control over all endpoints
Graphical Interface for all remote endpoint EDR operations.

Deep control of endpoints
interact with remote endpoints to control registry explorer, file explorer, process explorer with process tree hierarchy.

Total control at a distance
System Administrators can remotely dump process memory, raw disk, and raw drive dump.

Software Requirements

Operating Systems: Windows 7+ (Windows 7, 8, 8.1, 10, 11, 2008, 2012, 2016, 2019,)

MacOS (10.15 Catalina, 11 Big Sur, 12 Monterey+), M1 chips supported

Linux Debian family [Debian, Ubuntu, Mint, etc.], and Redhat family [CentOS, Redhat, Fedora, etc.]

Minimum Requirements: 200MB disk space, 4GB RAM 32 and 64 bit operating systems are supported

Additional Solution Features

Fully featured in an Air-Gap environment – RevBits Endpoint Security is fully deployable in an air-gap environment. All product features are functional and actionable without internet connection.

Catch and contain malware at the endpoint – RevBits Endpoint Security conducts a unique three-phase analysis on all new executables. This analysis includes signature scanning, machine learning and behavioral analysis, which maximizes the accuracy of malware detection and minimizes false positives.

Complete visibility and control with RevBits EDR – Thorough, low-level details of processes, threads, registry, filesystem and kernel are visible and controllable through RevBits EDR GUI, not a simple command-line. System administrators can execute commands in powershell or command prompt on workstations. Single click forensic evidence extraction, memory imaging and dish imaging features make RevBits EDR the most sophisticated EDR solution on the market.

Endpoint Security Benefits

Reduce the chance of a successful malicious execution – RevBits Endpoint Security protects against all types of endpoint threats in any kind of network through its unique three-phased analysis of new executables. From the least sophisticated to the most sophisticated malware, RevBits Endpoint Security is designed to detect and block its execution and save the network from a costly breach.

Stop malware before from executing – By isolating and thoroughly analyzing new executables the possibility of a successful attack is highly diminished.

Thorough forensics – By compiling highly useful information regarding executions, scripts, and commands the system administrators time spent on triage and cleanup are highly reduced. This capability expands the capability to meet compliance needs and standards.

Reduce the need to hire outside remediation and forensics firms – RevBits Endpoint Security's EDR module allows system administrators to conduct internal network investigations which minimizes the need for outside resource utilization.

Reduce the success of the insider threat – The cost to the organization posed by an Insider Threat is substantial. Costs associated with breaches and data theft can be mitigated and controlled through the extensive USB policy management capability of RevBits Endpoint Security agreement.

Intuitive dashboard revealing actionable insights – RevBits Endpoint Security provides an easy-to-understand, real-time view of threats through its modern web interface. The dashboard presents extensive historical information of all executables in a clear and simple mosaic, and maintains detailed process information for six months.

Detailed historical information of all executed commands – RevBits Endpoint Security records and reports all executed commands and scripts in all command and script interpreters including Windows Command Prompt, Powershell, VBScript and JScript.

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