RevBits
ENDPOINT DETECTION & RESPONSE

Powered by
Quick Heal

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

Protect your system with the most advanced endpoint protection software package the cybersecurity industry has to offer. As an entierely remote program, RevBits Endpoint Detection & Response gives you complete control and access to the breached system from anywhere. Conduct your own investigations and analyses with our file management system, RAM imagery capture, and easy-to-use EDR platform.

RevBits Endpoint Detection & Response

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 Detection & Response' 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 Detection & Response records all process execution and termination information, including their hashes (MD5, SHA1 and SHA2), workstation, username and timestamp for six months.

EFFECTIVE ANTI-RANSOMWARE MODULE

Through its sophisticated filesystem sandboxing feature, RevBits Endpoint Detection & Response 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.

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 Detection & Response integrates seamlessly with all SIEM solutions. Additionally, administrators will receive SMS and email notification when an incident occurs.

RevBits Response Module

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.

www.revbits.com
844-4REVBIT (844-473-8248)

RevBits®
Cyber Security Solutions

Benefits

REDUCE THE CHANCE OF A SUCCESSFUL MALICIOUS EXECUTION

RevBits Endpoint Detection & Response 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 Detection & Response 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 Detection & Response module allows system administrators to conductinternal 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 Detection & Response.

Software Requirements

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: 200MB disk space
4GB RAM

32 and 64 bit operating systems are supported

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

CATCHAND CONTAIN MALWARE AT THE ENDPOINT

RevBits Endpoint Detection & Response 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.

INTUITIVE DASHBOARD REVEALING ACTIONABLE INSIGHTS

RevBits Endpoint Detection & Response 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. Single-click hash whitelisting or blacklisting is also available.

DETAILED HISTORICAL INFORMATION OF ALL EXECUTED COMMANDS

RevBits Endpoint Detection & Response records and reports all executed commands and scripts in all command and script interpreters including Windows Command Prompt, Powershell, VBScript and JScript.

www.revbits.com
844-4REVBIT (844-473-8248)

Powered by Quick Heal

RevBits
Cyber Security Solutions