RevBits®

Cyber Intelligence Platform

Unified XDR Powered by Multiple Security Products and Controlled Through One Integrated Dashboard.

Expanding IT and cybersecurity infrastructure perimeters are spread across a complex ecosystem of multi-clouds, on-premises, and mobile and remote users. RevBits Cyber Intelligence Platform (CIP) provides unified visibility and control to thwart cyberattacks across this diverse ecosystem, with a single-view advantage.

The effort required to manage multiple, disparate security products and tools is time consuming and plagued by many security gaps. The lack of intelligence sharing across products creates poor visibility, making it difficult to find, correlate and rapidly eliminate threats.

RevBits Cyber Intelligence Platform

RevBits CIP leverages a powerful suite of best-in-class security products that are integrated and unified into a single intuitive dashboard. With single sign-on capability, administrators monitor, interact with, and control Endpoint Security, Email Security, Privileged Access Management, Deception Technology, and Zero Trust Networking.

Single sign-on for accessing and managing all RevBits products
Single sign-on puts power in the hands of administrators to quickly access, monitor, and control all RevBits product capabilities, with strong network protection.

Access all onboarded solutions with a single click
Access to any onboarded RevBits product is easy and one click away.

RevBits CIP provides a holistic and intuitive view into all types of threats across the entire enterprise technology landscape. Real-time information from multiple threat sources enables immediate detection and response, creating more reliable and faster outcomes.

Monitor diverse critical security statistics in one dashboard
Delivers a complete security view in one dashboard, eliminating the difficulty of managing multiple products and reporting environments. Complete situational awareness over the security posture puts control in the hands of administrators.

Immediate security knowledge and response for mobile devices
Enables an immediate response posture, independent of time of day or geographic location, through full mobile device support. Complete security, access, and environment control is always available.

Active alerting for all RevBits products
One window displays all active alerts with a single view and link to alerts for immediate threat mitigation. A single platform provides administrators with a heads-up display for all alert reporting on all onboarded RevBits products. With one click, administrators can launch to individual incidents, regardless of the product or alert.

Customizable dashboard
To better meet admin requirements, the dashboard is configurable with available widgets within RevBits various cybersecurity products.

For more information, go to www.revbits.com

Actionable intelligence
Brings XDR to life with multi-vector threat intelligence that becomes immediately actionable.

Cross-functional security and unified dashboard simplifies forensics
Collects, aggregates, processes, and preserves security data from all RevBits onboarded products. A unified dashboard provides a 360-degree view to analyze multi-vector cyberattack evidence. Combines intelligence between products, enabling analysts to uncover the digital evidence they need to improve and accelerate detection and rapidly mitigate events.

Aggregate and correlate diverse attack data
Correlates diverse protection measures within the cybersecurity infrastructure, empowering security analysts and forensic investigators with rapid results.

Reduce response time
Shortens mean time to respond (MTTR) with automated and single-click mitigation across all attack vectors and surfaces.

Remove security gaps
Eliminates security gaps associated with siloed solutions, disjointed data structures and languages, and disparate detection methods.

Seamlessly navigate incidents
Navigating through malware incident details becomes easier and more efficient utilizing integrated search capabilities, machine learning score graph, virus scan indicators, process trees, and radar graphs. Mouse-over functions provide even more granular information about IP addresses and indicators on attack IDs, with links to the MITRE Attack Framework Database.

Reduce response from days to minutes
Intuitive dashboard dramatically reduces false positives, allowing analysts to be more efficient, focusing on the most critical incidents.

RevBits CIP Product Capabilities

RevBits Endpoint Security (EPS)

RevBits EPS unique architecture has custom handlers, or proprietary application loading detection capabilities, that 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.

RevBits EPS evaluates the entire process, including executables, leaving no ability for malware to hide within legitimate programs and applications. It conducts a unique three-phase analysis on all new executables, including signature scanning, machine learning and behavioral analysis. This maximizes the accuracy of malware detection, and minimizes false positives.

USB device management - USB device policies can be used to whitelist or blacklist all USB devices. Whitelisting and blacklisting can be applied by Vendor ID, Product ID, or device type (e.g., webcams, wireless adapters, storage, etc.).

Patented anti-rootkit technology - Provides full visibility to the kernel and blocks all unauthorized signed or unsigned drivers from accessing the kernel.

Robust GUI-based EDR module - Provides admins with the capability to interact, control, isolate, and mitigate infected endpoints. The GUI-based EDR module provides in-depth forensics capabilities and enhanced management above other EPP/EDR solutions.

RevBits Email Security

RevBits Email Security Endpoint-Based Agent (EBA) is a native SaaS-delivered solution, also referred to as integrated cloud email security (ICES). The endpoint-based agent protects against malicious emails on endpoints, taking over where a secure email gateway leaves off. It fills in security gaps by leveraging distributed processing for deep analysis on remote user endpoints to detect and block malicious emails that get past the centralized layer of an organization's security stack. RevBits has two U.S. patents for email security - a patent for user inbox advanced email analysis, and another patent for a unique methodology that detects page impersonation attacks.

RevBits Secure Email Gateway (SEG) is cloud-based and globally deployed for dynamic scalability. It is also inherently redundant for reliable and dependable operations – anywhere in the world. RevBits SEG protects against email threats by blocking phishing, business email compromise (BEC), spam, social engineering, ransomware, and other malware. RevBits SEG is positioned as a front-line corporate email defense, inline within the email transportation route, and directly in the path of all traffic going to the corporate email server.

For more information, go to www.revbits.com

RevBits Deception Technology

By deploying decoys of real server-based honeypots in a dual-virtualization environment, malicious actions by external threats or insiders are detected and reported immediately. RevBits Deception Technology (DT) utilizes the most common database servers, file sharing services, and more.

RevBits DT is the only solution on the market with dual-layer virtualization and real honeypot servers. Easily deploy multiple honeypots with the click of a button, and minimal resource consumption. Automated implanted credentials lure attackers to honeypots, revealing the original breached system.

Privileged Access Management

RevBits PAM is an advanced access management solution that includes six modules and extensive session logging that captures keystroke and video. RevBits PAM has two U.S. patents - browser-based zero-knowledge encryption, and authentication authority that extends to various hardware security solutions. These unique access control capabilities reduce vendor relationship management efforts, and increase access management safeguards. As enterprise perimeters expand access management environments, the number of vendors needed to cover the evolving access landscape is increasing. RevBits PAM provides comprehensive access control, for on premises, and in the cloud.

RevBits PAM modules:

- **Privileged Access Management** - regulates access to critical resources, captures keystrokes and video records all privileged sessions.

- **Privileged Session Management** - provides keystroke and query logging for all sessions through the solution's Jump Server.

- **Password Management** - extends authentication security with hardware security modules, USB tokens, smart cards, near-field communications, and RFID.

- **CI/CD Integration** - The module seamlessly integrates the most popular CI/CD pipeline toolsets, supporting Jenkins, Puppet, Terraform, OpenShift, Ansible, Docker, Cloud Foundry, and Kubernetes with future tools under development. Adding the plug-in to your current

platform unlocks the capabilities of secure secret management across the CI/CD lifecycle for easy management of CI/CD users, credentials, and assets.

- **Service Account Management** - scans and onboards service accounts, and scheduled tasks for IIS web applications.

- **Key Management** - allows users to easily generate and store encryption keys.

- **Certificate Management** - reports all expired or soon-to-expire certificates and vulnerable implementations of SSL.

Zero Trust Networking (ZTN)

RevBits ZTN auto-scaling ability and key-point geolocation distribution makes RevBits ZTN the fastest zero trust networking solution on the market. Deep assessment of an endpoint's security posture inspects tunnel traffic for malicious content and data security.
RevBits ZTN creates an identity and context-based logical-access boundary that encompasses users and their applications. Applications are hidden from discovery, and access is restricted using a trust broker with a collection of named entities. The broker verifies the identity, context, and policy adherence of specified participants before allowing access.

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-bit and 64-bit operating systems are supported.

Deployment Options

RevBits CIP offers flexible deployment options. All hosting environments are supported, including on-premises, cloud, and hybrid. The cloud-based solution leverages global points of presence with elastic auto-scaling support for multi-site organizations. With 24 PoP locations around the world, RevBits CIP has built-in redundancy for rock-solid service resilience.

Cyber Intelligence Platform Benefits

Eliminates security gaps created by siloed security products – Enables more accurate detection and prevention capabilities and lower total cost of ownership (TCO), while achieving faster time to value. Integrates relevant data for faster, more accurate alert triage.

Improves productivity of security operations – Reduces the complexity of security configuration and incident response with alert and incident correlation, built-in automation and nearly zero false positive alerts. Collects, processes, preserves, and provides the visibility to analyze cyberattack evidence, identifying vulnerabilities and speeding mitigation.

Unifies embedded security products – Provides better security outcomes than siloed and isolated security products and tools. Integrates patented security modules into a single, unified security platform with multiple streams of telemetry, and multiple forms of detection.

Consolidates multiple cybersecurity capabilities – A cohesive cybersecurity platform that accelerates detection and response. Local and external threat intelligence is immediately shared between security modules to efficiently block threats across all components.

Supports on-premises and cloud-hosted environments – Combined with auto-scaling and advanced load balancing, RevBits CIP dynamically scales with demand. Provides centralized configuration and hardening capability with weighted guidance to help prioritize activities.

Additional Solution Features

A unified, yet modular and extensible cybersecurity solution – Can be deployed to work with Syslog, LogRhythm, Splunk, SIEM, and other log management and security platforms.

Best-in-class embedded security products – Email Security, Endpoint Detection & Response (EDR), Deception Technology, Privileged Access Management (PAM), and Zero Trust Networking (ZTN).

Multi-tenancy security platform – Can be deployed in the cloud or on-premises, and supports multi-cloud, on-premises, and hybrid environments.

Flexible architecture – Allows security teams to deploy whatever security capabilities they need. Choose products by adding or removing licenses within the CIP dashboard. Security products can also be independently deployed within existing security infrastructure.

Backed by 5 U.S. Patents – All patents are focused upon solving critical security issues.

Automates detection and remediation of anomalous activity – Fully cross-functional multi-layered security stack.

Coalesces cybersecurity products into a single intuitive dashboard – Enables rapid cyber forensics with analytics and context, to quickly resolve threats.

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