RevBits

PRODUCT BRIEF

Cyber Intelligence Platform

RevBits Unified Cybersecurity Reduces Vendor Sprawl

Multi-layered security and SOAR capabilities unified within a single, natively embedded platform.

Cybersecurity vendor sprawl has created complexity and fragmented security postures, placing undue stress upon IT and security operations. When cybersecurity leaders lose control, they call for industry standard interoperability. However, the idea of achieving industry standardized interoperability among cybersecurity vendors with widely different solutions is a panacea that will not happen anytime soon, if ever.

Cybersecurity is complex and diverse. Standardizing interoperability may not be feasible. To eliminate complexity, confusion and fragmented enterprise cybersecurity efforts, vendor consolidation may be the better solution.

Cybersecurity vendor reduction

Cybersecurity vendor reduction can occur when companies natively integrate multiple products into a single solution. As vendors expand their product offerings, eventually all the vendors from a declining product area will consolidate into an expanding market.

Consolidation also happens when one cybersecurity vendor acquires another vendor with complementary technology. Sometimes the acquiring company shelves the acquired product. If the product moves forward, it can take a year or more before the technology is incorporated within the acquiring company's product portfolio. Even then, the technology is almost never fully integrated. Remember, the acquired product had an historical direction and a roadmap for future expansion. It had a CTO that drove that direction for years. Now the product, and all or part of the development team, and other departments, must assimilate within a new company structure and culture. The result often reflects the juxtaposition of technology and talent. So, while the acquiring vendor may have eliminated a vendor, for all intents and purposes, the customers must still work with two different products.

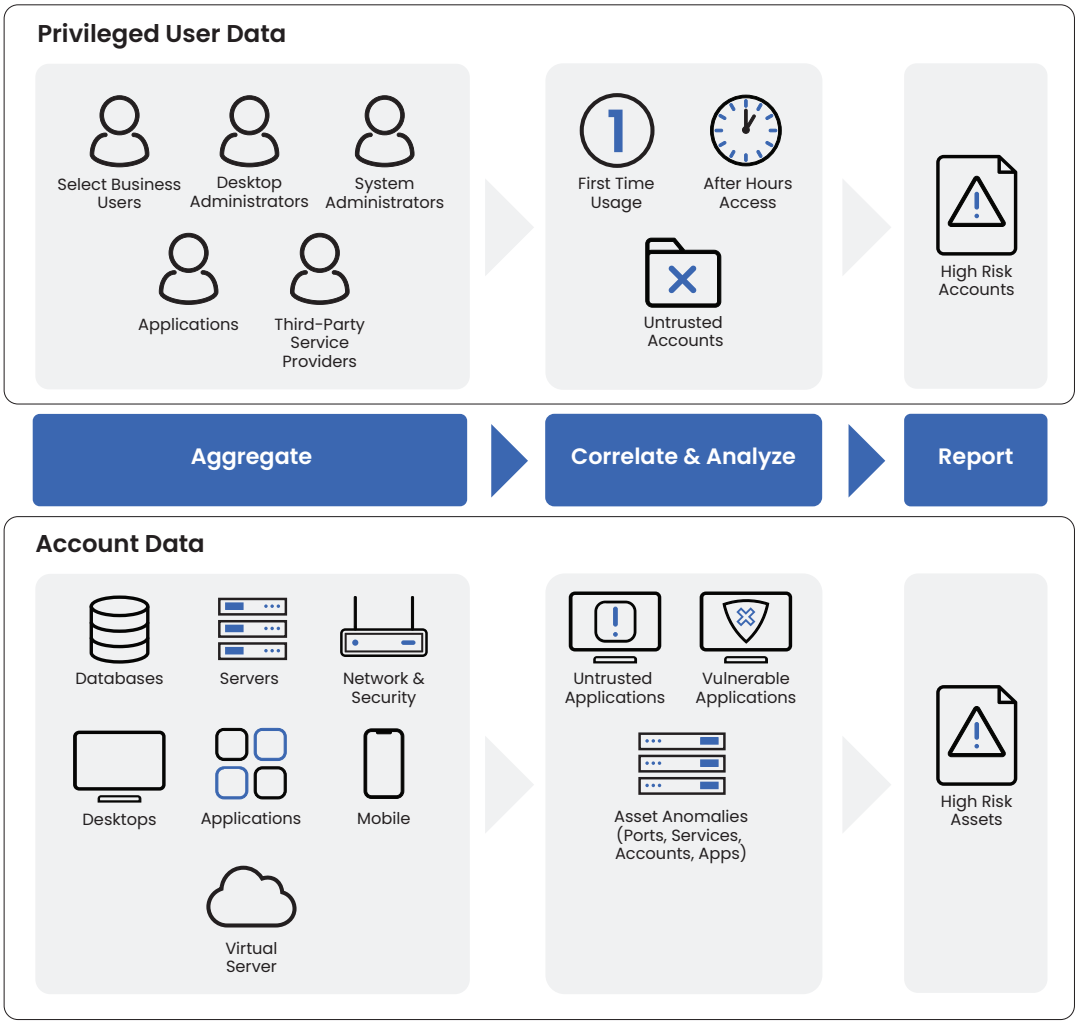
"As vendors expand their product offerings, eventually all the vendors from a declining product area will consolidate into an expanding market."

If you can't consolidate vendors, try consolidating their data

Disparate technology integration takes a lot of time and effort for both parties. For example, Security Orchestration, Automation, and Response (SOAR) vendors often have no motivation to collaborate with other third-party security products. Particularly if a product category has already been integrated. It is a highly competitive market and consolidation is on every cybersecurity vendor's mind. If a product does become integrated, when the vendor makes changes or upgrades, the SOAR vendor must also make those changes. This becomes amplified across every product integrated into the SOAR. There are also hazards along the way. When independent products are incorrectly integrated, risk is introduced.

SOAR is an approach that organizations use to streamline threat and vulnerability management, incident response, and the automation of security operations. SOAR is being consumed by XDR and SIEM solutions and is one of those products that is likely on its way to being consolidated within one of these markets.

While standalone SOAR can be a great addition to a large organization's security implementation, it has its disadvantages. For one, most are overly complex and difficult to integrate with other tools. Many are not a suitable fit with today's agile security environments leaning into democratizing cybersecurity management. Integrations require highly technical expertise and require custom code written by developers or IT engineers. A standalone SOAR does not reduce vendors, it requires third-party vendor technology, and aggregates and analyzes their data.



RevBits natively integrated security unifies security functions, analysis and reporting.

Natively integrated multi-function security and SOAR – unified within a single platform

A successfully integrated cybersecurity platform requires more than integrating security data, logs, alerts, user data and profiles. Every product has its own unique technology, format, structure, dataset, tables, logs, reporting and APIs.

A holistic cybersecurity platform requires natively integrated products with unified asset management, user management, roles, rules, and permissions. When logging into each of the security products, the user and asset management, rules, and permissions are seamlessly integrated. After the initial login, and based upon permissions, the user can click on the different security product links to access and work with them. Additionally, because the products are natively embedded, much of the product code can be shared.

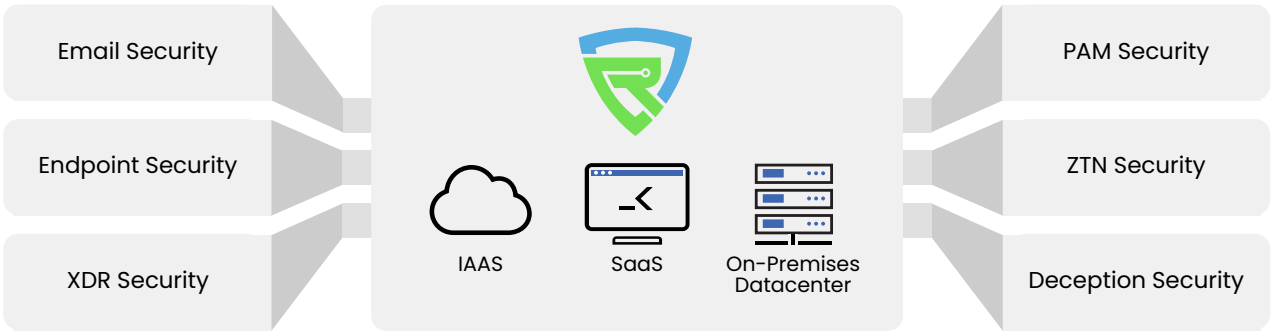
There's integration, and then there is INTEGRATION

RevBits Cyber Intelligence Platform (CIP) delivers unified, native multi-layered security and orchestration. We are advancing cybersecurity to a new level, taking down security barriers that formerly challenged enterprises and service providers. We are solving problems created by too many cybersecurity products that cause security gaps, leaving enterprises vulnerable to malware, man-in-the-middle, phishing and spear phishing, SQL injection, stolen credentials, cross-site scripting, and other attacks. RevBits CIP automates the detection and remediation of anomalous activity within a cross-functional multi-layered security stack. Coalescing multiple security products and their security data into a single intuitive GUI dashboard, RevBits enables rapid cyber forensics with analytics and context, to quickly resolve threats.

RevBits CIP, security products and modules (all natively integrated)

- Cybersecurity Intelligence Platform (CIP)
  - Security orchestration, automation, and response (SOAR)
- Email Security
  - Endpoint Email Security
  - Secure Email Gateway
- Endpoint Detection & Response (EDR)
- Endpoint Security (EPS)
- PAM
  - Privileged session management
  - Service account management
  - Web application access management
  - Third-party access management
  - Full-featured password management
  - Certificate management
  - Key management
- Zero Trust Network (ZTN)
- Deception Technology

Unified Security Platform



RevBits holistic security mesh seamlessly ingests and correlates cross-functional data with context, analyzes it, and shares data, logs, activities, sources, and reporting, across all security functions with a single view.

RevBits CIP dashboard monitors security data and metrics across all RevBits security products. Data from every product is coalesced to provide a comprehensive view of threats with automated detection and incident response. Threat intelligence and AI improve security personnel decision-making and automatically responds to threats. The automated responses and deep diagnostics reduce the time to resolve security events.

Orchestration

Orchestration is the core of RevBits CIP. Every RevBits security product, including their associated functional modules, flow into a single unified dashboard. RevBits CIP orchestration alerts, reports and takes action on all RevBits products and modules, which are natively integrated within the platform.

Orchestration collects data from the RevBits' natively integrated security products, complete with context to provide a complete perspective of security threats across all attack surfaces. Security event data is consolidated into one location and is easily visible to ease vulnerability management.

Event automation reduces the administrative burden for network administrators and security analysts. Automated workflows, alerts, and responses enable admins to automatically respond to security events and will automatically shut down a system or user account if anomalous activity is detected. Root-cause diagnostics and intelligence help the admin quickly find issues and provide the best actions to take to mitigate incidents.

Automation

With a single click, RevBits CIP delivers automation through direct action into the incident for investigation and mitigation. This is quite different from independent SOAR products that automate responses to the admin, that then go into third-party security products or tools to investigate the alerts.

Response

SOAR ingests alerts from onboarded third-party security products and tools and manages their alerts and reporting of incidents. The various workflows assign the incidents to the admin for triage and management.

Rather than having to go into the third-party security product or tool individual dashboards, RevBits CIP is inherently integrated with the RevBits security products and modules. For example, RevBits EPS is accessible with a single click within the RevBits CIP dashboard. The admin is at the alert within the actual product for immediate response.

RevBits CIP benefits

- RevBits security products can be integrated into 3rd-party SIEM, SOAR, and other incident response platforms
- Eliminates security gaps created by independent products
- Unified architecture lowers total cost of ownership (TCO), while achieving faster time to value
- Improves productivity of security operations with alert and incident correlation and built-in automation
- Reduces incident response complexity for better security outcomes over isolated products

RevBits CIP capabilities

- Local and external threat intelligence is immediately shared between security products to efficiently block threats across all threat surfaces
- Reduces missed alerts and false positives by correlating and confirming alerts automatically
- Integrates relevant data for faster, more accurate alert triage
- Centralized configuration and hardening capability with weighted guidance helps prioritize activities
- Collects, processes, and provides visibility to analyze cyberattack evidence to speed mitigation
- Patented security coalesces multiple streams of telemetry data, with multiple forms of detection

Improves security team productivity

- Converts a large stream of alerts into a small number of incidents that are more easily investigated
- Provides integrated incident responses with context from all security products to quickly resolve alerts
- Automates repetitive, time-consuming and tedious tasks
- Reduces training and support, through a common management and workflow experience across security products

The most efficient and effective security approach is one that natively embeds multiple security products and SOAR functionality within a unified platform and dashboard with a single view perspective. And that is what RevBits CIP achieves - delivering the best of both.

RevBits®, LLC • 34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248)