## The #1 Way to Eliminate Security Gaps

# Break Through the Deception with a 360-Degree Cybersecurity View

On a clear day the majestic Grand Canyon, with its awe-inspiring views, can leave you breathless with wonder. From the vantage point of the canyon floor, one can make that slow 360-degree turn and take in every facet of the enormous carved walls on all sides. It is one of the most incredible sights you can experience.

A 360-degree cybersecurity view is a term we often use at RevBits. It entails the whole panorama; every touch-point, from known and unknown signatures, and anomalous behaviors, to deceitful emails and websites with malicious code. Complete cybersecurity protection encompasses human and machine identities, privileged accounts and secrets, endpoints, applications, networks, and clouds, and all the vulnerable security gaps in-between. Behavior-based security proactively monitors and analyzes all activity so that deviations from normal behavior patterns are identified and dealt with quickly.

Simply put, if you can't see attacks clearly across all surfaces, you can't initiate a complete defense. 360-degree cybersecurity visibility includes views of the past, present and future, made available within a single intuitive dashboard.

This cybersecurity view presents a complete and accurate picture of every attack, by aggregating analytics from diverse attack vectors and surfaces across an organization. It provides a powerful defense, by symbiotically combining cross-functional cyber protection with the analysis and investigative capabilities necessary to protect against recent and in-process events, as well as protective measures for future attacks.

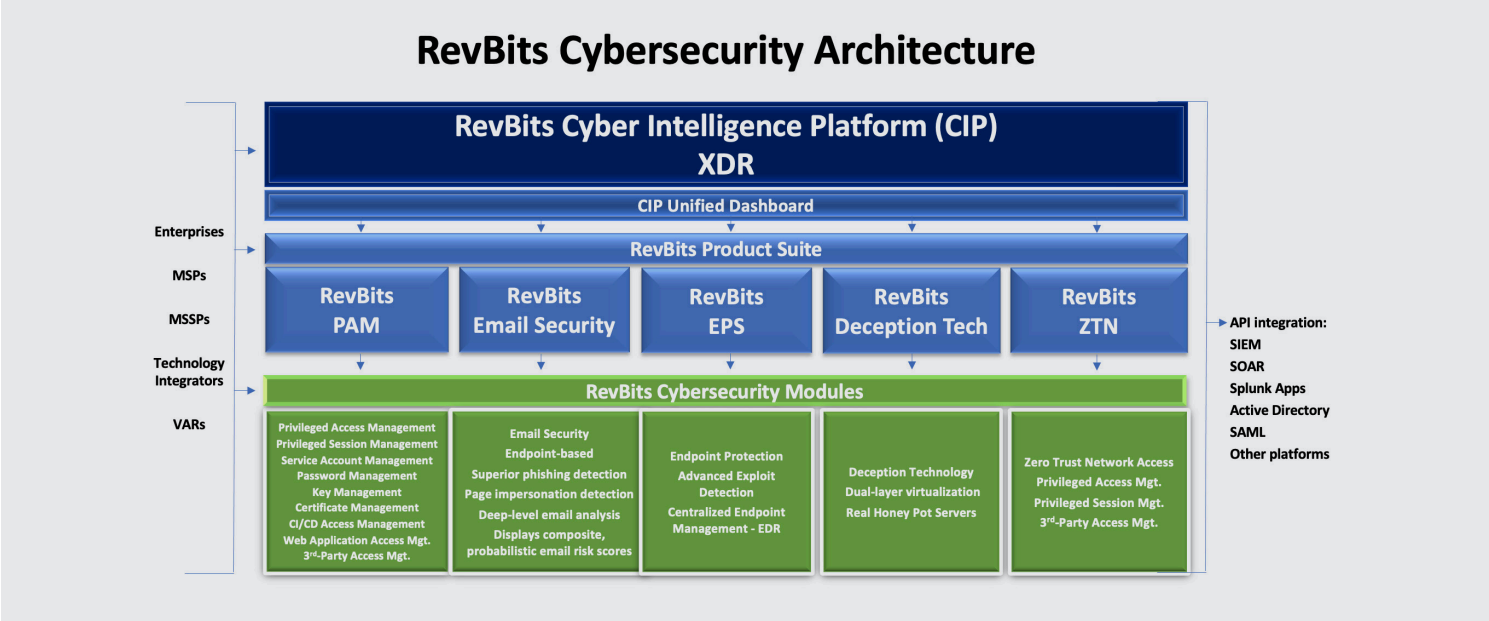
## No organization is safe

No amount of money or resources will enable complete protection. If bad actors target a company, they will eventually infiltrate their network. While organizations spend months, even years, protecting and defending their digital assets, at the right time and with the right technology, a hacker will break through their defenses. Once in, they can lay low for months, digging into and worming their way across the organization's digital infrastructure, and taking advantage of their vulnerabilities. To remain undetected, they use deception and evasive measures, and hidden malicious code. When they're ready to take over control, they unleash their attack until they've accomplished their objective. These nefarious operations, and the methods used and activities taken, encompass the entire attack timeline from beginning to end.

## View the entire cyberattack chain of events

Analyzing the entire cyberattack lifecycle requires deep intelligence and visibility into malicious and suspicious activity throughout the network. Bad actors use many different tactics, such as malware, phishing, SQL injection, zero-day exploits, man-in-the-middle, spear-phishing, and others. Cyberattacks have multiple stages that

**Complete cybersecurity protection encompasses human and machine identities**




are part of the attack chain of events. When attacks are discovered at the point of origin, they can be quickly stopped to minimize, and prevent damage. Every cyberattack has evidence that can be traced. Analyzing this evidence informs analysts so they can minimize and prevent attacks.

## Cross-functional security with a unified dashboard simplifies forensics

RevBits Cyber Intelligence Platform, or CIP, collects, processes, and preserves security data through its five security products. These include Endpoint Security, Email Security, Privileged Access Management, Zero Trust Networking, and Deception Technology. CIP has a unified dashboard that provides security analysts with a 360-degree view to analyze multi-vector cyberattack evidence. RevBits powerful security modules exchange intelligence, to uncover the digital evidence analysts need to optimize detection and rapidly mitigate events.

**Reduce Response Time -** RevBits shortens mean time to respond (MTTR) with automated and single-click mitigation across all attack vectors and surfaces. Organizations gain full insights into malicious activity, with centralized policy enablement and enforcement, and a contextualized and coalesced 360-degree view across the enterprise.

**Remove Security Gaps -** RevBits CIP eliminates security gaps associated with siloed solutions, disjointed data structures and languages, and disparate detection methods. We unify visibility to maximize the accuracy of malware detection and mitigation, while minimizing false positives. We authorize and authenticate access controls for human and machine identities, privileged accounts and secrets, endpoint security, and zero trust networking - all within a single interface.

**Seamlessly Navigate Incidents -** Navigating through malware incident details becomes easier and more efficient utilizing RevBits 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. Analysts and forensic investigators can quickly and easily view indicators, timelines, and tactics, and all of the steps that were taken, for both malicious and suspicious activities.

**Aggregate and Correlate Diverse Attack Data -** RevBits correlates diverse protection measures within the cybersecurity infrastructure, empowering security analysts and forensic investigators with rapid results. These automated results have greater impact by proactively protecting business assets, rather than reacting to false positives and other non-priority events. RevBits automates the detection and remediation of anomalous activity among a cross-functional multi-layered security stack. Everything is integrated into a single GUI dashboard. This intuitive interface enables rapid cyber forensics with analytics and context to provide efficient and expeditious threat resolution.

**Reduce Response from Days to Minutes -** RevBits intuitive GUI dashboard dramatically reduces false positives, allowing analysts to be more efficient, focusing on the most critical incidents. The ability to make the right decisions, when time is limited and the pressure is on, can dramatically limit an attack's impact. With RevBits, triaging and investigating are accomplished much more quickly, over manual event responses.

**Click here** to watch a brief video to learn more about how RevBits simplifies cybersecurity investigations, or visit **RevBits Cyber Intelligence Platform** for more details.

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