

7 Cybersecurity Platform Requirements and Important Questions for Vendors

Ask any cybersecurity leader, and they'll tell you the increasing number and sophistication of cyber breaches is only going to get more challenging. Cyber threats can jeopardize every digitally enabled organization. Lone wolf bad actors, syndicated hacking groups, organized crime, nation-state hacking groups, and malicious insiders all pose great threats and risks to organizations, large and small.

Table of contents

Protecting corporate resources and assets	3
Seven critical elements needed to defend against the ongoing barrage of cyber attacks	4
Questions to ask cybersecurity platform vendors	8
Below are key capabilities to look for in a cybersecurity platform	11
Cross-functional security and unified dashboard simplifies forensics	12

RevBits product line



Cyber Intelligence
Platform



Endpoint Security



Email Security



Privileged Access
Management



Zero Trust Network



Deception
Technology

Protecting corporate resources and assets

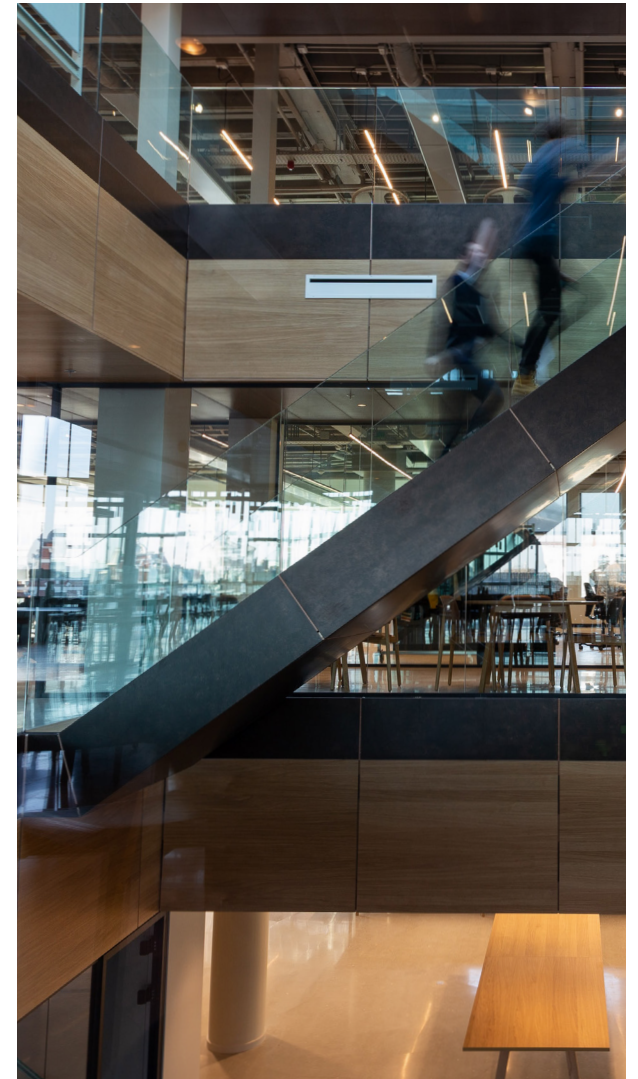
Many organizations have accumulated numerous single-function security products, like anti-virus software, anti-ransomware, privileged access management, email gateways, and other incongruent products, in an attempt to defend against ever-changing cybersecurity risks. Based upon the weekly barrage of breaches we read about, this approach is clearly not working.

Whether you're an enterprise or a managed security service provider, trying to integrate these products together won't provide a reliable, all-inclusive view of the organization's varied attack surfaces. These individual products won't provide a detailed cross-functional analysis of activity and behavior across the enterprise, let alone the time savings and cost efficiencies that enterprises need. Siloed security products have made it increasingly difficult for IT, security, and risk teams to protect the vulnerability gaps between security products and across their expanding digital infrastructure.

Organizations of all sizes and industries need solutions that allow their security teams to quickly and efficiently map out their security infrastructure, analyze abnormal behaviors, and validate digital identities and system vulnerabilities across the enterprise's digital ecosystem.

Disjointed security tools and disaggregated security data from myriad vendors create too many false positives, making a difficult task even harder for over-extended IT, security, and risk leaders and their teams. A unified and natively integrated security platform will automate many low-level manual tasks, and proactively defend the entire enterprise-wide technology landscape of on-premises infrastructure, legacy systems, cloud workloads, endpoints, mobile users, and IoT devices.

Selecting the right cybersecurity platform is one of the most important decisions for an organization. The purpose of this eBook is to equip decision-makers with the information they need, and questions to ask vendors, before selecting a cybersecurity platform and the security products and modules they encompass. How they work together as a unified solution is critical. We will also discuss the nuances and technology differentiation that make one cybersecurity platform better than another. Hopefully, as you evaluate vendors, this information will help identify some critical capabilities that some of the bestselling cybersecurity solutions are lacking.



Seven critical elements needed to defend against the ongoing barrage of cyber attacks

1 No single product will solve all cybersecurity challenges. In fact, as an increasing number of individual security products are added to the IT ecosystem, they make managing and mitigating threats more cumbersome and complex. Meanwhile, cybersecurity attacks continue to grow in number and sophistication. In response, we're now seeing many of the most forward-thinking organizations adopt a unified approach.

To secure their digital assets, businesses are leveraging unified security platforms that protect on-premises legacy systems, multi-cloud environments, remote and mobile workers, and IoT devices. An extensible security platform, with

embedded multi-function security capabilities, supports an ecosystem that synergistically and efficiently addresses the frequency, complexity, and rapidly changing nature of cyber-attacks. A single dashboard can forensically map multiple attack vectors, and coordinate analytics, machine learning, behavior analysis, identity, privileged access, and a zero-trust model. This unified approach can create a highly effective cybersecurity posture.

As is often the case with people, specialized technology solutions working together can achieve more than what can be accomplished with each solution working independently.

Endpoint security, email security, privileged access management, deception technology, and zero-trust networking all have their strengths. But when you fuse those solutions together, they produce a far greater cumulative strength. As we'll see throughout this document, RevBits Cyber Intelligence Platform, or CIP, with its ability to protect all enterprise digital assets, is a case where the whole is greater than the sum of its parts.

2 Email security is a foundational requirement, as email remains the leading source of malicious actions inflicted on unsuspecting users. Robust endpoint-based email security, complemented with a secure email gateway, and security awareness training, is needed to reliably and consistently thwart attacks.

The most advanced email scams are page impersonation attacks. This is where hackers discover that an organization uses, say Office 365. They create a fake Office 365 login page and author custom emails that are then sent to employees. Impersonation attacks take advantage of human errors in judgment. When employees unwittingly open and respond to the emails, they can provide hackers with their credentials and open access to the corporate network.



"Despite the fact that there's a huge market for cybersecurity software, the ever-increasing number of serious cyber breaches clearly demonstrates a need for better protection, and an integrated approach."

Hackers understand the limitations of gateway appliances with intelligence feeds and signature scanning and get around them with page impersonations, multi-layer attachments, links to files, link redirections, and many other evasive techniques. No organization is immune to an unknown, zero-day multi-layered email attack. Eventually, very determined bad actors that directly target them will break through their cyber defense.

There are three standards-based email security protocols used to address malicious email authentication methods. These include SPF, DKIM, and DMARC, which work together to help protect against email and domain name spoofing.

To prevent email and domain spoofing, Sender Policy Framework (SPF) hardens DNS servers by restricting who can send emails from a domain. Domain Keys Identified Mail (DKIM) ensures



email content is trusted, and not compromised. Domain-based Message Authentication, Reporting, and Conformance (DMARC) integrates SPF and DKIM protocols with consistent policies, links the sender's domain name with the "from header", and provides reporting back from email recipients. While these email security protocols are widely available, email authentication is a difficult and complex process, and it's typically chalked with configuration errors.

The legitimacy of an email's true owner is critical for communications. In the case of a Business Email Compromise (BEC) cyberattack, the result for the victimized organization can be financial loss, brand erosion, and the loss of consumer trust. Email authentication, using SPF, DKIM, and DMARC protocols to verify an organization's email and domain, provides proof that the users and devices sending outbound emails are legitimate. However, implementing, managing, and mitigating email authentication remains a cumbersome and fault-riddled process.

RevBits Email Authentication automates DKIM, DMARC, and SPF policy settings to prevent email and domain spoofing. We remove the complexity and difficulty of enabling DKIM, DMARC, and SPF, while enhancing the overall email security posture to protect the organization.

RevBits Email Security includes the Email Authentication module to automate workflows and reliably deploy standard email protocols that authenticate out-bound emails. RevBits enables administrators to simplify the process



of controlling their domain email addresses to minimize spam and spoofing. Additionally, admins can authorize third-party email marketing companies to send email campaigns out on their behalf.

3 Endpoints are a primary target for cyberthreats. Protecting against malware, ransomware, and fileless exploits requires NextGen advanced endpoint protection administered through a comprehensive endpoint security solution that detects and blocks known and unknown malware.

Microsoft Windows software drivers are becoming a critical exploit target for hackers. These malware attacks can be the most devastating that organizations can experience. Hackers use drivers to gain entry into a computer's operating system and kernel. Once in, they can cause massive damage. They can remain undetected within a system for as long as they need, before unleashing their payload. Not only are they dangerous because of the damage they can inflict, they're also almost impossible to detect and remove. Hackers can steal data, or take over a system for malicious purposes, all while remaining undetected. In most cases, the only way to completely remove this type of malware is to delete the operating system and rebuild it from scratch. Known as Rootkit malware, it requires specialized anti-rootkit software that detects, prevents, and removes the malware.

RevBits Endpoint Security includes unique anti-rootkit threat detection, prevention and removal capabilities. To remove known and unknown rootkit malware, RevBits identifies suspicious callback processes, hooks, registry keys, and modified files. RevBits' patented anti-rootkit capabilities protect computer systems and data by detecting, blocking and removing malicious drivers.

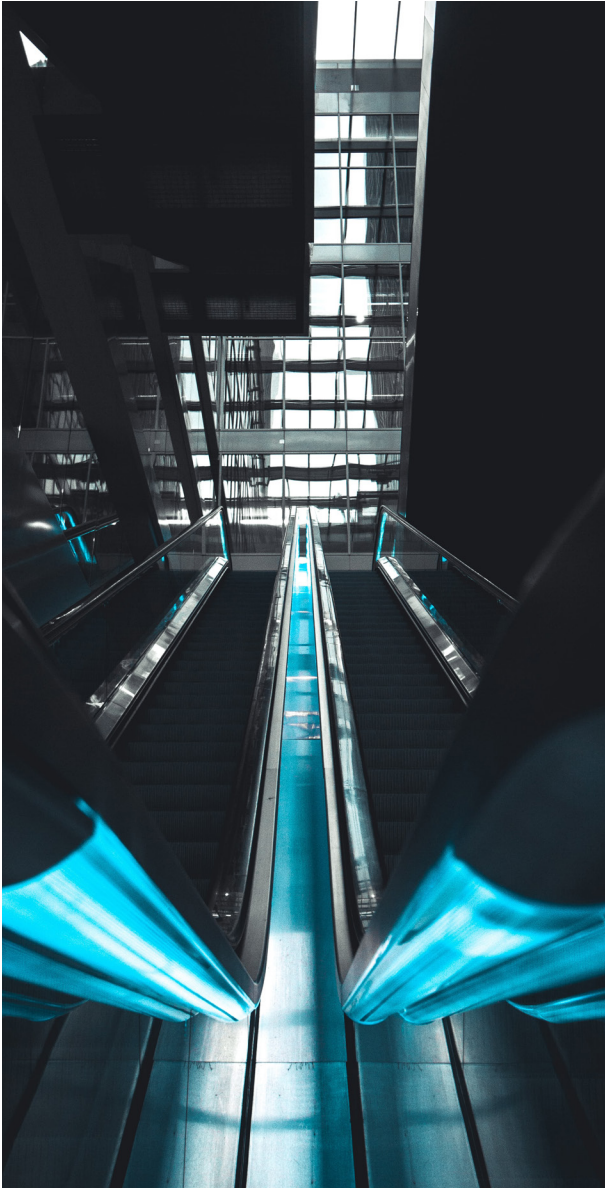
Behavioral analysis is the most advanced protection available within NextGen endpoint security solutions. Most vendors have one of the following: behavioral analysis, machine learning or signature scanning capabilities. RevBits Endpoint Security includes all three detection methods. It also has a scoring point system. Because

everything is built within a single product, the sources are aggregated together to take collective action based upon multiple data sources. This is an important distinction for not only detecting malware, but also for not producing false positives.

It's important to note, not all behavioral analysis methods are equal. RevBits behavioral analysis is integrated with the MITRE Attack Framework within our intelligence engine. Critical detection points with implanted "sensors" are in system threads, registries, file systems, networks, etc. We have accumulated a massive list of abnormal activities that have been classified and scored for broad coverage of any process, including API calls and accessing of system resources.

4 Privileged accounts are ripe pickings for hackers. When they are able to obtain a privileged users' credentials, they can park their malware on a mission-critical server and wait for the perfect time to laterally move throughout the network and infect whatever devices and applications they want. Privileged access management (PAM) is a business-critical security capability for protecting admin accounts. Controlling access is accomplished by implementing a least privilege principal through the PAM solution.





Unique to RevBits is how we have natively integrated PAM with zero trust networking (ZTN). We've combined the principles from our PAM with RevBits ZTN to deliver data encryption, comprehensive obfuscation, granular user and machine access controls, and recording, monitoring and auditing of sessions.

5 Look for a PAM solution that offers multiple access management aspects, like on-boarding and off-boarding of all privileged accounts. The PAM solution should have capabilities to implement robust password management for all employees and monitor and record sessions for all critical servers. It should provide 360-degree visibility into an organization's complete digital infrastructure. RevBits PAM and ZTN work natively together to generate random user credentials, and monitor URLs, sessions, web apps and Sequel connections.

6 With the increasing remote workforce and third-party access to network resources, applications and data, organizations need to expand their access security protocols beyond traditional VPNs. Assuming that simply providing VPN credentials to remote workers and third-parties will ensure remote access security is not a viable solution. Establishing a zero-trust network solution will deliver the secure access needed for the growing contingents of remote users.

7 Combating stealth with deception solutions will catch bad actors and malicious employees that represent insider threats. Deception solutions deploy realistic server-based honeypots with credentials deployed throughout endpoints and servers to help alert administrators to malicious activities occurring within the network. RevBits Deception Technology generates deception decoys or honeypots that mimic legitimate technology assets throughout the infrastructure. These honeypots are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials. To lure the attackers to these honeypots, fake credentials or breadcrumbs are planted across the network. Once an attacker attempts to access the honeypots, they are discovered and can be contained.

Questions to ask cybersecurity platform vendors

Selecting a vendor, their cybersecurity platform and products can be overwhelming, and choosing the wrong platform can be costly. We've compiled a list of important questions to ask vendors that can aid in the process. Hopefully, these will help you achieve a basic understanding of what capabilities to look for, ultimately guiding you to choose the right cybersecurity platform for your organization.

Those charged with protecting their organization can never have enough information. Here are some important questions to ask cybersecurity vendors. If their answers are incomplete or weak, they probably aren't the right fit for your business.

Can the security platform detect known and unknown threats?

Simply put, no single security solution can prevent all threats. The key is to have multi-layered security that detects known and unknown threats and have the ability to quickly block them.

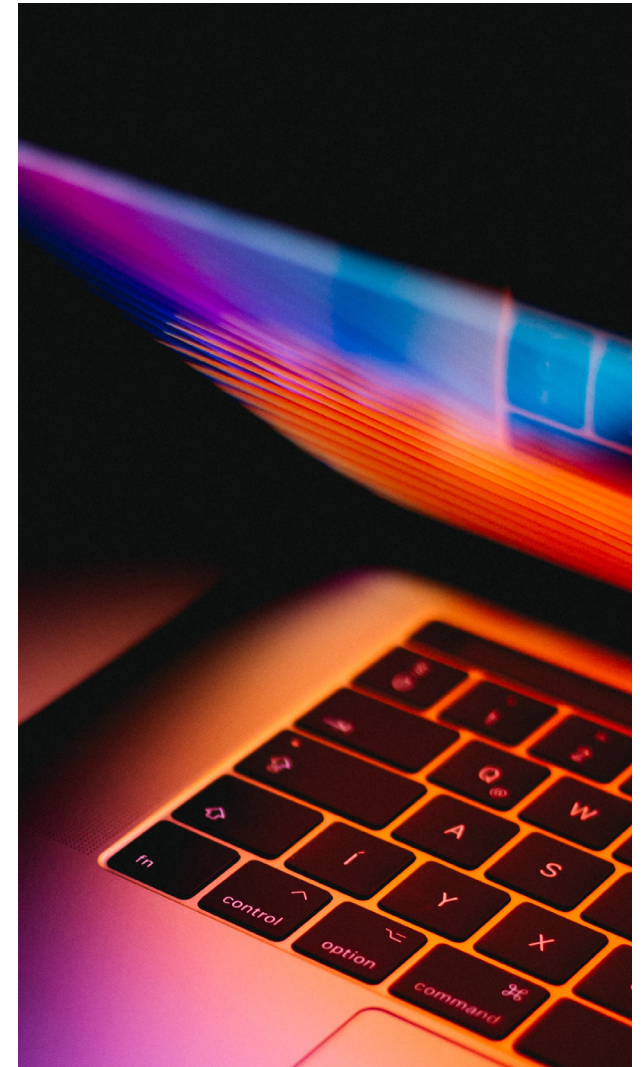
Ask: How broad is the platform's ability to detect both known and unknown malware, phishing, SQL injection, zero-day exploits, man-in-the-middle, spear-phishing, fileless and other attacks? What are the detection criteria and range of capabilities for detecting cyberattacks? Also determine if the vendor has complete capabilities themselves or are they relying upon other technology partners.

Ask: How easily does the platform generate reports and measure how the company's cybersecurity posture is adapting and maturing?

Ask: How does the platform provide metrics that map policy changes to the relevance of alerts?

What security products are integrated, and are they all native?

It's not uncommon for security vendors to have the basic checkmark features included within their platforms. The fact that some call them platforms can be misleading when they "integrate" other third-party products into their solutions. Without in-house developed and natively integrated solutions, many so-called security platforms create a disjointed and ultimately compromised defense. Without native cross-product integration, the exchange of security data cannot have seamless and comprehensive visibility throughout the entire enterprise technology ecosystem, and across all attack surfaces. Integrating security via APIs, only goes so far. Native integration enables full visibility and automatic and seamless data exchange across all of the cybersecurity platform's products.



Ask: Does your platform rely upon other third-party products?

Ask: Can it seamlessly exchange diverse security data that can be easily and readily visible? Can you demonstrate that capability?

How easily does the security platform conduct holistic forensics?

Tightly integrated cybersecurity technology and digital forensics are a requirement for a strong cybersecurity posture. This not only provides a powerful defense, but it also intrinsically couples cyber protection with the analysis and investigative capabilities necessary to protect against events in the process, as well as protective measures for future attacks.

Ask: How well does the platform's dashboard seamlessly integrate different products, functions, data, and analytics for fast identification of any type of attack?

Ask: Does it provide analysis of the entire cyber-attack lifecycle with deep intelligence and visibility into malicious and suspicious activity throughout the network?

Ask: How does the platform provide coverage for all threat vectors, and connect controls across networks, endpoints, clouds, and applications?

Is the platform licensing flexible?

Make sure the vendor's licensing structure is flexible and cost-efficient. Some vendors license their platforms on a per-application basis, which

might restrict your ability to switch product licenses. Make sure the licensing model fits your changing user needs.

Ask: How flexible is your license model?


How secure is the platform?

Vendor cybersecurity platforms require internal security processes.

Ask: How is your platform testing being conducted?

Ask: Is there a disclosure policy that guarantees it will fix bugs and notify customers?

Ask: Is the platform, and its products, automatically updated? What is the security update timeframe?



"Tightly integrated cybersecurity technology and digital forensics are a requirement for a strong cybersecurity posture."



Is the principle of least privilege and multi-factor authentication natively integrated into remote access?

Privilege access management is critical to ensure users are authenticated and validated before they can access a resource.

Ask: What data is needed for certain employees to perform their duties? How do you make the user experience simple and fast for remote workers and third-parties?

Ask: Is multi-factor authentication (MFA) required and enforced for remote access?

How much time and effort will the platform save?

It's important to consider how much time it will take to set up and maintain the platform.

Ask: What elements of the platform are automated?

How does the platform support the complete exploit and risk-management lifecycle?

Ask: What capabilities does the platform provide to support exploit and risk management lifecycles?

Ask: How does the dashboard support the complete cybersecurity lifecycle to unify visibility and control across all the security platform's products?

If compromised, how will the platform respond?

Cyberattacks have multiple stages that are part of the attack chain of events. When attacks are discovered close to their origin, they can be stopped more quickly to minimize damage.

Ask: How is cyberattack evidence traced?

Ask: How does the dashboard display the cyberattack stages, including reconnaissance, attack payload, payload delivery, and installation of malicious code on devices?

Ask: How does the analysis of these stages, and others, inform analysts so they can prevent future attacks?

Ask: How does the platform streamline workflows to enable automated responses and coordinated actions when investigating and responding to threats?

Below are key capabilities to look for in a cybersecurity platform:

- Large numbers of alerts are reduced to a small number of incidents and quickly investigated through an intuitive dashboard.
- Integrated incident responses that include context from all appropriate security products or modules for a fast resolution.
- Detection, response, and exploit removal, for on-premises infrastructure, multi-cloud apps, and workloads, networks, and endpoints.
- Ability to automatically correlate data across email, endpoints, servers, cloud workloads, and network security layers.

RevBits Cyber Intelligence Platform

RevBits Cyber Intelligence Platform (CIP) is a comprehensive Extended Detection and Response, or XDR solution. Consolidating multiple security capabilities into a cohesive, unified security platform, RevBits CIP unifies zero-trust networking, privileged access management, email security, security threat detection and incident response products, and deception technology. All security products are natively integrated into a cohesive security operations system.

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 is immediately detected and responded to, creating more reliable and faster outcomes. RevBits CIP includes the following security products:

- Email Security
- Privileged Access Management (PAM)
- Zero Trust Networking (ZTN)
- XDR/Endpoint Security

RevBits Cyber Intelligence Platform (CIP) is a comprehensive extended detection and response, or XDR solution.



Cross-functional security and unified dashboard simplifies forensics

RevBits CIP collects, aggregates, processes, and preserves security data from all included security products. Its unified dashboard provides a 360-degree view to analyze multi-vector cyber-attack evidence.

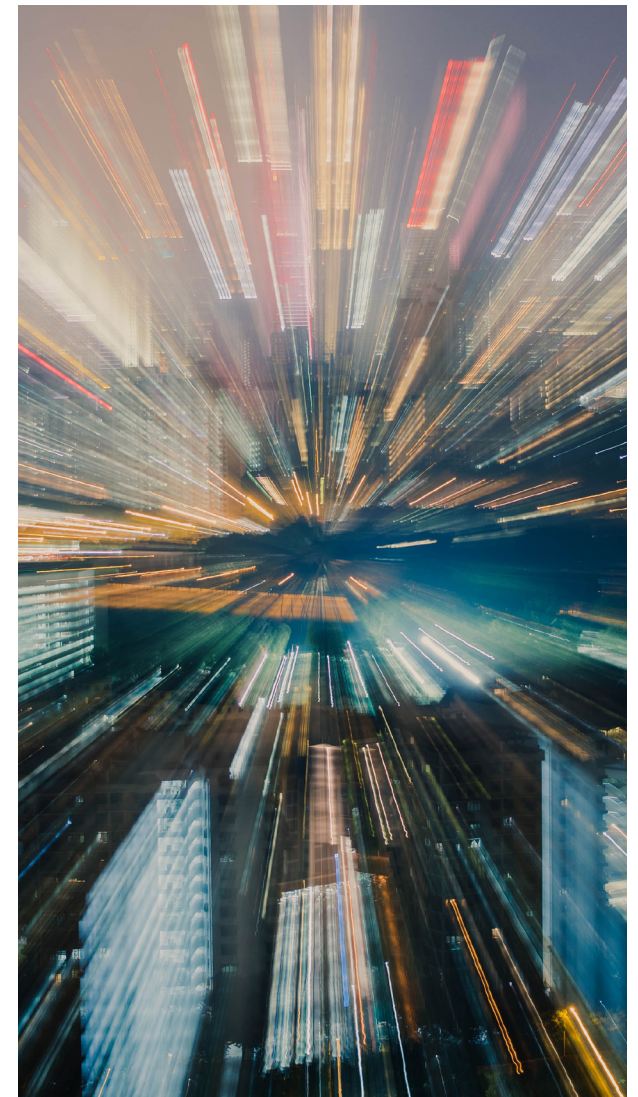
RevBits CIP combines intelligence between products, enabling analysts to uncover the digital evidence they need to improve and accelerate detection and rapidly mitigate events.

RevBits endpoint security conducts a unique three-phase analysis on all new executables. These include signature scanning, machine learning, and behavioral analysis. Together, these capabilities maximize the accuracy of malware detection and minimize false positives. The RevBits intuitive GUI dashboard provides in-depth details and easy navigation for forensic analysts and investigators.

RevBits makes it easy to navigate through malware incident details, with integrated search capabilities, a 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. These and many other attributes are at the fingertips of analysts and forensic investigators. They can quickly and easily view indicators, timelines, and tactics, and all of the steps that were taken, for both malicious and suspicious activities.

RevBits CIP empowers analysts and forensic investigators with greater productivity and effectiveness, by correlating diverse protection measures within the cybersecurity infrastructure. Leveraging RevBits' analytics and automation, they can provide 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 coalesced into a single intuitive GUI dashboard to quickly resolve threats.



Keep Your Enterprise Protected. Get a Demo or Free Evaluation.

To learn more, visit www.revbits.com



34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com

© 2023 RevBits, LLC. All rights reserved. This material is provided by RevBits, LLC. Further distribution is prohibited. RB-EB-CIP-Q_(01/2023) 048