

# The Game-Changing Cyber Security Platform

Achieve new levels of cyber protection, through a unified cybersecurity platform that empowers IT and security teams with reliable and highly scalable operations.

## Table of contents

Introduction.....	3
State of cybersecurity overview .....	4
Extended detection and response (XDR) overview .....	6
RevBits Cyber Intelligence Platform (CIP).....	7
RevBits security products and modules.....	8
Identity management overview.....	9
RevBits Privileged Access Management (PAM) .....	10
Email security overview .....	11
RevBits Email Security (ES) .....	11
Endpoint security overview .....	13
RevBits Endpoint Security (EPS).....	13
Zero trust network access overview .....	15
RevBits Zero Trust Network (ZTN).....	16
Deception technology overview.....	17
RevBits Deception Technology (DT).....	18

## RevBits product line



Cyber Intelligence Platform



Endpoint Security



Email Security



Privileged Access Management



Zero Trust Network

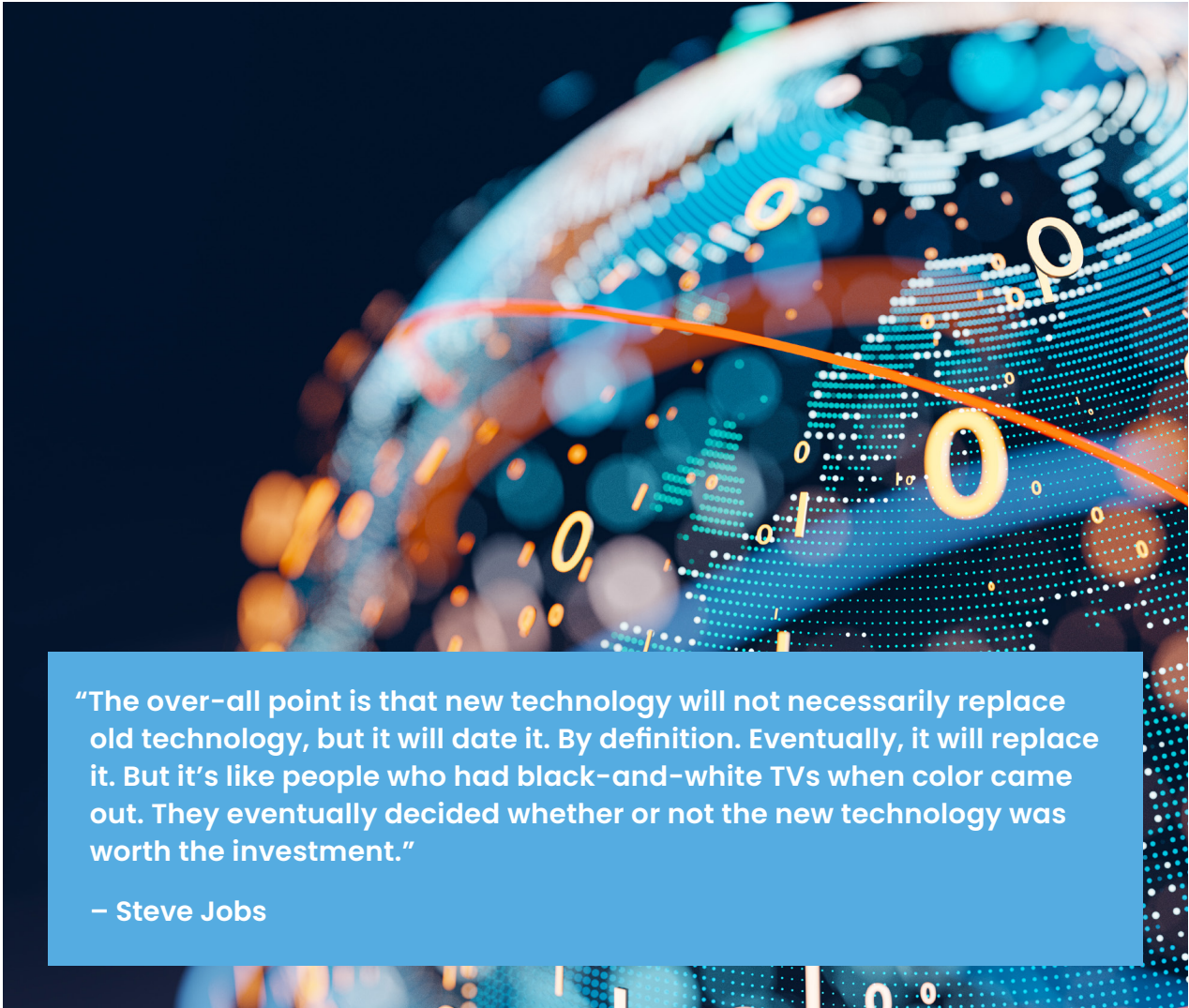


Deception Technology

## Introduction

The complexity and diversity of today's digital technologies are driving enterprises to move beyond the cost-prohibitive and rigid nature of traditional security deployments. In fact, security devices are going way beyond computers, tablets and smartphones. IoT devices are impacting healthcare, manufacturing, and virtually every other industry. Digitalization now involves a diverse array of endpoints, applications, systems, and identities that require a solid security foundation.

On-premises, cloud and hybrid-connected application environments are driving the demand for software-defined security capabilities that protect an entire ecosystem of users, applications, devices, data, and analytics. Digital transformation is an ongoing journey, that encompasses mission-critical legacy systems and modern cloud infrastructure and applications.



“The over-all point is that new technology will not necessarily replace old technology, but it will date it. By definition. Eventually, it will replace it. But it’s like people who had black-and-white TVs when color came out. They eventually decided whether or not the new technology was worth the investment.”

– Steve Jobs

## State of cybersecurity overview

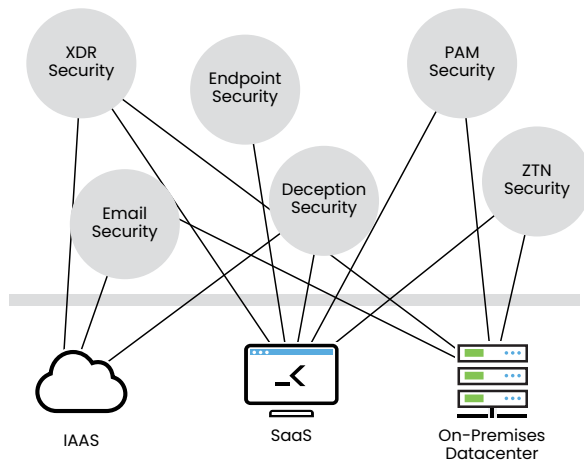
Despite the fact that there's a huge market for cybersecurity software, the ever-increasing number of serious cyber breaches clearly demonstrates a need for better protection, and an integrated approach. Both state and non-state sponsored hackers are becoming more sophisticated in their attack methods, and can only be stopped by more sophisticated solutions.

According to Gartner, worldwide spending on information security and risk management technology and services is forecast to reach \$170.4 billion in 2021. Suffice it to say that enterprises in virtually every industry are facing unprecedented challenges with remote workforces, staffing challenges, and limited budgets for vital cybersecurity initiatives.

The number of cyberattacks and breaches are going up exponentially. Organizations continue to struggle with security and regulatory demands. This is placing greater importance upon implementing automation and machine learning into the security ecosystem.

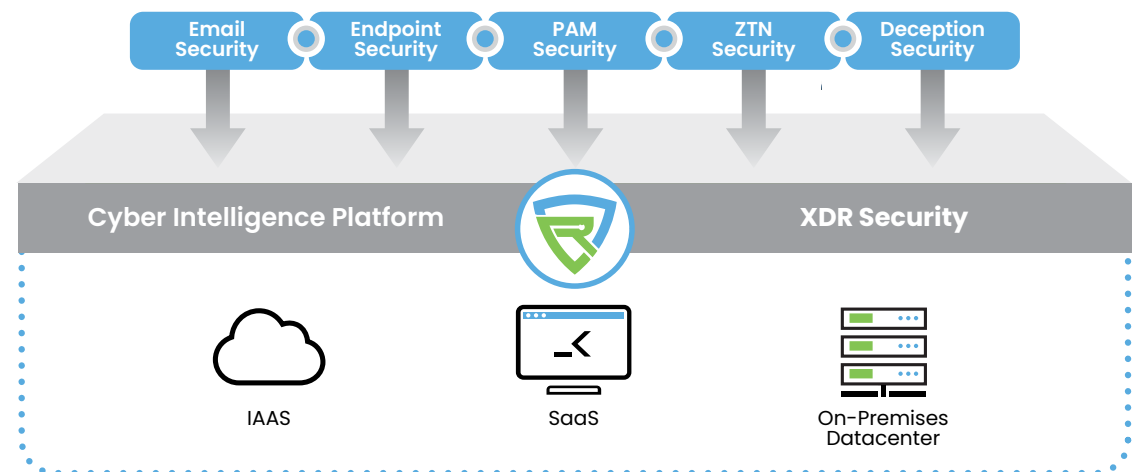
Requires coordinating threat detection, creates more false-positive alerts.

### Stand-alone Security Products



Holistic security mesh reliably and 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

### Unified Security Platform



For many years, organizations have been adding disparate security functions in an effort to mitigate risk and comply with regulations. Today, security and risk management leaders struggle with a host of heterogeneous devices and software products. These siloed solutions complicate the correlation of data and incident response, making it extremely difficult to fully leverage a solution's value by IT and security teams.

When security operations enable greater alignment with business needs and initiatives, enterprises can reduce risk and respond more effectively to cybersecurity events. Security risk is complex, and requires a layered approach with the right people, processes, and technologies. Just as digital transformation is a journey with iterative adjustments, so too is cybersecurity. The threat landscape is filled with potholes and speedbumps, that challenge even the most well-funded and well-prepared organizations.

The cybersecurity journey must be met with an agile security platform and operational foundation that supports on-premise, cloud, mobility, work from anywhere employees, and the Internet of Things. These issues represent part of the growing demands being placed upon organizations, and are increasing the vulnerabilities that expose threats. Unfortunately, there is no single security technology that solves every security problem.

Indeed, there are many security functions, like endpoint security, identity access and management, deception technology, privileged access and session management, and zero trust network access, to name a few. Every organization

with digital assets to protect, needs to have a clear understanding of the available security capabilities and use cases, so they can align them with their risk tolerance.

There are two significant and ongoing challenges that can quickly overwhelm security organizations. Finding, hiring and keeping technically savvy security operations staff is a stressful and burdensome task. Secondly, is the weighty challenge of building a security operations capability that can confidently maintain a defensive posture, while rapidly detecting and responding to events.

A plethora of single-function security products have resulted in too many vendors and products with very little integration or coordination. Security alerts become excessive, uncoordinated, and too often go unattended. Configurations are not actively maintained or tested for effectiveness, and lax security updates create ineffectiveness. SIEM tools are good at collecting logs, but rarely improve detection fidelity in most implementations.

It's difficult for organizations to build deep integrations across a heterogeneous environment. Security tools can provide integration across multiple components. But they become stifled by a lack of API integration, data merging issues, workflows that are disconnected from detection activity, and cross-functional visibility for rapid cyber forensics to conduct quick responses.

**“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.”**


To successfully implement a comprehensive cybersecurity posture in today's perimeter-less environment requires a combination of functions, that are synthesized within a centralized management platform. For organizations without the appropriate skills in-house, there are managed security service providers, or MSSPs, that can implement the appropriate security capabilities. Even organizations with more mature security postures, established teams, and security functions and controls in place, require continuous evaluation and changes. Keeping up with cybercriminals that are increasingly stealthy, sophisticated, and evasive, is a challenge for every organization, no matter their size.

Organizations that don't take advantage of cross-functional layered security solutions, and leverage the expertise of those who know how to best employ those technologies, will be at a fundamental disadvantage.

## Extended detection and response (XDR) overview

Cybercriminals are devious, clever and opportunistic. They lie in wait, looking for opportunities to hold data for ransom, embezzle money, and steal data for nefarious purposes. Security analysts respond to myriad alerts, moving from one product console to another, trying to process and triage disconnected attack viewpoints. Cybercriminals take advantage of security holes created by the myriad siloes of disparate, single-function security products.

XDR eliminates these siloes by using a unified approach to detect and respond. XDR platforms collect and correlate activity data across multi-layered security capabilities, protecting applications like email, endpoints, servers, cloud workloads, and enterprise networks. XDR leverages automated analysis of a superset of rich data, to detect and conduct thorough forensic investigations quickly, and with greater intelligence and rapid response.



**“Automatic aggregation of the chain of activities are brought into a comprehensive view to make high-confident decisions, with fewer alerts prioritized for quick action.”**



## RevBits Cyber Intelligence Platform (CIP)

RevBits Cyber Intelligence Platform (CIP) is a unified security platform. A single sign-on portal enables easy and intuitive management of the RevBits suite of security products and the activities they touch. Administrators can build customized dashboards to visualize intelligence from multiple deployed security modules. With a single click, they can launch incidents and manage alerts. Coordination of threat intelligence is realized and actionable, with full integration to any SIEM or other incident response platforms.

More than a detection and response platform, RevBits CIP includes integrated identity capabilities, from privileged access and privileged session management, and password, key, certificate management, to CI/CD access management, as well as, zero trust networking, and deception technology.

More insightful investigations foster intelligent, actionable responses. RevBits leverages the logical cross-connections of multiple security capabilities that provide deep contextual data within a unified view. RevBits CIP collects and provides access to

the security functions and activity data. Through the application of sophisticated analytics and threat intelligence, RevBits CIP provides an intuitive view of the full context of an attack, with complete visibility across the entire chain of events.

Automated processes eliminate manual steps, and provide rich data for analysis. Analysts can clearly see the timeline and attack path that may cross emails, endpoints, servers, clouds and networks. They can assess each step of the attack to quickly take the necessary action.

Cross-layered detection and response improves threat detection rates and response times. Automatic aggregation of the chain of activities are brought into a comprehensive view to make high-confidence decisions, with fewer and more prioritized alerts for quick action. generate random user credentials, and monitor URLs, sessions, web apps and Sequel connections.



## RevBits Security Products and Modules

More insightful investigations foster intelligent, actionable responses. RevBits leverages the logical cross-connections of multiple security capabilities that provide deep contextual data within a unified view. RevBits CIP collects and provides access to the security functions and activity data. Through the application of sophisticated analytics and threat intelligence, RevBits CIP provides an intuitive view of the full context of an attack, with complete visibility across the entire chain of events.

Automated processes eliminate manual steps, and provide rich data for analysis. Analysts can clearly see the timeline and attack path that may cross emails, endpoints, servers, clouds and networks. They can assess each step of the attack to quickly take the necessary action.

Cross-layered detection and response improves threat detection rates and response times. Automatic aggregation of the chain of activities are brought into a comprehensive view to make high-confidence decisions, with fewer and more prioritized alerts for quick action.

- **RevBits security functions controlled through one unified dashboard**

- Single sign-on to dashboard, security products and modules
- RevBits CIP dashboard operates under a single or multi-solution deployment based upon customer needs

- **Multi-tenancy-enabled**

- **Alert management and action**

- Cross-platform alert notification
- Actionable intelligence to reported incidents

- **Unified cloud console**

- API integration with SIEM, SOAR, and other incident response platforms





## Identity management overview

Unrestricted or inadequately monitored access privileges across an organization's IT infrastructure not only violates the basic security principle of least privilege, it severely limits the ability to establish accountability when privileged actions are carried out. Traditional IAM technologies, such as identity governance and administration and access management, provide controls for standard user access. However, they don't have sufficient capabilities to manage shared privileged accounts, controlled elevation of administrator privileges, and secrets access management within CI/CD development environments.

Security and risk management leaders focused on IAM, alleviate risk when they leverage solutions that help them manage and control privileged access. These solutions help streamline the mitigation of business risk associated with administrative privileges. In today's perimeter-less and work from anywhere environment, every employee should be seen as a privileged user, as unaccounted privileged access carries significant risk.

Privileged accounts are used for interactive administrative access to digital assets, including devices, applications, servers, control panels, etc. Privileged accounts can include:

- Personal privileged accounts
- Shared privileged accounts
- Built-in administrator accounts, such as local administrator and root
- Other shared administrator accounts set up by the organization's application accounts, and used by applications, scripts or batch jobs to access other services, databases, etc.
- Service accounts used by applications or services to interact with an operating system and other services





## RevBits Privileged Access Management (PAM)

RevBits Privileged Access Management (PAM) accounts are brokered for users, services and applications. Privileged session management establishes sessions that include privileged credential injection into sessions, with full session recording. Passwords and other credentials for privileged accounts are actively managed and changed at definable intervals, or after specific events.

RevBits PAM is an advanced privileged access management solution that includes seven modules, and extensive session logging that captures keystroke and video. RevBits PAM has two U.S. patents – a 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. RevBits PAM modules include:

**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.

**Service Account Management** – scans and onboards service accounts, 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.

**CI/CD Access Management** – supports the fast and agile development that CI/CD provides, while bringing secrets protection into the DevOps environment, with a frictionless process.

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. Additionally, RevBits PAM module provides application-to-application password management, with zero-install remote privileged access for IT staff and third-parties that don't require a VPN.

### Differentiating capabilities:

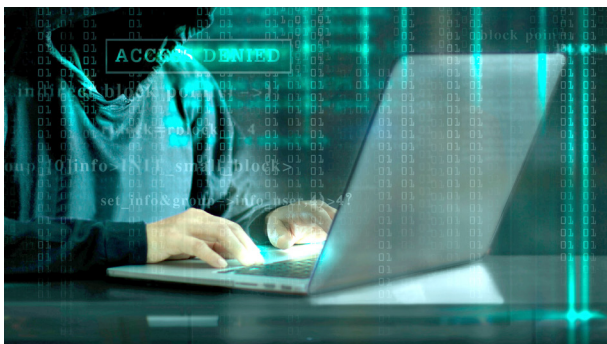
- Complete native client for all major operating systems and browsers.
- Native clients in all major sources: Oracle, MSSQL, PostgreSQL, Cassandra, MySQL. Reverse engineering of database protocol to monitor activity.
- Full directory services integration.
- Full SIEM integration (LogRhythm and Splunk).
- Seven access management modules in one product: privileged access, session management, password management, service account management, key management, certificate management, and CI/CD Access Management.
- Utilizes a zero-knowledge encryption model for maximum data security where data encryption takes place on the device. Data stored on the server is encrypted, and the encryption key never leaves the device (U.S. Patent).
- Automatic onboarding of cloud-based assets (i.e., AWS, Azure, Google Cloud).

## Email security overview

Email is the number one attack vector for opportunistic and targeted cyberattacks. The significant increases in successful phishing attacks, and the migration to the cloud, make it very clear that email security measures need to be re-examined and strengthened.

Cyberbreaches targeting the email inboxes of employees are a major source of data loss and ransom payments. As organizations migrate to the cloud and rapidly move to a remote from anywhere model, they need to fortify and prepare. They must have the necessary technology to protect against advanced email threats and attack vectors like malware, email attachments, web pages, pop-ups, instant messages, text messages, and social engineering.

Evading email breaches requires protection against URL-based advanced threats, full coverage from impersonation and social engineered attacks, and advanced threat intelligence.



## RevBits Email Security (ES)

Over the past several years, traditional email solutions have not evolved past static analysis, and continue using older methodologies where threats escape detection. RevBits Email Security (ES) addresses this problem.

**RevBits Email Security (ES)** is an advanced solution that detects and blocks sophisticated phishing emails. RevBits has two U.S. patents for email security – a patent for user inbox advanced email analysis, and another patent for a unique methodology for detecting page impersonation attacks.

**RevBits Cyber Intelligence Platform (CIP)** has a deep analytic-driven dashboard for administrator convenience and email review. Over 50 algorithms analyze emails for thorough protection. Located at the endpoint allows for superior phishing detection, without creating delivery latency. The existing email security stack is enhanced, without requiring adjustments to the email production system.

Sophisticated malicious emails are created to evade analysis limitations of a secure email gateway (SEG). Once in the user's inbox, interaction is likely. Corporate email security is strengthened by blocking the most sophisticated phishing emails that are often missed by email gateways and other email solutions. Once a malicious email makes it to the user's inbox, they may assume the email was analyzed and is safe. RevBits ES can be deployed as a standalone solution, or in conjunction with an existing gateway solution.

**RevBits ES is dual email security offering with a deployed SEG capability and an endpoint-based inbox analysis engine.**

**RevBits Email Security capabilities**

- Decentralizes analysis by operating at the endpoint workstation, laptop, tablet, or smartphone
- Conducts comprehensive policy-driven analysis definable at the user, group, or network level
- Provides admins with greater control over email analysis within the organization. This level of control is difficult to accomplish with a gateway
- Conducts email review on a deep level, operating at an endpoint, without creating delivery latency
- Provides analysis of email attachments including unpacking multi-layered attachments, and detecting password protected attachments and documents
- U.S. patented technology detects and blocks page impersonation attacks, which can result in credential harvesting and business email compromise
- Analyzes emails with Yara rules, which system administrators can customize
- Analyzes reported emails rapidly with advanced automated email analysis

- Defends against phishing emails that escape detection by gateways and cloud-based solutions
- Enables simple deployment, and compatible with other email security solutions
- Analyzes emails at the endpoint with 50+ algorithms to detect the most sophisticated phishing attacks

- Delegates email analysis to email clients (U.S. patent)
- Detects sophisticated and previously undetected credential harvesting via fake login pages - page impersonation (U.S. patent)
- Deploys as a standalone solution, or in conjunction with existing gateway solutions



## Endpoint Security Overview

According to Gartner, by the end of 2023, more than 50% of enterprises will have replaced older antivirus products with combined EDR and EPP solutions. For years, the complexity of cyberattacks and threats has developed at a pace exceeding the ability of siloed products and enterprise security teams to mount an adequate defense. The techniques and methods used by attackers to evade detection have also expanded. We now require robust detection engines and controls to identify them and produce alerts that inform defenders how they should respond to and remediate an event. Older antivirus solutions provide insufficient protection against today's advanced threats. They lack speed of response, and fail to show the root cause or damage done.

This dilemma was the impetus for RevBits to develop a more effective and flexible solution. RevBits EDR rapidly detects and responds to advanced threats. RevBits EDR enables small, medium and large enterprises to deploy a single solution that protects against attacks, and collects and provides analysis of log and configuration data. The visibility of user, device and application activity is combined with advanced reporting and direct intervention when abnormal activity is detected.

## RevBits Endpoint Security (EPS)

**RevBits EDR** enables small, medium and large enterprises to deploy a single solution that protects against attacks, and collects and provides analysis of log and configuration data. The visibility of user, device and application activity is combined with advanced reporting and direct intervention when abnormal activity is detected.

RevBits EDR combines modern prevention techniques with detect and response capabilities in a single, lightweight agent. RevBits CIP unifies EDR with our other security

modules, and coalesces them into a single dashboard. Automation frees security staff from manual manipulations, enabling rapid detection of advanced persistent threats, to provide fast remediation.

**RevBits Endpoint Detection and Response, (EDR)** 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.



Minimizing false-positives is crucial, because they generate a chain of events that can cost employees in lost productivity, and significant downtime. IT personnel that respond to false-positives consume their time restoring and reversing damage. False-positives that are blocked and then cleaned by deleting registry keys, can result in broken applications. It doesn't take thousands of false-positives to disrupt business operations. A handful can be just as damaging as an actual breach.

Our three-phase approach blocks advanced malware, and employs a sophisticated exploit detection engine to detect all common exploit methods. RevBits EDR provides complete control and access to systems from anywhere, overcoming the limitations of traditional anti-malware scanning tools by addressing new and emerging threats.

RevBits EDR has flexible deployment options integrated within our Cyber Intelligence Platform, using a single portal to access our suite of security modules. It can be deployed as a stand-alone solution, as well as integrated into existing security platforms.

#### RevBits EDR capabilities

- Immediately detects security incidents
- Enables rapid investigation of security incidents
- Reliably contains and remediates the exploit at the endpoint

#### RevBits Endpoint Security value proposition

RevBits EDR delivers real-time detection and response for all endpoints, with deep forensic



capabilities. Ransomware and malware incidents are accounts of failed endpoint security. RevBits endpoint security optimizes and enhances analysis to increase malware detection and blocking. Better endpoint protection makes networks safer, by preventing lateral movement within the enterprise.

#### Malware detection and blocking:

- Secure isolation of new executables
- Advanced exploit detection capabilities
- Deep detection on all endpoints
- Rapid response with real-time forensics and behavioral analysis.
- A three-phased approach conducts signature analysis, machine learning, and behavioral analysis
- Triple-analysis is conducted on new executables (Verizon's ICSA Labs – Q1 2021 Results: 99% Detection, 0 False-Positives)

- Complete control over endpoints, including processes, threads, registry, filesystem and kernel, in both GUI and command line functionality
- Full visibility to the kernel, blocking all unauthorized signed or unsigned drivers from accessing the kernel (U.S. patent)
- Robust detection engine, including zero-days, with no need to deploy updates for most advanced ransomware attacks
- Recording and reporting of all executed commands and scripts in Windows Command Prompt, PowerShell, VBScript, and JScript
- USB device policies can whitelist or blacklist all USB devices
- A single click enables complete cross-functional forensic evidence gathering

## Zero trust network access overview

The downside to a network perimeter is the implicit trust organizations enable. Once a hacker gets through the perimeter, they have free lateral movement on the network, with access to data on devices, applications, servers, and databases.

Organizations deploy VPN to secure remote network connectivity and access. VPNs enable connectivity for authorized remote users and managed devices, while zero trust networks restrict access to all users, at all times. Many

enterprises are replacing VPNs with ZTNA solutions to address the hardware and bandwidth limitations of VPN access. ZTNA also improves the flexibility, agility and scalability of application access, enabling digital businesses to expand, without exposing internal applications directly on the Internet.

Zero trust network access, or ZTNA, is a security architecture where only traffic from authenticated users, devices, and applications are granted

access to other users, devices, and applications within an organization. ZTNA solutions, by default, deny access to anyone, providing only the access to services the user has been explicitly granted. It's important to understand the security benefits ZTNA solutions provide, as more remote users join the network.





## RevBits Zero Trust Network (ZTN)

The key differentiation of RevBits Zero Trust Network (ZTN) is the auto-scaling ability to meet demand. Key-point geolocation distribution across 24 global datacenters makes RevBits ZTN the fastest zero trust solution. This capability deeply assesses an endpoint's security posture, inspects tunnel traffic for malicious content and data security, and provides better support for third-party users.

RevBits ZTN creates an identity and context-based logical-access boundary that encompasses a user and applications. Applications are hidden from discovery, and access is restricted using a trust broker to a collection of named entities. The broker verifies the identity, context, and policy adherence of specified participants before allowing access.

### SaaS-hosted proxy

- **Isolate, authenticate and protect** – RevBits ZTN is SaaS-hosted to provide easy access and onboarding of users and assets. RevBits puts security between the enterprise and its perimeter. Combined with auto-scaling and advanced load balancing, RevBits ZTN dynamically scales with demand.
- **Full remote session control** – Reduce perimeter risk with access control, governance, and audit capabilities.

- **No client installs required** – Deployment is a thing of the past with RevBits ZTN. The perimeter is extended to the end-user, so there's no need to spend time deploying host-based clients to secure the network. Onboarding a new remote access host is a breeze with the RevBits ZTN intuitive and high-availability access portal.

### RevBits ZTN features

- **Full remote session control** – from authentication to disconnection, RevBits ZTN provides all the tools needed to manage, control, and audit any remote session within the private network.
- **No client to install** – RevBits ZTN is a thin client. You can access all assets from any web browser or a smart device and still retain 100% control of the remote access session. Add the RevBits PAM module to bring session management to the next level in control and security.
- **SaaS-hosted proxy** – enterprises will connect to a safe and secure ZTN portal to protect their biggest assets, their perimeter. RevBits ZTN is hosted for ease of access and onboarding of new users and hosts.
- **Key-point geolocation distribution** – brings the perimeter to end-users, with distributed geolocation access points. RevBits ZTN is the fastest, most secure zero trust solution on the market.

- **Mobile device support for all** – RevBits ZTN supports all mobile devices with native applications for each ecosystem. This allows enterprises to authenticate their way, with support for fingerprint, facial recognition, MFA apps, and Yubikey.

### RevBits ZTN benefits

- Full session recording and auditing from beginning to end.
- Clientless install makes deployment effortless.
- Auto-scales to meet dynamic demand.
- Reduces risk to the perimeter with RevBits ZTN access control, governance, and audit capabilities.
- Connects from anywhere, and with any device.
- Full access and authentication support for all mobile platforms.
- Reduces the ongoing need to support VPN agents, using agentless identity and device-aware access, that facilitates access from managed and unmanaged devices.
- The RevBits ZTN mobile app is available in all major app stores.



## Deception technology overview

Deception platforms and tools are centrally managed for organizations to create, distribute and manage an entire deceptive environment. Deception technology entices, detects, engages, and confines bad actors. Fake artifacts, such as documents, users, devices, applications, services, and infrastructure, can fool automated hacking tools, and even hackers themselves.

Modern deception systems are much more sophisticated than honeypot systems of the past. Analytics and automation have made today's deception solutions easier to deploy and manage, with a better return on investment. Modern deception systems offer high-fidelity fake artifacts, like decoys, lures, and honeytokens, created to entice attackers to touch and engage. Hackers are statistically bound to trigger one, as they perform lateral movement within an organization.

Deception systems can service many different organizations and needs, from being the only detection system in a midsize enterprise, to augmenting a more robust detection practice within more mature organizations.



**RevBits deception technology 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.**



## RevBits Deception Technology (DT)

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. CISOs have peace of mind, knowing their enterprise network is protected with a complete “attract and trap” system, using real servers and related resources.

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.

### RevBits Deception Technology differentiating capabilities

- Utilizes the most common database servers, file sharing services, and more
- A dual-layer virtualization architecture provides superior encapsulation of attackers in honeypots

- Numerous honeypots can be launched within each virtual machine, minimizing system resource use and maximizing operational efficiency.
- Implants credentials on endpoints and servers that point to the honeypots.
- Supports multiple notification methods including SMS, email, and SIEM
- No complicated architecture needed for deployment – server hosted in client’s network, with Amazon, Google and Azure cloudy-ready images available.
- Deploys real server-based honeypots to appear authentic to the attacker
- Automatic or manual deployment of decoy data and credentials to direct attackers to the honeypots

### RevBits Deception Technology value proposition

The advanced architecture and use of real servers, routers, firewalls, etc., combined with the following features, make RevBits Deception Technology the most cost-effective and efficient solution available.

- Simple and rapid deployment
- Robust and continual monitoring
- Advanced integration and reporting
- Low resource consumption
- Manual and automated credentials to lure attackers

**RevBits is a leader in cybersecurity innovation** with a unified security platform that automates and integrates a best-in-class suite of detection and response (EDR and XDR), privileged access management (PAM), email security (ES), deception technology (DT), and zero trust networking (ZTN). RevBits Cyber Intelligence Platform provides critical security capabilities to empower security operations with a complete cyber defense. RevBits' integrated solution covers the entire digital landscape, including endpoints, applications, emails, servers, networks, clouds and privileged accounts. All of these vulnerable vectors are protected by RevBits' patented next-gen technology.

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

To learn more, visit [www.revbits.com](http://www.revbits.com)



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

© 2023 RevBits, LLC. All rights reserved. This material is provided by RevBits, LLC. Further distribution is prohibited. RB-EB-CIP-GC\_(01/2023) 049