

## Cyber Intelligence Platform

**DRE unificado, habilitado por múltiples productos de seguridad y controlado a través de una consola integrada.**



Los perímetros de infraestructura de ciberseguridad y TI en expansión se distribuyen en un ecosistema complejo de múltiples nubes, en las instalaciones y usuarios móviles y remotos. RevBits Cyber Intelligence Platform (CIP) proporciona visibilidad y control unificados para frustrar los ataques cibernéticos en este ecosistema diverso, con la ventaja de una vista unificada.

El esfuerzo requerido para administrar múltiples productos y herramientas de seguridad dispares requiere mucho tiempo y está plagado de muchas brechas de seguridad. La falta de intercambio de inteligencia entre productos genera poca visibilidad, lo que dificulta encontrar, correlacionar y eliminar rápidamente las amenazas.

### RevBits Cyber Intelligence Platform

RevBits CIP aprovecha un poderoso conjunto de los mejores productos de seguridad de su clase que están integrados y unificados en un único tablero intuitivo. Con la capacidad de inicio de sesión único. Los administradores monitorean, interactúan y controlan Endpoint Security, Email Security, Privileged Access Management, Deception Technology y Zero Trust Networking. Inicio de sesión único para acceder y administrar todos los productos de RevBits.

#### Inicio de sesión único para acceder y administrar todos los productos RevBits

El inicio de sesión único pone el poder en las manos de los administradores para acceder, monitorear y controlar rápidamente todas las capacidades del producto RevBits, con una sólida protección de la red.

**Acceda a todas las soluciones integradas con un solo clic**  
El acceso a cualquier producto RevBits contratado es fácil y está a un clic de distancia.

**RevBits CIP proporciona una visión holística e intuitiva de todos los tipos de amenazas en todo el entorno tecnológico empresarial. La información en tiempo real de múltiples fuentes de amenazas permite detección y respuesta inmediatas, creando resultados más confiables y rápidos.**

#### Supervise diversas estadísticas críticas de seguridad en un tablero

Ofrece una vista de seguridad completa en un panel, lo que elimina la dificultad de administrar múltiples productos y entornos de generación de informes. La conciencia situacional completa sobre el estado de seguridad pone el control en las manos de los administradores.

#### Conocimiento y respuesta de seguridad inmediata para dispositivos móviles

El conocimiento y respuesta de seguridad inmediata para dispositivos móviles, permite una posición de respuesta inmediata, independiente del tiempo del día o ubicación geográfica, a través de soporte completo para dispositivos móviles. El control completo de seguridad, acceso y entorno está siempre disponible.

#### Alertas activas para todos los productos RevBits

Una ventana muestra todas las alertas activas con una sola vista y las enlaza para mitigación inmediata de amenazas. Una única plataforma proporciona a los administradores una pantalla de visualización frontal para todos los informes de alerta en todos los

productos RevBits contratados. Con un solo clic, los administradores pueden revisar incidentes individuales, independientemente del producto o la alerta.

#### **Tablero personalizable**

Para cumplir mejor con los requisitos de administración, el tablero se puede configurar con widgets disponibles dentro de varios productos de ciberseguridad de RevBits.

#### **Inteligencia accionable**

Da vida a la DRE con inteligencia de amenazas de múltiples vectores que se vuelve procesable de inmediato.

#### **La seguridad funcional integrada y el tablero unificado simplifican el análisis forense**

Recopila, agrega, procesa y conserva datos de seguridad de todos los productos integrados de RevBits. Un tablero unificado proporciona una vista de 360 grados para analizar la evidencia de ataques cibernéticos de múltiples vectores. Combina inteligencia entre productos, lo que permite a los analistas descubrir la evidencia digital que necesitan para mejorar y acelerar la detección y mitigar rápidamente los eventos.

#### **Agregue y correlacione diversos datos de ataques**

Correlacione diversas medidas de protección dentro de la infraestructura de ciberseguridad, lo que permite a los analistas de seguridad e investigadores forenses obtener resultados rápidos.

#### **Reduzca el tiempo de respuesta**

Reduzca el tiempo medio de respuesta (TMR) con mitigación automatizada y con un solo clic en todos los vectores de ataque y superficies.

#### **Eliminar brechas de seguridad**

Elimine las brechas de seguridad asociadas con soluciones en silos, estructuras de datos e idiomas inconexos y métodos de detección dispares.

#### **Navegue sin problemas por los incidentes.**

Navegar a través de los detalles de incidentes de malware se vuelve más fácil y eficiente utilizando capacidades de búsqueda integradas, gráficos de puntaje de aprendizaje automático, indicadores de análisis de virus, árboles de procesos y gráficos de radar. Al hacer clic en las funciones, se brinda información aún más granular sobre direcciones IP e indicadores sobre ID de ataques, con enlaces a la base de datos MITRE Attack Framework.

#### **Reduzca la respuesta de días a minutos.**

El panel intuitivo reduce drásticamente los falsos positivos, lo que permite a los analistas ser más eficientes, centrándose en los incidentes más críticos.

## **Capacidades del producto RevBits CIP**



### **RevBits Endpoint Security (EPS)**

La arquitectura única de [RevBits EPS](#) tiene controladores personalizados o capacidades de detección de carga de aplicaciones patentadas, que encuentran actividades maliciosas en varias etapas que intentan suplantar las aplicaciones de Windows, los procesos de firma y los procesos confiables. RevBits EPS también tiene un motor de detección preciso que evita falsos positivos y un diseño arquitectónico distintivo para la lista blanca de aplicaciones, sandboxing, spawning y el análisis de procesos padre/hijo.

RevBits EPS evalúa todo el proceso, incluidos los ejecutables, y no permite que el malware se oculte en programas y aplicaciones legítimos. Realiza un análisis único de tres fases en todos los ejecutables nuevos, incluido el escaneo de firmas, el aprendizaje automático y el análisis de comportamiento. Esto maximiza la precisión de la detección de malware y minimiza los falsos positivos.

**Administración de dispositivos USB** – Las políticas de dispositivos USB se pueden usar para incluir en las listas blancas o en listas negras todos los dispositivos USB. Las listas blancas y negras se pueden aplicar por ID de proveedor, ID de producto o tipo de dispositivo (por ejemplo, cámaras web, adaptadores inalámbricos, almacenamiento, etc.).

**Tecnología anti-rootkit patentada** – Proporciona una visibilidad completa del kernel y bloquea el acceso al kernel a todos los controladores firmados o sin firmar no autorizados.

**Robusto módulo EDR basado en GUI** – Proporciona a los administradores la capacidad de interactuar, controlar, aislar y mitigar Endpoints infectados. El módulo EDR basado en GUI proporciona capacidades forenses profundas y una gestión mejorada por encima de otras soluciones EPP/EDR.



## RevBits Email Security

[RevBits Email Security Endpoint-Based Agent](#) (EBA) es una solución nativa proporcionada por SaaS, también conocida como seguridad integrada de correo electrónico en la nube (ICES). El agente basado en Endpoints protege contra correos electrónicos maliciosos, asumiendo el control en una puerta de enlace de correo electrónico segura. Llena las brechas de seguridad aprovechando el procesamiento distribuido para un análisis profundo en Endpoints de usuarios remotos para detectar y bloquear correos electrónicos maliciosos que superan la capa centralizada de la pila de seguridad de una organización. RevBits tiene dos patentes de EE. UU. para la seguridad del correo electrónico: una patente para el análisis avanzado de correo electrónico de la bandeja de entrada del usuario y otra patente para una metodología única que detecta ataques de suplantación de identidad de página.

**RevBits Secure Email Gateway (SEG)** está basado en la nube y se implementa globalmente para una escalabilidad dinámica. Es también inherentemente redundante para operaciones confiables, en cualquier parte del mundo. RevBits SEG protege contra las amenazas de correo electrónico al bloquear el phishing, el compromiso de correo electrónico comercial (BEC), el correo no deseado, la ingeniería social, el ransomware y otro tipo de malware. RevBits SEG se posiciona como una defensa de correo electrónico corporativo de primera línea, dentro de la ruta de transporte de correo electrónico y directamente en la ruta de todo el tráfico que va al servidor de correo electrónico corporativo.'



## RevBits Deception Technology

Mediante la implementación de señuelos de trampa basados en servidores reales en un entorno de virtualización dual, las acciones maliciosas de amenazas externas o internas se detectan y notifican de inmediato. [RevBits Deception Technology](#) (DT) utiliza los servidores de bases de datos más comunes, los servicios de intercambio de archivos y más.

RevBits DT es la única solución en el mercado con virtualización de doble capa y servidores trampa reales. Implemente fácilmente múltiples señuelos con solo hacer clic en un botón y con un consumo mínimo de recursos. Las credenciales implantadas automatizadas atraen a los atacantes a los señuelos, revelando el sistema violado original.



## Privileged Access Management

[RevBits PAM](#) es una solución avanzada de administración de acceso que incluye seis módulos y un amplio registro de sesiones que captura las pulsaciones de teclas y el video. RevBits PAM tiene dos patentes estadounidenses: cifrado de conocimiento cero basado en navegador y autoridad de autenticación que se extiende a varias soluciones de seguridad de hardware. Estas capacidades únicas de control de acceso reducen los esfuerzos de gestión de relaciones con los proveedores y aumentan las protecciones de gestión de acceso. A medida que los perímetros empresariales amplían los entornos de gestión de acceso, aumenta la cantidad de proveedores necesarios para cubrir el entorno de acceso en evolución. RevBits PAM proporciona un control de acceso integral, tanto en las instalaciones como en la nube.

Módulos de PAM de RevBits:

- **Gestión de Acceso Privilegiado** - Regula el acceso a los recursos críticos, captura las pulsaciones de teclas y graba en video todas las sesiones privilegiadas.
- **Gestión de sesiones privilegiadas** - Todas las sesiones a través del servidor Jump de la solución.
- **Gestión de Contraseñas** - Seguridad de hardware, tokens USB, tarjetas inteligentes, comunicaciones de campo cercano y RFID.
- **Integración CI/CD** - El módulo integra a la perfección los conjuntos de herramientas de canalización de CI/CD más populares y es compatible con Jenkins, Puppet, Terraform, OpenShift, Ansible, Docker, Cloud Foundry y Kubernetes con futuras herramientas en desarrollo. Agregar el complemento a su plataforma actual desbloquea las capacidades de administración segura de secretos en todo el ciclo de vida de CI/CD para una fácil administración de usuarios, credenciales y activos de CI/CD.
- **Gestión de Cuentas de Servicio** - Escanea e incorpora cuentas de servicio y tareas programadas para aplicaciones web IIS.
- **Gestión de Claves** - Permite a los usuarios generar y almacenar fácilmente claves de cifrado.
- **Gestión de Certificados** - Notifica acerca de todos los certificados caducados o próximos a caducar y las implementaciones vulnerables de SSL.



## Zero Trust Networking (ZTN)

La capacidad de escalado automático de [RevBits ZTN](#) y la distribución de geolocalización de puntos clave hacen de RevBits ZTN la red de confianza ero más rápida del mercado. La evaluación profunda de la situación de seguridad de un Endpoint inspecciona el tráfico del túnel en busca de contenido malicioso y seguridad de datos. RevBits ZTN crea un límite de acceso lógico basado en la identidad y el contexto que abarca a los usuarios y sus aplicaciones. Las aplicaciones se encuentran ocultas y el acceso está restringido mediante un agente de confianza con una colección de entidades con nombre. El intermediario verifica la identidad, el contexto y el cumplimiento de la política de los participantes especificados antes de permitir el acceso.

## Requerimientos de Software

**Sistemas operativos:** Windows 7+ (Windows 7, 8, 8.1, 10, 11, 2008, 2012, 2016, 2019)

MacOS (10.15 Catalina, 11 Big Sur, 12 Monterey+), M1 chips  
Familia Linux Debian compatible (Debian, Ubuntu, Mint, etc.), y familia Redhat (CentOS, Redhat, Fedora, etc.)

**Mínimo:** 200MB de espacio en disco, 4GB RAM, sistemas operativos de 32-bit y 64-bit están soportados.

## Opciones de Implementación

RevBits CIP ofrece opciones de implementación flexibles. Se admiten todos los entornos de alojamiento, incluidos los locales, la nube e híbridos. La solución basada en la nube aprovecha los puntos de presencia globales con soporte de escalado automático elástico para organizaciones con múltiples sitios. Con 24 ubicaciones PoP en todo el mundo, RevBits CIP tiene redundancia incorporada para una resiliencia de servicio sólida como una roca.

## Beneficios de Cyber Intelligence Platform

**Elimina las brechas de seguridad creadas por los productos de seguridad en silos** – Permite capacidades de detección y prevención más precisas y reduce el costo total de propiedad (TCO), al tiempo que logra un tiempo de valor más rápido. Integra datos relevantes para una clasificación de alertas más rápida y precisa.

**Mejora la productividad de las operaciones de seguridad** – Reduce la complejidad de la configuración de seguridad y la respuesta a incidentes con correlación de alertas e incidentes, automatización integrada y casi cero alertas de falsos positivos. Recopila, procesa, conserva y brinda visibilidad para analizar evidencia de ataques cibernéticos, identificar vulnerabilidades y acelerar la mitigación.

**Unifica los productos de seguridad integrados** – Proporciona mejores resultados de seguridad que los productos y herramientas de seguridad aislados y en silos. Integra módulos de seguridad patentados en una única plataforma de seguridad unificada con múltiples flujos de telemetría y múltiples formas de detección.

**Consolida múltiples capacidades de ciberseguridad** – Una plataforma cohesiva de ciberseguridad que acelera la detección y la respuesta. La inteligencia de amenazas locales y externas se comparte de inmediato entre los módulos de seguridad para bloquear de manera eficiente las amenazas en todos los componentes.

**Admite entornos locales y alojados en la nube** – En combinación con el escalado automático y el equilibrio de carga avanzado, RevBits CIP se escala dinámicamente con la demanda. Proporciona configuración centralizada y capacidad de refuerzo con orientación ponderada para ayudar a priorizar actividades.

## Funcionalidades Adicionales de la Solución

**Una solución de ciberseguridad unificada, pero modular y extensible** – Se puede implementar para trabajar con Syslog, LogRhythm, Splunk, SIEM y otras plataformas de seguridad y administración de registros.

**Los mejores productos de seguridad integrados de su clase** – Seguridad de correo electrónico, detección y respuesta de Endpoint (DRE), tecnología de engaño, administración de acceso privilegiado (PAM) y redes de confianza cero (ZTN).

**Plataforma de seguridad multiusuario** – Se puede implementar en la nube o en las instalaciones, y es compatible con entornos multinube, locales e híbridos.

**Arquitectura flexible** – Permite a los equipos de seguridad implementar cualquier capacidad de seguridad que necesiten. Elija productos agregando o eliminando licencias dentro del panel de PCI. Los

productos de seguridad también se pueden implementar de forma independiente dentro de la infraestructura de seguridad existente.

**Respaldado por 5 patentes estadounidenses** – Todas las patentes se centran en resolver problemas críticos de seguridad.

**Automatiza la detección y corrección de actividades anómalas** – Pila de seguridad multicapa totalmente interfuncional.

**Combina los productos de ciberseguridad en un único panel intuitivo** – Permite un análisis forense cibernético rápido con análisis y contexto para resolver amenazas rápidamente

**Mantenga su empresa protegida. [Obtenga una demostración o evaluación gratuita.](#)**  
**Para obtener más información, visite [www.revbits.com](http://www.revbits.com)**