

## Endpoint Security

# Software de seguridad intuitivo y de alto rendimiento que bloquea las amenazas de seguridad más avanzadas.



Como software de seguridad intuitivo y de alto rendimiento, RevBits Endpoint Security bloquea los ataques más sofisticados. RevBits Endpoint Security es la única solución disponible que realiza un análisis de amenazas en tres fases. El módulo completo y rico en funciones RevBits Endpoint Detection and Response (EDR) proporciona un control completo y acceso al sistema violado desde cualquier lugar.

### Funcionalidades de Análisis y Detección

#### Análisis trifásico de nuevos ejecutables

Los nuevos ejecutables se aíslan y analizan antes de su lanzamiento para proteger la red. El análisis se realiza primero con comparaciones de firmas; segundo con verificación de aprendizaje automático y tercero por análisis de comportamiento.

#### Detección avanzada de exploits

La detección de vulnerabilidades de RevBits Endpoint Security se superpone a aplicaciones y procesos vulnerables, incluidos, entre otros, navegadores web, software de autoedición (como Microsoft Office o Adobe Reader) y otros.

#### Grabación de procesos

RevBits Endpoint Security registra toda la información de terminación y ejecución de procesos, incluidos sus hashes (MD5, SHA 1 y SHA2), estación de trabajo, nombre de usuario y marca de tiempo durante seis meses.

#### Módulo anti-ransomware efectivo

A través de su sofisticada función de sandboxing del sistema de archivos, RevBits Endpoint Security puede detectar y bloquear todo tipo de ransomware simple y sofisticado.

#### Controlar dispositivos USB

Los administradores del sistema pueden establecer una amplia política de dispositivos USB a través del entorno de gestión de USB integrado.

#### Cortafuegos basado en host

Los administradores del sistema pueden ajustar las reglas de la red y del cortafuegos tanto para estaciones de trabajo individuales como para grupos de estaciones de trabajo.

#### Aislamiento inmediato del host

Proteja la red de forma automática o manual al confinar los hosts potencialmente infectados.

#### Extracción de evidencia

##### Forense automática

Extracción de evidencia forense previa al apagado automático o bajo demanda para ayudar en una respuesta rápida a incidentes.

**Endpoint Security con el poder de detectar y bloquear el malware más sofisticado y soporte por completo investigaciones y análisis de Endpoints a través de EDR real.**

#### Sistema de notificación avanzado

RevBits Endpoint Security se integra a la perfección con todas las soluciones SIEM. Además, los administradores recibirán una notificación por SMS y correo electrónico cuando ocurra un incidente.

## Capacidades de Investigación de Endpoints

### Verdaderamente innovador

Dos patentes de EE. UU. para un avance tecnológico único para detectar y bloquear el acceso al kernel de controladores firmados y no firmados.

### Capacidad de línea de comando

Powershell y terminal de solicitud de línea de comandos para interactuar con todos los Endpoints remotos.

### Menú EDR completo

Interactúe con endpoints remotos para incluir: Proceso, Explorador de archivos, Explorador de registro, Consola de comandos, Servicios, Controladores, Kit anti-root, Inicio y Herramientas.

### Control GUI sobre todos los puntos finales

Interfaz gráfica para todas las operaciones EDR de endpoint remoto.

### Control profundo de endpoints

Interactúe con endpoints remotos para controlar el explorador de registro, el explorador de archivos, el explorador de procesos con la jerarquía del árbol de procesos.

### Control total a distancia

Los administradores del sistema pueden volcar de forma remota la memoria del proceso, el disco sin procesar y el volcado de la unidad sin procesar.

## 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+), compatible con Chips M1

Familia Linux Debian [Debian, Ubuntu, Mint, etc.], y la familia Redhat [CentOS, Redhat, Fedora, etc.]

**Requisitos Mínimos:** 200 MB de espacio en disco, 4 GB de RAM Se admiten sistemas operativos de 32 y 64 bits

## Funcionalidades Adicionales

**Con todas las funciones en un entorno Air-Gap** – RevBits Endpoint Security se puede implementar por completo en un entorno Air-Gap. Todas las características del producto son funcionales y procesables sin conexión a Internet.

## Beneficios de Endpoint Security

### Reduzca la posibilidad de una ejecución maliciosa exitosa

– RevBits Endpoint Security protege contra todo tipo de amenazas de Endpoint en cualquier tipo de red a través de su exclusivo análisis de tres fases de nuevos ejecutables. Desde el malware menos sofisticado hasta el más sofisticado, RevBits Endpoint Security está diseñado para detectar y bloquear su ejecución y salvar la red de una filtración costosa.

### Detenga el malware antes de que se ejecute

– Al aislar y analizar minuciosamente los nuevos ejecutables, la posibilidad de un ataque exitoso se reduce en gran medida.

**Análisis forense exhaustivo** – Al recopilar información muy útil sobre ejecuciones, scripts y comandos, el tiempo de los administradores del sistema y los gastos en clasificación y limpieza se reducen considerablemente. Esta capacidad amplía la funcionalidad para satisfacer las necesidades y estándares de cumplimiento.

### Reduzca la necesidad de contratar empresas forenses y de remediación externas

– El módulo EDR de RevBits Endpoint Security permite a los administradores de sistemas realizar investigaciones internas de la red, lo que minimiza la necesidad de utilizar recursos externos.

**Reducir el éxito de la amenaza interna** – El costo para la organización que representa una amenaza interna es sustancial. Los costos asociados con las infracciones y el robo de datos se pueden mitigar y controlar a través de la amplia capacidad de administración de políticas USB del acuerdo RevBits Endpoint Security.

**Detecte y contenga malware en el punto final** – RevBits Endpoint Security realiza un análisis único de tres fases en todos los ejecutables nuevos. Este análisis incluye escaneo de firmas, aprendizaje automático y análisis de comportamiento, lo que maximiza la precisión de la detección de malware y minimiza los falsos positivos.

**Visibilidad y control completos con RevBits EDR –**

Los detalles completos y de bajo nivel de procesos, subprocesos, registro, sistema de archivos y kernel son visibles y controlables a través de la GUI de RevBits EDR, no una simple línea de comandos. Los administradores del sistema pueden ejecutar comandos en powershell o símbolo del sistema en las estaciones de trabajo. Las funciones de extracción de pruebas forenses con un solo clic, imágenes de memoria y imágenes de discos hacen de RevBits EDR la solución EDR más sofisticada del mercado.

**Tablero intuitivo que revela información procesable**

– RevBits Endpoint Security proporciona una vista en tiempo real y fácil de entender de las amenazas a través de su moderna interfaz web. El tablero presenta información histórica extensa de todos los ejecutables en un claro y simple mosaico y mantiene información detallada del proceso durante seis meses.

**Información histórica detallada de todos los comandos ejecutados**

– RevBits Endpoint Security registra e informa todos los comandos y scripts ejecutados en todos los intérpretes de comandos y scripts, incluidos Windows Command Prompt, Powershell, VBScript y JScript.

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