HOJA DE DATOS

WatchGuard Full Encryption

La primera línea de defensa para proteger datos de manera simple y efectiva

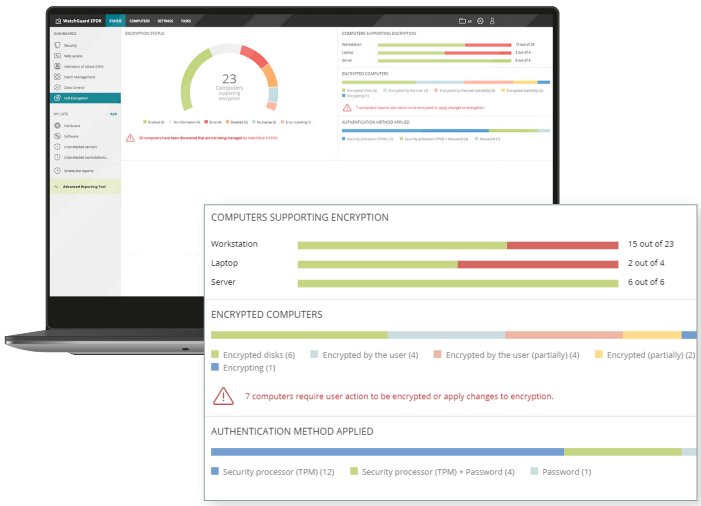
Según Gartner,[1] se roba una computadora portátil cada 53 segundos. El aumento sostenido de los datos almacenados en endpoints ha producido un claro aumento del interés en estos datos, junto con el riesgo de sufrir una vulneración de datos a través de la pérdida, el robo o el acceso no autorizado a información.

Esto hizo que las regulaciones como el GDPR[2] de la Unión Europea y la CCPA[3] de los Estados Unidos se volvieran cada vez más exigentes con el objetivo de reducir las probabilidades de pérdidas, robos o acceso no autorizado a datos y el grave impacto económico que esto supone.

FORTALECIMIENTO DE LA SEGURIDAD DE MANERA CENTRALIZADA CONTRA EL ACCESO NO AUTORIZADO

Uno de los modos más efectivos de minimizar la exposición de datos es la de cifrar de manera automática los discos duros en computadoras de escritorio, computadoras portátiles y servidores. Así, el acceso a los datos es seguro y cumple con los mecanismos de autenticación establecidos. Al establecer políticas de cifrado, las organizaciones obtienen una capa adicional de seguridad y control, aunque también se pueden ocasionar problemas de control y recuperación de datos si se pierde la clave.

WatchGuard Full Encryption protege los dispositivos Windows y macOS con cifrado de disco completo contra posibles violaciones de datos y acceso no autorizado. Aprovecha BitLocker en sistemas operativos Windows o FileVault en sistemas macOS para cifrar y descifrar discos sin afectar a los usuarios finales, lo que permite proporcionar a las organizaciones el valor agregado de controlar y administrar centralmente las claves de recuperación almacenadas en la plataforma de administración WatchGuard Cloud.



Panel de control de WatchGuard Full Encryption en la consola de administración web de WatchGuard, con indicadores clave del estado del cifrado de endpoints en toda la organización.

Impide la pérdida, el robo y el acceso no autorizado a datos sin afectar a los usuarios.

- Cifra sus discos y protege su contenido contra robo, pérdida accidental y amenazas internas maliciosas. El cifrado, descifrado y acceso a datos son automáticos e inmediatos, y transparente para los usuarios.
- Para su conveniencia, las claves de recuperación se almacenan y se recuperan de manera segura desde la plataforma en la nube y su consola web.

No se requiere implementación ni instalación. No se requieren servidores ni costos adicionales. Cero problemas.

- BitLocker viene preinstalado en la mayoría de los sistemas operativos Windows, mientras que FileVault se incluye en la mayoría de los dispositivos macOS. Con la consola web de la plataforma en la nube de WatchGuard, tendrá una única ubicación centralizada para administrar todos sus dispositivos.
- No tendrá que implementar ni instalar otro agente. Todas las soluciones basadas en Seguridad de Endpoints de WatchGuard comparten el mismo agente ligero.
- **WatchGuard Full Encryption** se puede habilitar de inmediato y se administra fácilmente desde la consola de la nube.

Cumplimiento normativo, reportes y administración centralizada

- WatchGuard Full Encryption facilita y simplifica el cumplimiento con las regulaciones de protección de datos, ya que supervisa e implementa el cifrado de datos.
- WatchGuard Full Encryption aprovecha BitLocker o FileVault, lo que permite a los administradores configurar políticas de cifrado y administrar de forma centralizada las claves de recuperación desde la nube.
- Todas las soluciones basadas en Seguridad de Endpoints de WatchGuard ofrecen paneles de control intuitivos, reportes detallados y registros de actividades del usuario para auditorías.

BENEFICIOS

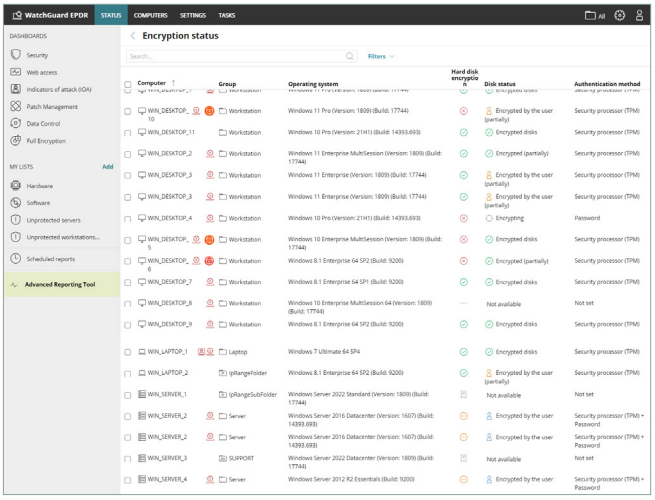
UNIDADES FLASH USB SEGURAS*

En el último año, en todo el mundo aumentó un 30% el uso de las memorias USB externas, especialmente en las organizaciones industriales. Los criminales informáticos notaron esta tendencia y utilizan unidades USB como punto de entrada para obtener acceso a un sistema e infectar toda la red o parte de ella.

En consecuencia, las organizaciones tienen más probabilidades de sufrir vulneraciones de datos o acceso no autorizado a información confidencial. Según un estudio realizado por Forrester, la pérdida o el robo de activos como computadoras portátiles o unidades USB generó un 17% de las vulneraciones de datos reportadas en 2023.

El primer paso para minimizar el riesgo de amenazas es contar con una política estricta que incluya pautas sobre el uso de unidades USB en la organización, los roles y los permisos en función de los perfiles del personal, y utilizar únicamente dispositivos proporcionados y verificados por el equipo de TI de la organización o el proveedor de servicios administrados (MSP).

No obstante, es posible que estas pautas no sean suficientes frente al número creciente de amenazas informáticas. **WatchGuard Full Encryption** proporciona una máxima protección de los datos en todos los endpoints cifrados. Permite implementar una autenticación previa al arranque, con la cual se verifica la identidad del usuario antes de que se inicie el sistema operativo. De esta manera, se evita la pérdida y el robo de computadoras portátiles, y el acceso no autorizado a los datos.



Lista de computadoras que indica el estado de cifrado, los grupos a los que pertenecen, sus sistemas operativos y el método de autenticación utilizado.

FUNCIONALIDADES CLAVE

La tendencia hacia la modalidad de trabajo híbrido, ya sea trabajo remoto o desde la oficina, convierte al cifrado de disco completo en una primera línea defensiva fundamental para dispositivos como computadoras portátiles y unidades USB.

WatchGuard Full Encryption es un módulo adicional de las soluciones de Seguridad de Endpoints de WatchGuard y está diseñado para administrar de manera centralizada el cifrado de disco completo y ofrecer las siguientes funcionalidades:

Cifrado y Descifrado Completo de Unidades

WatchGuard Full Encryption cifra las unidades de las computadoras portátiles, las computadoras de escritorio y los servidores de Windows o macOS, y las unidades de almacenamiento removibles (solo Windows). El panel de control de **WatchGuard Full Encryption** ofrece visibilidad global de los endpoints de red compatibles, su estado de cifrado y el método de autenticación utilizado. Además, permite a los administradores asignar configuración de cifrado y restringir permisos de cifrado.

Administración Centralizada de Claves de Recuperación

Si olvida la clave de acceso o hubo cambios en la secuencia de arranque, BitLocker le solicitará una clave de recuperación para iniciar el sistema afectado. En relación con macOS, si olvida la contraseña de usuario, FileVault también le solicitará una clave de recuperación para iniciar el sistema. En ambos casos, si es necesario, el administrador de red puede obtener las claves de recuperación a través de la consola de administración y enviarlas al usuario.

Listas, Reportes, Implementación Centralizada de Políticas

La lista de computadoras de la consola permite a los administradores aplicar varios filtros en función del estado de cifrado. Estas listas se pueden exportar para análisis de datos con herramientas externas.

Puede definir políticas de cifrado desde la consola y ver cambios de políticas a través de reportes de auditoría, que puede presentar a los organismos e instituciones reguladoras en caso de ser necesario.

[1] TechSpective

[2] GDPR: Reglamento General de Protección de Datos: obliga a las organizaciones a garantizar que la información personal esté protegida. La falta de cumplimiento con este reglamento puede derivar en elevadas multas y daños indirectos.

[3] CCPA: Ley de Confidencialidad del Consumidor de California de 2018: es la primera ley de Estados Unidos que sigue los pasos del GDPR de la Unión Europea. Se aplica a las empresas radicadas en California y a las empresas ubicadas fuera del estado.

[4] The State Of Privacy And Data Protection (El estado de la protección de la privacidad y los datos), 2023 - Forrester

* El cifrado y descifrado de unidades flash externas y USB solo son compatibles con los sistemas operativos Windows.

Requisitos de plataformas y sistemas compatibles con WatchGuard Full Encryption

Sistemas operativos compatibles con WatchGuard Advanced EPDR, WatchGuard EPDR, WatchGuard EDR y WatchGuard EPP: Windows and macOS..

Lista de navegadores compatibles: Google Chrome, Mozilla Firefox, Safari, and Microsoft Edge.

VENTAS EN EE. UU. 1.800.734.9905 VENTAS INTERNACIONALES +1.206.613.0895 SITIO WEB www.watchguard.com WatchGuard Technologies, Inc.