

DATALOCKER PORTBLOCKER

SOLUCIÓN DE BLOQUEO DE PUERTO USB GESTIONADO POR SAFECONSOLE



MANTENGA EL CONTROL DE SUS PUERTOS USB

PortBlocker es un enfoque "simply secure" para la prevención de pérdida de datos (DLP) para almacenamiento extraíble que limita cuales dispositivos de almacenamiento USB/discos duros externos pueden utilizarse en el Workstation de un usuario. Con PortBlocker, los usuarios solo pueden transferir datos a dispositivos encriptados seguros y aprobados, lo que evita las violaciones de datos debido al uso y acceso no autorizados. PortBlocker está integrado con SafeConsole, la solución líder de administración central para el almacenamiento encriptado seguro. Toda la actividad de los dispositivos de una empresa, cómo, cuándo y dónde se bloquea un dispositivo, se reporta a los registros de auditoría de SafeConsole para que los administradores los revisen.

CARACTERÍSTICAS PORTBLOCKER

- **Control de puerto de dispositivos**- aprobar y agregar a la lista blanca dispositivos de almacenamiento USB por ID de proveedor (VID), ID de producto (PID) y número de serie a través de SafeConsole.
- **Aplicación de políticas basadas en computadora** -las políticas se aplican según la ubicación de Workstation en Directorio Activo. Si es necesario, se pueden crear políticas individuales hasta el nivel de cada Workstation.
- **Desactivación / Habilitación Rápida** - los administradores pueden "Permitir todos" o "Bloquear todos" de forma remota a través de SafeConsole.
- **Auditorías de Actividad** - todos los eventos, como cuando se bloquea un dispositivo, cuando se registra un dispositivo y cuando hay ediciones o cambios de políticas, se informan a SafeConsole en los registros de auditoría.
- **Geofence** - los dispositivos se pueden bloquear automáticamente cuando el Workstation se usa fuera de la política de geolocalización que se aplica y configura a través de SafeConsole.

¿CÓMO FUNCIONA PORTBLOCKER?

Siempre en protección. Una vez instalado por un administrador, PortBlocker se iniciará automáticamente y se ejecutará en el Workstation del usuario en modo transparente (background). El agente PortBlocker no se puede desactivar o desinstalar sin privilegios de administrador.

Aplicación de Políticas. Restrinja los dispositivos de almacenamiento USB/ Discos duros a través de la política de la lista blanca de SafeConsole (VID, PID y número de serie). Las políticas se actualizan automáticamente desde SafeConsole.

Informes en tiempo Real. La administración central de PortBlocker a través de SafeConsole facilita la auditoría de quién, qué, cuándo y dónde se produjo una amenaza.

REQUERIMIENTOS MÍNIMOS

- Cuenta Activa SafeConsole (v5.4.0 +)
- Windows™ 7 o 10 (compatibilidad con macOS en el segundo trimestre de 2019)
- 512MB de RAM
- 1 GB de espacio disponible en el disco duro
- Conexión al servidor SafeConsole para Registro y actualizaciones de políticas
- Conexión de red de 1Mbps
- Intel Quad Core Atom processor, or equivalent x86 - x64 processor
- Utiliza la configuración de proxy del usuario del sistema WinINET (Internet Explorer). Configuración de proxy manual o una secuencia de comandos pac son compatibles.

Se requiere una cuenta de SafeConsole para utilizar y implementar PortBlocker. Para las nuevas cuentas de SafeConsole, también se requiere una tarifa base única. Entonces se requiere una licencia válida de PortBlocker para cada Workstation / sistema donde se implementa PortBlocker (licencias disponibles por 1 o 3 años).

🌐 datalocker.com/espanol

✉ latam@datalocker.com