

DATALOCKER PORTBLOCKER



BEHALTEN SIE DIE KONTROLLE ÜBER IHRE USB-PORTS

PortBlocker ist DataLockers DLP- (Data Loss Prevention) Lösung für USB-Massenspeicher. Dadurch kann konfiguriert werden, welche USB-Laufwerke an Anwender-PCs genutzt werden dürfen. Mit PortBlocker können Nutzer sensible Daten ausschließlich auf freigegebenen, verschlüsselten USB-Laufwerken speichern und somit einem Datenverlust durch nicht autorisierten Zugriff vorbeugen. PortBlocker ist als Option für SafeConsole, die führende USB-Device-Management-Lösung für sichere USB-Speicher, verfügbar. Alle Endpoint-USB-Aktivitäten werden in den SafeConsole Audit-Berichten gespeichert und können vom Administrator ausgewertet werden.

LEISTUNGSMERKMALE

- **Endpunkt USB-Port Kontrolle** - Beschränken Sie die Nutzung von USB-Speichern durch Freigabe-Richtlinien in SafeConsole, basierend auf Vendor ID (VID), Product ID (PID) und Seriennummer des Laufwerkes.
- **System-basierte Durchsetzung von Sicherheitsrichtlinien** - Richtlinien werden basierend auf Active DirectoryTM eingerichtet. Individuelle Richtlinien können bei Bedarf bis hinunter auf System-Ebene erstellt werden.
- **Sofortiges Aktivieren / Deaktivieren** - Administratoren können in SafeConsole festlegen, ob ALLE USB-Speichermedien freigegeben oder blockiert werden sollen.
- **Aktivitätsberichte** - Alle Ereignisse, wie blockierte Laufwerke, registrierte Endpunkte / PCs, sowie Änderungen der Richtlinien werden in den SafeConsole Audit-Berichten erfasst.
- **Geofence** - Laufwerke können automatisch blockiert werden sobald sich der Computer außerhalb von geografischen Standortanforderungen befindet.

WIE FUNKTIONIERT PORTBLOCKER?

Stets aktiver Schutz. Nach der Installation durch einen Administrator, startet PortBlocker automatisch auf der Benutzermaschine, läuft im Hintergrund und kann ohne Admin-Rechte nicht deaktiviert oder deinstalliert werden.




Durchsetzung von Richtlinien. Erlauben Sie die Nutzung von USB-Speichermedien durch die Freigabe in SafeConsole (VID, PID, Seriennummer). Die Richtlinien werden automatisch von SafeConsole aktualisiert.

Echtzeit-Berichte. Die zentrale Verwaltung der USB-Ports durch SafeConsole ermöglicht die Überprüfung wann und wo eine Bedrohung verursacht wurde, bzw. wer oder was diese verursacht hat.

SYSTEMANFORDERUNGEN

- Aktive SafeConsole (Version 5.4.0+)
- WindowsTM 7 oder 10 (macOS ab Q2/2019)
- 512MB Arbeitsspeicher
- 1GB verfügbarer Festplattenspeicher
- Verbindung zum SafeConsole Server zur Registrierung der Endpunkte und Aktualisierung der Richtlinien
- 1Mbps Netzwerk-Verbindung
- Intel Quad Core Atom Prozessor oder vergleichbarer x86 - x64 Prozessor
- Es werden die WinINET (Internet Explorer) Proxy-Einstellungen verwendet. Manuelle Proxy-Einstellungen und automatische Konfigurationskripte (pac) werden unterstützt.

Es wird eine aktive SafeConsole (SCOP-BASE / SCC-BASE) benötigt um PortBlocker bereitzustellen. Darüber hinaus wird eine PortBlocker Lizenz für jeden Endpunkt / PC benötigt, auf dem PortBlocker verwendet werden soll. Es sind 1- und 3-Jahres Lizenzen verfügbar.

 datalocker.com
 emea@datalocker.com
 +49 21 91 / 437 9702