DATALOCKER®
SIMPLY SECURE

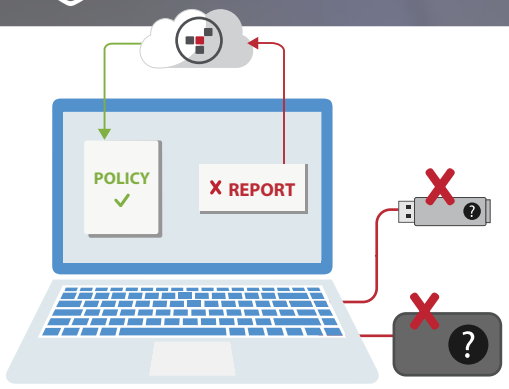
SAFECONSOLE PORTBLOCKER

Sécurité centralisée des ports USB et contrôle des périphériques

PortBlocker

PortBlocker assure une protection robuste et automatisée contre les accès USB non autorisés au sein de votre organisation. Grâce à une intégration transparente avec la plateforme de gestion SafeConsole, une surveillance en temps réel et un contrôle centralisé des politiques, PortBlocker garantit que seuls les périphériques USB autorisés peuvent se connecter aux postes de travail protégés, renforçant ainsi considérablement la sécurité des données, réduisant les risques liés aux logiciels malveillants et prévenant les pertes de données.

PortBlocker fonctionne en continu en arrière-plan, assurant la sécurité sans perturber les flux de travail des utilisateurs, tout en offrant aux administrateurs une visibilité et un contrôle complets sur l'accès USB sur le réseau.



Géré par
SAFECONSOLE®

Blocage simple et automatique des périphériques

PortBlocker bloque automatiquement les périphériques USB non autorisés dès leur insertion dans un port USB. Les administrateurs sont immédiatement avertis et chaque événement est consigné dans les journaux d'audit de SafeConsole. En quelques clics, les périphériques autorisés peuvent être ajoutés à la liste blanche ou bloqués définitivement.

Intégration transparente avec SafeConsole

PortBlocker s'intègre parfaitement à la plateforme de gestion SafeConsole, permettant un contrôle centralisé des ports USB tout en prenant en charge les politiques SafeConsole existantes. Une fois installé, il fonctionne discrètement en arrière-plan pour assurer une protection continue sans interrompre la productivité.

Supervision active et reporting

Les ports USB sont surveillés en temps réel. Toute activité est consignée dans les journaux d'audit SafeConsole, offrant ainsi aux administrateurs une visibilité sur l'état des terminaux et leur permettant de prendre des décisions de sécurité rapides et éclairées.

Protection permanente

Une fois déployé, PortBlocker s'exécute automatiquement en arrière-plan et ne peut pas être désactivé par les utilisateurs non autorisés. Les mises à jour sont distribuées de manière sécurisée par les administrateurs conformément aux politiques et procédures de l'organisation, garantissant ainsi une protection homogène sur tous les terminaux.

Application des politiques de sécurité

SafeConsole applique des politiques de liste blanche basées sur le VID, le PID et les numéros de série, avec des mises à jour en temps réel qui garantissent que seuls les périphériques USB autorisés peuvent se connecter aux systèmes protégés.

Audit des terminaux en temps réel

L'activité liée aux périphériques USB est enregistrée et signalée à SafeConsole, fournissant des rapports d'audit détaillés des terminaux sur la plateforme de gestion centralisée pour une investigation et une réponse rapides.

EXIGENCES MINIMALES

- Un compte SafeConsole actif
- Une licence PortBlocker valide pour chaque point de terminaison
- Windows 10 ou 11, ou macOS 15.x+ — Intel ou Apple Silicon
- Une connectivité réseau au serveur SafeConsole pour l'enregistrement et les mises à jour des stratégies

LICENCE

Un compte SafeConsole valide est requis pour déployer PortBlocker. Une licence PortBlocker est nécessaire par poste de travail, disponible pour une durée de 1 ou 3 ans.

DATALOCKER®
SIMPLY SECURE

Réservez une démo

datalocker.com | sales@datalocker.com

©2026 DATALOCKER, INC. TOUS DROITS RÉSERVÉS. DATALOCKER EST UNE MARQUE DÉPOSÉE DE DATALOCKER INC. TOUTES LES AUTRES MARQUES SONT LA PROPRIÉTÉ DE LEURS PROPRIÉTAIRES RESPECTIFS. 0726

Support au déploiement et prise en charge des plateformes

- Compatibilité multiplateforme : Windows et macOS
- Gestion centralisée via SafeConsole
- Distribution sécurisée des mises à jour administratives
- Modèle de déploiement évolutif pour l'entreprise

FONCTIONNALITÉS DE PORTBLOCKER

- Blocage automatique des périphériques USB non approuvés
- Gestion centralisée des politiques de sécurité USB via SafeConsole
- Autorisation des périphériques par liste blanche
- Identification des périphériques basée sur le VID, le PID et le numéro de série
- Supervision en temps réel des activités USB
- Génération d'alertes en temps réel
- Journalisation d'audit liée aux périphériques USB
- Reporting et visibilité centralisés
- Protection continue en arrière-plan
- Mécanismes de sécurité impossibles à contourner par des utilisateurs sans privilèges administratifs
- Mises à jour sécurisées contrôlées par l'administrateur
- Protection des données grâce à un contrôle centralisé des accès USB
- Réduction des risques liés aux logiciels malveillants grâce au contrôle des périphériques
- Intégration native et transparente à la plateforme SafeConsole
- Compatibilité multiplateforme (Windows et macOS)



Également disponible :

SafeConsole USB Device Management

Gestion sécurisée des périphériques USB
Administrez et contrôlez vos clés USB chiffrées via une gestion centralisée intégrant audit et politiques de sécurité.

SafeConsole USB Data Erasure

Effacement certifié des données USB
Effacement cryptographique certifié avec génération automatique de preuves d'effacement, certificats infalsifiables et conformité à la norme NIST SP 800-88.

SafeConsole Anti-Malware

Logiciel anti-malware pour périphériques USB sécurisés
Protégez vos clés USB grâce à un système anti-malware intégré qui analyse et signale les menaces de logiciels malveillants directement à SafeConsole.

DataLocker Simply Secure

Réservez une démo

datalocker.com | sales@datalocker.com

©2026 DATALOCKER, INC. TOUS DROITS RÉSERVÉS. DATALOCKER EST UNE MARQUE DÉPOSÉE DE DATALOCKER INC. TOUTES LES AUTRES MARQUES APPARTIENNENT À LEURS PROPRIÉTAIRES RESPECTIFS. 1026