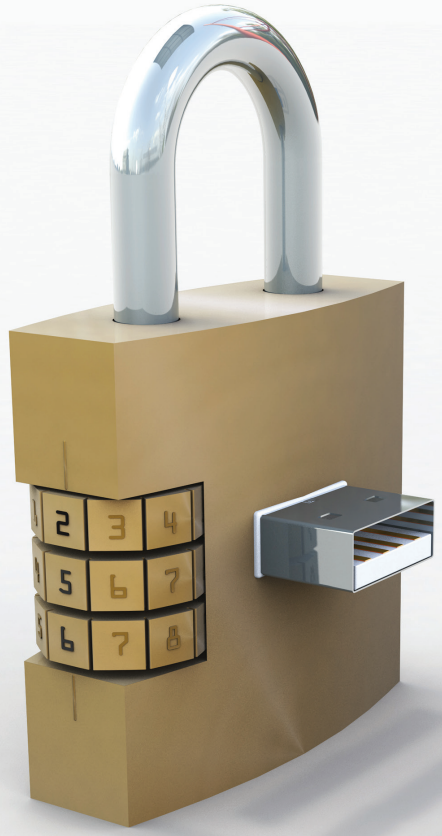
Contrôle complet sur l'utilisation de
stockage USB et autres appareils mobiles



Sensibilisation aux données

Evaluation des risques de fuite de données

Contrôle d'accès

Window Security.com READERS' CHOICE WINNER

SC MAGAZINE

OPSWAT. BRONZE CERTIFIED Device Access Control

Allez plus loin et commencez votre évaluation GRATUITE :

gfsfrance.com/endpointsecurity

Microsoft Partner
Gold Application Development
Silver Midmarket Solution Provider

GFI EndPointSecurity™

Contrôle des clés USB, iPods et autres périphériques d'entrée

Contrôle complet sur l'utilisation de stockage USB et autres appareils mobiles

La prolifération d'appareils grand public tels que les smartphones, lecteurs multimédias, périphériques de stockage mobiles, appareils connectés au réseau et clés USB faciles à dissimuler a augmenté le risque de fuites de données, d'infections virales, d'introduction de logiciels et de jeux sans licence et d'autres activités malveillantes sur les réseaux.

A l'heure où la plupart des sociétés sont équipées avec des antivirus, des pare-feu, des outils de sécurité de contenu web et email, peu réalisent à quel point il est facile de copier des quantités énormes de données commerciales sensibles sur un appareil de stockage mobile à l'insu de tous.

Verrouiller physiquement tous les ports USB ne représente ni une solution durable, ni une solution réalisable. La clé de la gestion de l'utilisation de périphériques portables consiste à installer une solution de sécurité qui offre à l'administrateur un contrôle sur quels périphériques sont en cours d'utilisation, l'ont été et par qui, ainsi qu'une connaissance approfondie sur les données copiées.

Comment ça marche ?

Pour contrôler l'accès, GFI EndPointSecurity installe automatiquement un agent caché et inviolable sur les machines de votre réseau. Cet agent peut être déployé sur l'ensemble des machines du réseau avec seulement quelques clics. Cet agent offre une protection inégalée contre les accès non autorisés même contre les utilisateurs avec des droits d'administrateur, permettant ainsi aux administrateurs informatiques de garder le contrôle quel que soit le problème.

Gérez les accès utilisateurs et protégez votre réseau contre les menaces des appareils mobiles

Avec GFI EndPointSecurity vous pouvez interdire l'accès aux utilisateurs de manière centralisée aux appareils de stockage mobiles, empêchant ainsi le vol de données ou l'introduction de données potentiellement nocives pour votre réseau. Même si vous pouvez désactiver certains ports de connexion physiques dans le BIOS, cette solution paraît peu réaliste, en outre les utilisateurs avancés peuvent facilement pirater le BIOS. GFI EndPointSecurity vous permet de prendre le contrôle d'une grande variété de périphériques.

Consignez les accès des périphériques portables sur votre réseau

En plus de bloquer l'accès aux médias de stockage mobiles, GFI EndPointSecurity consigne les activités des utilisateurs en rapport avec les périphériques à la fois dans le journal des événements et sur un serveur SQL central. Une liste des fichiers auxquels on a accédé sur un appareil donné est enregistrée chaque fois qu'un appareil autorisé est branché.

Chiffrez les appareils portables

Les utilisateurs peuvent être autorisés à stocker des données sur les périphériques USB à condition qu'elles soient chiffrées. L'accès à ces données en dehors du réseau de l'entreprise peut être contrôlé de manière stricte par une application "voyageur" ad hoc incluse dans GFIEndPointSecurity.

Autres fonctions :

- Assistant de création de stratégie pour un contrôle d'accès granulaire avancé
- Résumé quotidien/hebdomadaire
- Surveillance de statut et alertes en temps réel
- Rapports complets sur l'utilisation des périphériques avec le logiciel complémentaire GFI ReportPack
- Prise en charge de Windows 7 Bitlocker To Go
- Envoie des messages pop-up personnalisés aux utilisateurs qui souhaitent accéder à un périphérique verrouillé.
- Permet la navigation au sein des journaux d'activités et d'utilisation des périphériques via une base de données principale
- Possibilité de grouper les ordinateurs par service, par domaine, etc.
- Prise en charge de tous les systèmes d'exploitation dans une langue compatible avec Unicode
- Et plus !

Commencez votre évaluation gratuite sur **gfsfrance.com/endpointsecurity**

Avantages en un coup d'œil

Prévient les fuites et vols de données en contrôlant les accès aux périphériques mobiles de stockage avec une gestion minimale.

Empêche la perte de données accidentelle lorsque des périphériques de stockage amovibles sont perdus ou volés, grâce au chiffrement

Evalue le risque de fuite de données induit par les périphériques amovibles au niveau des points de terminaison et fournit des informations sur la façon de l'atténuer

Protège les données lorsque vous êtes en déplacement avec le chiffrement des volumes amovibles

Permet aux administrateurs de bloquer les périphériques par classe, extensions de fichier, port matériel ou ID de périphérique.

Permet aux administrateurs d'accorder un accès temporaire au périphérique ou port pendant une période donnée.

Pour une liste complète des avantages, visitez : **www.gfsfrance.com/endpointsecurity**

Configuration requise

Windows 2000 (SP4), XP, Vista, 7, 8, Windows Servers 8 et 2012 (versions x86 et x64)

Internet Explorer 5,5 ou ultérieur

.NET Framework version 4.0

Port : TCP port 1116 (défaut)

Base de données principale : SQL Server 2000/2005/2008 ; si ce logiciel n'est pas disponible,

GFI EndPointSecurity peut automatiquement télécharger, installer et configurer une version de SQL Server Express.

GFI®

www.gfsfrance.com

Pour une liste complète des bureaux et détails de contact de GFI dans le monde, veuillez visiter : www.gfsfrance.com/contact-us