

Protection contre la fuite de données et l'intrusion de menaces

Luttez efficacement contre le transfert illicite d'informations de ou vers des périphériques, médias amovibles ou connexions sans fil, tout en associant sécurité des données, productivité et confort des utilisateurs.

Administré de façon centralisée, DeviceLock est une solution logicielle qui renforce avec une grande précision la politique d'accès des ports et périphériques PC.



Contrôle d'accès aux ports et périphériques

► DeviceLock

Grâce à DeviceLock, contrôlez toutes les activités des périphériques de votre parc informatique : Iphone, clés USB, disques durs, clés 3G, presse-papier, copies écran, BlackBerry, etc.

Nouveautés de la version 7 :

- Processus d'installation amélioré et simplifié
- Analyse de texte dans les images : interception de fuite de données sous forme d'images, photos
- Presse papier analysé et surveillé comme les autres périphériques
- Fichiers compressés analysés et surveillés. L'analyse est faite sur tous les fichiers de l'archive
- Reconnaissance d'images dans les documents PDF/Microsoft Office
- Compatible avec BitLocker To Go intégré à Windows 7 (utilisation de médias amovibles chiffrés)

Options et modules additionnels

Outre les fonctionnalités haut de gamme de contrôle d'accès intégral aux ports et périphériques qui ont fait le succès de la solution, DeviceLock 7 est la première solution locale de DLP à incorporer un module de contrôle et de filtrage de contenu et un module de gestion des communications réseau.



Contrôle et de filtrage de contenus

► Module ContentLock

ContentLock permet un filtrage encore plus fin en inspectant le contenu des fichiers échangés à la recherche de mots clés ou expressions régulières : cartes de crédit, numéros de dossiers, etc. Vous atteignez un niveau de sécurité optimal en toute simplicité.



Gestion et contrôle des communications réseau

► Module NetworkLock

Maîtrisez la nature des informations qui transitent par le réseau vers l'extérieur, que le poste soit dans ou hors de l'entreprise. Vous évitez ainsi autant la fuite de données intentionnelle que les erreurs involontaires. Les moyens de communications courant sont pris en charge : Facebook, FTP, Yahoo Mail, ICQ, etc.



Indexation de documents et recherche de données

► Option DeviceLock Search Server (DLSS)

Étendez les capacités d'analyse de DeviceLock avec l'option DLSS qui permet une indexation et des recherches étendues/textuelles dans la base de données d'audit et d'instantanés de DeviceLock. DLSS est conçu pour faciliter la mise en conformité avec les processus d'audit, les enquêtes après incident, et les analyses légales plus précises, simples et rapides.



Pourquoi contrôler l'accès aux périphériques ?

Contrôler ce qui entre et sort d'un réseau par téléchargement est fondamental pour assurer la sécurité informatique d'une entreprise.

La popularité grandissante des outils de stockage amovibles représente pour la sécurité une menace évidente.

Ce marché croît avec la commercialisation de matériels de plus en plus rapides, disposant d'une capacité croissante et plus petits de jour en jour.

Un autre danger provient des périphériques Bluetooth qui, pour promouvoir leur facilité d'utilisation, sont configurés par défaut afin de communiquer avec tout client Bluetooth à l'intérieur d'une certaine zone qui peut être incroyablement étendue.

Témoignage

« Avec DeviceLock, j'ai l'esprit tranquille, il n'y a pas de faiblesses au niveau de l'utilisation des périphériques de stockage sur notre réseau interne. Par ailleurs, le recours à cette solution a été compris et accepté par l'ensemble des salariés, déjà impliqués dans la sécurité du système d'information de par notre charte »

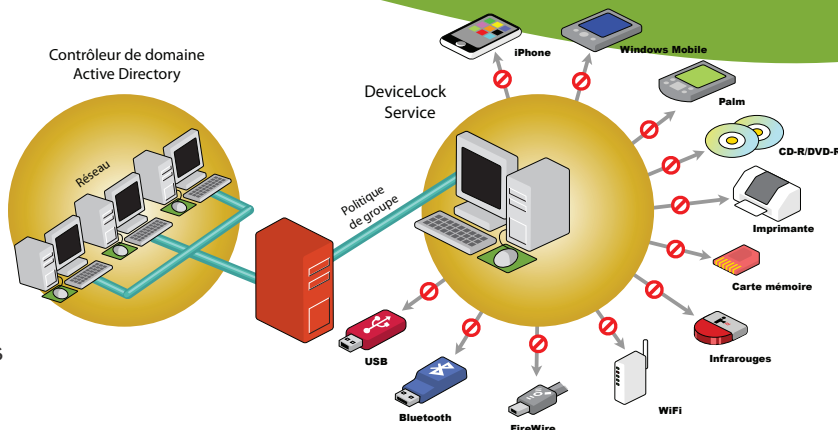
Julian OUTIN,
Responsable Informatique
de Moneo Payment Solutions
www.moneo.net

Intégration dans Active Directory

DeviceLock s'intègre directement, sans aucun ajout de script, de templates ADO, ni modification structurelle, dans :

- La console de gestion Microsoft (MMC) d'Active Directory
- La console de gestion des stratégies de groupe (GPMC)
- L'arborescence des utilisateurs et ordinateurs d'Active Directory (ADUC)

Contrôlez dynamiquement les points de fuite de données et les paramètres d'audit tout en assurant les tâches liées aux stratégies de groupe.



Intégration du chiffrement

Intégrez ou ajoutez la solution de chiffrement qui répond à vos besoins parmi les technologies les plus avancées :

- Windows 7 BitLocker To Go™
Chiffrement PGP® de disque entier pour un chiffrement certifié FIPS
- TrueCrypt® pour un chiffrement Open Source
- SafeDisk®
- SecurStar® DriveCrypt Plus Pack Enterprise (DCPPE)
- Clés USB Lexar JumpDrive SAFE S3000
- Clés USB Lexar SAFE PSD S 1100 pré-encryptées



Les stratégies de liste d'autorisations peuvent être appliquées aux supports amovibles pré-encryptés.



Instantanés de données (Shadow Copy)

Grâce à DeviceLock, dupliquez les données copiées vers des périphériques de stockage externe, imprimées, ou encore transférées via les ports série, parallèle ou réseau.

DeviceLock permet également de fractionner les images ISO produites par les graveurs CD/DVD en restaurant les fichiers originaux. Les fonctionnalités d'audit et d'instantanés de DeviceLock sont conçues pour une utilisation optimale des ressources de transmission et de stockage, avec compression à la volée, lissage de trafic, paramètres de performances/quota et sélection automatique du serveur DLES optimal.

Rapport de périphériques Plug and Play

Les administrateurs peuvent générer un rapport affichant les périphériques USB, FireWire, et PCMCIA connectés actuellement ou précédemment à des PC sur le réseau. Ce rapport permet également de compléter efficacement la liste d'autorisation des périphériques USB, en y ajoutant des modèles ou des périphériques uniques.

Rapports graphiques

DeviceLock peut générer automatiquement des rapports graphiques, basés sur les journaux d'audit et d'instantanés, aux formats HTML, PDF ou RTF.

Liste des revendeurs agréés sur
www.deviceclock.fr

Ports contrôlés

- USB
- FireWire
- Infrarouge
- Serial and parallel

Types de périphériques contrôlés

- Disquettes
- CD-ROM/DVD
- Médias de stockage (clés USB, cartes mémoire, etc.)
- Disques durs
- Lecteurs de bandes
- Adaptateurs WiFi
- Adaptateurs Bluetooth
- Windows Mobile, Palm OS, Apple iPhone/iPod touch/iPad et BlackBerry
- Imprimantes (locales, en réseau, virtuelles)

Contrôle du presse-papier

- Opérations de copier/coller entre applications via le presse-papier
- Contrôle séparé des types de données : types de fichiers, données textuelles, images, audio, non-identifiés
- Captures d'écran (Windows ou application tierce)

VOTRE REVENDEUR :