DeviceLock
Proactive Endpoint Security

Communiqué de presse

DEVICELOCK PROTÈGE LES TERMINAUX WINDOWS 7 GRÂCE À SA SOLUTION INTELLIGENTE DE PRÉVENTION CONTRE LA FUITE DE DONNÉES

Paris, le 21 octobre 2009 - DeviceLock, Inc., leader mondial pour le contrôle et la protection des informations en entreprises, annonce aujourd'hui la prise en charge de Windows 7, le nouveau système d'exploitation de Microsoft. Offrant un ensemble complet de fonctionnalités adaptatives au contexte de prévention contre la fuite de données, le logiciel DeviceLock® version 6.4.1 peut être installé sur tous les PC de bureau, ordinateurs portables et serveurs équipés de Windows 7, assurant ainsi leur protection immédiate contre les fuites de données d'origine interne.

« Avec la sortie imminente de Windows 7, nous sommes sûrs que de nombreux clients voudront sans tarder migrer vers la nouvelle plate-forme. C'est pourquoi nous avons souhaité ajouter aussi vite que possible la prise en charge de Windows 7 à notre logiciel, avant même le lancement de ce nouveau système d'exploitation », souligne Ashot Oganesyan, fondateur et Directeur de la Technologie de DeviceLock. *« Cet effort souligne une fois de plus notre souci constant : proposer à nos clients les meilleurs produits de protection, et les aider dans leurs démarches de mise en conformité aux normes et réglementations de plus en plus restrictives en matière de sécurisation des données confidentielles. »*

En allant bien au-delà des fonctionnalités de contrôle des périphériques offertes par Windows 7, DeviceLock permet aux clients de contrôler précisément, de consigner, de prendre des clichés instantanés et de surveiller l'accès des utilisateurs à l'ensemble des périphériques et des ports locaux d'un ordinateur (USB, FireWire, LPT, COM, IrDA, amovible, disque dur, disquette, DVD/CD-ROM, bande, Modem, Bluetooth, Wi-Fi, etc.).

Grâce à sa technologie brevetée de filtrage des synchronisations locales, DeviceLock permet aux administrateurs de définir de manière centralisée et granulaire les types de données que des groupes ou des utilisateurs spécifiques sont autorisés à synchroniser entre les PC de l'entreprise et leurs périphériques mobiles connectés localement (smartphones Windows Mobile®, Palm® et iPhone®, depuis la mise sur le marché de la version 6.4.1). DeviceLock 6.4.1 prend également en charge les périphériques BlackBerry® phase un, avec détection de présence du périphérique, contrôle d'accès et consignation d'évènements. Pour les protocoles Windows ActiveSync®, Windows Mobile Device Center, HotSync® et iTunes®, DeviceLock peut reconnaître et filtrer de nombreux types d'objets de données, permettant ainsi aux administrateurs d'autoriser ou d'interdire de façon sélective la synchronisation des fichiers, des e-mails, des comptes et pièces jointes, des contacts, des tâches, des remarques, des éléments d'agenda, des signets et de différents types de supports. Des stratégies basées sur différents éléments (heure, calendrier), de même que le contrôle directionnel des flux de données, peuvent également être appliqués aux synchronisations locales, afin de permettre des stratégies de sécurisation plus souples, précises et dynamiques.

En protégeant les entreprises contre toute activité d'impression non autorisée à partir des terminaux informatiques, DeviceLock place les impressions locales et de réseau sous le contrôle étroit des responsables de la sécurité. Grâce à l'interception, au filtrage et au suivi des opérations de spouleurs d'impression, DeviceLock permet une définition centralisée et une application locale de privilèges d'accès des utilisateurs sur n'importe quelle imprimante locale, réseau ou virtuelle, quel que soit son mode de connexion (y compris autre qu'USB).

En plus de ses différentes fonctionnalités de contrôle de ports, de périphériques et de données par une sécurité selon le type de données, DeviceLock prend désormais en charge la détection et le filtrage des types de fichiers réels. Cette fonctionnalité intercepte toute opération de lecture/écriture de fichiers système à partir de périphériques, effectue une analyse en temps réel de l'intégralité du contenu binaire des données transmises et applique les règles de sécurité applicables, par type de fichier.

Afin d'assurer une protection optimale des données stockées sur des périphériques mobiles, DeviceLock s'intègre également avec les principales solutions de chiffrement développées par PGP, Lexar, SecurStar et TrueCrypt. En outre, DeviceLock assure un blocage automatique des « espions de clavier » (*keyloggers*) matériels USB et PS/2.

DeviceLock permet également une gestion et une administration à la fois évolutives, centralisées et simples d'emploi, grâce à une extension personnalisée de la console MMC (Microsoft Management Console) qui s'intègre de façon native au Group Policy Object Editor dans Microsoft Active Directory. Les agents DeviceLock peuvent être totalement déployés, gérés et administrés à partir d'un domaine Microsoft Active Directory existant. Un composant distinct, le DLES (DeviceLock Enterprise Server), permet le recueil centralisé et automatique des données d'analyse et de réplication à partir des terminaux d'entreprise. Les configurations hautement granulaires de consignation d'évènements et de réplication de données permettent le suivi et l'analyse des actions des utilisateurs sur les ports et périphériques, des évènements système reliés et des données transmises aux périphériques. De plus, le DLES peut surveiller à distance et en temps réel les ordinateurs dotés de DeviceLock, afin de vérifier en permanence le statut de l'agent et la cohérence des modèles de stratégies adoptés.

DeviceLock 6.4.1 offre en outre une nouveauté : un composant additionnel optionnel (DeviceLock Search Server, ou DLSS), permettant des recherches textuelles complètes dans la base de données centralisée des journaux de réplication et d'évènements. Le DLSS a pour but d'améliorer la précision, la commodité et la rapidité d'exécution des lourds processus d'analyse de la conformité réglementaire, d'analyse des incidents et d'analyse légale.

L'ensemble complet d'options et de paramètres de stratégies configurables proposé par DeviceLock facilite la définition et la mise en œuvre de stratégies de sécurité basées sur des « droits d'accès minimaux ». Grâce à DeviceLock, les responsables de la sécurité sont en mesure de définir le rôle précis de chaque employé, groupe ou département et donc de spécifier pour chacun d'entre eux le socle minimal des opérations requises par leur fonction, afin de n'autoriser que celles-ci sur les périphériques et ports locaux. Cette approche réduit significativement le risque général de fuite de données, et aide les entreprises à mieux se conformer aux normes et réglementations en vigueur.

À propos de DeviceLock, Inc. :

Depuis sa création en 1996 sous le nom de SmartLine, DeviceLock, Inc. fournit des solutions logicielles de contrôle et de protection des informations en entreprises de toutes les tailles et tous les secteurs d'activité. Avec plus de 4 millions d'ordinateurs protégés dans plus de 58 000 organisations de par le monde, DeviceLock compte une vaste clientèle institutionnelle, parmi laquelle des établissements financiers, des organismes publics nationaux et fédéraux, des réseaux militaires classés, des prestataires de soins de santé, des entreprises de télécommunications et des établissements scolaires. DeviceLock, Inc. est une société internationale comptant des agences à San Ramon (Californie, États-Unis), Londres (Royaume-Uni), Ratingen (Allemagne), Moscou (Russie) et Milan (Italie).

Contact presse :

Mediasoft Communications – Carole Scheppler

Carole.scheppler@mediasoft-rp.com - 01 55 34 30 00

# # #