Communiqué de presse

DeviceLock
Proactive Endpoint Security

DEVICELOCK PRÉVIENT LA FUITE DE DONNÉES VIA LES SMARTPHONES IPHONE ET BLACKBERRY

Paris, le 04 novembre 2009 - DeviceLock, Inc., leader mondial pour le contrôle et la protection des informations en entreprises, prévient désormais la fuite de données lors des synchronisations avec les iPhones et les terminaux mobiles BlackBerry. Dans sa dernière version 6.4.1 disponible dès aujourd'hui, le logiciel DeviceLock® offre un contrôle hautement granulaire et indépendant de l'interface sur les synchronisations de données locales effectuées entre des périphériques mobiles de type iPhone® ou iPod® touch et des terminaux informatiques de l'entreprise (ordinateurs de bureau ou portables des employés). DeviceLock 6.4.1 prend également en charge les smartphones BlackBerry® (phase un), avec détection de présence du périphérique, contrôle d'accès et consignation d'évènements. Avec la prise en charge des smartphones iPhone et BlackBerry, DeviceLock garantit un niveau sans précédent de contrôle des synchronisations locales effectuées entre les ordinateurs protégés par DeviceLock et les terminaux mobiles plus répandus sur le marché (Windows Mobile®, Palm®, iPhone, BlackBerry, etc.).

« Les employés d'une entreprise ont de nombreuses raisons parfaitement légitimes pour connecter un smartphone à leur PC de bureau et effectuer une synchronisation locale en vue d'un transfert de données. Cependant, les personnes mal intentionnées savent parfaitement que de tels transferts court-circuitent complètement le réseau de l'entreprise et ne peuvent être contrôlés par une quelconque solution de sécurisation, » explique Ashot Oganesyan, fondateur et Directeur de la Technologie de DeviceLock. *« Une approche de type « tout ou rien » (tous les smartphones sont soit autorisés, soit interdits de synchronisation locale avec un ordinateur donné) s'avère bien trop risquée. Le « tout » pénalise la sécurité, le « rien » la productivité. Ce dont l'entreprise a besoin, c'est d'un moyen de définir et d'appliquer des permissions sur une base plus flexible et granulaire. Nos clients se reposaient déjà sur DeviceLock pour la gestion par permissions des périphériques de stockage amovibles. Il était donc naturel d'étendre cette couverture aux smartphones les plus courants. Grâce à DeviceLock, les responsables de la sécurité informatique peuvent imposer aux périphériques mobiles une stratégie basée sur des « droits d'accès minimaux », qui limite les transferts aux seuls types de smartphones et de données utiles à l'accomplissement des tâches de l'employé ».*

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, iPhone et iPod). En outre, les smartphones de type BlackBerry® sont désormais pris en charge, 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. Pour les périphériques Windows Mobile, les autorisations peuvent également être définies pour une installation et une exécution à distance des applications.

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, des stratégies de sécurisation plus souples, précises et dynamiques. DeviceLock détecte pour rendre présence de n'importe quel périphérique mobile raccordé, quelle que soit l'interface locale via laquelle il est connecté. Les smartphones connectés via une interface USB peuvent être identifiés et qualifiés « de confiance » avec une grande précision pouvant aller jusqu'au périphérique individuel.

Les solutions logicielles DeviceLock protègent de façon proactive les entreprises de toutes tailles et dans tous les secteurs d'activité contre la fuite de données, et contribuent à empêcher l'infiltration de programmes malveillants dans des réseaux d'entreprise, via les ports des PCs locaux. DeviceLock réduit considérablement les risques liés à la négligence, aux erreurs, aux pertes accidentelles ou aux actes malveillants intentionnels d'opérateurs internes. Les logiciels DeviceLock ont été développés pour les systèmes d'exploitation Microsoft Windows et incluent des consoles de gestion centralisée classiques ainsi qu'une console d'administration de conception unique, intégrée en natif aux règles de groupe Microsoft Active Directory®. 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 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.

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

# # #