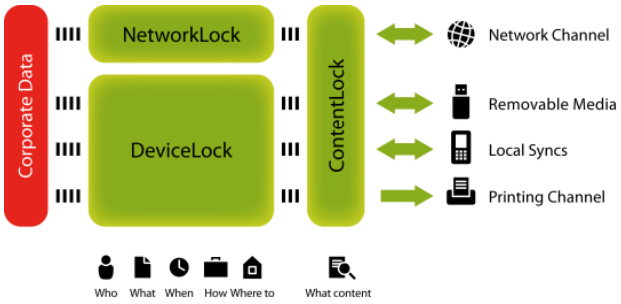
DeviceLock
Proactive Endpoint Security

Communiqué de presse

DEVICELOCK 7.0 : NOUVELLE SOLUTION DLP ASSOCIANT CONTROLE CONTEXTUEL ET FILTRAGE DE CONTENUS

Paris, le 22 février 2011 - DeviceLock, Inc., éditeur de solutions de prévention de fuite de données confidentielles sur les postes de travail, annonce la disponibilité de DeviceLock 7.0 Endpoint DLP Suite. La première version de son produit éponyme étend les contrôles contextuels des communications réseau et applique un filtrage des contenus sur les divers canaux de transmission de données entre les postes de travail de l'entreprise. Cette nouvelle solution complète offre un niveau de performances sans précédent parmi les produits DLP pour postes de travail dans la même gamme de prix.



DeviceLock 7.0 Endpoint DLP Suite répond aux besoins des entreprises en quête d'une solution simple et économique pour prévenir les fuites de données sur leurs postes de travail Microsoft Windows®. Au cœur du produit, DeviceLock 7.0 exerce un **contrôle contextuel sur les canaux locaux de données des ordinateurs protégés,** y compris l'ensemble de leurs ports et périphériques, les smartphones/PDA connectés, ainsi que l'impression de documents en local ou sur le réseau. A partir d'objets de stratégie de groupe (GPO) **Microsoft Windows Active Directory® centralisés et de consoles associées**, les administrateurs peuvent gérer de façon dynamique des agents distribués en appliquant des règles DLP définies au niveau central afin d'autoriser ou d'interdire les flux de données en fonction de l'utilisateur, du type de données, de l'interface, de la direction du flux, de l'état de cryptage, de la date et de l'heure, etc.

Le **composant NetworkLock™,** disponible sous licence séparée, étend le contrôle de protocole contextuel à FTP/S, HTTP/HTTPS, SMTP/S, Telnet, aux messageries instantanées, aux webmails et aux réseaux sociaux tels que Twitter™, Gmail™ et Facebook®.

Un **nouveau module, ContentLock™,** permet de contrôler et de filtrer le contenu textuel des fichiers et objets de données en fonction de règles faisant intervenir le contexte, des expressions rationnelles, des conditions numériques et des opérateurs booléens. Des modèles préconfigurés pour la détection de structures de données courantes, de mots-clés sensibles, de propriétés de documents, de types de fichiers, etc. sont fournis. Ils sont simples à adapter ou dupliquer pour en tirer des règles personnalisées.

« *L'affaire WikiLeaks a démontré de manière éclatante que les menaces de fuites de données sur les postes de travail ne relèvent pas du discours marketing mais constituent une dure réalité. Rares sont encore les entreprises qui ont mis en œuvre une solution, l'étude réalisée en 2010 par Forrester Research estime leur proportion à seulement 15%. L'adoption des technologies DLP a été principalement freinée par leur coût et leur niveau de complexité élevés. Cette nouvelle version de DeviceLock élimine ces freins. Dans le cas des postes de travail, comme l'a montré le scénario WikiLeaks impliquant un CD pirate, il est judicieux de commencer par traiter contextuellement les canaux de fuites évidents que sont les ports, les périphériques et le réseau, puis d'y ajouter le filtrage de contenus pour les flux de données les plus sensibles ou suspects. Grâce à sa structure modulaire et à son programme de licence, DeviceLock offre une solution DLP pratique et économique pour les entreprises quels que soient leur taille et leur budget, y compris les PME* », souligne Ashot Oganesyan, CTO et fondateur de DeviceLock.

Reconnaissant **plus de 80 formats de fichiers**, ContentLock extrait et filtre le contenu des données copiées sur des supports amovibles et des périphériques de stockage Plug & Play ou transmis via d'autres canaux d'E/S sur les postes de travail. Cela inclut les opérations dans le presse-papiers et – lorsque le module est utilisé en combinaison avec NetworkLock – les communications réseau par e-mail et webmail, les réseaux sociaux, les messageries instantanées, les accès Web, les transferts de fichiers et même les sessions Telnet. Une **fonction « Text in Picture » (TIP)** permet de détecter la présence de texte dans des images et une autre, similaire, dans les archives, afin de prévenir les fuites via ces types de fichiers.

NetworkLock y ajoute la détection et le filtrage des protocoles réseau et des applications indépendamment des ports, la reconstitution des messages et des sessions avec extraction des fichiers, données et paramètres, ainsi que la journalisation des événements et le « data shadowing » (réplication des éléments copiés sur un périphérique de stockage).

Avec la même efficacité qu'offrait déjà DeviceLock pour l'intégration avec TrueCrypt™, PGP™ et d'autres logiciels de cryptage des supports amovibles, DeviceLock 7.0 prend en charge la solution native de Windows 7 dans ce domaine, **BitLocker To Go™.** Il est ainsi désormais possible, sans surcoût, d'utiliser la technologie de chiffrement de Microsoft avec DeviceLock sur des postes Windows 7. Dans la mesure où BitLocker To Go et DeviceLock peuvent tous deux bénéficier d'une gestion centralisée via Active Directory, leur association procure toutes les fonctions DLP nécessaires pour les postes de travail, avec cryptage intégré des supports amovibles, ainsi que des avantages fonctionnels et des économies significatives.

Le filtrage de contenu fait franchir à **la fonction de « data shadowing »** de DeviceLock un nouveau palier en termes d'efficacité et d'évolutivité sur tous les canaux de transmission de données des postes de travail : supports amovibles et périphériques de stockage Plug & Play, communications réseau, synchronisation locale avec des smartphones, impression de documents. Dorénavant, les entreprises peuvent filtrer les flux de données enregistrés, et ce jusqu'au niveau des informations significatives pour les audits de sécurité, les enquêtes après incident et les expertises légales, avant leur sauvegarde dans les journaux masqués (« shadow log »). Cela a pour effet de réduire considérablement l'espace de stockage et la bande passante réseau nécessaires à la collecte de ces journaux dans la base de données centrale.

DeviceLock Endpoint DLP est conçu de manière à s'adapter en toute transparence aux installations de toutes tailles et à faciliter le déploiement et la gestion d'une solution DLP. Les entreprises peuvent ainsi renforcer la sécurité des données sur leurs postes de travail avec des outils de contrôle des contenus et des réseaux à travers une interface de gestion éprouvée de type MMC (Microsoft Management Console), déjà bien connue des administrateurs de sécurité Windows.

Quelques jours suffiront à la plupart des nouveaux utilisateurs pour se familiariser avec DeviceLock et configurer l'application. DeviceLock Group Policy Manager, une extension MMC sur mesure pour Windows Group Policy Object Editor, permet le déploiement, l'administration et la maintenance d'agents DeviceLock dans l'ensemble de l'entreprise, depuis un domaine Active Directory existant.

Les composants DeviceLock 7.0 Endpoint DLP Suite sont tarifés sur une base modulaire. DeviceLock 7.0, le composant-phare de contrôle d'accès aux ports et aux périphériques, peut être acquis séparément. Tous les composants étant inclus d'emblée dans chaque installation de la suite, les clients utilisateurs intéressés par les modules additionnels ContentLock et NetworkLock pourront déployer leur solution DLP de manière progressive, en activant simplement de nouvelles fonctionnalités au fur et à mesure de l'évolution de leurs besoins et de leur budget en matière de sécurité.

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 60 000 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 Cousin
Carole.cousin@mediasoft-rp.com - 01 55 34 30 00