

DUSK Suite de DeltaCrypt

Les récentes fuites de données de Wikileaks démontrent une fois de plus qu'à notre époque de blogues et de réseautage social sur l'Internet, de nuage informatique, d'ordinateurs plus minces qu'un magazine, de téléphones intelligents et de dispositifs mobiles USB qui peuvent stocker plus d'information que vous ne pouvez en générer, plus rien ne peut demeurer secret.

Risques de Pertes de Données

Nous aimons les dispositifs mobiles pour leur flexibilité et leur côté pratique, mais cette mobilité représente un défi de taille pour les administrateurs TI chargés de sécuriser les données et les réseaux des sociétés. Voici quelques risques découlant de cette mobilité:

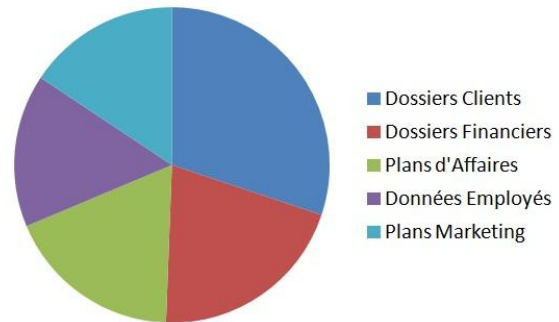
- Source inattendue de fuite de données: coulage interne
- Embarras et dommages financiers causés par les incidents de vols d'identité
- Publicité négative dans les medias
- Divulgateion indésirable auprès des autorités
- Dommage involontaire causé à d'innocentes victimes soit les propriétaires des données
- Non respect des lois et règlements gouvernementaux édictés pour protéger l'information mobile
- Implantation inappropriée de mesures et de politiques de sécurité
- Comportements de travail délinquants



Comment Les Dispositifs Mobiles Augmentent Les Risques De Perte De Données

Les dispositifs mobiles font partie du milieu des affaires aujourd'hui. Téléphones intelligents, ordinateurs portatifs, tablettes PC, clés USB, CD-ROM et DVD, tous vous permettent d'apporter le bureau où vous allez.

- **Données corporatives retrouvées sur les clés USB personnelles.**



- **Mobilité accrue en environnement de travail**

200 millions d'ordinateurs portatifs, 174 millions de téléphones intelligents, 250 millions dispositifs USB ont été vendus en 2009 seulement. Ces nombres augmentent à chaque année. A ce rythme, les dispositifs mobiles sont omniprésents de nos jours.

- **Fréquence des pertes de données (vols ou pertes de dispositifs)**

En 2009 seulement, 498 bris de sécurité ont exposés les dossiers d'environ 16 millions d'américains. Que ces bris soient intentionnels ou non, nous sommes tous à risque.

- **Incidents impliquant des dispositifs mobiles**

Il est démontré que lorsqu'un bris de sécurité implique un dispositif mobile, les dommages sont plus onéreux. Tout simplement dit, la mobilité a un coût.

Problèmes résolus par le DUSK Suite

DeltaCrypt croit qu'en combinant la prévention avec de la protection, le DUSK Suite résout les risques engendrés par la mobilité en milieu corporatif.

DUSK Suite :

- Réduit les vulnérabilités de la mobilité
- Préviend les intrusions illégales
- Accroît les connaissances environnementales
- Préviend les fuites de données et les dommages découlant de bris de sécurité
- Protège la réputation des sociétés
- Rencontre les exigences strictes des marchés

Comment?

Chiffrement Validé FIPS

DeltaCrypt offre de la protection par chiffrement validé FIPS. Le *American Federal Information Processing Standard (FIPS) Publication 140-2, FIPS PUB 140-2*, est un standard du gouvernement américain servant à accréditer les modules cryptographiques.

<u>Clés Symétriques</u> AES-128 bits AES-192 bits AES-256 bits	<u>Intégrité des messages</u> HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512	<u>Hashing</u> SHA-1 SHA-256 SHA-512
<u>Générateur de nombres aléatoires</u> DRBG (FIPS 800-90)	<u>Signature</u> RSA-1024 RSA-2048 RSA-4096	

Sécurité Proactive

DUSK Suite émet des alertes par courriels et dans les registres. Non seulement enregistre-t-il les activités de vos dispositifs et de vos fichiers, il attire l'attention de votre Administrateur réseau sur des activités spécifiques en cours.

Avec des rapports détaillés, de meilleures pratiques peuvent être implantées que ce soit pour gérer vos utilisateurs récalcitrants envers la sécurité ou pour mieux protéger les postes les plus vulnérables contre les fuites de données et les bris de sécurité.

Protection de Fuites de Données

A l'aide du contrôle de fichiers, des messages électroniques sont transmis lorsque certains fichiers quittent vos locaux ou lorsqu'on tente de les copier. Des registres détaillés sur les activités de vos fichiers et de vos dispositifs sont également enregistrés. Des copies fantômes peuvent être également prises de façon transparente lors de la sortie de vos fichiers.

Outil significatif de Réduction de Risque

En renforçant l'utilisation de dispositifs cryptés pour prévenir la vulnérabilité de votre information, le DUSK Suite permet aussi de détecter les intrusions en enregistrant des alertes et en transmettant des avis électroniques lorsque des dispositifs non protégés sont branchés à votre réseau.

Protection des Données Mobiles

La protection versatile du DUSK Suite sécurise les clés USB, les disques durs USB, les Firewire et les cartes de mémoire peu importe le manufacturier et la capacité du dispositif. Cette solution sans pilote, fonctionne parfaitement avec des ordinateurs à privilèges restreints. DUSK Suite offre également de la protection pour disques CD-ROM et DVD.

Accès Sélectif aux Données Mobiles

Les permissions et restrictions de DUSK Suite sont applicables aux individus, à des groupes d'utilisateurs ou d'ordinateurs ou une combinaison des deux, le tout selon votre définition de groupe par Active Directory de Windows.

Retour sur Votre Investissement

Pour un moindre coût que celui d'acquisition d'une clé protégée d'un manufacturier, obtenez de multiples protections et contrôlez vos données mobiles. Soyez assuré que votre investissement rapporte en ne permettant pas de contourner l'utilisation de la protection pour clés USB. De plus, la protection étant indépendante du support matériel, ceci vous permet de bénéficier du meilleur coût pour l'achat de vos dispositifs sans vous préoccuper de la protection à y installer.

Outil de Travail Efficace

Des copies de sauvegarde sont disponibles afin de récupérer les fichiers des clés USB en un temps record. Une clé de recouvrement est incorporée dans la protection si jamais votre société doit avoir accès aux données. Un système de mot de passe temporaire est aussi disponible pour dépanner vos utilisateurs à distance en cas de perte ou d'oubli du mot de passe.

Solutions Taillée Sur Mesure

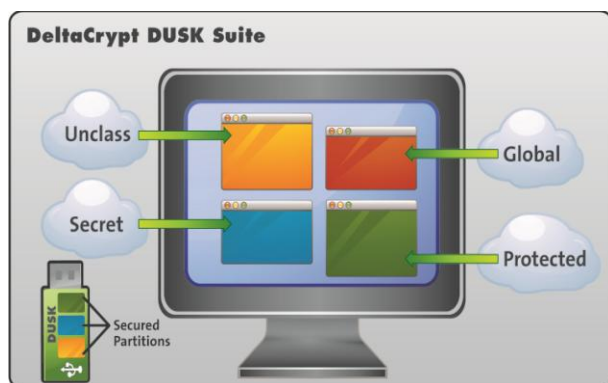
Ne laissez pas vos exigences vous empêcher de protéger et de contrôler vos données corporatives. Le DUSK Suite peut être adapté pour répondre à vos besoins.

Innovation: Multiples Partitions

Si vous devez brancher votre clé USB à plusieurs réseaux qu'ils soient de niveau de sécurité différent ou non, les dispositifs protégés par DUSK-USB peuvent être divisés en plusieurs partitions sécurisées, chacune associée à un réseau spécifique.

Le nombre de réseau accessible par partition est flexible et configurable. Les partitions peuvent être restreintes à des domaines en particulier ou plusieurs partitions peuvent y accéder.

Avec ces partitions sécurisées, tous vos besoins de mobilité sont résolus par un seul dispositif éliminant ainsi le besoin de transporter avec vous plusieurs clés USB.



© 2011. DeltaCrypt Technologies Inc.

La solution DUSK Suite permet aux organisations de bénéficier sécuritairement de la mobilité offerte par la technologie d'aujourd'hui. Son chiffrement validé FIPS assure que votre information demeure protégée qu'elle soit perdue ou volée.

Au Sujet de DeltaCrypt

Les Technologies DeltaCrypt Inc. est une société canadienne se spécialisant dans les solutions de chiffrement.

Depuis 2000, l'équipe de professionnels de DeltaCrypt se concentre sur le développement et l'adaptation de plusieurs produits reliés à la sécurité corporative. Des sociétés prestigieuses provenant des quatre coins du globe comptent parmi la clientèle de DeltaCrypt.

Le DUSK Suite a été commandité à deux reprises par la Défense Nationale Canadienne pour les démonstrations CWID 2009 et 2010. La technologie s'y est vue accorder une mention de technologie «La Plus Performante» par le Canada.

DeltaCrypt agit comme sous-contractant pour General Dynamics Canada dans le cadre d'un projet pour la Défense Nationale Canadienne.

Pour Nous Contacter

Les Technologies DeltaCrypt Inc.

Ann Marie Colizza

1-866-279-7139

annmarie.colizza@deltacrypt.com

www.deltacrypt.com