

DUSK et DUSKWatch pour protéger et contrôler les dispositifs USB

Le nombre de télétravailleurs fera un bond à plus de 850 millions dans le monde en 2009. Les possibilités pour les gens de travailler à partir de n'importe où est dû en partie à la disponibilité croissante des ordinateurs portatifs, des dispositifs mobiles et de la technologie des communications à haute vitesse. Les données sensibles sont par conséquent toutes aussi mobiles et le risque de leur perte ou leur vol s'accroît exponentiellement.

Conformité et législations

Les dépenses en sécurité de l'information sont justifiées par de nombreuses préoccupations – conformité réglementaire, vol d'identité et gestion d'identité étant les trois premiers. La législation suivante requière du cryptage pour les informations stockées:



- HIPAA (États-Unis – Le "Health Insurance Portability and Accountability Act")
- SOX (États-Unis – la loi "Sarbanes Oxley")
- GLBA (États-Unis – la loi "Gramm-Leach-Bliley")
- Californie SB 1386 (États-Unis)
- PIPEDA (Canada – Le "Personal Information Protection and Electronic Documents Act")
- DPA (UK- "Data Protection Act")

La Protection DUSK pour dispositifs USB

La protection DUSK de DeltaCrypt permet de sécuriser les informations mobiles sur disques à l'aide d'un cryptage glisser-déposer ("drag'n drop"). Son caractère unique réside dans ses fonctions faciles d'utilisation combinées au cryptage à clé publique pour la protection de vos dispositifs mobiles USB. La technologie DUSK fait l'objet d'une application de brevet déposée.

Comment DUSK fonctionne

- A l'installation, DUSK remplit toute le disque USB de sa protection forçant ainsi les Utilisateurs à protéger tous les fichiers qu'ils sauvegardent sur leur dispositif USB.
- L'Utilisateur est ensuite guidé à configurer un mot de passe pour ouvrir l'application. Une fois ouverte, pour crypter des fichiers, l'Utilisateur n'a qu'à glisser-déposer sa sélection du panneau gauche de DUSK représentant son ordinateur vers le panneau de droite représentant le disque sécurisé. L'inverse est également vrai pour décrypter des fichiers sur le disque USB protégé.
- Une Clé Maître de l'Administrateur TI est intégrée à l'application DUSK pour ainsi permettre la récupération des fichiers advenant que l'Utilisateur oublie son mot de passe. Le mot de passe de l'Administrateur servira à ouvrir l'application pour accéder aux fichiers s'y trouvant en cas de besoin



Bénéfices Du DUSK

- S'installe sur plusieurs type de dispositifs de stockage de masse USB peu importe leur marque ou leur taille
- Ecrit, lit et crypte à l'extérieur du réseau sans restriction
- Aucune possibilité de placer des fichiers dans une partition non protégée sur le disque USB
- Clé de récupération de l'Administrateur en cas de mot de passe oublié ou perdu par l'Utilisateur
- Consolide les investissements antérieurs dans l'acquisition de dispositifs mobiles USB
- Enregistre les détails de fichiers copiés sur des dispositifs protégés et autorisés pour mieux évaluer leur contenu si perdus ou volés
- Fonctionne de pair avec DUSKWatch pour contrôler les dispositifs USB

FONCTIONNALITÉS DE DUSK EDITION CORPORATIVE	
Ecrit, lit, crypte/décrypte (« drag'n drop ») à l'extérieur du réseau sans restriction	Configuration par Active Directory Nouveau
Protège des clés USB, des disques durs USB, des cartes mémoires et des Firewires.	Fonctionne avec des privilèges limités (Utilisateur) et illimités (Administrateur)
Clé Maître de récupération	Windows 2000, XP, et Vista Nouveau
Pas besoin d'installer d'application (ou de pilote) sur les ordinateurs pour décrypter	Unique: Se combine au DUSKWatch pour contrôler les dispositifs mobiles USB
Aucune partition non protégée sur le disque USB	Mise à jour transparente lorsqu'utilisé avec DUSKWatch Nouveau
Journal des logs des fichiers copiés sur les disques USB Nouveau	Options d'installation (Administrateur / Utilisateur)

DUSKWatch pour contrôler vos dispositifs mobiles USB

Aucune organisation ne peut totalement se fier sur la bonne volonté de ses Utilisateurs pour appliquer des politiques de sécurité. Qu'arrive-t-il si un Utilisateur juge qu'une information mobile n'est pas assez importante pour la protéger alors que la direction le voit autrement? Et si un Utilisateur voulait court-circuiter la protection qui lui est offerte? Qui en sera responsable en cas de fuite?

L'implantation technologique et de protection pour parer aux fuites importantes d'informations permet aux sociétés de faire en sorte que la mobilité de ses informations ne représente plus une menace.

Paix d'esprit avec DUSKWatch

Si les politiques de votre organisation sont à l'effet de protéger obligatoirement vos informations mobiles, DUSKWatch procurera la paix d'esprit recherchée en vous assurant que seulement que des dispositifs mobiles protégés par DUSK seront utilisés pour sortir vos fichiers corporatifs.

Utilisé seul, DUSKWatch permet aux Administrateurs de décider quel périphérique sont contrôlés et pour qui. Grâce à la configuration par Active Directory, une sélection de dispositifs peuvent être désactivés ou non, pour un groupe d'Utilisateurs ou de postes de travail. Contrôler l'information mobile devient une tâche facile. La technologie de DUSKWatch fait l'objet d'une application de brevet déposée.



Comment DUSKWatch contrôle les périphériques

- En utilisant le fichier .ADM fourni pour fins de configuration par Active Directory, un Administrateur peut implanter des politiques en sélectionnant les périphériques utilisés ou bloqués dans l'organisation
- L'Administrateur sélectionne ensuite le groupe d'Utilisateurs ou de postes de travail auquel la politique s'applique
- L'installateur .msi installe le DUSKWatch à distance avec GPO ou SMS

Comment DUSKWatch fonctionne avec la protection DUSK pour les dispositifs USB

- L'Administrateur configure le DUSKWatch pour n'autoriser que des dispositifs USB protégés par DUSK et détermine le groupe auquel cette politique s'applique
- L'installateur .msi installe le DUSKWatch à distance avec GPO ou SMS
- Une fois installé, si un Utilisateur branche un dispositif USB protégé et autorisé, DUSKWatch en permettra l'usage de façon transparente. Cependant, lorsqu'un Utilisateur branchera un dispositif non protégé ou non autorisé, DUSKWatch empêchera tout simplement l'utilisation de ce dispositif

Bénéfices Du DUSKWatch

- Peut assurer que les dispositifs mobiles sont protégés en tout temps
- Peut bloquer des dispositifs de masse USB tels que clés USB, disques durs USB, iPods, caméras, cartes de mémoire, CD-ROM, DVD et disquettes
- Informe sur le branchement de dispositifs autorisés et non autorisés afin d'identifier les postes les plus vulnérables
- Travaille de pair avec la protection DUSK pour les dispositifs mobiles USB

CONFIGURATION PAR ACTIVE DIRECTORY	FONCTIONNALITÉS DU DUSKWATCH
<ul style="list-style-type: none"> • CD-ROM et DVD • Dispositifs USB protégés par DUSK • Dispositifs de stockage de masse USB tels que iPods, MP3, cartes mémoire, disques durs USB, caméras • Dispositifs Bluetooth, WiFi, Infrarouge A venir • Liste de dispositifs mobiles bloqués • Lecteurs de disquettes • Mode de lecture seule de dispositifs de stockage de masse non protégés • Politiques applicables à: <ul style="list-style-type: none"> ○ un Utilisateur ou un groupe d'Utilisateurs ○ un poste de travail ou un groupe de postes 	<ul style="list-style-type: none"> • Peut forcer l'utilisateur de dispositifs de stockage de masse USB protégés par la protection DUSK et autorisés dans votre organisation. Unique • Permet de retirer le privilège d'utiliser un dispositif USB autorisés Unique • Installation à distance et transparente aux Utilisateurs (Administrateur) • Fonctionne avec des privilèges limités (Utilisateur) et illimités (Administrateur) • Configuration par Active Directory Nouveau • Compatible avec Windows 2000, Serveur 2003, XP et Vista Nouveau • S'utilise également comme utilitaire de la protection DUSK (installation/mises à jour) Nouveau

Pourquoi DeltaCrypt?

DeltaCrypt procure aux dirigeants d'organisations une quiétude dans la gestion d'informations corporatives de plus en plus valorisées. Des données sur leurs clients, aux échanges et communications entre partenaires, DeltaCrypt offre de la protection cryptographique de haut niveau contre les intrusions externes et les indiscretions internes.

Gamme complète de produits de cryptage

DeltaCrypt offre une gamme complète de protection cryptographique à clé publique. Que ce soit pour protéger votre ordinateur, vos échanges de fichiers, vos courriels, vos clés USB ainsi que vos copies de sauvegarde, DeltaCrypt a la solution pour vous.

Solution sur mesure

Ne laissez pas vos exigences particulières vous empêcher de protéger vos renseignements corporatifs sensibles. DeltaCrypt peut adapter ses protections spécifiquement à vos besoins. Offrez à vos utilisateurs des outils de sécurité spécialement adaptés à leur environnement de travail.

Technologie brevetée

La protection DUSK et l'application DUSKWatch font l'objet de demandes de brevet.



Certification FIPS 140-2

La technologie de cryptage de DeltaCrypt est présentement en cours de certification FIPS 140-2 Certification (Federal Information Processing Standard--FIPS-- Publication 140-2 est un standard de sécurité informatique du gouvernement américain pour les modules cryptographiques).

Présence importante dans les organisations et industries soucieuses de maintenir un niveau de sécurité élevé

Gouvernements, R&D, hautes technologies, institutions financières, loteries, industrie pétrolière, etc.

Produits québécois

Les Technologies DeltaCrypt est une entreprise québécoise. En achetant les protections de cryptage de DeltaCrypt vous encouragez l'ingéniosité et la créativité technologique du Québec.

Solutions et service bilingues

Les applications de cryptage de DeltaCrypt s'utilisent en français ou en anglais à la discrétion de l'utilisateur. Le support et le service à la clientèle sont également disponibles en français et en anglais.



Contactez-nous

Les Technologies DeltaCrypt Inc. www.deltacrypt.com

Par téléphone au 1-888-500-3563

Par courriel au dtiinfo@deltacrypt.com