SafeBoot Content Encryption

Protégez les données confidentielles contenu dans les répertoires et fichiers.

Vous pouvez désormais préserver la confidentialité de vos données indépendamment de l'endroit où celles-ci sont stockées. Entièrement intégré à Windows, SafeBoot Content Encryption n'exige aucune action de la part de l'utilisateur, la solution est complètement transparente. SafeBoot Content Encryption vous protège y compris de vos équipes techniques internes.

Les administrateurs peuvent spécifier le cryptage de tous les fichiers ou d'un seul. Par exemple un fichier Excel est chiffré ou la totalité des données d'un répertoire telles que Mes Documents. Un groupe d'utilisateurs a la possibilité de partager des droits d'accès aux mêmes répertoires.

Chiffrement transparent des fichiers & répertoires

Une fois qu'un administrateur a indiqué les fichiers et répertoires à chiffrer, tout se fait d'une manière transparente. Les utilisateurs ne notent pas même la phase de chiffrement et déchiffrement car il n'y a aucune perte de performance, aucune action n´est requise de la part de l'utilisateur SafeBoot Content Encryption est totalement intégrée a Windows l'utilisation est rendu simple pour les utilisateurs. Si un utilisateur veut chiffrer un fichiers particulier, il doit simplement clicker droit sur le fichiers et l'option chiffrement apparaît.

Partager et déplacer les fichiers sans limitations

Les groupes d'utilisateurs avec les mêmes droits d'accès peuvent partager des fichiers à travers le réseau. Grâce au logiciel SafeBoot Content Encryption les informations confidentielles stockées sur le réseau reste cryptées même pour l'administrateur. Des fichiers confidentiels, tels que les rapports d'un conseil d'administration, peuvent être vus seulement par un groupe avec la clef de chiffrement correspondant au fichier. Les utilisateurs ayant droit d'accès aux répertoires peuvent les visualiser immédiatement exactement comme s'ils consultaient des documents non cryptés.

Les répertoires restent cryptés avec la technologie

Une fois la mise en place de la solution, Safeboot Content Encryption est facilement administrable via le GUI de la console d'administration ou une interface web.

Renforcement de la sécurité via des politiques exécutoires

Avec SafeBoot Content Encryption, les politiques de sécurité sont obligatoires et imposées et l'utilisateur ne peut que s'y conformer. Les administrateurs installent SafeBoot Content Encryption de sorte que des types ou les répertoires spécifiques de fichiers soient chiffrés sans qu'aucune action soit requise de la part de l'utilisateur. Persistent Encryptions Technology (PET), et ceci independamment de l'endroit où ils sont sauvegardés. Même si un fichier est ouvert et visible sur un ordinateur, un utilisateur qui essaye de le sauvegarder sur un media de stockage, celui ci, lors de la lecture ne verra qu'un fichier chiffré et illisible Seul un utilisateur autorisé pourra lire et voir ce dossier.

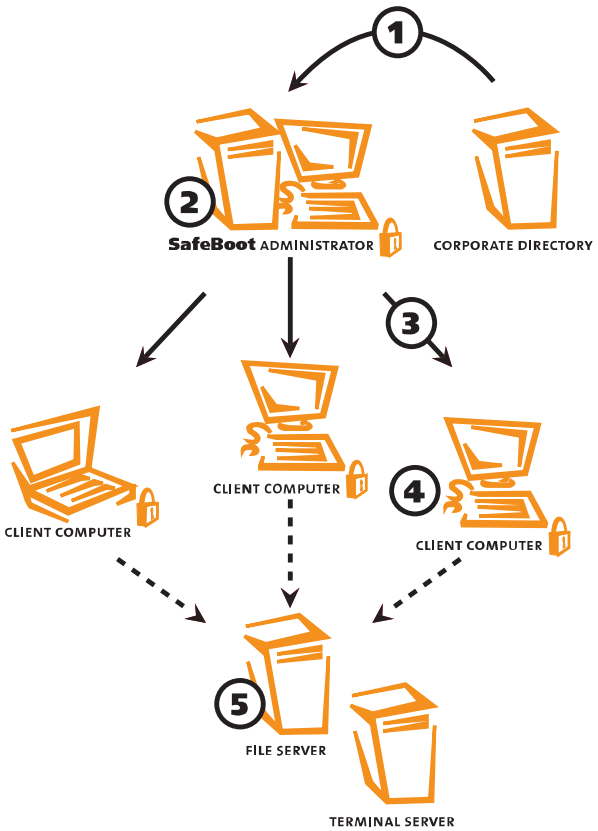
SafeBoot Content Encryption

Déploiement et administration centralisée

SafeBoot est la seule solution de sécurité sur le marché qui offre une administration centralisée des utilisateurs. Un déploiement du logiciel sur 1.000 utilisateurs peut être accompli en juste un jour à partir d'un seul point. De plus le nombre d'utilisateurs contrôlés depuis la console d'administration est pratiquement illimité. Le processus de déploiement est d'autant plus aisé que la solution s'intègre parfaitement aux architectures informatiques quelque soient leur taille ou complexité. L'administrateur peut indiquer des droits d'accès pour des groupes d'utilisateurs ou d'individus selon les politiques de sécurité mise en place par votre entreprise.

Principales fonctionnalités

- Support des principales clefs Usb et carte à puce du marché pour un niveau de sécurité élevé
- Un système de partage de clés uniques qui permet à des utilisateurs de partager l'accès a des répertoires en toute sécurité.
- Intégration avec Active Directory, Novell NDS et PKI …
- Services de recouvrement et support international
- Administration a partir d'un point Unique
- Plusieurs Algorithmes supportés dont AES-256



Fonctionnement de Safeboot Content encryption

1. L'administrateur de SafeBoot crée des groupes d'utilisateurs ou les importe à partir des annuaires d'entreprise tels que Active Directory, LDAP, Novell NDS ou un environnement de type PKI.

2. Les clés de chiffrement, les droits et les politiques de sécurité sont créés via la console d'administration centralisée SafeBoot et assignés aux utilisateurs et aux groupes. Les utilisateurs de clef USB ou carte à puce peuvent également être déclares via cette même console.

3. Les clés de chiffrement sont distribuées aux machines reliées au réseau. Des clés et les politiques de chiffrement sont cachés localement pour permettre le travail off line avec des données chiffrées.

4. Fichiers et répertoires sont chiffrés automatiquement sur la machine locale et sur les supports amovibles tels que les clés de stockage USB. Le chiffrement est totalement transparent pour l'utilisateur.

5. Les répertoires et les fichiers stockés sur le réseau sont chiffrés automatiquement selon les politiques de chiffrement en vigueur au sein de l'entreprise. Des répertoires et des fichiers peuvent également être chiffrés dans des environnements de type terminal Server

SafeBoot
MOBILE DATA SECURITY

Plus d'informations sur les spécifications et les revendeurs SafeBoot:
► E. info-fr@safeboot.com ► I. www.safeboot.com

SafeBoot is developed by Control Break International