SafeBoot® Device Encryption™

Solutions de sécurité pour PC, Portables et Tablettes PC

La protection des données sensibles devient aujourd'hui une préoccupation majeure dans les entreprises. La solution de chiffrement SafeBoot® Device Encryption™ est une solution évolutive à léchelle de l'entreprise.Elle propose un contrôle d accès fort et un cryptage puissant pour empêcher l'accès non autorisé ou l'utilisation des PCS, des portables, et des Tablettes PCS mais aussi protèges les données sur les supports amovibles externes

Dans les organisations modernes, des données critiques pour l'entreprise se déplacent librement sur les réseaux et l'internet. Elles sont stockées sur des PC, des portables, des Tablettes PC, et divers appareils mobiles tels que des disques de stockage amovibles. SafeBoot Device Encryption pour PC, Portables et Tablettes PC fait appel à un contrôle d'accès renforcé et à un système de protection préalable au démarrage, afin d'authentifier les utilisateurs. Il supporte le principe Single Sign-On (SSO) et utilise des algorithmes comme RC5-1024 et AES-256 pour crypter des données sur tous les supports de stockage. Les opérations de cryptage et décryptage sont transparentes pour l'utilisateur et exécutées à la volée, sans dégradation de la performance.

Outre des technologies d'authentification et de cryptage primées devenues de véritables références dans l'industrie, SafeBoot Device Encryption pour PC, Portables et Tablettes PC offre des fonctions de gestion centralisée, des règles de sécurité extensives et obligatoires, ainsi qu'une possibilité de recouvrement sécurisée.

Contrôle d'accès renforcé, protection préalable au démarrage et intégration des certificats

SafeBoot Device Encryption offre une fonction d'hibernation sécurisée et authentifie à la fois les utilisateurs et les équipements avant de démarrer le système (il propose aussi une fonction de consignation des événements préalables au démarrage). Outre l'authentification par mot de passe, SafeBoot Device Encryption supporte l'authentification bi factorielle avant le démarrage (F2-PBA), ce qui oblige les utilisateurs à «connaître quelque chose» et à «posséder quelque chose» avant de pouvoir démarrer leur PC, leur portable ou leur Tablette PC. SafeBoot Device Encryption propose également diverses options supportant la sécurité bi factorielle, telles que des cartes à puce (smart cards) et la technologie à token USB. Il supporte l'authentification via des certificats PKI et offre un accès à des infrastructures PKI du marché.

Fonctions de gestion centralisée et diminution du TCO

Via SafeBoot Management Center, SafeBoot Device Encryption met à la disposition des administrateurs une méthode unique, performante et économique pour préserver la sécurité de l'entreprise. Parmi les fonctions de gestion centralisée, citons le déploiement central, les mises à niveau à distance, la gestion des politiques et règles, un outil de scripting, la révocation à chaud, des fonctions d'audit, le recouvrement centralisé sécurisé et la synchronisation des politiques avec l'Active Directory®, Novell NDS®, Public Key Infrastructure (PKI), etc. Ces fonctionnalités permettent aux entreprises d'aujourd'hui d'augmenter leur retour sur investissement et d'abaisser le coût total d'acquisition (TCO).

Sécurité obligatoire extensive

Grâce au système de gestion centralisée de SafeBoot Device Encryption, les administrateurs disposent des outils nécessaires pour établir et appliquer aisément des politiques de sécurité extensives obligatoires. Les utilisateurs n'ont aucune influence sur les politiques de sécurité SafeBoot, car celles-ci sont appliquées de manière transparente. Les administrateurs apprécieront aussi la facilité avec laquelle ils peuvent définir des politiques de sécurité obligatoires pour les utilisateurs.

Restauration sécurisée

Si un utilisateur a oublié son mot de passe, perdu son token ou quitté l'entreprise, des outils intégrés dans SafeBoot Device Encryption permettent de restaurer en toute sécurité les systèmes protéger sans devoir faire appel à un mot de passe de référence en guise de 'porte dérobée'. Le recouvrement des mots de passe et des tokens est très simple: un coup de téléphone ou la consultation d'une page Web suffit. L'outil Web de recouvrement SafeBoot® WebHelpdesk permet au service d'assistance de rétablir à distance le mot de passe d'un utilisateur après que celui-ci ait réussi un test verbal de questions & réponses ainsi que la procédure d'authentification auprès du service d'assistance de l'administrateur. Cet échange d'informations s'effectue par téléphone.

SafeBoot® Device Encryption™

Avantages de SafeBoot Device Encryption

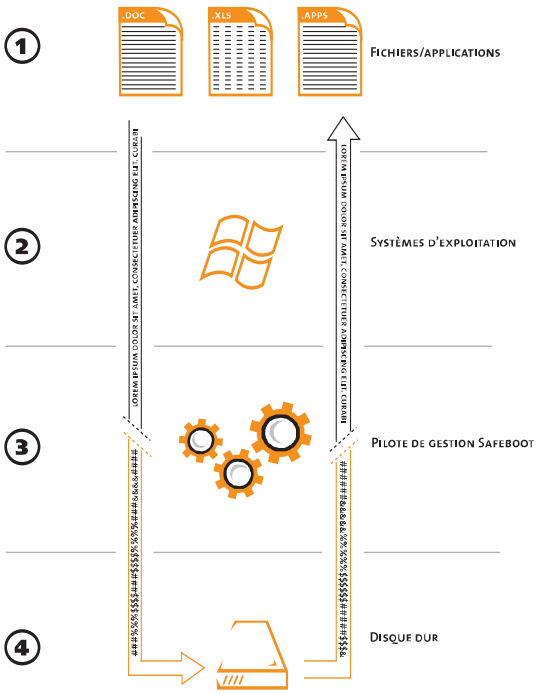
SafeBoot Device Encryption pour PC, Portables et Tablettes PC offre les fonctions et avantages suivants aux utilisateurs et aux entreprises:

- Protège les PC, Portables et Tablettes PC contre des tentatives d'intrusion
- Cryptage intégral des données sur disque dur
- Elimine la nécessité de 'broyer' les disques durs
- Facilite la mise en conformité par rapport aux réglementations en vigueur (notamment Sarbanes-Oxley, HIPAA, etc.)
- Contribue à l'application des politiques de sécurité obligatoires, à l'échelle de toute l'entreprise
- Protection lors du démarrage, authentification préalable au démarrage, consignation des événements avant le démarrage, protection contre les virus affectant la procédure de démarrage
- Cryptage transparent des données à la volée; aucune formation de l'utilisateur n'est requise
- Supporte la procédure Single Sign-On (SSO) et toutes les cartes à puce ainsi que les tokens les plus répandus
- Supporte toutes les langues courantes, tous les claviers et systèmes d'exploitation Windows® les plus populaires
- Utilise de nombreux algorithmes standardisés tels que RC5-1024 et AES-256
- Gestion centralisée et pratique pour les opérations d'administration, déploiement, mise à jour, audit, révocation à chaud, restauration, synchronisation, etc.
- Réseau de support international 24h/24h et 7j/7j.

En plus des fonctions intégrées SafeBoot Device Encryption pour les PC, les utilisateurs de Tablettes PC peuvent s'authentifier à l'aide d'un stylet avant le démarrage.

Une technologie certifiée et primée

Avec plus de 2 millions d'utilisateurs, SafeBoot possède la plus vaste base installée en tant que solution de sécurisation des données et des appareils. SafeBoot a obtenu plusieurs fois d'affilée une cote de 4 à 5 étoiles dans SC Magazine, et remporté le Prix du Meilleur Produit de Cryptage décerné par SC Magazine 2004 Reader Trust. SafeBoot fait également l'objet de plusieurs certifications, y compris le certificat FIPS 140-2 qui garantit que les solutions SafeBoot font appel à de puissantes technologies de cryptage et de gestion sécurisée des clés. Partout dans le monde, la solution est largement utilisée par des banques, des compagnies d'assurances, des cabinets de consulting, des organismes gouvernementaux, laboratoires, hôpitaux.



Principe de fonctionnement de SafeBoot

① Les fichiers sont en mode texte normal et peuvent être intégralement visualisés par les utilisateurs et les applications autorisés.

② Les fichiers sont convertis en secteurs

Les secteurs sont assemblés en fichiers

③ Les secteurs sont cryptés en mémoire

Les secteurs cryptés sont décryptés en mémoire

④ Les secteurs sont stockés sur disque dur

Les secteurs sont lus depuis le disque dur

SafeBoot
MOBILE DATA SECURITY

POUR EN SAVOIR PLUS SUR LES SPÉCIFICATIONS ET REVENDEURS DE PRODUITS SAFEBOOT:
► INFO@SAFEBOOT.COM ► WWW.SAFEBOOT.COM

SAFEBOOT A ÉTÉ DÉVELOPPÉ PAR CONTROL BREAK INTERNATIONAL