Protégez vos biens les plus précieux.

McAfee Endpoint Encryption

(Anciennement SafeBoot® Encryption)

Sécurisation des données sur les postes de travail, les ordinateurs portables, les PC tablettes et les PDA

La protection des données est devenue la priorité absolue des responsables de la sécurité informatique[1]. McAfee® Endpoint Encryption est une solution de sécurité d'entreprise évolutive qui met en œuvre un chiffrement puissant et un contrôle d'accès robuste pour bloquer l'accès non autorisé aux données enregistrées sur les postes de travail, les ordinateurs portables, les PC tablettes, les téléphones intelligents (Smartphones) et les assistants numériques personnels (PDA).

PRINCIPAUX AVANTAGES

Chiffrement puissant et contrôle d'accès

- **Protection contre l'accès non autorisé et la divulgation des données grâce à un chiffrement puissant des périphériques et une authentification pré-amorçage robuste**
- **Chiffrement des données transparent et « à la volée », sans interaction ni formation requise de l'utilisateur final**
- **Garantie du chiffrement permanent des fichiers et dossiers, quelle que soit la destination de leur enregistrement ou de leur transfert**

Conformité aux impératifs de sécurité internes et externes

- **Mise en œuvre de stratégies de sécurité obligatoires à l'échelle de l'entreprise**
- **Démonstration du respect par l'entreprise de la législation sur la confidentialité des données**
- **Contrôle des applications auxquelles les utilisateurs sont autorisés à accéder**

Gestion centralisée simplifiée et coût de possession réduit

- **Large éventail de fonctionnalités de gestion centralisée**
- **Synchronisation et intégration de la solution avec Active Directory, Novell, LDAP et la technologie PKI**
- **Identification unique et prise en charge des mécanismes d'authentification forte les plus répandus**
- **Prise en charge complète des langues, claviers et systèmes d'exploitation Windows les plus courants**

Protection des ressources et de la marque

Les fuites de données confidentielles — fiches clients, dossiers du personnel, éléments de propriété intellectuelle, documents commerciaux, etc. — sont devenues un véritable fléau pour les entreprises du monde entier. Une étude réalisée en 2007 par le Ponemon Institute a révélé que 85 % des répondants ont reconnu que leur société avait connu un incident lié à une divulgation de données[2]. Selon ce même bureau d'études, le coût moyen d'une divulgation de données s'élève à 6,3 millions de dollars[3].

Optimisation de la sécurité des données grâce au chiffrement complet des disques

Pour les entreprises d'aujourd'hui, la protection des données constitue un enjeu majeur. La solution McAfee Endpoint Encryption répond à vos besoins en la matière. Elle met en œuvre un contrôle de l'accès robuste par une authentification pré-boot et des algorithmes certifiés par le gouvernement américain pour chiffrer les données sur les postes clients, qu'il s'agisse de postes de travail, d'ordinateurs portables, de tablettes, de téléphones intelligents ou encore de PDA. Le chiffrement et le déchiffrement sont effectués de façon transparente pour l'utilisateur et « à la volée », sans pratiquement aucune baisse de performances. McAfee Endpoint Encryption s'intègre parfaitement avec les systèmes d'entreprise existants et son efficacité garantit un coût total de possession peu élevé.

Protection des fichiers et des dossiers, à tout emplacement et toute destination

Déterminez avec précision les fichiers ou dossiers à chiffrer. McAfee Endpoint Encryption permet aux administrateurs d'exercer un contrôle très fin sur les ressources concernées par le chiffrement : contenu de certains dossiers, fichiers créés par des applications particulières, fichiers d'un certain type... Des groupes d'utilisateurs se voient accorder des droits d'accès à des dossiers et fichiers spécifiques, et peuvent partager des fichiers sur le réseau en toute sécurité.

Quelle que soit la destination de l'enregistrement ou du transfert des fichiers, les données restent chiffrées grâce à la technologie Persistent Encryption Technology™. Si un utilisateur non autorisé tente d'enregistrer un fichier consultable au départ d'un ordinateur portable de la société, vers un périphérique de stockage non approuvé, il se retrouve avec un fichier chiffré et illisible.

Respect des impératifs de conformité et coût de possession réduit

Prévenez les fuites de données, quelle que soit leur destination, et respectez les impératifs de conformité réglementaires grâce à une gamme complète de solutions de sécurisation et de chiffrement, toutes gérées à partir d'une seule et même console centrale. McAfee Endpoint Encryption propose de multiples fonctionnalités de gestion centralisée : administration, déploiement, mises à niveau à distance, gestion des stratégies de sécurité obligatoires, outil de création de scripts, révocation à chaud, récupération, synchronisation et bien d'autres encore. Des fonctions d'audit complètes permettent de démontrer que le périphérique était chiffré au moment du vol ou de la perte, apportant ainsi la preuve de sa conformité. Les stratégies de sécurité obligatoires peuvent être mises en œuvre en toute transparence par les administrateurs. McAfee Endpoint Encryption prend également en charge l'identification unique et la récupération hors ligne sécurisée des informations utilisateur.

[1] Enquête menée par Merrill Lynch en 2007 auprès de responsables de la sécurité informatique en entreprise
[2] Ponemon Institute : « The Business Impact of Data Breach », 2007 (Etude sur l'impact des divulgations de données sur les entreprises)
[3] Ponemon Institute : Etude annuelle 2007 « Cost of a Data Breach » (Coût des divulgations de données)

CONFIGURATION SYSTÈME REQUISE

Postes de travail, ordinateurs portables et tablettes

Systèmes d'exploitation

- Microsoft Windows Vista (versions 32 et 64 bits)
- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows Server 2003

Configuration matérielle requise

- Processeur : compatible Pentium
- Mémoire RAM : 128 Mo au minimum
- Espace disque : 5–35 Mo disponibles, selon l'emplacement et le nombre de périphériques
- Connexion réseau : TCP/IP pour l'accès distant

Postes clients mobiles

Systèmes d'exploitation

- Microsoft Windows Mobile 6.0 pour Smartphone
- Microsoft Windows Mobile 6.0 pour PDA
- Microsoft Windows Mobile 5.0 pour Smartphone
- Microsoft Windows Mobile 5.0 pour Pocket PC

Configuration matérielle requise

- Processeur : 195 MHz au minimum
- Mémoire RAM : 64 Mo au minimum
- Connexion réseau : TCP/IP pour l'administration à distance et Activesync 4.5 ou version ultérieure pour l'installation et les mises à jour de stratégies par câble

Gestion centralisée

Systèmes d'exploitation

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

Configuration matérielle requise

- Mémoire RAM : 128 Mo, 512 Mo recommandés
- Espace disque : 200 Mo
- Processeur : compatible Pentium

Chiffrement puissant et contrôle d'accès

Prévenez l'accès ou l'utilisation non autorisés des postes de travail, ordinateurs portables, tablettes, téléphones intelligents et PDA et protégez les données hébergées sur leurs disques durs grâce au chiffrement complet des disques.

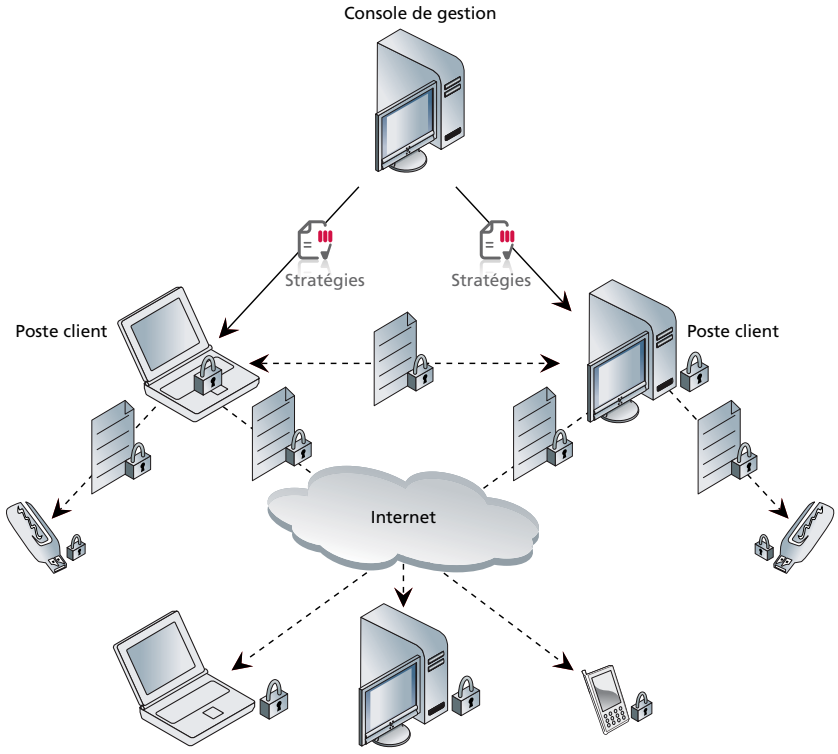
- Authentifiez l'utilisateur et l'ordinateur avant le démarrage de la machine grâce à une authentification pré-amorçage à deux niveaux, en plus de l'authentification par mot de passe.
- Bénéficiez d'une protection inégalée grâce à une technologie de chiffrement de pointe primée, basée sur des algorithmes tels que AES-256 et RC5-1024.
- Chiffrez les périphériques de façon transparente sans incidence sur les opérations journalières et sans formation requise de la part des utilisateurs finaux.
- Assurez-vous que les fichiers et les dossiers restent chiffrés, où qu'ils se trouvent, grâce à la technologie Persistent Encryption Technology.

Respect des impératifs de sécurité internes et externes

- Une piste d'audit complète apporte la preuve de votre conformité aux principes de la Sphère de sécurité[4]. Ainsi, la perte d'un portable ou d'un périphérique USB ne constitue en rien une faille dans le système de sécurité et n'exige pas de déclaration à ce sujet.
- Définissez et appliquez des stratégies de sécurité obligatoires complètes.
- Déterminez par vous-même les fichiers ou dossiers spécifiques à chiffrer sans aucune intervention de l'utilisateur final.
- Profitez des certifications pour la norme FIPS 140-2 et l'évaluation Common Criteria (CC EAL4).

Gestion centralisée simplifiée et coût de possession réduit

- Evitez les fuites de données de toute nature grâce à une gamme complète de solutions de sécurisation et de chiffrement, toutes gérées à partir d'une seule et même console centrale.
- Démontrez votre conformité à la législation sur la confidentialité des données, protégez vos actifs et votre marque, assurez la fidélisation de la clientèle et bénéficiez d'un avantage concurrentiel.
- Déployez et gérez les stratégies en toute simplicité dans l'ensemble de l'entreprise, économisant ainsi du temps et de l'argent.
- Récupérez les mots de passe et les mécanismes d'authentification forte à distance et en toute sécurité. Le mot de passe d'un utilisateur peut être réinitialisé après une étape de vérification et de demande d'authentification/réponse verbale, ce qui fait un gagner un temps précieux au centre d'assistance.



Chiffrement des données, quelle que soit leur destination

McAfee Endpoint Encryption

Pour plus d'informations sur la protection des données, consultez notre site à l'adresse *www.mcafee.com/data_protection*.

[4] L'accord Sphère de Sécurité (Safe Harbor) précise les règles minimales en termes de protection des données personnelles. Les entreprises s'y conformant auront le droit de transférer et d'utiliser les données concernant les internautes européens.

McAfee, Inc., Tour Franklin, La Défense 8, 92042 Paris La Défense Cedex, France, +33 1 47 62 56 00 (standard), www.mcafee.com/fr

1-dp-ee-001-0108