



McAfee Complete Data Protection

Une solution complète de chiffrement des terminaux

Principales fonctionnalités

- Drive Encryption
- File and Removable Media Protection
- Management of Native Encryption
- McAfee ePO Deep Command

Principaux avantages

- Prévenez les fuites de données perpétrées par des logiciels malveillants (malware) sophistiqués qui détournent les informations personnelles et sensibles.
- Sécurisez les données où qu'elles soient stockées : sur les postes de travail, les ordinateurs portables, les tablettes ou dans le cloud.
- Gérez le chiffrement natif proposé par Apple FileVault et Microsoft BitLocker sur les terminaux directement à partir de McAfee ePO.
- Communiquez avec les terminaux et prenez-en le contrôle au niveau matériel, même si ceux-ci sont chiffrés, hors tension ou hors service. Mettez un terme aux interventions physiques sur les postes de travail et aux appels interminables au centre d'assistance à la suite d'incidents de sécurité, d'attaques informatiques ou de la réinitialisation de mots de passe de chiffrement malencontreusement oubliés.

Les données sensibles sont constamment exposées aux fuites, aux vols ainsi qu'aux divulgations inopportunes. Dans bien des cas, les données sortent par la grande porte, sur un ordinateur portable ou une clé USB. Pour une entreprise, être victime d'une fuite de données est synonyme de lourdes conséquences : sanctions réglementaires, divulgation publique, préjudice porté à la marque, pertes financières, etc. Selon un rapport du Ponemon Institute, 7 % des ordinateurs portables d'entreprise seront perdus ou volés à un moment ou l'autre de leur durée de vie¹. La prolifération de terminaux mobiles dotés d'une grande capacité de stockage et capables, pour la plupart, d'accéder à Internet augmente encore les risques de fuite ou de vol de données. Il est dès lors plus que jamais essentiel de protéger les informations propriétaires, d'identification personnelle et autres données sensibles. McAfee® Complete Data Protection permet de régler ces questions — et bien d'autres.

Chiffrement de disques adapté aux besoins des entreprises

Protégez vos données confidentielles grâce à une solution de chiffrement des terminaux d'entreprise qui est certifiée FIPS 140-2 et Common Criteria EAL2+ et qui met en œuvre le jeu d'instructions Intel AES-NI (Intel® Advanced Encryption Standard – New Instructions). McAfee Complete Data Protection utilise le chiffrement des disques allié à un contrôle d'accès robuste, via une authentification pre-boot à deux facteurs, pour bloquer tout accès non autorisé aux données sur les terminaux tels que les postes de travail, les stations de travail VDI, les ordinateurs portables, les tablettes Microsoft Windows, les clés USB, etc.

Chiffrement des fichiers, des dossiers, des supports amovibles et des espaces de stockage dans le cloud

Assurez-vous que des dossiers et fichiers spécifiques demeurent en permanence chiffrés, indépendamment du support sur lequel les données sont modifiées, copiées ou enregistrées. McAfee Complete Data Protection propose une fonction de chiffrement du contenu qui permet de chiffrer de façon transparente et automatique les dossiers et les fichiers de votre choix à la volée, avant qu'ils ne se déplacent au sein de l'entreprise. Vous pouvez créer des stratégies centralisées en fonction des utilisateurs et des groupes et les appliquer à des dossiers et fichiers spécifiques, sans interaction de l'utilisateur.

Principaux avantages (suite)

- Démontrez la conformité grâce à des fonctionnalités avancées d'audit et de génération de rapports ; surveillez les événements et générez des rapports détaillés qui démontreront aux auditeurs et autres parties prenantes votre parfaite conformité aux exigences de confidentialité internes et réglementaires.

Fonctionnalités propres à McAfee ePO Deep Command

- Réduction des temps de correction
- Correction à distance de tout ordinateur, partout dans le monde grâce à un accès au matériel
- Amélioration de la productivité des utilisateurs
- Exécution de tâches gourmandes en ressources pendant les heures creuses, pour limiter l'impact sur les utilisateurs
- Diminution des coûts informatiques grâce à la réduction des interventions répétées sur site et des appels interminables au support technique
- Réduction de la consommation et de la facture énergétiques par l'adoption d'initiatives d'économies d'énergie tout en conservant un accès aux systèmes pour la sécurité ou la correction par patches
- Découverte et mise en service rapides de la technologie Intel AMT grâce à l'identification aisée des ordinateurs dotés d'Intel vPro, puis à l'activation rationalisée de la technologie Intel AMT et de ses fonctions

Management of Native Encryption

Le logiciel Management of Native Encryption permet aux clients de gérer la fonction de chiffrement natif proposée par Apple FileVault sur Mac OS X et par Microsoft BitLocker sur les plates-formes Windows directement à partir du logiciel McAfee® ePolicy Orchestrator® (McAfee ePO™). Ce produit assure une compatibilité immédiate avec les correctifs OS X et Windows, les mises à niveau et les mises à jour de micrologiciel d'Apple et de Microsoft, de même qu'il permet une prise en charge immédiate du nouveau matériel Apple. Il permet aux administrateurs d'importer manuellement les clés de récupération lorsque les utilisateurs ont déjà activé FileVault et BitLocker.

Réduction des coûts d'exploitation grâce à la gestion hors bande à distance

Basé sur la technologie Intel® vPro Active Management Technology (Intel vPro AMT), McAfee ePO Deep Command contribue à réduire les coûts d'exploitation, améliore la sécurité et la conformité et accélère les procédures de correction à distance. Il permet de réactiver les ordinateurs, de mettre à jour les stratégies, puis de remettre les systèmes dans leur état d'activation initial².

Gestion centralisée de la sécurité et génération avancée de rapports

Au moyen de la console centralisée McAfee ePO, mettez en œuvre des stratégies de sécurité obligatoires à l'échelle de l'entreprise pour contrôler le chiffrement et la surveillance des données et pour les protéger contre les fuites. La console permet de définir, de déployer, de gérer et de mettre à jour des stratégies visant à chiffrer, à filtrer et à surveiller les données sensibles, ainsi qu'à bloquer tout accès non autorisé à celles-ci.

Caractéristiques de McAfee Complete Data Protection

Chiffrement de disques adapté aux besoins des entreprises

- Chiffrez automatiquement des équipements complets sans action ni formation requise de l'utilisateur, et sans impact sur les ressources système.
- Identifiez et contrôlez les utilisateurs autorisés à l'aide de mécanismes puissants d'authentification multifacteur.

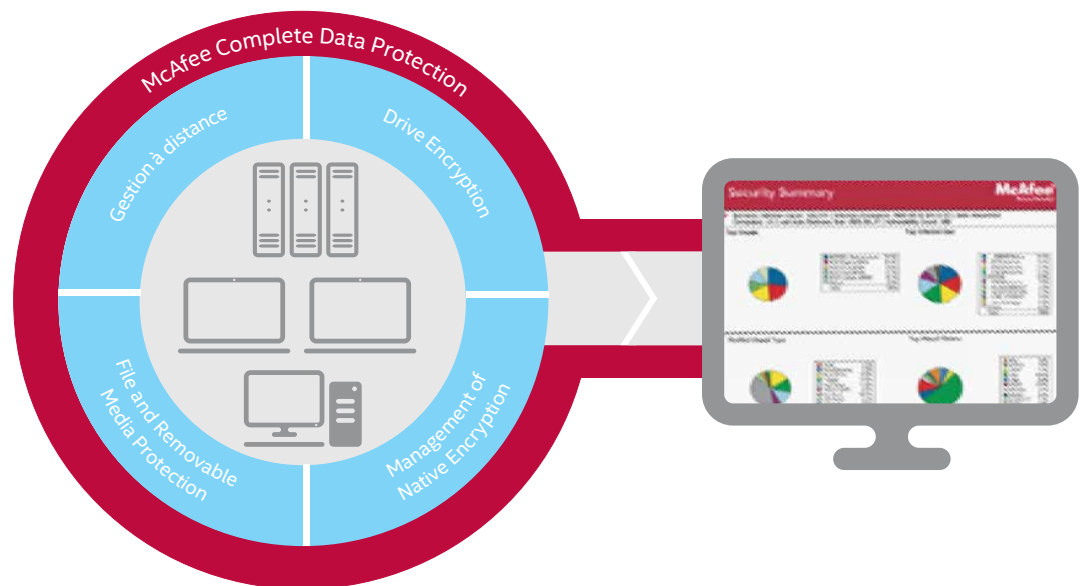


Figure 1. Suite McAfee Complete Data Protection

Spécifications de McAfee Complete Data Protection

Systèmes d'exploitation Microsoft Windows

- Microsoft Windows 7, 8 et 10 (32 et 64 bits)
- Microsoft Windows Vista (32 et 64 bits)
- Microsoft Windows XP (32 bits uniquement)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 (32 bits uniquement)

Configuration matérielle requise

- Processeur : ordinateurs portables et de bureau avec processeur Pentium III 1 GHz ou plus puissant
- Mémoire RAM : 512 Mo minimum (1 Go recommandé)
- Disque dur : 200 Mo d'espace disponible sur le disque dur

Systèmes d'exploitation Apple Mac

- Mac OS X El Capitan, Yosemite, Mountain Lion et Mavericks

Configuration matérielle requise

- Processeur : ordinateur portable Mac à processeur Intel avec EFI 64 bits
- Mémoire RAM : 1 Go minimum
- Disque dur : 200 Mo d'espace disponible sur le disque dur

Gestion centralisée

- Pour les spécifications techniques, voir la fiche technique consacrée à la plate-forme McAfee ePO.

Spécifications de McAfee ePO Deep Command

- Prise en charge d'Intel vPro AMT versions 6.1.2, 7.0, 7.1.4 et 8.0 Intel Setup and Configuration Software (SCS) 8.2

Chiffrement des supports amovibles

- Tirez parti d'un chiffrement automatique « à la volée » pour pratiquement n'importe quel support de stockage mobile, mis à disposition ou non par l'entreprise.
- Chiffrez ou bloquez l'écriture sur les supports amovibles au niveau des stations de travail VDI.
- Accédez aux données chiffrées depuis n'importe quel emplacement, sans qu'il soit nécessaire d'installer des logiciels supplémentaires ou de bénéficier de droits d'administrateur local sur l'équipement hôte.

Chiffrement des fichiers, des dossiers et des espaces de stockage dans le cloud

- Préservez la sécurité des dossiers et des fichiers où qu'ils soient enregistrés : disques durs locaux, serveurs de fichiers, supports amovibles ou espaces de stockage dans le cloud (p. ex. Box, Dropbox, Google Drive ou Microsoft OneDrive).

Gestion du chiffrement natif sur les terminaux Mac et Windows

- Gérez FileVault sur tout terminal Mac exécutant Mac OS X Mountain Lion, Mavericks, Yosemite et El Capitan, directement à partir de McAfee ePO.
- Gérez BitLocker sur les systèmes Windows 7, 8 et 10 directement à partir de McAfee ePO, sans qu'il soit nécessaire de disposer d'un serveur Microsoft MBAM (BitLocker Management and Administration) distinct.
- Rendez compte du niveau de conformité grâce à divers rapports et tableaux de bord de McAfee ePO.

Gestion hors bande à distance

- Gérez les ordinateurs à distance au-delà du système d'exploitation, au niveau du matériel.
- Mettez un ordinateur sous tension et réactivez-le (même en cas de chiffrement) pour effectuer des tâches de sécurité.

Console de gestion centralisée

- Utilisez l'infrastructure de gestion logicielle McAfee ePO pour gérer le chiffrement complet des disques, des dossiers et des fichiers. Contrôlez la gestion des stratégies et des correctifs, récupérez les mots de passe perdus et démontrez le respect des réglementations officielles.
- Synchronisez les stratégies de sécurité avec Microsoft Active Directory, Novell NDS, PKI (Public Key Infrastructure) et d'autres annuaires.
- Démontrez que les équipements sont chiffrés grâce aux fonctionnalités d'audit complètes.
- Enregistrez les transactions de données pour conserver des informations telles que l'expéditeur, le destinataire, l'horodatage, les éléments de preuve, la date et l'heure de la dernière connexion, la date et l'heure de la dernière mise à jour et les indications de réussite ou d'échec du chiffrement.

Pour plus d'informations sur les solutions de protection des données de McAfee, consultez notre site à la page www.mcafee.com/fr/products/data-protection/index.aspx.



McAfee. Part of Intel Security.

Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com

1. *The Billion Dollar Lost Laptop Problem Study* (Étude du problème des pertes d'ordinateurs portables estimées à plusieurs milliards de dollars), Ponemon Institute, septembre 2010.
2. *Keep Your Client PCs Safer, Wherever They Go* (Sécurité renforcée des ordinateurs clients en tout lieu) : <http://www.mcafee.com/fr/resources/solution-briefs/sb-keep-your-client-pcs-safer.pdf>