

McAfee Data Loss Prevention Endpoint

Pour une protection efficace contre les compromissions de données

Votre société subit-elle des fuites de données à votre insu ? Il se peut qu'au moment même où vous lisez ces lignes, vos données financières, vos fiches clients, vos éléments de propriété intellectuelle, voire les dossiers de vos salariés, échappent au contrôle de votre entreprise. Bien souvent, les coupables ne sont même pas des pirates informatiques, mais des membres de votre personnel. Qu'elles soient accidentelles ou dues à la malveillance, les fuites de données peuvent se produire par l'intermédiaire des canaux de diffusion courants (messagerie électronique, publication web, enregistrement sur clés USB, téléchargements dans le cloud) et se solder parfois par des pertes financières qui se chiffrent en millions. Chaque jour, des entreprises subissent d'importantes fuites de données, qu'elles soient accidentelles ou malveillantes. Et s'il était possible d'empêcher facilement et efficacement les fuites de données ? En assurant de surcroît la mise en conformité aux réglementations sectorielles et nationales, de même que la protection de la propriété intellectuelle ? En réalité, tout cela est possible, grâce à la solution complète McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).

Protection contre les fuites de données, des équipements jusqu'au cloud

McAfee DLP Endpoint est intégré avec MVISION Cloud DLP. Les stratégies DLP sur site peuvent être étendues facilement au cloud, d'un simple clic et presque instantanément (en moins d'une minute dans certaines configurations)¹. Les balises de classification DLP définies sur site sont partagées avec les stratégies DLP cloud pour garantir une détection cohérente des fuites de données.

Fonctionnalités de protection évoluées

McAfee DLP Endpoint assure la protection complète de tous les canaux de fuite potentiels, comme les périphériques de stockage amovibles, le cloud, la messagerie électronique et instantanée, le Web, les impressions, le Presse-papiers, la capture d'écrans, les applications de partage de fichiers et bien d'autres.

Principaux avantages

- **Protection contre les fuites de données, des équipements jusqu'au cloud** : Étendez facilement au cloud les stratégies DLP définies sur site, pour une détection cohérente des fuites de données.
- **Fonctionnalités de protection évoluées** : Exploitez les empreintes numériques, la classification et le marquage de fichiers pour protéger les données sensibles et non structurées, telles que la propriété intellectuelle et les secrets commerciaux.
- **Gestion centralisée** : Optimisez la gestion des stratégies et des incidents grâce à l'intégration native avec McAfee® MVISION ePolicy Orchestrator® (MVISION ePO™)².
- **Mise en œuvre de la conformité** : Assurez la conformité en contrôlant les actions des utilisateurs au quotidien : échange d'e-mails, publications dans le cloud, téléchargements sur des supports amovibles, etc.

Gardez le contact



FICHE TECHNIQUE

Principales fonctionnalités de McAfee DLP Endpoint :

- Possibilité de définir des étiquettes Microsoft Azure Information Protection (AIP) pour les données en mouvement et de reconnaître les fichiers avec étiquette AIP³.
- L'intégration avec une solution d'analyse comportementale des utilisateurs et des entités (UEBA) permet de contrer les menaces internes. Cette solution exécute des analyses de sécurité pour détecter les comportements inhabituels et à risque des utilisateurs et des entités.
- La classification manuelle permet aux utilisateurs de classer manuellement leurs documents, améliore la sensibilisation des employés à la protection des données et réduit la charge administrative.
- L'analyse et la correction initiées par l'utilisateur permettent aux utilisateurs finaux d'exécuter des analyses de découverte de terminaux et de prendre des mesures auto-correctives.
- Le système de classification flexible comprend des dictionnaires, des expressions régulières, des algorithmes de validation et des documents enregistrés et prend en charge des solutions de classification d'autres éditeurs, destinées aux utilisateurs.
- Une technologie de marquage unique permet d'identifier les documents en fonction de leur origine. Les informations sensibles provenant d'applications web, d'applications réseau et de partages réseau ne peuvent pas être dupliquées ou renommées ni quitter le périmètre de l'entreprise.

- La prise en charge améliorée de la virtualisation permet de protéger les postes de travail distants et les infrastructures de postes de travail virtuels (VDI).

Gestion centralisée

- La solution est administrée par une console native au cloud (MVISION ePO) pour optimiser la gestion des stratégies et des incidents⁴.
- McAfee DLP Endpoint utilise les mêmes moteurs de stratégies et de classification et les mêmes workflows d'incidents que McAfee® MVISION Cloud (CASB) et McAfee® Network DLP.
- Les nombreux jeux de règles et stratégies réutilisables permettent de définir des stratégies DLP multiples dans toute l'entreprise, ou de créer des stratégies spécifiques en fonction de chaque bureau, département, réglementation, etc.
- La gestion des incidents plus granulaire permet d'interroger, de filtrer ou de visualiser les incidents en fonction de leurs propriétés (numéro de série de l'équipement, nom du fichier de preuve et groupes, par exemple).
- La solution propose des fonctionnalités centralisées d'audit et de surveillance des événements.
- L'administrateur dispose d'un meilleur contrôle d'accès basé sur les rôles (également appelé « séparation des responsabilités ») pour la gestion des stratégies ainsi que pour l'analyse des incidents.
- L'utilisateur peut facilement accéder à une interface de centre d'assistance.

- **Sensibilisation et formation des utilisateurs** : Bénéficiez d'un feedback en temps réel grâce à des messages instantanés informatifs, qui favorisent la sensibilisation et la formation des utilisateurs à la sécurité.

Plates-formes prises en charge

- Windows 10 (32 et 64 bits)
- Windows 8 ou 8.1 (32 et 64 bits)
- Windows 7 (32 et 64 bits)
- Windows Server 2019
- Windows 2016 (64 bits)
- Windows 2012 (64 bits) et Windows 2012 R2 (64 bits)
- Windows 2008 (32 et 64 bits) et Windows 2008 R2 (32 et 64 bits)
- macOS Catalina 10.15 ou version ultérieure
- macOS Mojave 10.14 ou version ultérieure
- macOS High Sierra 10.13 ou version ultérieure
- macOS Sierra 10.12 ou version ultérieure
- OS X El Capitan 10.11 ou version ultérieure
- OS X Yosemite 10.10 ou version ultérieure
- OS X Mavericks 10.9.0 ou version ultérieure

Navigateurs pris en charge

- Internet Explorer version 11 ou version ultérieure

Mise en œuvre de la conformité et formation de l'utilisateur

Avec la disparition du périmètre d'entreprise, il est devenu plus difficile pour les sociétés de mettre en œuvre la conformité aux normes et réglementations. McAfee DLP Endpoint peut non seulement vous aider à surveiller les comportements des utilisateurs au quotidien, mais aussi assurer la conformité par la sensibilisation de vos collaborateurs. La création de rapports détaillés McAfee DLP Endpoint s'effectue d'un

simple clic. Il est donc facile de produire les preuves de la conformité interne et réglementaire à l'intention des auditeurs, des cadres supérieurs et de toute autre partie intéressée. La solution propose des modèles de stratégies pour les réglementations et des cas d'utilisation, ce qui facilite la mise en conformité. Vos utilisateurs reçoivent également un feedback en temps réel via des messages instantanés liés à la mise en œuvre de la stratégie d'entreprise : autant d'occasions de former le personnel à la sécurité et de favoriser une véritable culture d'entreprise dans ce domaine.

- Mozilla Firefox 48 ou version ultérieure
- Google Chrome 65 ou version ultérieure

Versions de McAfee ePO prises en charge

- McAfee ePO 5.9.1 et 5.10 pour DLP 11.1 ou version ultérieure

Prise en charge pour McAfee MVISION ePO (SaaS)

- Pour DLP 11.5 ou version ultérieure, il n'est pas nécessaire d'installer de logiciel ou d'extension DLP. Un nom d'utilisateur et un mot de passe sont nécessaires à l'authentification pour accéder à MVISION ePO.

Pour obtenir la liste complète des plates-formes, navigateurs et logiciels pris en charge, consultez la [base de connaissances McAfee](#).

En savoir plus

Pour en savoir plus, visitez notre site à l'adresse : www.mcafee.com/fr/products/dlp-endpoint.aspx.

1. Sur la base de tests internes systématiques réalisés en laboratoire par McAfee.
2. McAfee DLP Endpoint 11.5 ou version ultérieure
3. Ibid.
4. Ibid.



11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr

McAfee et le logo McAfee, ePolicy Orchestrator et McAfee ePO sont des marques commerciales ou des marques commerciales déposées de McAfee, LLC ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs.
Copyright © 2020 McAfee, LLC. 4456_0520
MAI 2020