



McAfee Data Loss Prevention Endpoint

Pour une protection efficace contre les compromissions de données

Principaux avantages

- **Prévention en temps réel des exfiltrations de données** — L'intégration avec McAfee Threat Intelligence Exchange et McAfee Data Exchange Layer garantit une visibilité et une surveillance en temps réel.
- **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** — L'intégration native avec McAfee® ePolicy Orchestrator® (McAfee ePO™) permet de rationaliser la gestion des stratégies et des incidents.
- **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.
- **Formation des utilisateurs finaux** — 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.

Votre société subit-elle des fuites d'informations 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 d'informations 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 d'informations, qu'elles soient accidentelles ou malveillantes. Les compromissions de données et les mesures correctives subséquentes sont extrêmement coûteuses. Selon le dernier rapport du Ponemon Institute *Cost of Data Breach Study* (Coût des compromissions de données)¹, le coût moyen de chaque enregistrement perdu ou volé contenant des informations sensibles et confidentielles s'élève à 201 dollars. Le coût total moyen subi par les entreprises est de 5,9 millions de dollars. 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).

Prévention en temps réel des exfiltrations de données

En plus d'assurer rapidement et facilement la surveillance des activités utilisateur en temps réel, McAfee DLP Endpoint permet d'appliquer des stratégies de sécurité gérées de façon centralisée afin de réglementer ou de restreindre les transferts de données sensibles, sans affecter la productivité du personnel. Intégré à McAfee Threat Intelligence Exchange et à McAfee Data Exchange Layer (DXL), McAfee DLP Endpoint communique avec cette couche DXL et bloque les données sensibles

au niveau des applications identifiées comme malveillantes, ou applique des stratégies de sécurité plus strictes pour les terminaux non approuvés. Connecté à votre infrastructure de sécurité globale, McAfee DLP Endpoint procure des réponses instantanées aux menaces persistantes avancées (APT, Advanced Persistent Threats) et bloque les exfiltrations 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.

La liste ci-dessous présente quelques-unes des fonctionnalités clés.

- **Nouveau ! Classification manuelle** — Permet aux utilisateurs finaux de classer manuellement leurs documents, améliore la sensibilisation des employés à la protection des données et réduit la charge administrative.
- **Nouveau ! Analyse et correction initiées par l'utilisateur** — Permet aux utilisateurs finaux d'exécuter des analyses de découverte de terminaux et de prendre des mesures auto-correctives.

Plates-formes prises en charge

- Windows 7 Service Pack 1 ou version ultérieure (éditions Entreprise et Professionnel), 32 et 64 bits
- Windows 8, 8.1 ou version ultérieure (éditions Entreprise et Professionnel), 32 et 64 bits
- Windows Server 2008 R2, 2008 SP2 ou version ultérieure, 32 et 64 bits
- Windows Server 2012, 2012 R2 ou version ultérieure, 64 bits
- Mac OS X Mountain Lion 10.8.5
- Mac OS X Mavericks 10.9.5
- Mac OS X Yosemite 10.10

Navigateurs pris en charge

- Internet Explorer versions 8 à 11
- Mozilla Firefox 34 ou version ultérieure
- Google Chrome 31 ou version ultérieure

Logiciel et agents McAfee ePO

- Logiciel McAfee ePO 4.6.9 et 5.1.1
- McAfee Agent for Windows 4.8 Patch 2 et 5.0
- McAfee Agent for Mac 4.6 Patch 3, 4.8 Patch 2 et 5.0

- **Nouveau !** Prise en charge optimisée de Mac OS — Améliore la protection en fonction du contenu pour Mac OS à plusieurs niveaux : périphériques de stockage amovibles, accès aux fichiers d'applications et partages réseau.
- **Nouveau !** Aucun redémarrage — Accroît l'efficacité administrative sans redémarrage après les mises à niveau pour McAfee DLP Endpoint 10.0 et les versions supérieures.
- 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 finaux.
- 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).
- Les nombreux jeux de règles et stratégies réutilisables permettent de définir des stratégies DLP multiples dans toute l'organisation, 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.
- Il est possible d'accéder à une interface de centre d'assistance.

Gestion centralisée

McAfee DLP Endpoint bénéficie désormais d'une intégration native avec McAfee® ePolicy Orchestrator® (McAfee ePO™) et peut donc être déployé de façon centralisée et administré facilement. L'interface de gestion totalement remaniée de McAfee DLP Endpoint procure des ensembles de règles flexibles et réutilisables, avec une granularité plus fine et une convivialité accrue.

La liste ci-dessous présente quelques-unes des fonctionnalités clés.

- Grâce à cette intégration native avec McAfee ePO, McAfee DLP Endpoint ne nécessite plus l'installation d'un contrôle ActiveX dans Internet Explorer pour son administration.

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

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 stratégies prédéfinies 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.

En savoir plus

Pour en savoir plus, visitez notre site à l'adresse : www.mcafee.com/fr/products/dlp-endpoint.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. 2014 Cost of a Data Breach Study: United States (Rapport 2014 sur le coût des compromissions de données – États-Unis), Ponemon Institute, septembre 2014