McAfee Data Loss Prevention Discover

Localisation, classification et protection de vos données sensibles, où qu'elles se trouvent

Les informations sensibles enregistrées sur les ordinateurs portables, les serveurs de fichiers partagés et dans le cloud peuvent être synonymes de risques pour votre entreprise. Aussi doivent-elles être protégées efficacement. Cependant, leurs volumes colossaux (exprimés en téraoctets, voire en pétaoctets) rendent cette tâche particulièrement complexe, d'autant que les données sensibles ne sont pas toujours correctement cataloguées. De plus, la plupart des entreprises ne disposent pas de méthode leur permettant de déterminer si ces données sont à risque, ou de savoir où elles ont été diffusées, et ce même lorsque des contrôles d'accès sont en place. Pour couronner le tout, parmi les informations sensibles figurent généralement des données non structurées comme des éléments de propriété intellectuelle, plus difficiles à définir que les données structurées telles que les numéros de carte de crédit ou de sécurité sociale. McAfee® Data Loss Prevention Discover (McAfee DLP Discover) vous aide à localiser et à classer vos données sensibles, mais aussi à déterminer comment elles sont utilisées, tout en offrant une protection contre les vols et les fuites de données.

Fonctionnalités principales

McAfee DLP Discover vous aide à identifier et gérer les risques de fuites de données, sur site comme dans le cloud. Ses techniques avancées vous permettent de localiser, classer et protéger tous les types de données critiques de l'entreprise.

- Correspondance exacte des données (EDM) — Nouveau critère de classification créé lors du téléchargement d'un fichier CSV contenant des informations confidentielles, dans lequel les cellules de chaque ligne sont liées. Les correspondances exactes de données sont prises en charge pour les analyses de référentiels CIFS, SharePoint et Box.

Principaux avantages

Identification des risques de fuites de données

- Analyse de données stockées sur site ou dans le cloud (Box)
- Identification des emplacements de stockage des données sensibles et de leur propriétaire
- Recherche et affichage de toutes les données analysées à partir d'une interface intuitive

Stratégies et rapports personnalisés

- Utilisation de stratégies prédéfinies en matière de conformité, de gouvernance d'entreprise et de propriété intellectuelle
- Enregistrement des informations sensibles sur des systèmes de sécurité des données adjacents

Gardez le contact

- Solution exclusivement logicielle permettant de réaliser des économies supplémentaires, dans la mesure où aucune appliance virtuelle ou matérielle n'est nécessaire.
- Gestion et déploiement complets au moyen du logiciel McAfee® ePolicy Orchestrator® (McAfee ePO™) — Extension de gestion et stratégie de prévention des fuites de données identiques à celles de McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).
- Identification par empreinte des données structurées dans les bases de données et les feuilles de calcul Microsoft Excel, grâce à la correspondance exacte des données (EDM). Vous pouvez ainsi définir plusieurs critères de déclenchement d'une stratégie DLP pour une meilleure précision.
- Compatibilité totale avec les fonctionnalités de classification de McAfee DLP Endpoint.
- Compatibilité avec Microsoft Windows Server 2008, Windows Server 2012 et Windows Server 2016.
- Prise en charge des déploiements distribués qui permettent d'exploiter les capacités inutilisées des serveurs existants et de disperser les systèmes sur une zone géographique étendue.
- La reconnaissance optique de caractères reconnaît et protège le texte contenu dans des images et des formulaires. Elle permet aux clients d'inspecter les fichiers graphiques intégrés à la recherche de contenu sensible dans les ressources réseau, y compris les partages de fichiers, SharePoint et les bases de données[1].

Prévention des fuites de données sensibles

Le patrimoine informationnel de l'entreprise est essentiel pour votre marque, votre réputation et votre avantage concurrentiel — qu'il s'agisse de code source, de secrets industriels, de projets commerciaux ou de propriété intellectuelle. La protection des données lors de leur transmission est certes cruciale, mais la priorité doit être donnée à la sécurité des données sensibles avant tout accès ou déplacement inapproprié ainsi qu'à l'identification des emplacements où elles résident.

McAfee DLP Discover vous aide à protéger votre entreprise contre les fuites de données. Contrairement à des solutions des générations précédentes, qui partent du principe que vous savez exactement quel contenu doit être protégé, McAfee DLP Discover couvre non seulement les informations clairement à risque, mais vous permet également d'identifier celles qui sont plus difficilement repérables.

Identification des informations à protéger

Pour déterminer les informations et les risques de diffusion illicite, McAfee DLP Discover peut être configuré de manière à analyser des référentiels spécifiques et à identifier les données nécessitant une protection explicite. En outre, toutes les données balayées par la solution sont indexées et accessibles via une interface intuitive, de sorte que vous pouvez rechercher rapidement des données potentiellement sensibles afin de déterminer leur propriétaire et leur emplacement de stockage.

Classification et analyse des fuites de données, application de mesures correctives

- Filtrage et contrôle des informations sensibles au moyen d'une classification multivectorielle
- Indexation de tout le contenu, puis interrogation et exploration des données pour déterminer leur niveau de sensibilité
- Enregistrement et génération de signatures afin de protéger les documents et les informations qu'ils contiennent, même en cas de plagiat ou de transposition
- Envoi d'une alerte si du contenu viole des stratégies de protection

Spécifications

Types de contenus

Prise en charge de la classification des fichiers pour plus de 300 types de contenus, y compris :

- Stockage dans le cloud de type « Box »
- Documents Microsoft Office
- Fichiers Adobe
- Fichiers multimédias
- Code source
- Fichiers de conception
- Archives
- Fichiers chiffrés
- Stratégies intégrées
- Propriété intellectuelle

Définition de stratégies de protection

Une fois les informations à protéger correctement identifiées, McAfee DLP Discover vous permet de les sécuriser de façon précise. Vous pouvez créer et gérer des stratégies, ou encore générer des rapports, de manière à la fois intuitive et centralisée. Vous bénéficiez ainsi d'un contrôle accru sur votre stratégie de protection des données stockées passivement. Les stratégies, les règles et la fonctionnalité de classification de McAfee DLP Discover offrent notamment les avantages suivants :

- Nombreuses stratégies prédéfinies, utilisables facilement dès l'installation
- Moteur de construction de règles puissant, qui gère tant les données structurées simples (numéros de sécurité sociale et cartes de crédit) que les informations complexes (propriété intellectuelle)
- Création et validation simplifiées des règles par le transfert de l'analyse des résultats de recherche à une règle de protection
- Intégration à des vecteurs de sécurité des informations adjacents pour garantir une protection continue
- Exclusion de documents publics et de texte courant afin d'empêcher les informations sans risque de générer des incidents

Analyse du réseau à la recherche de violations

Une fois les stratégies définies, vous pouvez configurer McAfee DLP Discover de sorte qu'il analyse régulièrement les ressources réseau afin d'identifier toute violation de stratégies. Les options de planification, d'une grande souplesse, permettent d'effectuer des analyses continues, quotidiennes, hebdomadaires ou mensuelles.

McAfee DLP Discover analyse automatiquement toutes les ressources accessibles, dont les ordinateurs portables, les postes de travail, les serveurs, les référentiels de documents, les portails et les emplacements de transfert de fichiers, afin d'identifier de potentielles violations des stratégies. Vous pouvez définir des groupes d'analyse en fonction d'adresses IP, d'intervalles d'adresses IP, de sous-réseaux ou de chemins réseau. Vous pouvez également cibler les opérations d'analyse à l'aide de paramètres spécifiques, par exemple en analysant seulement le dossier Mes documents pour tous les utilisateurs, mais pas les dossiers système, ou en recherchant les fichiers appartenant à des utilisateurs précis, d'un certain type ou d'une taille donnée.

Évaluation des violations et application de mesures correctives

McAfee DLP Discover élimine ou minimise la diffusion non autorisée des informations sensibles grâce à une gestion intégrée des cas et du workflow des incidents. Si la solution détecte du contenu qui viole les stratégies de protection, elle génère des incidents et envoie des notifications. Les incidents créés par McAfee DLP Discover peuvent être ajoutés au cadre de gestion des cas, qui permet la collaboration de spécialistes de différents départements de l'entreprise à la résolution de la violation. En outre, grâce aux tableaux de bord des risques, le personnel responsable de la sécurité peut, en toute simplicité, examiner le profil des violations et générer des rapports en fonction des paramètres pertinents relatifs aux données au repos.

Référentiels pris en charge

- Common Internet File System (CIFS)/Server Message Block (SMB)
- Microsoft SharePoint
- Bases de données : Microsoft SQL, Oracle, DB2, MySQL Enterprise

Enregistrement des documents

Il est possible d'enregistrer des documents à partir de tout référentiel. Les signatures de documents enregistrés peuvent être utilisées en local afin de détecter la diffusion illicite de contenu sensible ou être mises à la disposition d'autres appliances McAfee DLP.

Rapports

Le moteur d'analyse puissant génère des vues des incidents et des résultats de recherche. De plus, il permet de personnaliser les vues synthétiques en partant de deux points de référence contextuels. L'affichage peut être détaillé, sous forme de liste ou synthétique avec des données de tendance. Le système propose de nombreux rapports prédéfinis et personnalisables.

Capture et analyse des données stockées

En plus d'analyser les ressources réseau pour détecter les violations de stratégies, McAfee DLP Discover indexe la totalité du contenu stocké passivement sur le réseau et vous offre la possibilité d'exécuter des requêtes sur ces informations et de les explorer afin d'améliorer votre visibilité sur vos données sensibles. Dès lors, vous savez avec précision de quelle façon ces dernières sont utilisées, qui en est le propriétaire, à quel endroit elles sont stockées et où elles ont été transférées.

Classification des données complexes

McAfee DLP Discover permet à votre entreprise de protéger tous types de données sensibles : depuis les données de format fixe courantes jusqu'aux éléments de propriété intellectuelle extrêmement variables et complexes. La solution recourt à divers mécanismes de classification des objets et combine leurs résultats pour établir une classification multivectorielle extrêmement précise, qu'elle utilise pour filtrer et contrôler les informations sensibles et effectuer des recherches visant à identifier les risques cachés ou inconnus. Ces mécanismes sont les suivants :

- **Classification multiniveau :** couverture des informations contextuelles et du contenu dans un format hiérarchique
- **Enregistrement des documents :** génération de signatures appliquées aux informations à mesure qu'elles sont modifiées
- **Analyse grammaticale :** détection de la grammaire ou de la syntaxe dans tout contenu, des documents de texte aux feuilles de calcul, en passant par le code source
- **Analyse statistique :** suivi du nombre de correspondances de mots clés, de modèles ou de signatures décelés dans un document ou fichier donné
- **Classification des fichiers :** identification des types de contenus, quelle que soit l'extension du fichier ou la compression
- **Classification des documents :** prise en charge de la réaction « Classer le ficher en tant que » par les règles Discover pour CIFS, Box et SharePoint. Cette réaction intègre l'ID de classification dans des formats de fichier qui prennent en charge les classifications intégrées.

Spécifications logicielles

McAfee DLP Discover est disponible en version logicielle. La configuration système minimale est décrite ci-dessous.

Configuration matérielle requise

- Processeur : Intel Core 2 64 bits
- Mémoire RAM : 4 Go minimum
- Espace disque : 100 Go minimum

Plates-formes prises en charge

- Windows Server 2008 R2 Standard, 64 bits
- Windows Server 2012 Standard, 64 bits
- Windows Server 2012 R2 Standard, 64 bits
- Windows Server 2016 Standard, 64 bits

Systèmes de virtualisation pris en charge

- VMware vSphere utilisant vCenter Server 6.0, 6.5 ou 6.7
- vCenter Server 5.0 Update 2

Logiciel et agents McAfee ePO

- McAfee ePO 5.3.3, 5.9.1 et 5.10
- McAfee Agent 5.0.6, 5.5 et 5.5.1

1. Intégré avec DLP Discover : aucun serveur distinct n'est requis. Il s'agit d'un module complémentaire pour la référence SKU McAfee Total Protection for DLP.

McAfee
Together is power.

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