McAfee Data Loss Prevention Discover

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

Principaux avantages

Identification des risques de fuites de données

- Stockage des données d'analyse sur site ou dans le cloud
- 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

- Exécution de requêtes et transfert de leurs résultats à une règle de protection
- Utilisation de stratégies de conformité, de gouvernance d'entreprise et de propriété intellectuelle prédéfinies
- Enregistrement des informations sensibles sur des systèmes de sécurité des données adjacents

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

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 efficace leur permettant de déterminer ou de vérifier si ces données sont à risque ou encore 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 (DLP) Discover vous aide à localiser et à classer vos données sensibles, ainsi qu'à déterminer comment elles sont utilisées, tout en offrant une protection contre le vol et les fuites de données.

Nouveautés de McAfee DLP Discover

McAfee DLP Discover permet désormais d'analyser et de protéger les données enregistrées dans le cloud, notamment sur la plate-forme Box. Grâce à sa plate-forme de gestion centralisée, le logiciel McAfee ePolicy Orchestrator® (McAfee ePO™) permet quant à lui de définir des stratégies en toute facilité, mais aussi d'automatiser et de programmer à l'avance les analyses. Des fonctionnalités spéciales de génération de rapports sur les incidents et d'analyses détaillées sont également disponibles.

Fonctionnalités et points forts :

- 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 ePO ; extension de gestion et stratégie DLP identiques à celles de la solution DLP Endpoint
- Compatibilité totale avec les fonctionnalités de classification de DLP Endpoint
- Compatibilité avec Windows Server 2008 et Windows Server 2012
- 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

intel Security

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 multimédias
- Code source
- Fichiers de conception
- Archives
- Fichiers chiffrés
- Stratégies intégrées
- Propriété intellectuelle

Référentiels pris en charge

- Common Internet File System (CIFS)/Server Message Block (SMB)[1]
- Network File System (NFS)
- HTTP/HTTPS
- FTP/FTPS
- Microsoft SharePoint[1]
- EMC Documentum
- 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 prolifération 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 et vous 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 plus de 20 rapports prédéfinis et personnalisables.

- Licence compatible avec l'appliance DLP Discover 9.3.x ou avec la version exclusivement logicielle DLP Discover 9.4

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 prolifération, 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.

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 prolifération 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.

Spécifications : logiciel uniquement

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

Systèmes de virtualisation pris en charge

- vSphere ESXi 5.0, mise à jour 2
- vCenter Server 5.0, mise à jour 2

Logiciel et agents McAfee ePO

- McAfee ePO 4.6.8 ou version ultérieure ; et 5.1 ou version ultérieure
- McAfee Agent 4.8.2 ou version ultérieure ; et 5.0 ou version ultérieure

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.

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 : application de signatures biométriques des 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 grammaticales, biométriques ou de signatures décelées dans un document ou fichier donné
- Classification des fichiers : identification des types de contenus, quelle que soit l'extension du fichier ou la compression

Spécifications : appliance McAfee DLP 5500

McAfee DLP Discover est disponible sous la forme d'une appliance physique ou virtuelle. Les spécifications des appliances sont décrites ci-dessous.

Composant	Description
Processeur	2 processeurs Intel E5-2620 6 cœurs 2 GHz avec cache de 15 Mo, débit Intel QPI de 7,20 GT/s
Mémoire	32 Go de mémoire DDR3 1 333 MHz
Alimentation électrique	2 modules de 760 W remplaçables à chaud
Disques durs	8 disques SATA 7 200 tr/min de 2 To
Carte réseau	Module E/S Intel Ethernet double port 1 Gbit/s cuivre
IPMI	Intel Remote Management Module 4 (AXXRMM4)
Encombrement	Format 2U montable en rack

Spécifications : machines virtuelles

McAfee DLP Discover est disponible sous la forme d'une appliance virtuelle qui peut être exécutée dans un environnement VMware. La configuration matérielle minimale requise pour l'appliance virtuelle est décrite ci-dessous.

Composant	Critère
Processeur	4 processeurs virtuels Intel x86
Mémoire	16 Mo de mémoire RAM
Disque(s) dur(s)	Disque 1 : capacité minimale de 100 Go pour le logiciel de machine virtuelle Disque 2 : capacité minimale de 512 Go pour l'image virtuelle DLP
Réseau	4 cartes réseau virtuelles
BIOS	Activation de la thread de virtualisation (VT)

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. McAfee DLP Discover 9.4 en version exclusivement logicielle prend actuellement en charge le système CIFS, Microsoft SharePoint 2010 et Microsoft SharePoint 2013.