McAfee DLP Prevent

Mise en œuvre de stratégies pour la protection de vos informations sensibles

Plus les utilisateurs partagent des données au format électronique, plus la probabilité est forte que des données sensibles soient transmises, par inadvertance ou intentionnellement, à un utilisateur non autorisé, mettant ainsi en danger les données d'entreprise confidentielles. Messagerie électronique, messagerie instantanée, Internet ou encore FTP : tous ces canaux électroniques sont des vecteurs potentiels de fuites d'informations. Si certains messages ou transactions peuvent être autorisés, ils doivent néanmoins être chiffrés pour garantir la confidentialité des données. D'autres types de communications sont par contre simplement inacceptables et leur transmission doit être bloquée. Pour garantir la sécurité des données, la conformité aux réglementations et la protection du capital intellectuel, il est essentiel de mettre en œuvre les stratégies adéquates au bon moment.

Mise en œuvre de stratégies de sécurité pour les données en transfert

Dans tous les départements de toutes les entreprises, les employés partagent des données à l'aide d'une multitude d'applications et via divers protocoles. Prévenez les fuites de données accidentelles ou intentionnelles en empêchant proactivement les informations sensibles de quitter le réseau et en mettant en œuvre les processus métier adéquats.

McAfee® DLP Prevent vous aide à appliquer des stratégies régissant les informations qui quittent le réseau via des canaux tels que la messagerie électronique, la messagerie web, la messagerie instantanée, les wikis, les blogs, les portails et les transferts HTTP/HTTPS ou FTP. Pour cela, il s'intègre avec des passerelles de type agent de transfert des messages (MTA) via des serveurs proxy web compatibles avec ICAP (Internet Content Adaptation

Principaux avantages

Utilisation de l'infrastructure existante

- Protection de la messagerie électronique d'entreprise par l'intégration avec des passerelles servant d'agents MTA et utilisant SMTP avec des en-têtes X-header pour le blocage, le retour, le chiffrement, la mise en quarantaine et la redirection des e-mails
- Application de stratégies de sécurisation du trafic grâce à l'intégration d'ICAP avec des serveurs proxy web compatibles afin de réduire les violations de stratégies relatives au contenu au niveau de la messagerie instantanée, de la messagerie web et du trafic FTP, HTTP et HTTPS

Gardez le contact

Protocol) ou SMTP (Simple Mail Transfer Protocol). En cas de violation de stratégie, McAfee DLP Prevent permet à l'entreprise de prendre une série de mesures, dont le chiffrement, le blocage, la redirection, la mise en quarantaine, etc. Vous pouvez ainsi assurer la conformité avec les réglementations en matière de confidentialité des informations sensibles et réduire le risque de menaces pour la sécurité.

Intégration avec le logiciel McAfee ePolicy Orchestrator pour une infrastructure unifiée

McAfee DLP Prevent est intégré avec le logiciel McAfee® ePolicy Orchestrator® (McAfee ePO™) et McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) pour vous offrir une gestion unifiée des stratégies, des cas et des incidents. Les administrateurs peuvent créer une seule stratégie de protection de la messagerie électronique et de l'environnement web et la déployer sur les terminaux et le réseau. En outre, McAfee DLP Endpoint et McAfee DLP Prevent partagent un moteur de classification commun qui permet de mettre en œuvre une stratégie unique pour le trafic e-mail et web. Une syntaxe des expressions régulières et des dictionnaires communs garantissent une parfaite continuité lors de la création des règles de protection e-mail et web. Grâce à une gestion centralisée, les solutions McAfee DLP offrent une visibilité centralisée qui améliore l'efficacité des opérations et allège la charge administrative.

Surveillance de la messagerie électronique mobile

McAfee® DLP Prevent pour la messagerie électronique mobile offre une protection intelligente du contenu en interceptant les messages téléchargés sur les terminaux mobiles via le proxy ActiveSync à l'aide des fonctions DLP. En outre, il est capable d'intercepter les messages téléchargés via ActiveSync tant sur la solution Microsoft Exchange sur site que sur la plate-forme Microsoft Office 365 Hosted Exchange. Cette fonctionnalité est entièrement gérée à partir du logiciel McAfee ePO et incluse dans la licence McAfee DLP Prevent. Aucun agent ne doit être installé sur les équipements mobiles. Les entreprises peuvent ainsi surveiller les e-mails à des fins de conformité et de collecte de preuves, mais aussi protéger les équipements mobiles managés et non managés.

Mise en œuvre proactive de stratégies pour tous types d'informations

- Protection de plus de 300 types de contenus uniques
- Application de stratégies de protection pour les informations sensibles que vous connaissez et pour celles dont vous ignorez peut-être l'existence
- Évolutivité permettant la prise en charge de centaines de milliers de connexions simultanées

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

- Filtrage et contrôle des informations sensibles afin de protéger l'entreprise contre les risques cachés ou inconnus
- Indexation de tous types de contenus et mise en œuvre de stratégies de sécurisation granulaires
- Application de stratégies relatives à l'accès aux partages de fichiers internes afin d'empêcher les utilisateurs d'accéder à des informations ou référentiels sans autorisation

Intégration avec les serveurs proxy web et les MTA pour une protection renforcée

McAfee DLP Prevent s'intègre avec des serveurs proxy web (utilisant ICAP) et avec des MTA (utilisant des en-têtes X-header) pour exécuter les actions requises. Étant donné qu'elle met fin aux transactions non autorisées au niveau de la couche Application plutôt que de simplement provoquer l'abandon de la session TCP (ce qui ne modifie pas le comportement de l'application), la solution avertit l'application à l'origine de la transmission que cette dernière a été refusée en raison d'une violation de stratégie. McAfee DLP Prevent mémorise ainsi les éléments qui doivent être protégés et empêche l'application de reproduire un tel comportement, ce qui permet à l'entreprise de bénéficier d'une protection accrue.

Protection des informations sensibles, connues et inconnues

Capable de classer plus de 300 types de contenus différents, McAfee DLP Prevent vous aide à garantir la sécurité des informations dont vous connaissez le caractère confidentiel, telles que les numéros de sécurité sociale, les numéros de cartes de crédit et les données financières. En outre, la solution permet d'identifier les autres informations ou documents qui nécessitent une protection, par exemple les éléments de propriété intellectuelle complexes. McAfee DLP Prevent comprend un large éventail de stratégies prédéfinies, régissant notamment la conformité, l'utilisation acceptable ou encore la propriété intellectuelle. Celles-ci vous permettent de mettre en correspondance des documents entiers ou partiels avec un ensemble complet de règles, de façon à protéger la totalité de vos données sensibles, qu'elles soient connues ou inconnues.

Vues et rapports d'incidents personnalisables

Le logiciel McAfee ePO vous permet de personnaliser les vues synthétiques des incidents de sécurité et les actions subséquentes sur base de deux points de référence contextuels. L'affichage peut être détaillé, sous forme de liste ou synthétique avec des données de tendance. McAfee DLP Prevent propose également une multitude de rapports prédéfinis que vous pouvez consulter, enregistrer pour référence ultérieure ou générer de façon périodique.

Spécifications

Débit système

Jusqu'à 150 Mbit/s pour l'analyse, l'indexation et le stockage de la totalité du contenu

Intégration au réseau

Intégration au réseau sous la forme d'une appliance déployée hors du chemin réseau et active au sein du chemin de données à l'aide d'agents MTA et de serveurs proxy web compatibles ICAP

Types de contenus

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

- Documents Microsoft Office
- Fichiers multimédias
- Peer-to-peer
- Code source
- Fichiers de conception
- Archives
- Fichiers chiffrés

Classification des données complexes

McAfee DLP Prevent 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 qui constituent ensemble un moteur de classification pointu et extrêmement précis. Celui-ci bloque les informations sensibles et identifie 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 à mesure que les informations 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

Fonctionnalité d'investigation numérique et d'optimisation des stratégies

Une technologie de capture unique vous permet d'exploiter vos propres données historiques pour mettre en œuvre un déploiement beaucoup plus rapide et efficace. Fini de travailler sur de simples hypothèses, de tâtonner pendant de longs mois ou de perturber les activités. Les stratégies DLP (notamment en matière de classification) sont plus faciles à optimiser et vous bénéficiez d'une meilleure précision qui suit l'évolution de vos besoins métier. La technologie de capture peut également faciliter l'investigation numérique en servant d'enregistreur numérique et en reproduisant les incidents a posteriori pour une investigation approfondie. La technologie de capture est disponible soit sous forme d'environnement virtuel, soit sous forme de baie de stockage 2U de 16 To connectée à une appliance NDLP 6600 via un câble SAS.

Options de déploiement

McAfee DLP Prevent est disponible sous la forme d'une appliance matérielle ou virtuelle. Pour en savoir plus, consultez la **fiche technique de l'appliance matérielle McAfee DLP 6600**.

Protocoles pris en charge

Prise en charge des protocoles HTTP, HTTPS, FTP ainsi que de protocoles de messagerie instantanée vers des serveurs proxy compatibles avec ICAP. Renseignez-vous auprès de votre fournisseur de serveur proxy pour connaître les protocoles que celui-ci prend en charge. La solution prend également en charge SMTP par le biais de l'intégration avec des agents MTA.

Stratégies intégrées

- Large éventail de stratégies et de règles prédéfinies répondant aux besoins courants, notamment la conformité réglementaire, la protection de capital intellectuel et l'utilisation acceptable
- Possibilité de personnaliser intégralement les règles en fonction des besoins de l'entreprise, en tirant parti de la base de données de capture de McAfee

McAfee
Together is power.

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