



# McAfee Data Loss Prevention Monitor

## Protection des données critiques

### Principaux avantages

#### Identification et protection des données sensibles

- Identification rapide des informations sensibles via un moteur de recherche intuitif
- Investigations numériques permettant de mettre en corrélation les événements de risque passés et présents, de détecter les tendances des risques et d'identifier les menaces
- Création instantanée de règles pour bloquer certains comportements

#### Identification et indexation de l'ensemble du trafic réseau

- Filtrage et contrôle des informations sensibles afin d'identifier les risques cachés ou inconnus
- Indexation de tous types de contenus, puis interrogation et exploration des données pour déterminer leur niveau de sensibilité et leur destination
- Surveillance de l'accès aux partages de fichiers internes

À l'heure actuelle, toutes les entreprises doivent protéger les informations confidentielles de leurs clients et de leur personnel, qu'il s'agisse de numéros de carte de crédit, de numéros de sécurité sociale ou d'autres données personnelles. La divulgation accidentelle d'informations due à des erreurs commises par les employés et la perte d'ordinateurs portables ou de clés USB représentent des problèmes de sécurité pour pratiquement chaque entreprise. Pour ne rien arranger, les données peuvent être divulguées ou tomber dans de mauvaises mains lorsqu'elles sont transmises et partagées à l'aide d'applications web telles que Google Gmail, Yahoo! Mail, la messagerie instantanée et Facebook. McAfee® Data Loss Prevention (DLP) Monitor est une solution de prévention des fuites de données hautes performances, capable d'analyser toutes les communications Internet et de déterminer si des informations sont transférées vers des destinations inappropriées. Elle vous aide à minimiser la charge de travail de votre équipe de sécurité, à respecter les exigences en matière de conformité et à protéger votre propriété intellectuelle, de même que d'autres actifs stratégiques.

### Surveillance et suivi des données en mouvement, et génération de rapports connexes

Toute entreprise doit disposer de la visibilité nécessaire pour identifier avec précision les informations sensibles transférées, indépendamment de l'application, du protocole et du port qu'elles utilisent, et quelle que soit leur forme.

McAfee DLP Monitor permet de suivre en temps réel les données en mouvement à travers le réseau et de générer des rapports connexes.

Vous identifiez ainsi les données qui circulent entre les utilisateurs et l'extérieur, ainsi que la manière dont ce transfert se déroule. Appliance haute performance spécialisée, McAfee DLP Monitor détecte de façon unique plus de 300 types de contenus transitant par n'importe quel port ou employant n'importe quel protocole. Elle permet de déceler les menaces pour les données et de prendre les mesures nécessaires afin de protéger l'entreprise contre les fuites d'informations. En outre, au travers d'une fonction de notification des utilisateurs,

### Définition et optimisation de règles élaborées

- Identification de plus de 300 types de contenus uniques transmis via n'importe quels ports et applications
- Classification du trafic réseau indépendamment du port
- Évolutivité permettant la prise en charge de centaines de milliers de connexions simultanées

### Spécifications

#### Débit du système

- Classification du contenu à une vitesse allant jusqu'à 200 Mbit/s, sans échantillonnage

#### Intégration au réseau

- Intégration passive au réseau à l'aide d'un port SPAN ou d'un point de dérivation réseau physiquement en ligne (en option)

#### 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

McAfee DLP Monitor peut également servir d'outil de formation du personnel concernant les violations à l'origine de telles fuites, afin d'améliorer les comportements avec un minimum d'efforts.

### Recherche et analyse des informations en temps réel

Intégré au réseau via un port SPAN ou TAP, McAfee DLP Monitor balaie et analyse en temps réel le trafic réseau. Il met en correspondance des documents entiers ou partiels avec un ensemble de règles complet, constitué de plus de 150 règles prédéfinies régissant notamment la conformité, l'utilisation acceptable, la propriété intellectuelle et même la détection du plagiat. Toute anomalie au sein du trafic réseau, qu'il soit faible ou élevé, est ainsi identifiée.

### Découverte des risques méconnus

En conjuguant classification détaillée, indexation et stockage de l'ensemble du trafic réseau (et pas uniquement des informations correspondant à ses règles en temps réel), McAfee DLP Monitor vous permet d'exploiter rapidement des informations historiques pour identifier les données sensibles, déterminer comment et par qui elles sont utilisées, et suivre leurs transferts. Vous pouvez en outre réaliser une investigation granulaire et une inspection historique sur les informations afin de détecter les événements de risque et les risques de compromission qui n'ont peut-être pas été pris en compte auparavant. Déployée conjointement avec McAfee DLP Discover, la solution vous permet également d'identifier les emplacements de stockage des données sur le réseau et les propriétaires de ces données.

### Actions ciblées grâce aux rapports d'incidents

Une fois le trafic balayé, analysé et classé par son moteur de classification, McAfee DLP Monitor stocke les informations pertinentes dans une base de données propriétaire. À l'aide d'une interface de recherche intuitive, vous pouvez afficher des rapports complets sur vos données, leurs expéditeurs, leurs destinations et leur mode de transfert. En cas de fuite, vous pouvez déterminer où et comment celle-ci s'est produite et quelles informations sont concernées. Grâce à ces renseignements, vous pouvez éliminer les risques en prenant une série de mesures visant à garantir la conformité aux réglementations et à protéger les données sensibles.

### Classification de tous les types de données

McAfee DLP Monitor permet à votre entreprise d'analyser 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, ensemble, constituent un moteur de classification pointu et extrêmement précis. Celui-ci filtre les informations sensibles et effectue 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

## Fiche technique

### Protocoles pris en charge

- Toutes les transmissions sur n'importe quel protocole ou port utilisant TCP comme protocole de transport
- Gestionnaires de protocoles pour HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, etc.

### Stratégies intégrées

- Large éventail de stratégies et de règles prédéfinies répondant aux besoins courants, notamment la conformité réglementaire, la propriété intellectuelle 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

- **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

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 (AXRMM4)
Encombrement	Format 2U montable en rack



#### 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

Intel et les logos Intel et McAfee sont des marques commerciales d'Intel Corporation ou de McAfee, Inc. aux États-Unis et/ou dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs. Copyright © 2016 Intel Corporation. 568\_0716