McAfee Host Data Loss Prevention

Les scandales sur les fuites de données font la une des journaux : ne soyez pas la prochaine entreprise à défrayer la chronique

Des informations s'échappent-elles de votre société 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 le fait d'erreurs humaines ou de vols qualifiés, les fuites d'informations surviennent la plupart du temps via des canaux de diffusion courants (messagerie électronique, publication web, enregistrement sur clés USB, impression) et peuvent se solder par des pertes financières qui se chiffrent en millions.

Principaux avantages

Protection hors pair
- Contrôle des transferts de données en tout lieu : au travail, au domicile et lors des déplacements

Gestion complète des périphériques
- Surveillance et blocage de la copie des données confidentielles sur tout périphérique de stockage amovible, par un filtrage détaillé des données en fonction du contenu

Défense multiniveau
- Protection des données sur tous les postes clients, quels que soient les systèmes d'exploitation ou les types de périphériques

Gestion centralisée avec ePO
- Exploitation de votre plate-forme de gestion des risques de sécurité McAfee pour empêcher les fuites de données

Visibilité complète
- Démonstration de la conformité aux stratégies internes et aux réglementations officielles auprès des auditeurs, de la direction et des autres parties prenantes

Blocage proactif des fuites de données

Chaque jour, des sociétés telles que la vôtre sont la proie d'importantes fuites d'informations, qu'elles soient accidentelles ou malveillantes. D'après une étude récente, plus de 75 % des sociétés du classement Fortune 1000 ont subi ce type d'incident. Une autre étude a par ailleurs montré que plus de 55 % des employés sortent chaque semaine des données confidentielles de leur lieu de travail, par le biais de périphériques portables[1]. Pour une entreprise, la divulgation de données et l'application subséquente de mesures correctives sont extrêmement coûteuses. En 2008, le préjudice financier moyen s'est élevé à 6,65 millions de dollars[2].

Et s'il était possible d'empêcher facilement et efficacement les fuites d'informations ? Comment, en outre, gérer les problèmes de conformité aux réglementations sectorielles et officielles ? Une seule solution McAfee répond désormais à ces différents besoins : elle assure la surveillance, l'audit et la maîtrise des comportements d'utilisateur qui touchent aux données sensibles.

Protection et conformité

McAfee® Host Data Loss Prevention (Host DLP) vous garantit une visibilité et un contrôle absolus sur les transferts de vos données les plus sensibles. Il assure une surveillance instantanée de vos informations confidentielles afin de prévenir les fuites sur le lieu de travail, au domicile et en déplacement. Cette solution protège votre entreprise contre des risques tels que les dommages financiers, le préjudice porté à la marque, la perte de clientèle, le recul face à la concurrence ou encore la non-conformité.

Host DLP offre de nombreuses fonctions : surveillance instantanée et aisée des événements en temps réel, application de stratégies de sécurité gérées de façon centralisée afin de réglementer, voire de restreindre, l'utilisation et les transferts de données sensibles par le personnel, ou encore génération de rapports détaillés à des fins d'analyse port-mortem. Le tout sans perturber les activités de votre entreprise. Protégez cette dernière contre les vecteurs de fuite internes, comme la messagerie électronique ou instantanée, la gravure de CD, la publication web, la copie sur clé USB et l'impression. Empêchez en outre les fuites perpétrées par les chevaux de Troie, les vers ou les applications de partage de fichiers qui détournent l'identité des employés à leur insu.

Protection sans perturbation

Prévenez les pertes et fuites d'informations sans interrompre le cours normal des activités de l'entreprise, même lorsque les données sont modifiées, copiées, collées, compressées ou chiffrées. Protégez vos contenus grâce à une prise en charge étendue couvrant plus de 390 types de fichiers. Des algorithmes de contrôle d'empreintes uniques et des options de marquage de contenu (par emplacement, application, type de fichier, expressions régulières, mots clés, etc.) vous procurent le niveau de protection et la couverture étendue dont vous avez besoin pour mettre les données de votre entreprise parfaitement à l'abri.

Gestion simplifiée de la conformité

Une gestion simplifiée via la console McAfee ePolicy Orchestrator® (McAfee ePO™) permet de surveiller les événements et de collecter des données détaillées sur les incidents afin de démontrer la conformité aux stratégies internes et aux réglementations officielles auprès des auditeurs, du conseil d'administration et des autres parties prenantes. L'intégration de Host DLP avec ePO permet de recueillir des données d'utilisation critiques, notamment des éléments de preuve relatifs à l'expéditeur, au destinataire, aux données et à l'horodatage. La surveillance des événements et la création de rapports détaillés s'effectuent à l'aide d'un simple clic : il est aisé de produire les preuves de la conformité interne et réglementaire aux auditeurs, aux cadres supérieurs et à toute autre partie intéressée.

Des résultats tangibles : une protection des données inégalée

Vous disposez d'une visibilité et d'un contrôle absolus sur les transferts de données à partir des postes clients : jamais votre entreprise n'aura à subir de pertes sèches et à faire les gros titres pour des affaires de

1. Illuminas, étude 2007, « Threats Within Volume II: Data Loss Disaster » (La menace venue de l'intérieur, volume II — Les effets désastreux d'une fuite de données)
2. Ponemon Institute, étude 2008, « Cost of Data Breach » (Coût des divulgations de données)

Configuration système requise

Serveur ePO

Systèmes d'exploitation

- Microsoft® Server 2003 Service Pack 1, Release 2

Postes de travail et ordinateurs portables

Systèmes d'exploitation

- Microsoft Windows® XP Professionnel Service Pack 1 ou ultérieur
- Microsoft Windows 2000 avec Service Pack 4 ou ultérieur

Configuration matérielle requise

- Processeur : Pentium III 1 GHz ou plus puissant
- Mémoire RAM : 512 Mo recommandés
- Espace disque : 200 Mo au minimum
- Connexion réseau : TCP/IP pour l'accès à distance

fuites de données.Host DLP fait partie d'une solution totale de protection des données. Dans McAfee Total Protection™ for Data, il est couplé à McAfee Endpoint Encryption pour offrir une solution de protection des données encore plus complète.

Fonctionnalités

Protection hors pair

- Contrôlez l'accès aux données confidentielles, leur impression et leur envoi sur le réseau, via des applications et vers des périphériques de stockage. Protégez les données lors de leurs transferts quelle que soit l'application (messagerie électronique, web et instantanée ; communications Skype ; partage en réseau peer-to-peer), le type de transfert (HTTP, HTTPS, FTP ou Wi-Fi) ou le matériel (périphérique USB, lecteur CD ou DVD, imprimante, télécopieur, support de stockage amovible).
- Différentes options d'application de DLP :
  - » Surveiller (autoriser le transfert de données)
  - » Empêcher (bloquer le transfert de données)
  - » Avertir (signaler un événement aux administrateurs et aux utilisateurs finaux)
  - » Chiffrer (procéder au chiffrement avant le transfert de données)*
  - » Mettre en quarantaine (attendre l'autorisation)*

*Option incluse dans l'appliance McAfee Data Loss Prevention

Gestion complète des périphériques

- Contrôlez et bloquez la copie de données confidentielles sur des périphériques USB, des iPod et autres périphériques de stockage amovibles.
- Spécifiez et classez en catégorie les périphériques pouvant être utilisés par paramètre de périphérique Windows, tel que l'ID de produit, l'ID de fournisseur, le numéro de série, la classe de périphériques, le nom de périphérique, etc.

Défense multiniveau pour les postes clients

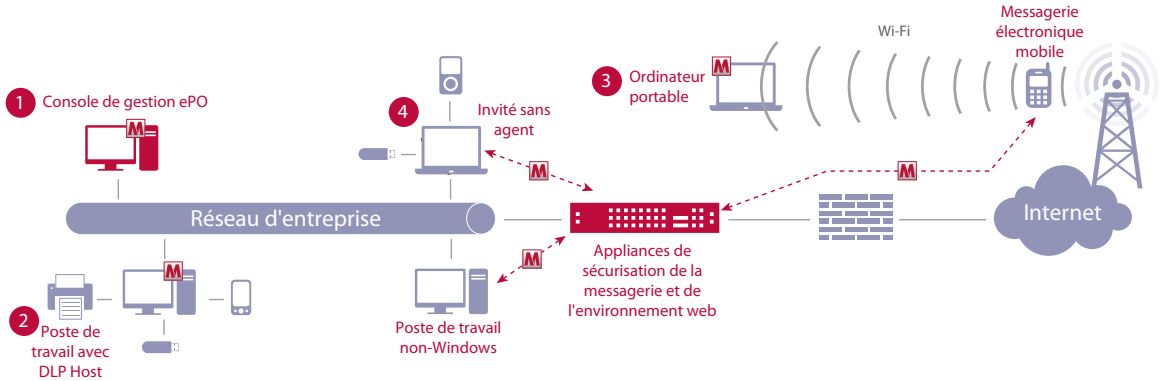
- La protection basée sur l'hôte bloque les fuites de données émanant des postes clients en assurant la surveillance et la prévention des comportements des utilisateurs susceptibles de constituer un risque pour vos données les plus sensibles.
- Allié à McAfee Endpoint Encryption, Host DLP offre une approche multiniveau complète en termes de prévention des fuites de données.

Gestion centralisée avec ePO

- Accédez à la fonction de surveillance des événements et aux stratégies centralisées de Host DLP via la console de gestion ePO.
- Utilisez ePO pour gérer les stratégies et surveiller les événements de manière centralisée.
- Déployez et mettez à jour les agents à partir d'ePO.
- L'intégration avec ePO 4.0 vous permet de bénéficier d'une gestion avancée via le Web et de fonctionnalités étendues d'audit et de génération de rapports.

Visibilité complète, sans effort

- Les fonctions complètes de surveillance et de génération de rapports sur les incidents de Host DLP vous permettent de collecter toutes les données nécessaires à des fins d'analyse et d'évaluation des risques, pour améliorer les procédures d'enquête et d'audit, mais aussi dans le cadre de la limitation des dommages. Parmi ces informations essentielles, citons entre autres ces divers éléments de preuve que sont l'expéditeur, le destinataire ou encore l'horodatage.



1 Console de gestion ePO — Centralisation des fonctions de gestion des stratégies, d'audit, de création de rapports et de distribution de logiciels. Garantit une adéquation optimale entre vos stratégies de sécurité et vos activités et processus métier.

2 Host DLP et Endpoint Encryption — Surveillance, génération de rapports, contrôle et prévention des comportements d'utilisateur susceptibles de poser un risque pour vos données. Le chiffrement puissant, certifié FIPS, de la totalité des disques ou de dossiers et fichiers individuels protège l'intégrité des données en cas de perte ou de vol.

3 Endpoint Encryption for Mobile — Création d'un espace chiffré (protégé) sur les équipements mobiles pour accueillir les données sensibles. Préserve l'intégrité et la confidentialité de ces données en cas de perte ou de vol de l'équipement.

4 Device Control et Endpoint Encryption — Contrôle des comportements d'utilisateur en relation avec les périphériques amovibles, tels que les clés USB ou les iPod, en vue de prévenir toute perte de données sensibles. Le chiffrement complet des disques rend l'équipement mobile inutilisable en cas de perte ou de vol.

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

9726ds_host-dlp_0710_fnl