

Trend Micro™

LeakProof™ 3.0

Protection complète des données confidentielles, qu'elles soient stockées, en cours d'utilisation ou en cours de transfert

La perte d'informations confidentielles et de propriété intellectuelle peut entraîner un risque d'amendes ou de litiges, nuire à l'image de marque de votre société ou susciter de mauvaises critiques dans la presse. Pour protéger leurs données confidentielles, les entreprises ont besoin d'une solution de prévention de fuites de données efficace contrôlant les éventuelles fuites d'information au niveau du point d'utilisation. L'affluence de systèmes de messagerie, de réseaux sans fil et de dispositifs de stockage USB ces derniers temps a cependant rendu difficile la protection des données d'entreprise à caractère confidentiel. En conséquence, les entreprises constatent une augmentation des cas de perte et de vol d'actifs de données subis par les employés ou sous-traitants, victimes de problèmes de fuites de données accidentelles ou liées à des activités malveillantes.

De plus, la conformité aux réglementations de direction d'entreprise et de protection de la confidentialité telles que les lois SB-1386, Gramm-Leach-Bliley (GLBA), EU Data Protection Directive (EU DPD), Sarbanes-Oxley et HIPAA exigent l'application de stratégies de sécurité complètes afin de protéger le secret des informations et la confidentialité des clients. Pour répondre à ces critères, les entreprises ont besoin de solutions de filtrage de contenu intelligentes qui appliquent les stratégies de sécurité et informent les employés sur les méthodes appropriées de traitement des informations.

Trend Micro™ LeakProof™ empêche les fuites de données grâce à une approche unique combinant une application de la protection au niveau des points finaux à une technologie d'empreinte digitale haute précision et une méthode de correspondance de contenus. La solution LeakProof complète se compose d'un client logiciel et d'une appliance :

- **LeakProof Anti-Leak Client** : inclut un logiciel de contrôle et d'application non intrusif puissant qui détecte et empêche les fuites de données au niveau de chaque point final. Le client communique avec l'appliance DataDNA™ Server afin de recevoir des mises à jour de stratégies et d'empreintes digitales et de signaler au serveur les cas de violation de sécurité.
- **LeakProof DataDNA™ Server** : appliance constituant un point central pour la visibilité, la définition de stratégies et l'extraction d'empreintes digitales depuis des sources de contenu. Une interface Web prend en charge un flux de travail administratif pour effectuer des tâches de détection, classification, définition de stratégies, surveillance et génération de rapports.

PROTECTION COMPLÈTE : DONNÉES, PORTS, CANAUX, RÉSEAUX

LeakProof offre la plus large couverture disponible pour le périmètre du réseau et les points finaux. Cette couverture inclut les canaux de réseau comme HTTP/S, SMTP, Webmail, FTP et les messageries instantanées, de même que les entrées/sorties au niveau des points finaux tels que les transferts de fichiers vers des pilotes USB ou des graveurs de CD/DVD. Des modules de filtrage intégrés inspectent le contenu avant que celui-ci soit chiffré afin de protéger les activités menées via le navigateur Web et les applications de messagerie. Les responsables de ressources informatiques peuvent facilement désactiver des dispositifs spécifiques.

DÉTECTION PRÉCISE GRÂCE À LA TECHNOLOGIE DATADNA™

Cette technologie en cours d'homologation détecte les données confidentielles avec une précision et des performances d'un niveau optimal. Plusieurs moteurs de correspondance fournissent un filtrage en temps réel à l'aide de méthodes d'empreintes digitales, d'expressions rationnelles, de mots de passe et de métadonnées. Des algorithmes puissants extraient des informations à partir des contenus pour créer une séquence d'ADN unique ou « empreinte digitale » pour chaque document. Cette « empreinte digitale » permet une application de la protection au niveau des points finaux, en ligne ou hors connexion.

NOUVEAU ! MOYENS INTERACTIFS POUR INFORMER LES EMPLOYÉS, CHIFFREMENT ET FLUX DE TRAVAIL

Des « alertes » interactives permettent aux responsables de ressources informatiques de définir des boîtes de dialogue sensibles s'affichant directement sur l'écran d'ordinateur de l'employé. Ces boîtes de dialogue contiennent des liens URL personnalisés dont le but est d'informer les employés sur les méthodes appropriées de traitement des informations confidentielles. Les transferts non autorisés sont bloqués, ou les employés peuvent être amenés à utiliser le module intégré de chiffrement des données pour copier des données sur des dispositifs USB.

DÉTECTION DE DONNÉES ET SCANS DE SÉCURITÉ

Grâce à un système de surveillance en continu, LeakProof™ propose aux agents préposés aux réglementations de sécurité de l'entreprise et de conformité une option comparable au fonctionnement d'un radar permettant de localiser les informations à caractère confidentiel et de diminuer le risque de vol de données. LeakProof détecte les informations dont la divulgation n'est pas autorisée résidant au niveau des points finaux, y compris les ordinateurs portables, postes de travail et serveurs.

PRÉVENTION DES FUITES DE DONNÉES

- À l'échelle mobile, locale et de l'entreprise
- Points finaux, en ligne et hors connexion
- Réseaux d'entreprise
- Réseaux publics
- USB, Réseaux Bluetooth, WiFi, messageries électroniques
- Données stockées, en cours d'utilisation ou en cours de transfert

PROTECTION CONTRE LES MENACES

- Fuites de données
- Perte de données
- Menaces internes

PRINCIPAUX AVANTAGES

- **Protection de la confidentialité** : surveille et empêche une utilisation inappropriée des informations de clients et d'employés
- **Protection de la propriété intellectuelle** : détecte, classe et protège les actifs essentiels de l'entreprise
- **Conformité aux réglementations sur la confidentialité** : surveille l'utilisation, scanne les points finaux et informe les employés afin de réduire les risques
- **Annonces aux employés** : boîtes de dialogue interactives personnalisées pour informer les employés et maintenir le flux de travail
- **Détection des données confidentielles** : recherche les données confidentielles sur les ordinateurs portables, postes de travail et serveurs

« Trend Micro LeakProof™ offre aux administrateurs un meilleur contrôle des activités informatiques autorisées et non autorisées des employés, et ce, par l'intermédiaire de boîtes de dialogue interactives à caractère informatif et utile pour résoudre les problèmes de sécurité ».

Martin Hodgett, Responsable des technologies de l'information
Orchard Supply Hardware (OSH)

RÉCAPITULATIF DES CARACTÉRISTIQUES DE LA SOLUTION DE PRÉVENTION DES FUITES DE DONNÉES LEAKPROOF

Correspondance des informations confidentielles

- Méthodes de correspondance via empreintes digitales, expressions rationnelles, mots-clés et métadonnées
- Données structurées et non structurées
- Correspondance partielle de fichiers texte et correspondance exacte de fichiers binaires
- Fonctionne indépendamment de la langue

Stratégies de sécurité granulaires

- Journalisation, alertes côté serveur, alertes côté client, blocage, chiffrement, justification
- Stratégies distinctes pour les cas de violation en ligne et hors connexion
- Stratégies de sécurité basées sur des groupes et domaines de points finaux
- Limites de sécurité configurables : réseaux locaux, ordinateurs personnels, domaines de messagerie sécurisés/non sécurisés

Étude et gestion de la topologie des points finaux

- Détection des ordinateurs de points finaux d'entreprise
- Affichage en temps réel sous forme de carte de l'état des points finaux
- Surveillance et administration centralisées de l'état des clients
- Affichage détaillé de l'état des points finaux
- Détection de dispositifs d'entrée/sortie non autorisés au niveau des points finaux

Contrôle des dispositifs et des applications

- Contrôle de tous les dispositifs d'entrée/sortie : USB, CD/DVD, disquettes, Bluetooth, IrDA, dispositifs d'imagerie, port de communication et port LPT, etc.
- Blocage de la fonction Impr. écran

Surveillance et génération de rapports

- Rapports en temps réel de cas de violation de sécurité et tableau de bord par points finaux, utilisateurs, etc.
- Analyse des tendances et rupture de chaîne de violations
- Rapports programmés et à la demande relatifs aux violations de sécurité
- Une fonction facultative de capture d'expertise permet de consigner sur le serveur DataDNA le fichier de violation de sécurité en lui-même, lequel fichier vous pourrez consulter par la suite.

Modèles de conformité

- Classifications préconfigurées et stratégies assurant la conformité aux réglementations, telles que PCI, GLBA, SB-1386 et SOX
- Règles intégrées avec modules de validation pour les entités telles que les informations de sécurité sociale, numéros de carte de crédit, routage ABA, cartes d'identités nationales canadiennes et chinoises et reconnaissance de noms américains.

Administration système et évolutivité

- Interface de gestion de navigateur Web
- Administration à base de rôles et contrôle de l'accès aux contenus confidentiels
- Intégration à LDAP et Active Directory
- Regroupement de serveurs d'administration pour une meilleure évolutivité à l'échelle de l'entreprise
- Communication sécurisée entre le point final et le serveur via SSL

CONFIGURATION MINIMALE REQUISE

Logiciel LeakProof Anti-Leak Client

- **Plates-formes prises en charge** : Microsoft Vista, Windows XP, Windows 2000, Windows 2003 Server

Appliance LeakProof DataDNA Server

- Appliance 1U spécifique pouvant être montée en rack
- Sécurité renforcée
- Carte NIC d'1 Go
- Processeur simple ou double cœur
- Mémoire : 2 Go/4 Go
- Stockage : 160 Go/300 Go RAID

COUVERTURE COMPLÈTE DES TYPES DE FICHIERS, APPLICATIONS ET DISPOSITIFS



LeakProof DataDNA Server

L'appliance LeakProof DataDNA Server fonctionne en parallèle avec le logiciel LeakProof Anti-Leak Client afin de protéger les actifs d'informations confidentielles contre la perte de données, le vol de données et les menaces internes.

Types de fichiers pris en charge

- Reconnaît et traite plus de 300 types de fichiers
- Fichiers Microsoft™ Office, y compris Office 2007 : Microsoft Word, Excel, PowerPoint, messagerie Outlook™ Lotus™ 1-2-3, OpenOffice, RTF, Wordpad, Text, etc.
- Fichiers graphiques : Visio, Postscript, PDF, TIFF, etc.
- Fichiers logiciels/de programmation : C/C++, JAVA, Verilog, AutoCAD, etc.
- Fichiers archivés/compressés : Win ZIP, RAR, TAR, JAR, ARJ, 7Z, RPM, CPIO, GZIP, BZIP2, Unix/Linux ZIP, LZH, etc.

Réseaux/applications contrôlés

- Messagerie : Microsoft Outlook, Lotus Notes et messagerie SMTP
- Courrier Internet : MSN/Hotmail, Yahoo, GMail, AOL Mail, etc.
- Messagerie instantanée : MSN, AIM, Yahoo, etc.
- Protocoles de réseau : FTP, HTTP/HTTPS et SMTP

Dispositifs de point final contrôlés

- USB, SCSI, (S)ATA, EIDE, PCMCIA, CD/DVD, disquettes, réseaux Bluetooth, IrDA, WiFi, imprimantes, dispositifs d'imagerie port de communication, port LPT, etc.



Trend Micro, le logo t-ball de Trend Micro, DataDNA et LeakProof sont des marques commerciales ou des marques déposées de Trend Micro, Incorporated. Tous les autres noms de produit ou de société peuvent être des marques commerciales ou des marques déposées de leurs propriétaires.
[DS05_TMLP_071203FR]