

Les solutions de sécurité Cisco IronPort intègrent la technologie RSA de prévention des fuites de données (DLP)

Les services et les technologies e-mail, Web et DLP de l'éditeur offrent une solution complète pour prévenir la fuite de données

Issy-les-Moulineaux, 26 juin 2009 - Alors que le travail collaboratif, le « cloud computing » et la mobilité modifient le mode de fonctionnement des entreprises, Cisco IronPort annonce de nouvelles solutions complètes, fiables et simples d'utilisation pour assurer la sécurité des données en circulation. Cisco IronPort aide ainsi les entreprises à protéger les données sensibles de leurs clients et employés, à se conformer aux réglementations et à sauvegarder leur image de marque.

L'éditeur lance de nouvelles fonctions de prévention des fuites de données (DLP) qui s'intègrent de manière transparente dans les produits de sécurisation de messagerie Cisco IronPort.

En parallèle, Cisco IronPort annonce aussi des fonctionnalités permettant de détecter et d'éviter la fuite de données sensibles lors des transferts Web et FTP, avec sa passerelle de sécurité web IronPort.

Enfin, pour les entreprises désireuses d'évaluer leur vulnérabilité aux fuites de données, Cisco IronPort lance un nouveau service de sécurité facilitant la mise en place d'une stratégie de prévention.

Contexte/Nouvelles offres

Les entreprises ont besoin d'une sécurité robuste intégrée au réseau de façon à pouvoir collaborer en toute confiance. Cette annonce apporte ainsi une réponse aux risques de fuite de données inhérents aux communications par e-mail et via le Web.

A l'automne 2008, Cisco IronPort a en effet présenté les résultats d'une étude mondiale de sécurité sur les fuites de données. Celle-ci révèle notamment que la fuite de données par e-mail vient en tête des préoccupations des professionnels de l'informatique, tandis que 70% d'entre eux déclarent que l'accès des employés à des applications et sites Web 2.0 non autorisés (réseaux sociaux, logiciels de téléchargement musical, sites de commerce en ligne) est à l'origine de la moitié des fuites de données de leur entreprise.

Les outils de sécurité e-mail Cisco IronPort intègrent la technologie RSA de prévention des fuites de données ? Cisco IronPort enrichit la plateforme de gestion de règles, d'analyse hautes performances et de reporting des passerelles de sécurité E-Mail en y intégrant la technologie DLP de RSA, la division sécurité d'EMC.

La solution Email DLP de Cisco IronPort, qui incorpore les règles et fonctions de classification de contenu RSA DLP, est disponible sous la forme d'un abonnement logiciel entièrement intégré aux produits et services de sécurisation de messagerie Cisco IronPort.

Cette solution jointe offre un filtre de contenu fiable et simple permettant de détecter les données sensibles avant qu'elles ne sortent de l'entreprise. Plus d'une centaine de règles globales prédéfinies, dont la maintenance et la mise à jour sont assurées par l'équipe de cognitivistes de RSA, alliées au moteur d'analyse de contenu de Cisco IronPort ainsi qu'à un workflow simple pour la gestion des violations et à des capacités de

reporting et d'audit, fait d'Email DLP une solution complète pour la prévention des fuites de données par e-mail.

Grâce à ce partenariat, les administrateurs de messagerie peuvent déployer une technologie DLP de pointe dans une appliance totalement intégrée sans recourir à des consoles, produits ou services externes.

En outre, la solution peut être facilement étendue à la protection des données au repos ou en cours d'utilisation par l'intégration avec le produit RSA Enterprise Manager. En associant la fonctionnalité DLP à ses propres capacités anti-spam, anti-virus et de chiffrement, Cisco IronPort procure à ses clients une solution complète pour le contrôle et la sécurité des messages entrants et sortants.

Cisco IronPort S-Series avec fonction DLP

Les appliances de sécurité web Cisco IronPort applique des règles de sécurisation des données pour les transferts de contenu effectués par les utilisateurs via des canaux tels que les webmails, blogs et réseaux sociaux ou encore les sites FTP.

La fonction Onbox Data Security offre des contrôles simples et de bon sens qui sont rapides et faciles à mettre en œuvre, tandis que l'intégration avec des produits DLP tiers permet une analyse de contenu et une application de règles évoluées.

En complément de la protection contre les fuites de données résultant des actions des utilisateurs, les filtres Cisco IronPort Web Reputation Filters, le moteur Cisco IronPort DVS (Dynamic Vectoring & Streaming) et le moniteur de trafic de niveau 4 opèrent ensemble pour interdire l'entrée du réseau aux codes malveillants (malware) destinés au vol de données, tout en bloquant les connexions extérieures générées par d'éventuels malwares déjà infiltrés.

Service Cisco IronPort d'évaluation des risques DLP

Ces services professionnels aident les entreprises à évaluer leur vulnérabilité aux fuites de données et à concevoir des stratégies de prévention en la matière, en mettant en adéquation les ressources humaines, les processus et les technologies.

Ces services comprennent trois phases :

- l'examen des règles, processus et besoins en matière de prévention des fuites de données;
- l'état des lieux dans ce domaine ;
- et enfin l'analyse des données et la formulation de recommandations.

Cette prestation aide les entreprises à satisfaire leurs obligations réglementaires, sectorielles et environnementales en identifiant les écarts spécifiques entre les capacités DLP désirées ou requises et leur situation réelle.

Tarification et disponibilité des services

Cisco IronPort S-Series avec DLP, ainsi que les services Cisco IronPort Data Loss Prevention sont disponibles dès à présent. Cisco IronPort C-Series avec DLP sera disponible à partir de la fin de l'année 2009. Pour plus d'informations : <http://www.cisco.com/go/dlp>

Le service Cisco IronPort d'évaluation des risques DLP est disponible dès à présent auprès de Cisco, IronPort et des partenaires Cisco IronPort certifiés. Pour plus d'information contactez votre représentant Cisco IronPort et visitez le site www.cisco.com/go/services/security

Citation

Sébastien Commérot, Responsable Marketing Europe du Sud, Moyen-Orient et Afrique, chez Cisco IronPort :

« La prévention des fuites de données revêt un caractère essentiel pour nos clients. Aujourd'hui, nous proposons des solutions fiables et intuitives pour la surveillance du trafic et la prévention des fuites de données là où cela est le plus critique, dans les échanges par e-mail et sur le Web. Ces solutions donnent immédiatement à nos clients une longueur d'avance pour réduire leurs risques de fuite de données. Nous sommes ravis d'avoir noué un partenariat avec RSA dans le cadre de notre solution Email DLP et pensons que Cisco IronPort est dans une position unique pour offrir une solution complète de prévention des fuites de données en circulation sur le réseau. »

A propos de Cisco Systems

Cisco (NASDAQ: CSCO) est le leader mondial des technologies réseaux qui transforment la façon dont les gens communiquent, se connectent et travaillent ensemble. Vous trouverez davantage de renseignements sur Cisco à <http://www.cisco.com>. Pour des informations en continu, rendez-vous sur <http://newsroom.cisco.com>.

Cisco, le logo Cisco Systems et Cisco Capital sont des marques déposées ou des marques commerciales de Cisco Systems, Inc. et/ou de ses filiales aux Etats-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document appartiennent à leurs propriétaires respectifs. L'emploi du mot « partenaire » n'implique pas l'existence d'une relation de partenariat entre Cisco et une autre société. Le présent document contient des informations publiques de Cisco.