

Proofpoint, Nouvelle plate-forme de sécurisation des e-mails

Sécurité

Posté par : JulieM

Publié le : 10/11/2009 0:00:00

Proofpoint Inc., le leader des solutions de prévention des pertes de données et de sécurisation unifiée des messageries, présente **Proofpoint 6**, sa nouvelle plateforme de **sécurisation des e-mails et de prévention des pertes de données**, disponible sous forme de SaaS.

Proofpoint 6 est composé de Proofpoint Encryption, une nouvelle solution simple d'emploi pour le chiffrement des e-mails, qui améliore les échanges au sein du workflow, qui est dotée

d'une compatibilité accrue avec l'authentification des e-mails par DKIM (DomainKeys Identified Mail) et qui est complétée par plusieurs fonctions innovantes d'administration.

Proofpoint Encryption : chiffrement des e-mails en fonction de la politique de sécurité en mode SaaS



proofpoint

La nouvelle plate-forme de sécurisation des e-mails de Proofpoint intègre des fonctions de prévention des pertes de données et de chiffrement des e-mails, effectués par le nouveau module Proofpoint Encryption et le Proofpoint Hosted Key Service. Cette solution de chiffrement est désormais intégrée à la suite Proofpoint ENTERPRISE Privacy. Elle peut être déployée dans le cadre de l'offre SaaS Proofpoint on Demand, ou sur site sous forme virtuelle ou en mode logiciel classique.

Les règles de chiffrement sont gérées et appliquées au niveau de l'entreprise à partir d'un emplacement central, via l'interface d'administration de Proofpoint. Une fois définies, ces règles sont appliquées automatiquement au niveau de la passerelle, éliminant tout risque d'erreur au niveau des utilisateurs. Ces règles peuvent être extrêmement fines et être déclenchées par n'importe **quelle combinaison des éléments suivants** :

Une correspondance de données structurées : par exemple des informations médicales ou financières confidentielles telles que des codes HIPAA, numéros de routage ABA, numéros de cartes bancaires nationales et internationales, numéros de sécurité sociale des États-Unis, numéros de carte d'identité britannique et autres éléments d'identification détectés par le module Proofpoint Regulatory Compliance.

Une correspondance de données non structurées : par exemple la présence d'informations confidentielles détectées par le module Digital Asset Security.

• Des mots clés : (ou des expressions rationnelles ou des correspondances pondérées dans un dictionnaire) identifiés dans l'objet ou le contenu des messages.

• L'origine ou la destination du message : le chiffrement étant déclenché en fonction du destinataire (un partenaire ou un fournisseur donné), de l'expéditeur ou d'autres attributs structurels.

Tarif et disponibilité

[La plate-forme Proofpoint 6](#), le module Proofpoint Encryption et les suites ENTERPRISE Protection et Proofpoint ENTERPRISE Privacy seront disponibles en novembre 2009. Proofpoint

ENTERPRISE Privacy (avec Proofpoint Encryption) est proposé à moins de 17 dollars par utilisateur et par an, pour des organisations avec 5 000 à 10 000 comptes de messagerie.