Communiqué de presse
Paris, le 4 Novembre 2009

Proofpoint présente sa nouvelle plate-forme de sécurisation des e-mails et de respect de la confidentialité, avec fonction de cryptage, disponible via SaaS et en format classique

Proofpoint 6 propose des fonctions simples d'emploi « Defense in Depth » pour prévenir les pertes de données, avec chiffrement intégré, authentification DKIM des e-mails et améliorations de l'administration des systèmes.

Proofpoint Inc. (http://www.proofpoint.com), le leader des solutions de prévention des pertes de données et de sécurisation unifiée des messageries, présente Proofpoint 6, sa nouvelle plate-forme de sécurisation des e-mails et de prévention des pertes de données, disponible sous forme de SaaS.
Proofpoint 6 est composée 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 doté 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.

« *Pour protéger totalement les données privées contenues dans les e-mails, il faut non seulement détecter avec exactitude la présence d'informations confidentielles et empêcher leur fuite, mais aussi pouvoir chiffrer automatiquement les contenus sensibles* », déclare Peter Galvin, directeur marketing de Proofpoint. « *Avec Proofpoint, le chiffrement se fait en fonction de règles. Il sécurise les données confidentielles dans les e-mails, garantissant leur intégrité ainsi que le respect des réglementations des secteurs de la santé et des finances. Il participe également à éviter les dépenses importantes liées aux notifications des fuites de données et à leur règlement.* »

Proofpoint 6 diminue la complexité des environnements de messagerie électronique, en combinant l'action d'un antispam et d'un antivirus pour les emails entrants et en permettant de prévenir des pertes de données via les emails sortants. Cette solution assure un chiffrement des e-mails grâce à l'application de règles internes, le tout dans une même plate-forme de contrôle abordable, simple à utiliser et à gérer.

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

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, effectuées 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.

« *En tant que sous-traitant de services de ressources humaines, nous devons échanger des informations confidentielles par e-mail avec nos clients, nos partenaires et les utilisateurs* », déclare Jeff Caracci, vice-président informatique chez Merit Resources. « *Nous recherchions une solution efficace pour que nos administrateurs et notre personnel puissent travailler avec les e-mails en toute sécurité, sans pour autant alourdir leurs tâches. Proofpoint Encryption répond parfaitement à nos besoins. Il est simple à installer et simple à utiliser pour envoyer des e-mails en toute sécurité et dans le respect des réglementations. Et nos administrateurs sont ravis que le système demande si peu de maintenance.* »

Proofpoint Encryption apporte un chiffrement des e-mails simple à gérer et à utiliser, à la portée de tous les expéditeurs, destinataires et administrateurs. 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'émetteur ou d'autres attributs structurels.

Basé sur un algorithme à clef secrète (qui utilise le chiffrement fort AES-256), Proofpoint Encryption élimine les difficultés généralement associées aux solutions de chiffrement au niveau de l'administration et des utilisateurs. La gestion des clés est en effet l'une des principales difficultés de ce genre de solution. Proofpoint Encryption élimine les opérations de gestion, de sauvegarde et d'administration des clés, grâce à Proofpoint Hosted Key Service™. Celui-ci utilise l'infrastructure SaaS Proofpoint on Demand™ pour assurer des fonctions de stockage de clés totalement redondantes, sécurisées, efficaces et hautement disponibles.

L'association de Proofpoint Encryption et du Proofpoint Hosted Key Service autorise un contrôle extrêmement fin du chiffrement, au niveau de chaque message. Par exemple, un message adressé à un destinataire donné peut être refusé sans aucune conséquence sur les autres utilisateurs ou les autres messages adressés au même destinataire.

Le reporting intégré apporte aux administrateurs une visibilité complète sur les tendances globales de chiffrement des messages complétée par une visibilité pour chacune des règles.

Proofpoint Encryption est tout aussi sûr et facile d'emploi pour les destinataires des e-mails. Il envoie les messages chiffrés par push aux destinataires, lesquels peuvent les déchiffrer en suivant un lien (inclus avec l'e-mail chiffré) vers Web Proofpoint Secure Reader™.

Quelle que soit la configuration de Proofpoint Encryption (en SaaS ou sur serveur Proofpoint), les messages sont déchiffrés par une système isolé de Proofpoint Secure Reader, hébergé dans au sein du service Proofpoint on Demand pour le client ou sur le serveur Proofpoint Messaging Security Gateway™ du client.

« *Le chiffrement des e-mails est devenu une nécessité commerciale et légale pour la plupart des entreprises et des organismes publics, à cause de la quantité croissante de données sensibles envoyées et conservées dans les e-mails, de l'augmentation des exigences en gouvernance et des conséquences coûteuses des fuites de données* », déclare Michael Osterman, directeur d'Osterman Research. « *Proofpoint Encryption apporte de solides fonctions de chiffrement des e-mails en fonction de règles, qui peuvent faciliter la protection des informations confidentielles et le respect des réglementations.* »

Améliorations de la sécurité et du workflow de prévention des pertes de données

Proofpoint 6 s'appuie sur les fonctions de Proofpoint 5.5 en matière de workflow, de gestion et de résolution des incidents de fuites de données, et les renforce pour améliorer la sécurité des messages placés en quarantaine.

Lorsqu'un message est placé en quarantaine en vue d'un examen ultérieur, les diverses infractions aux règles peuvent imposer de restreindre la vérification de certains types de contenus à certains administrateurs, responsables de la conformité ou autres utilisateurs. Dans ce contexte, de nouvelles fonctions de contrôle d'accès au niveau des dossiers apportent un contrôle plus fin sur les utilisateurs autorisés à consulter, vérifier, commenter et suivre les infractions aux règles en sortie.

Compatibilité élargie avec les standards d'authentification des e-mails

Proofpoint 6 ajoute la signature DKIM aux messages sortants pour lutter contre la falsification des adresses e-mail (par exemple l'utilisation d'en-têtes d'e-mail contrefaits dans les attaques de phishing). L'authentification DKIM consiste à apposer une signature numérique à chaque message sortant de l'entreprise, de sorte que le serveur de messagerie du destinataire (s'il gère la validation DKIM) peut s'assurer que le message provient réellement de cette entreprise et n'est pas une tentative de phishing.

Comme dans les versions précédentes, Proofpoint 6 accepte également le standard SPF (Sender Policy Framework) d'authentification de l'expéditeur. Chaque message entrant peut être vérifié par rapport aux enregistrements SPF, et déclencher en cas d'échec ou de réussite des règles configurées à l'avance pour les mesures à prendre.

Améliorations au niveau du moteur de règles et de l'administration

Dans le cas d'une entreprise qui gère un grand nombre de domaines, Proofpoint 6 apporte de nouvelles fonctionnalités d'administration pour configurer et appliquer aisément les règles de messagerie en fonction du domaine de l'utilisateur. On peut créer manuellement ou automatiquement des groupes de domaines, et appliquer des règles données aux messages provenant ou à destination de ces domaines.

Proofpoint 6 simplifie la personnalisation de toutes les interfaces utilisateur, notamment celle du résumé des e-mails, de l'accès Web et de Proofpoint Secure Reader. Dans l'interface d'administration de Proofpoint, l'administrateur de la messagerie utilise le pointer-cliquer pour personnaliser les interfaces avec une grande facilité.

Proofpoint 6 apporte également davantage de finesse dans la gestion des messages entrants adressés à plusieurs destinataires. Grâce à la nouvelle fonction « envelope splitting », chaque message peut être traité en fonction de règles différentes pour chaque utilisateur, ce qui améliore le contrôle sur la distribution.

Proofpoint continue de proposer des solutions de sécurité de la messagerie qui demandent un minimum d'administration et de maintenance. Proofpoint 6 rend les mises à jour et les mises à niveau encore plus faciles, apportant davantage d'informations sur le processus et réduisant la durée de l'indisponibilité.

Des solutions classiques ou en SaaS pour simplifier la sécurité de la messagerie

Les nouvelles fonctionnalités de Proofpoint 6 seront disponibles simultanément pour les services SaaS (Proofpoint on Demand™) et pour serveurs (Proofpoint Messaging Security Gateway™). Avec le lancement de Proofpoint 6, la solution phare de sécurité de la messagerie de Proofpoint, Proofpoint ENTERPRISE™ est également proposée à la demande et sur site, sous forme de deux nouvelles suites qui répondent aux besoins les plus courants de protection et de prévention des pertes de données :

- **Proofpoint ENTERPRISE Protection,** qui apporte la totalité des composants Proofpoint de sécurisation et d'administration des e-mail entrants, avec les fonctionnalités suivantes : gestion avancée de la connexion, détection du spam avec Proofpoint MLX™, protection antivirus zero-hour et via des fichiers de signature, pare-feu de messagerie, inspection approfondie des contenus et filtrage en sortie pour appliquer des règles d'utilisation acceptable pour les contenus et les pièces jointes, traçage avancé des messages et chiffrement TLS.

- **Proofpoint ENTERPRISE Privacy,** est destinée aux entreprises qui ont des besoins sophistiqués en matière de conformité aux réglementations et de confidentialité des données. Cette suite assure une protection approfondie « defense in depth » des informations confidentielles de tous types. Elle protège ces informations dans les e-mails, évite les fuites d'informations confidentielles et garantit la conformité aux réglementations courantes de protection des données, telles que HIPAA, GLBA et PCI. Proofpoint ENTERPRISE Privacy intègre maintenant les puissantes fonctions de chiffrement de Proofpoint Encryption, apportant le maximum de contrôle et de souplesse pour la prévention des pertes de données. Ce chiffrement est appliqué automatiquement en fonction des règles internes, limitant les risques d'infractions aux réglementations et à la politique de sécurité de l'entreprise.

  Les fonctionnalités sont les suivantes : détection performante et très précise des informations privées ou confidentielles dans les données structurées et non structurées, application de règles préconfigurées de protection des données, console d'administration simple à utiliser, chiffrement intégré des e-mails en fonction des règles, et gestion solide des incidents.

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.

À propos de Proofpoint Inc.
Proofpoint sécurise et améliore l'infrastructure de messagerie électronique des entreprises, grâce à des solutions de sécurité, d'archivage et de chiffrement des e-mails, et de prévention des pertes de données. Ces solutions protègent contre le spam et les virus, évitent les fuites d'informations privées et confidentielles, chiffrent les e-mails sensibles et archivent les messages pour simplifier la gestion des boîtes de courrier et répondre aux réglementations en matière de conservation et de e-discovery. Les solutions Proofpoint peuvent être déployées à la demande (modèle SaaS), sur site par des appareils autonomes, ou dans le cadre d'une architecture hybride SaaS-appareils, apportant ainsi le maximum de souplesse et d'évolutivité. Pour plus d'informations, veuillez consulter le site http://www.proofpoint.com.

# # #

Proofpoint est une marque déposée de Proofpoint Inc. Proofpoint on Demand, Proofpoint ENTERPRISE, Proofpoint Encryption, Proofpoint MLX et Proofpoint Messaging Security Gateway sont des marques de Proofpoint Inc. Toutes les autres marques citées ici appartiennent à leurs propriétaires respectifs.