Proofpoint Adaptive Email DLP

Bloquez les fuites de données sensibles en renforçant la DLP basée sur des règles grâce à l'IA

Principaux avantages

- Prévention des fuites de données accidentelles et intentionnelles par email
- Réduction des risques d'atteinte à la réputation et d'attrition des clients
- Réduction des amendes engendrées par des infractions au RGPD et à la loi CCPA
- Amélioration de la sensibilisation à la sécurité informatique dans l'ensemble de l'entreprise

Malgré les contrôles de prévention des fuites de données par email (DLP) existants, les « données envoyées par email à la mauvaise personne » constituent le principal type de violation de données signalé en vertu du RGPD. Si la DLP basée sur des règles joue un rôle essentiel dans la protection des données sensibles connues telles que les données personnelles, les numéros de sécurité sociale et les données de carte de paiement, elle ne détecte pas tous les risques. C'est notamment le cas des données sensibles envoyées à la mauvaise personne et des collaborateurs qui exfiltrent des données vers eux-mêmes et d'autres destinataires non autorisés.

Proofpoint Adaptive Email DLP s'appuie sur l'IA comportementale pour identifier les comportements normaux de vos collaborateurs en matière d'envoi d'emails, leurs relations de confiance et la façon dont ils communiquent des données sensibles. Il analyse ensuite chaque email pour détecter les comportements anormaux et informe les administrateurs des fuites de données potentielles. Il avertit l'utilisateur en temps réel et prévient les fuites de données sensibles par email.

Blocage des emails envoyés au mauvais destinataire

Il peut arriver qu'un utilisateur envoie accidentellement un email à la mauvaise personne. Il s'agit d'une source courante de compromissions des données dans toutes les entreprises. Ce problème est difficile à résoudre au moyen d'approches basées sur des règles.

Proofpoint Adaptive Email DLP peut bloquer ces compromissions. Il s'appuie sur des graphiques relationnels, une inspection approfondie du contenu et une analyse comportementale pour comprendre les comportements habituels des collaborateurs et identifier les fuites de données. Les données sensibles de votre entreprise sont donc protégées lorsque des emails sont envoyés au mauvais destinataire ou que des collaborateurs partagent la mauvaise pièce jointe.

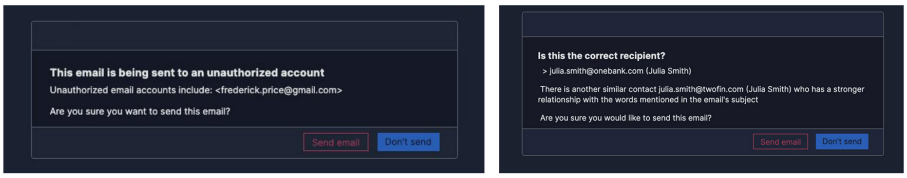

Figure 1. Proofpoint Adaptive Email DLP avertit les utilisateurs en temps réel des messages potentiellement adressés au mauvais destinataire afin de prévenir les fuites de données sensibles par email.

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.

Figure 2. Les équipes de sécurité ont une confiance accrue dans la visibilité sur les fuites de données par email.

Prévention des pièces jointes erronées

On parle de pièce jointe erronée lorsqu'un utilisateur envoie un email à la bonne personne, mais joint accidentellement le mauvais fichier.

Lorsque l'IA comportementale détecte une pièce jointe qui semble inhabituelle pour un destinataire, Proofpoint Adaptive Email DLP résout le problème. Il avertit automatiquement l'utilisateur en temps réel avant que des informations sensibles ne soient envoyées par inadvertance à la mauvaise personne.

Blocage des exfiltrations par email

Une DLP basée sur des règles est essentielle pour prévenir les fuites de données sensibles, mais seulement pour des risques prédéfinis (données personnelles, données de carte de paiements, numéros de sécurité sociale, etc.). Elle ne permet toutefois pas d'empêcher toutes les compromissions de données, car les utilisateurs internes partagent des données sensibles qui ne sont pas prédéfinies avec des adresses email personnelles et d'autres comptes non autorisés.

Proofpoint Adaptive Email DLP bloque les exfiltrations de données sensibles en classifiant automatiquement les données sensibles. Il détecte également les comptes de messagerie personnels des utilisateurs en fonction de leur comportement. Ainsi, si un collaborateur essaie d'exfiltrer des données en se les envoyant à lui-même ou les transmettant à d'autres personnes, ces tentatives sont automatiquement bloquées ou surveillées en fonction de la configuration.

Affichage d'avertissements au moment opportun

L'affichage d'avertissements au moment opportun peut aider les utilisateurs à éviter de commettre des erreurs et d'enfreindre les règles avant que le mal ne soit fait. En complément des formations de sensibilisation à la sécurité informatique, Proofpoint Adaptive Email DLP forme vos utilisateurs aux risques liés aux emails en temps réel. Les utilisateurs peuvent ainsi corriger leurs erreurs et éviter des fuites de données sensibles.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.