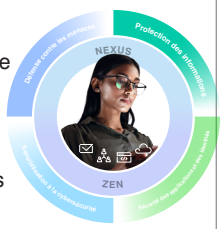
Prévention des fuites de données lors des fusions et acquisitions

Utilisez Proofpoint Adaptive Email DLP pour prévenir les fuites de données sensibles lors des fusions et acquisitions

Principaux avantages

- Prévenez les fuites de données accidentelles et intentionnelles par email.
- Évitez les atteintes à la réputation de votre entreprise.
- Améliorez la sensibilisation à la cybersécurité dans l'ensemble de votre entreprise.
- Profitez d'une protection de la messagerie efficace, simple à gérer et qui limite les perturbations de l'activité des utilisateurs.
- Réduisez le délai de rentabilisation grâce à une protection active en seulement 48 heures.

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.



Les fusions et acquisitions augmentent considérablement le nombre de personnes qui partagent des informations confidentielles entre les entreprises par email. Pour les équipes de sécurité des informations, il est également difficile de surveiller tous les collaborateurs et tiers impliqués. Ces facteurs augmentent le risque de fuite de données sensibles.

Proofpoint Adaptive Email Data Loss Prevention (DLP) résout ces problèmes. Proofpoint Adaptive Email DLP s'appuie sur l'intelligence artificielle (IA) comportementale pour identifier les comportements de vos collaborateurs en matière d'emails, leurs relations de confiance et la façon dont ils partagent des données. Notre solution analyse les emails afin de détecter les comportements anormaux et d'en informer les administrateurs. Elle avertit aussi les utilisateurs en temps réel, avant que des fuites critiques ne se produisent.

Pourquoi les fusions et acquisitions augmentent les risques

Lors des fusions et acquisitions, les entreprises doivent partager de nombreuses informations hautement confidentielles : données personnelles, documents du conseil d'administration, données du capital-investissement, etc.

D'après une étude de Gartner, ces transactions augmentent le risque de fuite de données pour plusieurs raisons :

- Il peut y avoir des conflits entre les pratiques de sécurité des deux entreprises.
- L'incertitude ou le secret qui entoure la transaction peut engendrer de l'anxiété, ce qui peut amener les collaborateurs à agir de façon inhabituelle ou dommageable.
- De nouveaux besoins techniques apparaissent souvent. Par exemple, une fois la transaction finalisée, il est possible que les entreprises doivent adopter trois modes d'exploitation différents — avant la fusion, pendant la transition et après la fusion. La surface d'attaque est bien plus large pendant cette période.

Comment Proofpoint Adaptive Email DLP protège vos données sensibles

Les fuites de données sensibles peuvent ternir la réputation de votre entreprise et être coûteuses à corriger. Proofpoint Adaptive Email DLP vous évite ces déconvenues. Notre solution s'appuie sur l'IA comportementale pour détecter et bloquer les fuites de données accidentelles et intentionnelles par email. L'IA analyse plus de 12 mois de données de messagerie pour identifier les comportements de vos collaborateurs en matière d'emails, leurs relations de confiance et la façon dont ils gèrent les données sensibles.

Proofpoint Adaptive Email DLP utilise l'IA ainsi entraînée pour identifier les comportements anormaux en temps réel : envoi d'un email au mauvais destinataire, envoi de données sensibles à un compte non autorisé et moins sécurisé, exfiltration délibérée d'informations, etc. Lorsqu'il détecte des problèmes, Proofpoint Adaptive Email DLP affiche des messages d'avertissement en temps réel aux utilisateurs. Ceux-ci peuvent alors corriger leurs actions afin d'éviter toute fuite de données, sans intervention supplémentaire d'un administrateur.

Dans le cadre de fusions et acquisitions, ces fonctionnalités permettent d'éviter que des données confidentielles ne tombent entre de mauvaises mains, tout en assurant la continuité des communications stratégiques.

Bloquez les emails adressés au mauvais destinataire

Il peut arriver qu'un utilisateur envoie un email à la mauvaise personne. Il s'agit d'une cause courante de fuite de données dans les entreprises. Ces incidents sont difficiles à prévenir au moyen de règles. En se familiarisant avec les habitudes des collaborateurs en matière d'emails, Proofpoint Adaptive Email DLP peut avertir les utilisateurs avant qu'ils n'envoient un email à la mauvaise personne.

Prévenez les pièces jointes erronées

On parle de pièce jointe erronée lorsqu'un utilisateur envoie un email à la bonne personne, mais joint le mauvais fichier. Comme pour l'envoi d'emails au mauvais destinataire, Proofpoint Adaptive Email DLP s'appuie sur l'IA pour détecter les pièces jointes erronées. Il avertit ensuite les utilisateurs en temps réel.

Bloquez les exfiltrations par email

Les règles de messagerie peuvent bloquer efficacement les fuites de données. Toutefois, celles-ci ne fonctionnent que pour des types connus prédéfinis de données : informations personnelles, données du secteur des cartes de paiement, numéros de sécurité sociale, etc.

Proofpoint Adaptive Email DLP identifie et classe vos données sensibles. Il identifie également les comptes de messagerie personnels des utilisateurs en fonction de leur comportement. Si un collaborateur essaie de s'envoyer des données sensibles ou de les envoyer à d'autres personnes, notre solution peut bloquer ou surveiller ses activités, en fonction de sa configuration.

Figure 1. Proofpoint Adaptive Email DLP avertit les utilisateurs en temps réel en cas d'envoi d'emails au mauvais destinataire.

Figure 2. Le tableau de bord Proofpoint Adaptive Email DLP offre aux équipes de sécurité des informations une visibilité totale sur les menaces véhiculées par email.

Formez les utilisateurs en temps réel

L'affichage de messages de formation en temps réel aide les utilisateurs à éviter de commettre des erreurs et d'enfreindre les règles. En complément des formations de sensibilisation à la cybersécurité, Proofpoint Adaptive Email DLP forme les utilisateurs aux risques liés aux emails. Grâce à ces messages de formation, les utilisateurs peuvent corriger les erreurs en temps réel et éviter les fuites de données.

Identifiez les menaces auxquelles vous êtes exposé

Le tableau de bord Proofpoint Adaptive Email DLP offre aux équipes de sécurité des informations un aperçu de tous les emails vérifiés par le système. Le tableau de bord affiche les emails à risque détectés et bloqués, y compris les emails envoyés au mauvais destinataire et les pièces jointes erronées, ainsi que les tentatives d'exfiltration par email. Il indique également les améliorations de la sécurité au fil du temps pour les utilisateurs et l'entreprise.

Des renseignements tels que les principales règles personnalisées et les utilisateurs les plus à risque permettent aux analystes de se concentrer sur l'essentiel. Ces informations accélèrent les investigations et aident les équipes de sécurité à collaborer avec les utilisateurs pour améliorer la façon dont ils gèrent les données.

Bénéficiez d'une gestion simplifiée

Proofpoint Adaptive Email DLP ne requiert qu'une configuration et une gestion minimales. En seulement 48 heures, il commence à prévenir les fuites de données par email. Il permet des interventions précises et efficaces, sans perturber les activités habituelles de vos utilisateurs.

EN SAVOIR PLUS

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

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web.
Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.