proofpoint.

FICHE SOLUTION

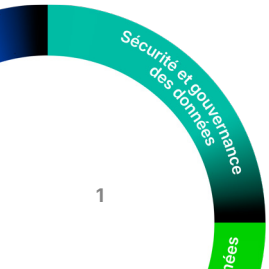
Moderniser la sécurité des données de messagerie avec une approche adaptative

Pour bénéficier d'une protection multicouche contre les fuites de données par email, adoptez Proofpoint Adaptive Email DLP

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
- Diminution des amendes engendrées par les infractions au règlement général sur la protection des données (RGPD) et à la loi CCPA (California Consumer Privacy Act)
- Amélioration de la sensibilisation à la cybersécurité dans l'ensemble de votre entreprise

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 fuites de données sensibles peuvent être particulièrement pénalisantes et préjudiciables pour votre entreprise. Selon le rapport *Data Loss Landscape 2024* de Proofpoint, 85 % des entreprises interrogées indiquent avoir subi une fuite de données au cours de l'année écoulée. Pour 50 % d'entre elles, cet incident a provoqué des perturbations de leurs activités. Les utilisateurs négligents ont été cités comme la cause la plus courante de fuites de données.

La prévention des fuites de données (DLP) par email est une composante essentielle de la stratégie globale de sécurité des données de votre entreprise. Elle protège les données sensibles contre toute exposition indésirable par email. Un programme efficace de DLP par email allie analyse du contenu, alertes en temps réel, application de règles et formation des utilisateurs. Il prévient les fuites de données et assure votre conformité aux exigences légales et réglementaires.

Les produits traditionnels de DLP par email peuvent créer des bases solides en appliquant des règles et des politiques définies pour les risques connus. Il est toutefois possible d'améliorer grandement votre stratégie de protection des données de messagerie en vous appuyant à la fois sur un produit traditionnel de DLP par email et sur Proofpoint Adaptive Email DLP. Cette solution combinée offre une approche plus dynamique et centrée sur les personnes de la prévention des fuites de données par email.

Voici les avantages que peut vous offrir l'ajout de Proofpoint Adaptive Email DLP à votre solution :

Protection plus complète

- Les **produits traditionnels de DLP par email** mettent l'accent sur le contenu. Ils assurent une protection basée sur les règles contre les risques connus, comme l'envoi de données sensibles par email. Ils sont efficaces pour protéger les données structurées connues et bien définies, comme les données personnelles et les numéros de carte de crédit.
- **Proofpoint Adaptive Email DLP** s'intéresse quant à lui au contexte. Il permet d'élargir la couverture assurée par les produits traditionnels de DLP par email, de manière à vous protéger également contre les menaces inconnues et en constante évolution. Proofpoint Adaptive Email DLP s'appuie sur l'IA comportementale pour détecter les comportements inhabituels des utilisateurs. Il peut s'agir d'un utilisateur qui envoie des données sensibles au mauvais destinataire ou un email à un compte non autorisé, ou qui partage des fichiers de manière inhabituelle.

Détection adaptative

Proofpoint Adaptive Email DLP a recours à l'IA comportementale pour détecter l'activité email qui diffère des comportements normaux des utilisateurs. Notre IA ne se contente pas de rechercher des modèles de données spécifiques.

1/3 des utilisateurs

ont envoyé un ou deux emails au mauvais destinataire.

Source : rapport *Data Loss Landscape 2024* de Proofpoint

84 %

des emails envoyés au mauvais destinataire l'année dernière contenaient des pièces jointes.

Source : rapport *Data Loss Landscape 2024* de Proofpoint

50 %

des compromissions dues à une erreur survenues en 2023 découlaient de l'envoi d'emails au mauvais destinataire.

Source : Verizon, *2024 Data Breach Investigations Report* (Rapport d'enquête 2024 sur les compromissions de données)

> 160 000

emails adressés au mauvais destinataire ont été bloqués par Proofpoint Adaptive Email DLP en 2024.

Source : Proofpoint

Elle analyse un contexte plus large, qui inclut :

- Les personnes à qui les utilisateurs ont l'habitude d'envoyer des emails
- Les types de pièces jointes que les utilisateurs partagent généralement
- La façon dont les utilisateurs ont l'habitude de gérer les données sensibles

Proofpoint Adaptive Email DLP s'adapte aux comportements de vos collaborateurs et aux tendances en matière d'emails. Il permet de détecter les fuites de données potentielles, même lorsque les données ne sont pas clairement définies. Imaginons par exemple qu'un collaborateur qui n'a pas l'habitude d'envoyer des données financières essaie soudainement d'envoyer une pièce jointe contenant de telles informations à un contact externe non autorisé. Proofpoint Adaptive Email DLP détectera le compte de messagerie non autorisé et la pièce jointe sensible, et effectuera un signalement.

Blocage des emails adressés au mauvais destinataire

Il peut arriver qu'un utilisateur envoie accidentellement un email à la mauvaise personne. Ces emails adressés au mauvais destinataire sont une source courante de compromissions de données. D'après les données de Proofpoint, 33 % des collaborateurs envoient un ou deux emails à la mauvaise personne chaque année. Il s'agit également de l'incident de fuite de données le plus signalé à l'ICO (Information Commissioner's Office) au Royaume-Uni[1]. En outre, Verizon a découvert que 50 % des compromissions dues à une erreur survenues en 2023 découlaient de l'envoi d'emails au mauvais destinataire[2].

L'envoi d'emails à la mauvaise personne est un problème difficile à résoudre avec des produits traditionnels de DLP par email. En revanche, Proofpoint Adaptive Email DLP s'appuie sur l'inspection approfondie du contenu et l'analyse comportementale de Proofpoint Nexus® Relationship Graph (RG) pour identifier les emails adressés au mauvais destinataire avant leur envoi. Lorsqu'un utilisateur tente d'envoyer un email à la mauvaise personne, Proofpoint Adaptive Email DLP détecte l'erreur et génère un avertissement. D'après les données de Proofpoint, Proofpoint Adaptive Email DLP a empêché l'envoi de plus de 160 000 emails adressés au mauvais destinataire en 2024.

Prévention des pièces jointes erronées

On parle de pièce jointe erronée lorsqu'un utilisateur envoie un email à la bonne personne, mais joint le mauvais fichier. Lorsque notre IA comportementale détecte une pièce jointe qui semble inhabituelle pour un destinataire donné, elle avertit l'utilisateur en temps réel. Celui-ci peut alors corriger le problème avant la survenue d'une grave fuite de données.

1. ICO (Information Commissioner's Office), « Common data protection mistakes (and how to fix them) » (Erreurs courantes en matière de protection des données, et comment les corriger), février 2025.
2. Verizon, *2024 Data Breach Investigations Report* (Rapport d'enquête 2024 sur les compromissions de données), 2024.

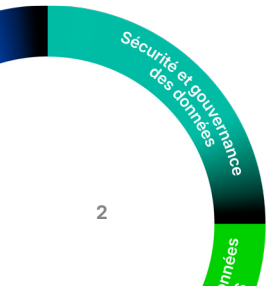


Figure 1. Le tableau de bord Proofpoint Adaptive Email DLP offre aux équipes de sécurité des informations une visibilité totale et une confiance accrue dans la prévention des fuites de données.

> 1 100 000

emails exfiltrant des données ont été détectés par Proofpoint Adaptive Email DLP en 2024.

Source : Proofpoint

Blocage des exfiltrations de données par email

Les exfiltrations de données sensibles par email sont coûteuses à corriger pour les entreprises. Selon le Ponemon Institute, une équipe de sécurité a besoin de 48 à 72 heures pour identifier et corriger un incident d'exfiltration de données[3]. Proofpoint Adaptive Email DLP allège ce fardeau grandissant qui pèse sur votre équipe. Il analyse et classe automatiquement vos données sensibles, et identifie les comptes de messagerie personnels ou non autorisés appartenant à vos utilisateurs. Si un utilisateur essaie de s'envoyer des données sensibles ou de les transférer à d'autres personnes, Proofpoint Adaptive Email DLP bloque ou surveille ses activités, en fonction de sa configuration. D'après les données de Proofpoint, Proofpoint Adaptive Email DLP a détecté plus de 1 100 000 emails exfiltrant des données en 2024.

3. Ponemon Institute, « Email Data Loss Prevention: The Rising Need for Behavioral Intelligence » (Prévention des fuites de données par email : le besoin croissant d'une threat intelligence comportementale), mai 2022.

Figure 2. Proofpoint Adaptive Email DLP avertit les utilisateurs en temps réel en cas d'envoi d'emails à des comptes non autorisés ou au mauvais destinataire.

Formation des utilisateurs en temps réel

La formation des utilisateurs en temps réel permet de prévenir les erreurs et les infractions aux règles. En complément des formations de sensibilisation à la cybersécurité, Proofpoint Adaptive Email DLP forme les utilisateurs aux risques liés aux emails en temps réel. Les utilisateurs peuvent alors corriger leurs propres erreurs sans l'aide d'un administrateur.

L'union fait la force

Les conséquences d'une fuite de données sensibles peuvent être dévastatrices. Ces incidents peuvent entraîner des amendes réglementaires, une atteinte à la réputation et une perte de revenus. Ils peuvent également augmenter les coûts de main-d'œuvre en raison des investigations et des rapports réglementaires et de conformité requis.

En intégrant à la fois un produit traditionnel de DLP par email et Proofpoint Adaptive Email DLP, votre entreprise peut mettre en place une approche moderne et multicouche de la sécurité des données de messagerie. Cette solution combine une protection robuste contre les risques connus et une détection intelligente et dynamique des menaces de fuites de données inconnues centrées sur les personnes. Vous profitez ainsi d'une protection améliorée des données, d'une meilleure conformité des utilisateurs, d'une réduction des frais opérationnels et d'un niveau de sécurité des données de messagerie global renforcé.

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 risque 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 du classement 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 la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

Suivez-nous : LinkedIn

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →