Proofpoint Adaptive Email DLP pour renforcer MS Purview

Pour une prévention plus robuste et plus intelligente des fuites de données par email, associez Microsoft Purview à 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 solutions Microsoft Purview et Proofpoint Adaptive Email DLP ont toutes deux pour but de prévenir les fuites de données (DLP). Elles adoptent toutefois une approche distincte et réduisent des risques différents. Pour élaborer la stratégie de protection la plus complète et la plus robuste possible contre les fuites de données par email, optimisez votre déploiement Purview grâce aux informations fournies par Proofpoint Adaptive Email DLP.

Comparaison entre Microsoft Purview et Proofpoint Adaptive Email DLP

Purview suit une approche basée sur des règles qui offre la plupart des fonctionnalités des passerelles de messagerie sécurisées, dont le chiffrement des communications ainsi que la gouvernance et la rétention des données. Cependant, Purview s'appuie sur des règles gérées par un administrateur dont la mise en œuvre est lente et propice aux erreurs, qui sont difficiles à gérer et qui ne sont pas suffisantes pour bloquer tous les risques. Par ailleurs, Purview n'effectue aucune analyse comportementale permettant de comprendre les intentions de vos utilisateurs. Cette compréhension est pourtant essentielle pour distinguer les véritables risques des faux positifs.

Proofpoint Adaptive Email DLP s'appuie sur l'intelligence artificielle (IA) comportementale pour prévenir les fuites de données accidentelles et intentionnelles par email. En bloquant les emails adressés au mauvais destinataire, les pièces jointes erronées et les tentatives d'exfiltration de données, la solution réduit les risques auxquels vous êtes exposé et les coûts de correction. Et comme votre équipe de sécurité consacre moins de temps à l'investigation des faux positifs, elle peut se concentrer sur l'optimisation de votre protection.

Purview ne bloque pas les emails adressés au mauvais destinataire

Les règles de messagerie de Purview peuvent s'avérer efficaces pour ce qui est d'éviter que des types prédéfinis de contenu ne quittent votre entreprise, mais elles ne peuvent pas empêcher un utilisateur d'envoyer un email à la mauvaise personne. Le blocage des emails adressés au mauvais destinataire exige une compréhension plus approfondie des comportements habituels des collaborateurs, sur la base du contexte et du contenu des emails historiques.

Proofpoint Adaptive Email DLP analyse plus de 12 mois de données email historiques pour identifier les schémas de communication habituels entre les expéditeurs et les destinataires. Il s'appuie sur ces informations pour identifier et bloquer les emails adressés au mauvais destinataire avant leur envoi.

Purview est inefficace contre l'exfiltration de données par email

La plupart des exfiltrations de données par email ont lieu lorsque des collaborateurs s'envoient des données sensibles. Cette situation peut se produire lorsqu'un collaborateur quitte l'entreprise pour rejoindre la concurrence.

Dans Purview, le blocage global des services de messagerie gratuits comme Gmail et Yahoo ne fonctionne pas, car les emails professionnels légitimes sont également bloqués. Il ne peut pas non plus empêcher un utilisateur d'envoyer des données à un domaine de messagerie personnel. Le signalement de chaque interaction avec des services de messagerie gratuits génère trop de faux positifs pour analyse par votre équipe de sécurité.

Proofpoint Adaptive Email DLP s'appuie sur une IA avancée entraînée avec les données les plus riches du secteur. En analysant les comportements de vos collaborateurs en matière d'emails, il apprend à distinguer les communications normales des échanges suspects. Les alertes sont ainsi plus précises et pertinentes, ce qui accélère les investigations et vous permet de gagner du temps et d'économiser des ressources.

Proofpoint Adaptive Email DLP forme les utilisateurs en temps réel

Dans Purview, vous pouvez faire en sorte d'afficher des messages d'avertissement lorsque des collaborateurs enfreignent les règles de messagerie. Leur configuration et leur optimisation sont toutefois chronophages. Et lorsque les avertissements sont trop fréquents, les utilisateurs peuvent commencer à les ignorer, un phénomène connu sous le nom de baisse de vigilance face aux alertes.

Sans aucune configuration supplémentaire, Proofpoint Adaptive Email DLP fournit aux utilisateurs des avertissements contextuels en temps réel concernant leurs comportements à risque. Les utilisateurs peuvent alors corriger les emails adressés au mauvais destinataire ou les pièces jointes erronées avant envoi. Si un collaborateur essaie de s'envoyer des données confidentielles ou de les transférer à d'autres personnes, Proofpoint Adaptive Email DLP peut bloquer ou surveiller ses activités, en fonction de sa configuration.

L'union fait la force

Les fuites de données par email peuvent avoir de graves conséquences. 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.

Pour protéger vos données les plus sensibles et éviter ces répercussions, vous avez besoin d'une solution de prévention des fuites de données par email flexible et intelligente qui ne se limite pas à une approche statique basée sur des règles.

En associant Purview à notre solution Proofpoint Adaptive Email DLP optimisée par l'IA, votre entreprise peut mettre en place une protection complète et robuste contre les fuites de données par email.

Visitez le site proofpoint.com/fr pour en savoir plus