Proofpoint Email DLP and Encryption

Identifiez les données sensibles dans les emails afin de prévenir les fuites et d'automatiser la conformité

Principaux avantages

- Gestion et application centralisées de la prévention des fuites de données et du chiffrement des emails sur la passerelle de messagerie de pointe de Proofpoint
- Détection et analyse des données sensibles dans les emails et les pièces jointes
- Intégration avec Proofpoint Information Protection pour une prise en charge complète de tous les scénarios de fuite de données centrés sur les personnes

Conformité

- Accès à des centaines d'identifiants de données intégrés
- Norme PCI, loi SOX, loi GLBA, termes relevant du délit d'initié définis par la SEC, ainsi que d'autres modèles internationaux propres à chaque pays
- RGPD, loi britannique sur la protection des données, directive européenne sur la protection des données, loi canadienne sur la protection des renseignements personnels et les documents électroniques, numéro d'assurance nationale britannique, numéros de cartes de crédit japonaises
- Code PII, loi HIPAA, CIM-9, CIM-10, CIM-11, Code national américain des médicaments, ainsi que d'autres codes sanitaires

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.

L'email est un vecteur critique de fuite de données en sortie. Limiter le risque de fuite de données sensibles doit donc faire partie des priorités des équipes de sécurité. Pour respecter les exigences de conformité, elles doivent être capables de détecter et de contrôler les données dans les emails. Proofpoint Email Data Loss Prevention (DLP) and Encryption réduit le risque de compromission de données par le biais d'emails et de pièces jointes. Il vous permet également de définir et d'appliquer de façon dynamique des règles de chiffrement granulaires afin de sécuriser les emails transitant entre des utilisateurs internes et des partenaires commerciaux externes.

Les fuites de données ne se produisent pas par magie. Ce sont les utilisateurs qui en sont à l'origine. D'après le rapport DBIR 2023 de Verizon[1], 74 % des compromissions qui entraînent la divulgation de données à un tiers non autorisé impliquent une intervention humaine. La plupart des analystes constatent que les utilisateurs d'entreprise perdent généralement des données. La cause sous-jacente de ces incidents peut être une simple négligence, les utilisateurs négligents constituant les principales sources de fuites de données par email.

Proofpoint Email DLP and Encryption identifie avec précision les informations sensibles. Il détecte les exfiltrations de données par email et bloque les fuites de données critiques. Il vous offre également un contrôle accru sur vos données sensibles afin de vous aider à respecter les exigences de conformité.

Identification des données propres à votre entreprise

Proofpoint Email DLP and Encryption identifie les données propres à votre entreprise. Il s'accompagne de centaines d'identifiants de données et de dictionnaires prédéfinis et éprouvés. Ceux-ci incluent des numéros de compte de services financiers, des formulaires d'identification locaux et des numéros de dossier médical. Par ailleurs, vous pouvez facilement charger ou créer des dictionnaires ou identifiants personnalisés propres à votre entreprise, ainsi qu'affiner la valeur de correspondance des termes des dictionnaires et des exceptions. Vous pouvez ainsi analyser les données dans les emails qui comptent le plus pour votre entreprise.

1 Verizon, « 2023 Data Breach Investigations Report » (Rapport d'enquête 2023 sur les compromissions de données), juin 2023.

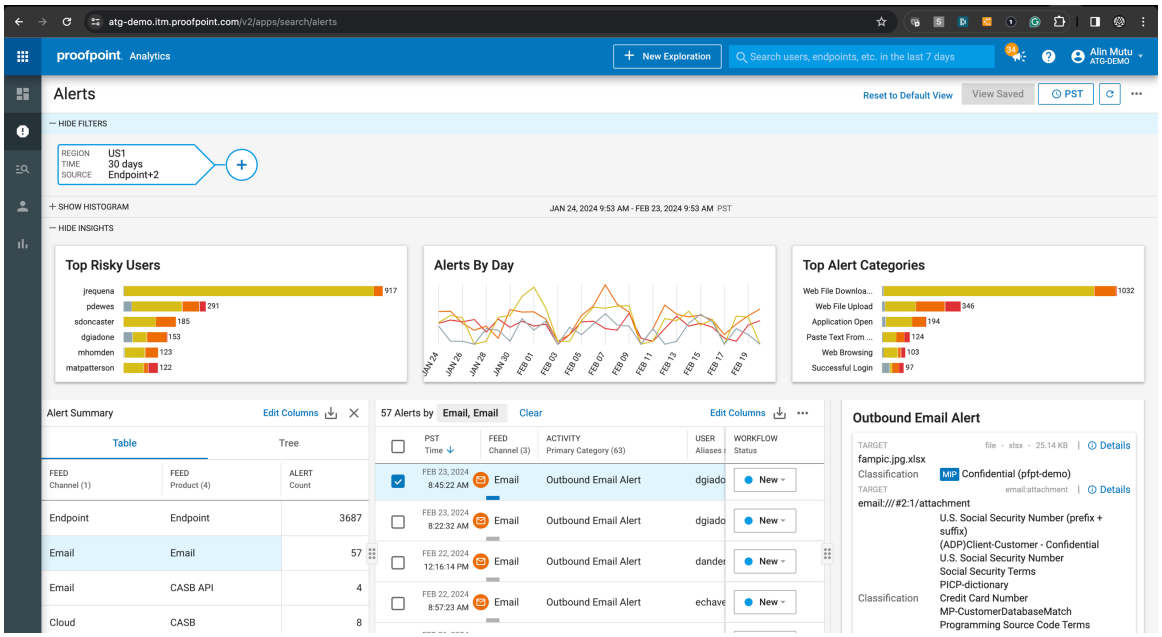

Figure 1. Proofpoint Email DLP and Encryption vous permet de gérer tous les scénarios de fuite de données centrés sur les personnes via une interface unifiée de gestion des alertes.

Analyse approfondie et analyse de l'empreinte numérique

Proofpoint Email DLP and Encryption permet de détecter avec précision les données sensibles dans du contenu non structuré. Plus de 300 types de fichiers différents peuvent être analysés dès la mise en service de la solution. La solution s'assure que les données sensibles présentes dans des pièces jointes dans un format autre que Microsoft 365 ou PDF sont correctement traitées. Vous pouvez également utiliser l'outil de profilage des types de fichiers pour prendre en charge des types de fichiers nouveaux, personnalisés et propriétaires, tels que les brevets et les notes de service.

L'empreinte numérique des documents sensibles est analysée grâce à des fonctionnalités de correspondance complète et partielle, même si les données résident dans des fichiers de formats différents. Vous pouvez également employer des méthodes avancées de mise en correspondance du contenu et d'extraction de texte à partir d'images. Cela inclut la correspondance de documents indexés, la correspondance exacte de données et la reconnaissance optique des caractères (OCR).

Automatisation de la conformité réglementaire

Proofpoint Email DLP and Encryption recherche automatiquement toutes les formes standard de contenu soumis à des réglementations et détecte rapidement les données sensibles grâce à ses dictionnaires prédéfinis. Les contrôles algorithmiques détaillés intégrés dans des identifiants intelligents réduisent les faux positifs pour les numéros de carte de crédit et un large éventail d'informations sensibles. Les analyses avancées de proximité et de corrélation améliorent l'analyse des détections.

La solution permet aux entreprises de se conformer à la norme PCI, à la loi SOX, au RGPD, au code PII, à la loi HIPAA et plus encore.

Rapports en temps réel

Proofpoint Email DLP and Encryption offre la visibilité et le workflow nécessaires pour vous aider à prendre des décisions rapides et à les mettre en œuvre. Il permet de consulter les statistiques et les tendances en temps réel, ainsi que de gérer les incidents en cours. Vous pouvez également prendre les mesures appropriées en cas de messages non conformes, tout cela depuis un tableau de bord centralisé. Vous pouvez examiner tous les incidents en détail. Une vue côte à côte de sections spécifiques d'un email ou d'une pièce jointe permet d'identifier les éléments du contenu qui s'écartent du document ou des règles d'origine. Vous pouvez commenter, suivre et rechercher les infractions dans le gestionnaire d'incidents, de même qu'exporter les messages correspondants.

Amélioration de l'efficacité opérationnelle

La prévention des fuites de données via la messagerie fait partie de notre approche DLP d'entreprise. Vous pouvez ainsi localiser, surveiller et protéger les données des emails, des applications cloud et des endpoints. La solution combine les données d'analyse des contenus, des comportements et des menaces de ces canaux, ce qui vous permet de gérer tous les scénarios de fuite de données centrés sur les personnes via une interface unifiée de gestion des alertes. En outre, vous pouvez facilement appliquer des détecteurs de données communs pour déployer des règles DLP cohérentes sur tous les canaux. Vous gagnez ainsi un temps précieux et évitez les casse-têtes liés à l'administration.

Des règles de routage telles que Smart Send facilitent la tâche de vos analystes DLP. Les emails peuvent être renvoyés à l'expéditeur afin qu'il corrige ses propres infractions aux règles de sortie, ou transmis à quelqu'un d'autre, par exemple aux RH, au service informatique ou au dirigeant de l'entreprise, dans le cadre du workflow.

Chiffrement, visibilité et contrôles assurés

Proofpoint Email DLP and Encryption assure la sécurité de vos communications d'entreprise. Il sécurise les communications externes et internes grâce à un ensemble robuste de contrôles et à une gestion des clés sans intervention. Optimisée par un moteur DLP basé sur des règles, la solution vous permet de définir et d'appliquer de façon dynamique des règles de chiffrement granulaires au niveau mondial, des groupes et des utilisateurs grâce à des intégrations avec LDAP et Active Directory.

Vous pouvez automatiser le chiffrement en fonction de la destination (c'est-à-dire par partenaire commercial ou fournisseur), de l'expéditeur ou des attributs du message, tels que les types de pièces jointes. Vous pouvez également permettre aux utilisateurs d'appliquer le chiffrement de manière sélective. Le chiffrement des emails peut également servir de TLS de secours afin de garantir un chiffrement fiable. Les destinataires disposent d'options flexibles pour accéder aux messages chiffrés, notamment un portail Web, un navigateur mobile et un client Outlook.

Pour des communications fluides et sécurisées avec les partenaires commerciaux qui utilisent aussi Proofpoint Email DLP and Encryption, notre outil Trusted Partner Encryption offre une expérience transparente à vos utilisateurs. Les messages sont chiffrés par la passerelle d'envoi. La passerelle Proofpoint du partenaire commercial peut ensuite les déchiffrer automatiquement avant qu'ils ne soient distribués à l'infrastructure de messagerie interne.

Expérience du destinataire optimisée

En offrant une expérience utilisateur transparente, Proofpoint Email DLP and Encryption dissuade les collaborateurs de contourner les règles en place. La solution propose de nombreuses options pour permettre aux utilisateurs d'accéder aux messages chiffrés, dont les suivantes :

- **Secure Reader –** Permet aux utilisateurs de cliquer sur une pièce jointe HTML chiffrée à partir du message ou de cliquer sur un lien dans un email. L'utilisateur est alors dirigé vers un portail Web, où il peut facilement accéder au message chiffré.
- **Boîte de réception de Secure Reader –** Offre aux utilisateurs une expérience transparente lors du traitement des messages chiffrés. Elle permet en outre à l'entreprise de gérer facilement les messages.
- **Modules d'extension Microsoft Outlook –** Permettent aux utilisateurs d'envoyer et de lire facilement des messages chiffrés en un seul clic.
- **Chiffrement des messages internes –** Utilisé pour les communications sensibles entre collaborateurs.

Expertise pour réduire le délai de rentabilisation

La prévention des fuites de données n'est pas une mince affaire. Des connaissances techniques et des produits ne suffisent pas. Elle requiert également une compréhension approfondie des objectifs du programme, ainsi que de la gouvernance et de l'administration des données. Nous pouvons devenir votre partenaire de confiance pour garantir le succès de votre programme DLP. Notre service managé vous offre une expertise qui peut vous aider à optimiser votre investissement technologique, à soutenir la continuité de vos opérations et à faire évoluer votre stratégie de protection des données.

EN SAVOIR PLUS

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