Forcepoint

Présentation succincte

Data Loss Prevention for Cloud Email de Forcepoint

Sécurisez et gardez le contrôle de vos courriels en vous appuyant sur la technologie DLP la plus fiable du secteur.

Le Défi

- Les données sensibles sortent des entreprises en quantités croissantes en suivant plusieurs voies.
- Le courriel est cité comme l e vecteur d'attaque le plus populaire.
- Il n'a jamais été aussi vital et complexe de sécuriser les données sans nuire à la productivité des entreprises.

La Solution

- Forcepoint dispose de la solution Data Loss Prevention (DLP) la plus fiable du secteur pour gérer la sécurité de vos courriels.
- Surveillez avec précision et empêchez la perte de données sensibles par courriel.
- Tirez parti d'une solution cloud entièrement gérée de protection des courriels sortants, adaptée aux besoins de votre entreprise.

Résultat

- Gagnez en efficacité en réduisant considérablement le nombre d'incidents de faux positifs dans les courriels.
- Augmentez votre niveau de conformité via des politiques prédéfinies – nous en proposons trois fois plus que tout autre prestataire DLP.
- Migrez votre DLP vers Forcepoint en 6 semaines seulement, en tirant parti de l'expertise de Forcepoint, de ses politiques prêtes à l'emploi et d'un transfert de connaissances de sommet de gamme.

La sécurité des données est aujourd'hui au cœur des préoccupations des entreprises du monde entier. Que leurs employés travaillent dans le cadre conventionnel d'un bureau ou selon la nouvelle norme de travail hybride ou à distance, sécuriser les données sur de multiples canaux est devenu bien plus complexe. Le courriel est un canal essentiel sur lequel les entreprises doivent gagner visibilité et contrôle afin d'empêcher l'exfiltration indésirable de données, de propriétés intellectuelles et de fichiers importants. Voici quelques exemples courants de perte de données par courriel:

→ **Envoi de fichiers ou de données de l'entreprise** à des comptes de messagerie privés via le courriel de l'entreprise.

→ **Des données sensibles** quittent l'entreprise à cause de la négligence des utilisateurs ou à cause d'identifiants compromis.

→ **Un acteur interne mal intentionné envoie des données et des fichiers sensibles à des concurrents,** des médias d'information ou à des sites web externes. Le but est souvent de commettre une fraude, de nuire à l'entreprise ou de voler des données exclusives.

→ **Les attaques par phishing, via malwares, adwares et spam** poussent à leur insu des utilisateurs internes par ailleurs bien intentionnés à coopérer avec des criminels pour exfiltrer des données critiques et des PI.

« Le courriel est le vecteur de menace le plus utilisé par les assaillants pour diffuser des malwares dans une entreprise. Le courriel est également une ligne de contact direct entre les utilisateurs et les cybercriminels, qui entraîne chaque année des milliards de dollars de pertes dues à la fraude et la compromission de courriels d'entreprise. »

IDC, PARTS DE MARCHÉ DE LA SÉCURITÉ DES MESSAGERIES DANS LE MONDE, 2021 : LE TRAVAIL HYBRIDE SOULIGNE LA NÉCESSITÉ D'INTÉGRER LES ENQUÊTES SUR LES MENACES, DOC # US49144522, JUIN 2022

Il est impératif que les entreprises aient une bonne visibilité et un contrôle adéquat de leurs courriels sortants pour protéger leurs propriétés intellectuelles des attaques ciblées et des diffusions accidentelles. La technologie qui permet d'atteindre cet objectif est la protection contre la perte de données DLP. Selon IDC, « les 24 derniers mois ont vu une renaissance du marché des technologies de lutte contre la perte de données. Les techniques de classification manuelles et complexes sont remplacées par l'apprentissage automatique et l'automatisation. Le contexte est devenu le principal agent de motivation. L'efficacité et l'efficience des solutions se sont améliorées. » [1] La sécurité du courriel, combinée à toutes les nouvelles avancées DLP qui permettent de découvrir, protéger et contrôler le flux des informations sensibles, est essentielle pour contrôler un vecteur aussi majeur qu'est le courriel. Si vous ne disposez pas de solides capacités DLP, les atteintes à la sécurité perpétrées par le biais de courriels peuvent nuire gravement à l'activité et à la réputation de votre entreprise.

La supériorité de Forcepoint DLP for Cloud Email

En tant que leader des solutions de sécurité des données, DLP for Cloud Email de Forcepoint apporte une visibilité et un contrôle sans précédent sur les courriels sortants. Associé à DLP for Endpoints, Cloud, Web and Network, DLP for Cloud Email de Forcepoint est la solution multicouches la plus puissante pour protéger les données d'une entreprise. La solution DLP de Forcepoint est conçue pour empêcher la perte de données, partout où vos employés travaillent et où que se trouvent vos données.

« Identification extrême » des données

La DLP de Forcepoint fournit plus de 1600 classificateurs et modèles prédéfinis qui permettent un déploiement rapide et l'identification immédiate des données sensibles. Elle s'appuie également sur des technologies avancées, utilisant l'analyse du langage naturel, l'apprentissage automatique et l'une des technologies de prise d'empreinte numérique les plus puissantes du secteur pour identifier précisément les données statiques, en mouvement et en service. Pour sécuriser les données, une bonne visibilité est essentielle. DLP Discover de Forcepoint donne une forte visibilité suivie d'une identification formelle des données, afin que toutes les formes de données puissent faire l'objet d'un contrôle optimisé. Ceci est important pour de multiples raisons :

- → **La Conformité.** Forcepoint DLP couvre les réglementations les plus importantes comme le RGPD, la HIPA et bien d'autres encore, couvrant les normes de 83 pays afin de s'assurer que les entreprises respectent constamment les standards de conformité.
- → **La Simplicité.** Créer et mettre en œuvre des classificateurs qui répondent aux besoins d'une entreprise et à ses exigences commerciales prennent énormément de temps et de ressources lors d'un déploiement DLP. Grâce aux modèles et aux classificateurs prédéfinis proposés par Forcepoint, les entreprises peuvent rapidement implémenter des classificateurs spécifiques à une série de secteurs et de types de données, ce qui simplifie considérablement le déploiement de leur DLP.
- → **Efficacité.** Grâce à sa technologie intégrée d'identification des données, Forcepoint DLP réduit considérablement le nombre de faux positifs, tout en classant et en prioritisant les incidents critiques pour faciliter les enquêtes.

Contrôle unifié des politiques

Une stratégie DLP solide doit s'étendre à tous les canaux principaux, tels que les terminaux, le cloud, le web et le courriel. Souvent, les entreprises compartimentent et isolent chacun de ces canaux avec des produits DLP disparates qui se concentrent sur un seul aspect du problème, comme le cloud ou le courriel. Avec Forcepoint, vous pouvez sécuriser tous ces canaux avec une solution unique, et les gérer à partir d'une seule politique. La méthodologie « Écrire une fois et déployer plusieurs fois » permet d'exercer un niveau de contrôle inégalé sur les données de votre entreprise, via une interface unique couvrant tous les canaux critiques où se produisent les pertes de données. L'utilisation de politiques avec DLP for Cloud Email peut également permettre une visibilité sur des dispositifs supplémentaires, comme les tablettes et les téléphones, qui ne sont généralement pas couverts par les solutions de terminaux courantes

Une modularité sans égale

Forcepoint DLP for Cloud Email présente l'avantage d'être un service entièrement géré dans le cloud, ce qui lui offre la flexibilité attendue dans un déploiement cloud. Si, par exemple, il y a une surcharge de courriels sortants à un moment donné, DLP for Cloud Email déclenchera une expansion puis une réduction rapide des ressources pour répondre efficacement à cette surcharge ponctuelle. Il active également un service DLP continu pour répondre aux demandes croissantes de votre entreprise, sans avoir à déployer et à configurer du matériel supplémentaire pour cela.

Protection adaptative au risque

Forcepoint est le premier prestataire de l'industrie à proposer un système DLP adaptatif au risque. En surveillant en permanence l'activité de vos utilisateurs, la solution permet à votre personnel de travailler sans entraves, car elle n'intervient que lorsqu'une activité ou des modèles de comportement à risque sont identifiés. L'automatisation permet une application en temps quasi réel d'une politique : autrement dit, elle peut anticiper et arrêter une infraction avant qu'elle ne se produise.

1 IDC, Parts du marché mondial des technologies contre les pertes numériques, 2020 : La DLP est morte, Vive la DLP, Doc # US48261521, octobre 2021

Solutions DLP for Cloud Email de Forcepoint

DLP for Cloud Email – sécuriser les données sortantes

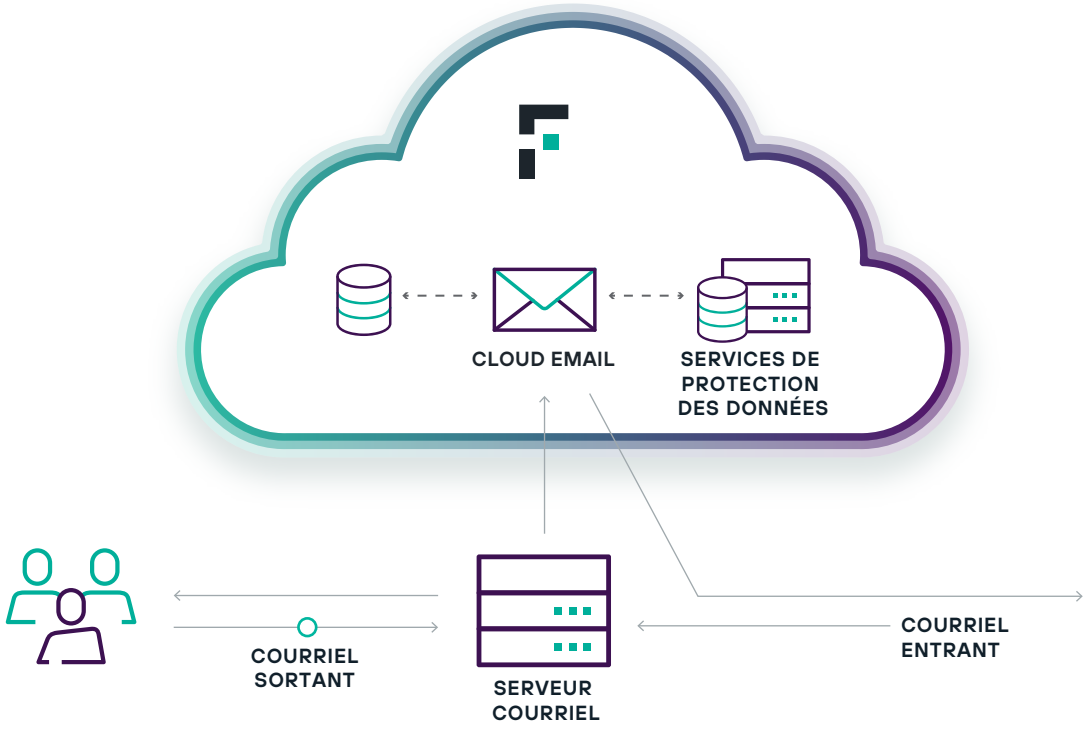
Forcepoint simplifie le déploiement de DLP for Cloud Email en travaillant conjointement avec votre prestataire de sécurité cloud pour analyser les courriels sortants. Grâce aux connecteurs DLP for Cloud Email Universal, Forcepoint intègre des produits de prestataires tiers populaires, tels Google et Microsoft, pour transférer tous les courriels sortants, ou certains d'entre eux, vers le cloud de Forcepoint. Là, Forcepoint DLP effectue des analyses selon les politiques DLP et effectuera des actions selon votre plan DLP prédéfini. Les courriels peuvent être autorisés, mis en quarantaine ou chiffrés (avec le module de chiffrage séparé) avant d'être envoyés. Des notifications concernant le courriel en quarantaine sont envoyées. Ces courriels peuvent être configurés pour être conservés jusqu'à 30 jours, à moins qu'ils ne soient autorisés à circuler par un administrateur. Afin de préserver la réputation d'une entreprise, tous les courriels sortants sont également analysés pour détecter les spams, les virus et les malwares.

Fonctions standard :

- → **Interface simple de gestion de politiques** offrant une protection contre les virus, les malwares et le spam
- → **Tableaux de bord, journaux et rapports de présentation**
- → **Abonnement personnel au courriel**

Modules complémentaires :

- → **Historique étendu des rapports pour Forcepoint Cloud Email** (options pour 6, 12 et 18 mois)
- → **Module de Chiffrement Forcepoint Email Security**
- → **Module d'analyse d'image Forcepoint Email Security**



forcepoint.com/contact