LA PRÉVENTION DE LA PERTE DE DONNÉES (DLP, DATA LOSS PREVENTION)

PROTECTION DES DONNÉES DANS UN MONDE SANS FRONTIÈRES

FORCEPOINT

Forcepoint DLP

UNE SÉCURITÉ AXÉE SUR LE FACTEUR HUMAIN

Préserver la sécurité des données est un challenge sans fin. Les entreprises du secteur IT doivent se maintenir au niveau des règlementations et protéger leurs propriétés intellectuelles contre les attaques ciblées et les failles accidentelles. De plus, elles doivent s'adapter aux macro mouvements qui secouent l'informatique, comme l'adoption des applications cloud, les environnements cloud hybrides et les tendances PAP : tout cela génère une augmentation des facteurs de fuite des données de votre entreprise.

La croissance de la surface d'attaque pose un défi majeur pour protéger les données critiques. Les équipes chargées de la sécurité des données adoptent l'approche la plus logique pour suivre les données en les trouvant, en les répertoriant et en les contrôlant. Cependant, les approches traditionnelles contre la perte de données ne sont plus efficaces aujourd'hui, car elles ne prennent pas en compte la plus importante variable en sécurité des données : les personnes avec qui vous travaillez.

Plutôt que de se concentrer uniquement sur les données, la sécurité devrait commencer, et se terminer, par les personnes. Le point clé est d'acquérir une visibilité sur les interactions entre les utilisateurs, les données et les applications. Une fois que cela est en place, vous pouvez appliquer un niveau de contrôle basé sur le risque spécifique de l'utilisateur et la confidentialité ou la valeur des données.

Le programme de protection des données d'une entreprise doit tenir compte du facteur humain – le point d'intersection des utilisateurs, des données et des réseaux. De plus, l'entreprise doit maintenir sa vigilance sur les données, tandis qu'elles transitent dans l'entreprise et servent aux personnes qui peuvent créer, toucher et déplacer des données.

La protection des données doit :

- **Sécuriser les données règlementées** avec un point de contrôle unique utilisé par toutes les applications que les personnes utilisent pour créer, sauvegarder et déplacer les données.
- **Protéger les propriétés intellectuelles** avec une solution DLP avancée qui analyse comment les personnes utilisent les données, qui enseigne à vos utilisateurs comment prendre les bonnes décisions avec leurs données, et qui priorise les incidents par catégorie de risque.

Visibilité et contrôle là où se trouvent les salariés et les données

- Applications Cloud (Avec Forcepoint CASB)
- Terminal
- Réseau
- Découverte

La solution Forcepoint DLP s'adresse aux risques posés par le facteur humain en vous donnant visibilité et contrôle partout où travaillent vos employés et où se trouvent vos données. Les équipes de sécurité appliquent des scores de risque selon l'utilisateur sur les événements qui sont les plus significatifs et pour accélérer la mise en conformité avec les règlementations mondiales affectant les données.

www.forcepoint.com

ACCÉLÉREZ VOTRE MISE EN CONFORMITÉ

Les environnements IT modernes posent un défi colossal aux entreprises souhaitant être en conformité avec des dizaines de règlementations de sécurité des données au niveau mondial, spécialement quand elles s'orientent vers les applications cloud et la force de travail mobile. De nombreuses solutions de sécurité offrent une forme de DLP intégré, comme celui que l'on retrouve dans les applications cloud. Cependant, les équipes de sécurité doivent faire face à une complexité indésirable et à des frais supplémentaires quand elles déploient et gèrent des politiques distinctes et incohérentes an niveau des terminaux, des applications cloud et des réseaux.

Le DLP Forcepoint accélère vos efforts de mise en conformité en proposant une couverture générique des règlementations mondiales, combinée à un contrôle central réparti dans tout votre environnement informatique. Le DLP Forcepoint permet de sécuriser efficacement les informations clients confidentielles et les données règlementées, afin que vous puissiez prouver en toute confiance votre respect des normes en cours.

- **Couverture de règlementations** respectant les exigences de conformité de plus de 370 politiques, pour couvrir les exigences légales dans 83 pays.
- **Repérez et intervenez sur les données règlementées** en allant les découvrir dans le réseau, dans le cloud et sur les terminaux.
- **Un contrôle centralisé et des politiques cohérentes** à travers l'environnement informatique.

PERMETTEZ À CHACUN DE POUVOIR PROTÉGER LES DONNÉES

Un DLP proposant uniquement un contrôle préventif frustre les utilisateurs, qui contourneront les mesures pour pouvoir terminer une tâche. Contourner les mesures de sécurité fait prendre des risques superflus et peut générer une fuite des données par inadvertance.

Le DLP Forcepoint admet que vos salariés sont en première ligne face aux cybermenaces.

- **Repérez et contrôlez les données où qu'elles se trouvent**, qu'elles soient dans le cloud, sur le réseau, dans les messageries et sur les terminaux.
- **Éduquez les employés à prendre les bonnes décisions,** en diffusant des aides à la décision, des informations sur les politiques et de validation des intentions de l'utilisateur lors des interactions avec les données critiques.
- **Collaborez en toute sécurité avec des partenaires de confiance** en utilisant des politiques à cryptage automatique qui protègent les données dès qu'elles quittent votre organisation.
- **Automatisez l'étiquetage des données et leur classification** avec l'intégration de solutions haut de gamme de classification de données (par ex. Microsoft Information Protection, Titus, Boldon James).

DÉTECTION ET CONTRÔLES AVANCÉS QUI SUIVENT LES DONNÉES

Les fuites de données accidentelles et malveillantes sont des incidents complexes, et pas de simples événements. Le DLP Forcepoint est une solution éprouvée que des analystes comme Gartner, Radicati et d'autres identifient parmi les leaders du secteur. La solution DLP Forcepoint est disponible en deux versions : DLP pour la Conformité et DLP pour la Protection des IP.

Le DLP Forcepoint pour la Conformité fournit une capacité importante à résoudre la mise en conformité à l'aide des fonctionnalités suivantes:

- **La reconnaissance optique de caractères (OCR)** identifie les données présentes dans les images, statiques ou en mouvement.
- **Une identification solide des Informations personnelles d'identification (PII)** pour offrir des vérifications de validation des données, une détection de nom réel, des analyses de proximité et des identifiants de contexte.
- **L'identification à cryptage personnalisé** permet de repérer les données cachées lors de la découverte et de leur donner des contrôles applicables.
- **Analyse cumulative** pour une détection de microfuites DLP (données qui s'échappent lentement au fil du temps)
- **Intégration avec Microsoft Information Protection** pour analyser les fichiers cryptés et appliquer des contrôles DLP appropriés à ces données.

Forcepoint DLP pour la Protection des IP inclut les fonctionnalités ci-dessus, mais applique en plus la détection la plus avancée et contrôle les pertes de données potentielles avec des fonctionnalités comme:

- **L'apprentissage machine** pour former les utilisateurs à identifier des données pertinentes et jamais vues précédemment. Les utilisateurs fournissent au moteur des exemples positifs et négatifs pour lui signaler des documents commerciaux identiques, du code source et et autres.
- **Lesempreintes des données structurées et non structurées** permettent aux propriétaires de données de définir les types de données, pour ainsi identifier des correspondances totales et partielles à travers les documents commerciaux, les schémas techniques et les bases de données, puis appliquer ensuite le type de contrôle ou la politique adéquats avec ces données.
- **Les analyses identifient les changements dans le comportement des utilisateurs** alors qu'elles établissent des liens entre les interactions des données, pouvant par exemple remarquer un usage plus intensif du courriel personnel.

AGISSEZ SELON LES RISQUES

Les approches DLP traditionnelles noient les utilisateurs avec des faux positifs, tout en oubliant des données en situation de danger. Le DLP Forcepoint applique des analyses avancées pour corréler des événements DLP n'ayant en apparence aucun lien, et les passe en incidents prioritaires. Le Classement des risques des incidents (IRR) du DLP Forcepoint fusionne les indicateurs DLP dans le cadre de réseaux bayésiens, qui évaluent la probabilité des scénarios mettant les données en danger, comme le vol et les processus commerciaux non respectés.

- **Concentrez les efforts des équipes d'intervention** avec la priorisation des incidents, soulignant des personnes responsables des risques, les données critiques en danger et des modèles de comportement des utilisateurs.
- **Enquêtez et intervenez** avec des flux de travail qui relient entre eux des événements disparates, qui montrent le contexte de risque pour les données et qui donnent aux analystes les informations dont ils ont besoin pour agir.
- **Préservez la confidentialité des utilisateurs** avec des options d'anonymisation et de contrôle d'accès .
- **Ajoutez le contexte aux données** aux analyses élargies du comportement des utilisateurs avec une intégration en profondeur de Forcepoint Insider Threat et Forcepoint UEBA.

UNE VISIBILITÉ TOTALE OÙ QUE SOIENT VOS EMPLOYÉS, UN CONTRÔLE TOTAL SUR VOS DONNÉES OÙ QU'ELLES SE TROUVENT

Les entreprises d'aujourd'hui doivent affronter des environnements complexes, dans lesquels les données sont partout et demandent à être protégées dans des endroits qui ne sont pas gérés ou possédés par l'entreprise. Le DLP Forcepoint pour les applications cloud élargit les analyses et les politiques DLP aux applications cloud critiques pour que vos données soient toujours protégées, où qu'elles se trouvent.

- **Identifiez et protégez les données** à travers vos applications cloud, les stockages réseau, les bases de données et les terminaux gérés.
- **Gagnez en visibilité** sur les téléchargements, le partage de données et les données stockées sur les applications cloud les plus utilisées par les entreprises, notamment Office 365, Google Apps, Box, Salesforce, etc.
- **Unifiez l'application des politiques** via une console unique pour définir et appliquer des stratégies de découverte de données sur tous les canaux – cloud, réseaux et terminaux.
- La **solution hébergée Forcepoint** étend les fonctionnalités DLP de l'entreprise, y compris lesempreintes et l'apprentissage automatique des applications cloud

Le DLP Forcepoint inclut des modèles d'analyse et de politiques de réglementation avancées, à partir d'un point de contrôle unique lors de chaque déploiement. Les entreprises peuvent choisir les options de déploiement selon leurs environnements informatiques.

ANNEXE A : VUE D'ENSEMBLE DES COMPOSANTS DE LA SOLUTION DLP

DLP Forcepoint – Terminal	Forcepoint DLP – Terminal protège vos données critiques sur les terminaux Windows et Mac, connectés ou non au réseau de l'entreprise. Il inclut une protection et un contrôle avancés pour les données au repos (découverte), en transit et en cours d'utilisation. Il s'intègre avec Microsoft Information Protection pour analyser les fichiers cryptés et appliquer des contrôles DLP appropriés à ces données. Permet aux employés de prendre eux-mêmes en charge le risque lié aux données en se basant sur les indications de la boîte de dialogue de formation DLP. La solution surveille les téléchargements sur le Web (y compris via le protocole HTTPS) ainsi que les téléchargements vers des services cloud comme Office 365 et Box Enterprise. Intégration complète avec Outlook, Notes et des clients de courriel
Forcepoint DLP – Applications Cloud	Utilisant Forcepoint CASB, DLP – Applications Cloud élargit le champ des analyses et du contrôle avancées du DLP de Forcepoint aux applications cloud critiques, notamment Office 365, Salesforce, Google Apps, Box, ServiceNow et plus encore.
Forcepoint DLP – Découverte	Forcepoint DLP – Découverte vous permet d'identifier et de sécuriser les données sensibles sur votre réseauet dans des services cloud comme Office 365 et Box Enterprise. Des empreintes digitales de pointe identifient les données réglementées et les propriétés intellectuelles inactives, et protège ces données en appliquant un cryptage et des contrôles appropriés.
Forcepoint DLP – Réseau	Forcepoint DLP – Réseau permet d'arrêter le vol de données en transit via les messageries ou le web. La solution aide à identifier et empêcher la perte de données malveillante et accidentelle découlant d'attaques externes ou de menaces internes. La reconnaissance optique de caractères (OCR) permet de repérer des données dans une image. Un système DLP analyse et identifie les pertes de données pour stopper le vol de données au niveau de chaque fichier, et détecte aussi d'autres comportements à risque.

ANNEXE B : VUE DÉTAILLÉE DES COMPOSANTS DE LA SOLUTION DLP

	FORCEPOINT DLP – TERMINAL	FORCEPOINT DLP – CLOUD APPLICATIONS	FORCEPOINT DLP – DÉCOUVERTE	FORCEPOINT DLP – RÉSEAU
Comment cela est-il déployé ?	Forcepoint One Endpoint	Forcepoint Cloud	Serveur de découverte Géré par le service IT	Appareils réseau ou cloud public
Quelle est sa fonction principale ?	Collecte d'informations sur le terminal de l'utilisateur	Découverte des données et application de politiques dans le cloud ou avec des applications fournies par le cloud	Découverte, examen et intervention sur les données au repos se trouvant dans les centres de données	Visibilité et contrôle pour les données en transit via le web et les meessageries
Où se trouvent toutes les données découvertes et protégées quand elles sont au repos ?	Terminaux Windows Terminaux MacOS Terminaux Linux	Exchange Online Sharepoint Online Box	Serveurs de fichiers sur site et stockage réseau Serveur Sharepoint Serveur Exchange	
Où sont protégées les données en mouvement ?	Messagerie électronique Web : HTTP(S) Imprimantes Supports amovibles Appareils mobiles Serveurs de fichiers/NAS	Envoi, téléchargement et partage pour Office 365, Google Apps, Salesforce.com, Box et ServiceNow		Courriel/Courriel/ Proxy ActiveSync Web : HTTP(S) ICAP
Où sont protégées les Données en cours d'utilisation ?	Messagerie instantanée, VOIP; partage de fichiers, applications (clients de stockage cloud), presse-papier du système d'exploitation	Pendant les activités collaboratives via des applications Cloud		
Classement des risques d'incidents*	Inclus	Inclus		Inclus
Reconnaissance optique de caractères			Inclus	Inclus
Classification des données et Intégrations d'étiquetage	Microsoft Information Protection, Boldon James, Titus			
Quelles sont les données aux empreintes digitales ?	Structurées (bases de données), Non structurées (documents), Binaires (fichiers non textuels)			
Gestion unifiée des Politiques	Configuration et application des politiques via une console unique			
Importante bibliothèque de politiques	Découverte et application depuis une large bibliothèque de politiques			

*fonctionnalités disponibles seulement dans la version Protection des IP

À PROPOS DE FORCEPOINT

Forcepoint préserve les utilisateurs, les données et les réseaux contre les assaillants les plus déterminés, contre les menaces internes accidentelles ou malveillantes et contre les agresseurs externes, pendant tout le cycle de vie d'une menace. Forcepoint protège les données n'importe où – dans le clou, en déplacement ou au bureau – et simplifie la mise en conformité tout en permettant de prendre de meilleures décisions pour uniformiser la sécurité.Forcepoint donne aux entreprises le pouvoir de se concentrer sur ce qui est le plus important pour elles, tout en automatisant les tâches routinières de sécurité. Des milliers d'entreprises et d'entités gouvernementales, dans plus de 150 pays, font confiance à Forcepoint. Basé à Austin, au Texas, avec des contrats passés dans le monde entier et possédant ses propres laboratoires de sécurité, de service et de développement, Forcepoint est une joint-venture entre les entreprises Raytheon Company et Vista Equity Partners.

CONTACT

www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_DATA_LOSS_PREVENTION_FR] 400026.112618