Forcepoint

Fiche technique

Forcepoint DLP

Prévention de la perte des données de pointe avec gestion unifiée sur tous les canaux

La sécurité des données est critique, mais elle ne doit pas être compliquée. La main-d'œuvre hybride d'aujourd'hui a besoin d'accéder aux informations sensibles depuis n'importe quel appareil et en tout lieu. Forcepoint Data Loss Prevention (DLP) simplifie la protection des données pour l'entreprise moderne en offrant une prévention complète des pertes de données sur site sans sacrifier les performances ou la productivité.

Avec une visibilité profonde sur les mouvements de données sur les terminaux, les réseaux et le stockage, Forcepoint DLP protège vos actifs critiques et assure la conformité réglementaire. Il offre la capacité unique d'étendre les politiques de Forcepoint Security Manager (FSM) à des canaux supplémentaires, ce qui permet une protection transparente des données sur les applications SaaS cloud et sur le Web tout en assurant une application de politique cohérente et unifiée. Bénéficiez d'analyses avancées, d'une intégration transparente, de l'évolutivité et d'une solution qui s'adapte aux besoins de votre entreprise.

Rationalisez la conformité des données

- → **Réguler la couverture** pour répondre facilement aux exigences de conformité et les maintenir, grâce à plus de 1 800 modèles, politiques et classificateurs prédéfinis, dont plus de 70 couvrant les identifiants de pays, clés et jetons, applicables aux obligations réglementaires de plus de 90 pays et plus de 160 régions.
- → **Localisez et corrigez** les données réglementées avec la découverte du réseau, du cloud et des terminaux.
- → **Contrôle centralisé** et politiques cohérentes sur tous les canaux, y compris le cloud, les terminaux, le réseau, le web et le courriel.

Fournir une protection complète des données

- → **Découvrez et contrôlez les données** où qu'elles se trouvent, qu'elles soient dans le cloud, sur le réseau, dans les courriels ou 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 le cryptage automatique basé sur des politiques qui protège les données dès qu'elles quittent votre organisation.
- → **Automatisez l'étiquetage et la classification des données** grâce à l'intégration avec Forcepoint Data Classification et Microsoft Purview Information Protection.

Utilisez des fonctionnalités et des contrôles avancés

- **La reconnaissance optique des caractères (OCR)** intégrée au moteur de politiques identifie les données dans les images, qu'elles soient statiques ou en mouvement, que ce soit sur site ou dans le cloud, simplifiant l'infrastructure et garantissant une application hybride cohérente.
- **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 des contrôles applicables.
- **Analyse cumulative** pour une détection de microfuites DLP (les données qui s'échappent lentement au fil du temps)
- **L'analyse avancée des fichiers** détecte l'exfiltration des données partielles en examinant des sections aléatoires de fichiers volumineux, empêchant les exfiltrateurs de cacher des informations sensibles.
- **Intégration à Forcepoint Data Classification**, en tirant parti de modèles d'IA/LLM hautement qualifiés pour fournir une classification très précise des données en cours d'utilisation et des données au repos avec Forcepoint Data Security Posture Management (DSPM).
- L'**IA générative avancée** permet aux utilisateurs d'entraîner le système et de construire un modèle d'IA auto-apprenant, en trouvant, catégorisant et classifiant automatiquement toutes vos données pour gagner du temps et augmenter considérablement la précision.
- Les **empreintes** des données structurées (p. ex. les bases de données) et non structurées (p. ex. les documents), qui 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 adéquate pour ces données.
- Avec la **Risk-Adaptive Protection**, le Forcepoint DLP devient encore plus efficace en tirant parti des analyses de comportement pour comprendre le niveau de risque d'un utilisateur. Ce niveau est ensuite utilisé pour appliquer automatiquement des politiques adaptatives au risque posé par l'utilisateur.

Rechercher et atténuer les risques de protection des données

- **Concentrez les efforts des équipes d'intervention** avec la priorisation des incidents, en mettant en avant les personnes responsables des risques, les données critiques en danger et les modèles de comportement des utilisateurs.
- **Utilisez l'outil d'aide Smart Search alimenté par l'IA** et intégré directement dans la solution pour trouver rapidement des informations de support spécifiques sans quitter la console de gestion.
- **Sensibilisez le personnel** à la manipulation de données et d'IP sensibles grâce à l'encadrement des employés sur Windows et macOS, en plus de les faire participer à Forcepoint Data Classification comme Boldon James et Microsoft Azure Information Protection.
- **Mettez en œuvre des capacités d'identification des données DLP avancées**, par exemple la prise d'empreintes, sur les terminaux distants et dans les applications d'entreprise situées dans le cloud.
- **Permettez aux propriétaires de données et aux cadres de l'entreprise** de passer en revue les incidents DLP et d'y répondre grâce à un flux de travail distribué par courrier électronique.
- **Préservez la confidentialité des utilisateurs** avec des options d'anonymisation et de contrôle d'accès.
- **Ajoutez du contexte aux données** aux analyses élargies du comportement des utilisateurs avec une intégration en profondeur de la Protection adaptative au risque de Forcepoint.
- **Les intégrations d'identité** prennent en charge Entra ID cloud-native pour l'accès administratif comme pour l'application des politiques destinées aux utilisateurs finaux, renforçant ainsi la cohérence de la sécurité et simplifiant la gestion.

Obtenez une visibilité sur l'ensemble de vos données

- → **Donnez aux administrateurs** les moyens d'identifier et de protéger les données dans les applications cloud, les magasins de données réseau, les bases de données et les terminaux gérés et non gérés.
- → **Identifiez et empêchez automatiquement le partage** de données sensibles avec des utilisateurs externes ou des utilisateurs internes non autorisés.
- → **Protégez les données en temps réel** pour les téléchargements vers et depuis des applications cloud critiques, notamment Office 365, Teams, SharePoint, Salesforce, Box, Dropbox, Google Apps, AWS, ServiceNow, Zoom, Slack, et bien d'autres.
- → **Unifiez l'application des politiques** via une console unique pour définir et appliquer des stratégies de découverte sur les données statiques et en transit à travers tous vos canaux – cloud, réseaux, terminaux., web et e-mail.
- → **Conservez la propriété des données** avec une solution DLP sur site et des options hybrides pour étendre les fonctionnalités avancées telles que la prise d'empreintes, l'apprentissage machine et l'application de politiques aux applications Cloud et aux canaux Web. Idéal pour les industries hautement réglementées - permet d'assurer la souveraineté des données en conservant en toute sécurité les données d'incidents et d'investigation dans votre centre de données tout en prenant en charge les exigences de conformité.
- → **Affichez et gérez les incidents en utilisant des outils tiers** via des API REST exposées. Automatisez les flux de gestion des incidents et soutenez les processus d'entreprise en fonction des incidents DLP grâce à des outils d'automatisation et de service tels que ServiceNow, Nagios et Tableau, ainsi que les solutions SIEM/SOAR telles que Splunk et XSOAR.

Pour plus d'informations sur nos solutions Enterprise DLP, demandez une démo.

Annexe A : vue d'ensemble des composants de la solution DLP

Forcepoint DLP Endpoint	Forcepoint DLP Endpoint protège vos données critiques sur les terminaux Windows et Mac, sur le réseau de l'entreprise ou en dehors. Il comprend une protection et un contrôle avancés pour les données au repos (découverte), en transit et en cours d'utilisation. Il s'intègre à Microsoft Azure Information Protection pour analyser les données chiffrées et appliquer les contrôles DLP appropriés. Il permet aux employés de prendre eux-mêmes en charge les risques liés aux données en se basant sur les indications de la boîte de dialogue de formation DLP. La solution surveille les téléversements sur le web, y compris HTTPS, ainsi que les téléversements vers des services cloud comme Office 365 et Box Enterprise. OCR intégrée dans le moteur de politiques, permettant de visionner les données contenues dans les images. Intégration complète avec Outlook, Notes et les clients de messagerie.
Forcepoint CASB	Basé sur Forcepoint CASB, étendez les analyses avancées et le contrôle unique de Forcepoint DLP aux applications cloud autorisées, y compris Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack et bien d'autres. Maîtrisez en permanence les données critiques, quel que soit l'endroit où se trouvent les utilisateurs et l'appareil qu'ils utilisent.
Forcepoint Web Security	Forcepoint Web Security vous permet d'accéder en toute sécurité à n'importe quel site Web ou de télécharger n'importe quel document tout en bénéficiant des performances Web à haut débit sur lesquelles votre équipe compte. Intégrez à RBI pour un rendu sécurisé des sites à risque, et à Zero Trust CDR pour une désinfection complète de tous les documents téléchargeables.
Forcepoint DLP Discover	Forcepoint DLP Discovery identifie et sécurise les données sensibles sur les serveurs de fichiers, SharePoint (on-premises et dans le cloud), Exchange (on-premises et dans le cloud), et la détection dans les bases de données telles que SQL Server et Oracle. La technologie avancée d'empreinte digitale identifie les données réglementées et la propriété intellectuelle au repos et protège ces données en appliquant le chiffrement et les contrôles appropriés. OCR intégrée dans le moteur de politiques, permettant de visionner les données contenues dans les images.
Forcepoint DLP Network	Forcepoint DLP Network fournit le point d'application critique pour arrêter le vol de données en transit via les courriels, les canaux web et FTP. La solution aide à identifier et à prévenir l'exfiltration des données et la perte accidentelle de données due à des attaques externes ou à des menaces internes. OCR intégrée dans le moteur de politiques, permettant de visionner les données contenues dans les images. Analytics fournit Drip DLP pour arrêter le vol lent et progressif de données (un fragment de fichier à la fois), ainsi que d'autres comportements d'utilisateurs à haut risque.
Forcepoint DLP for Cloud Email	Forcepoint DLP for Cloud Email empêche l'exfiltration non autorisée de vos données et de votre adresse IP par le biais du courriel sortant. Vous pouvez les combiner avec les autres solutions de canaux Forcepoint DLP telles que Endpoint, Network, Cloud et Web pour simplifier votre gestion DLP, en rédigeant une seule politique et en déployant cette politique sur plusieurs canaux. Contrairement aux solutions non cloud, Forcepoint DLP for Cloud Email permet un énorme potentiel d'évolutivité en cas d'augmentation imprévue du trafic de courriel. Inclut l'OCR pour une application cohérente dans les déploiements hybrides. Elle permet également à votre trafic de courriel sortant de croître avec votre entreprise, le tout sans avoir à configurer et à gérer des ressources matérielles supplémentaires.
Forcepoint DLP App Data Security API	Forcepoint DLP App Data Security API permet aux entreprises de sécuriser facilement les données dans leurs applications et services personnalisés internes. Il permet d'analyser le trafic de fichiers et de données et d'appliquer des actions DLP telles que l'autorisation, le blocage, la demande de confirmation par le biais d'une fenêtre contextuelle personnalisée, le chiffrement, l'annulation du partage et la mise en quarantaine. Il s'agit d'une API REST facile à comprendre et à utiliser sans formation approfondie ou maîtrise des protocoles complexes. Il est également indépendant du langage, ce qui permet de développer et d'utiliser n'importe quel langage de programmation ou n'importe quelle plateforme.

Annexe B : aperçu des composants de la solution DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Quelle est sa fonction principale ?	Découverte des données et application des politiques de protection des données sur les terminaux des utilisateurs via les applications, le Web, les documents imprimés et les supports amovibles, pour n'en nommer que quelques-uns.	Découverte des données et application des politiques dans le cloud ou avec les applications fournies par le cloud	Visibilité et contrôle des données en transit via les courriels sortants	Découverte, analyse et correction les données au repos dans les centres de données et autres environnements locaux	Visibilité et contrôle des données en mouvement via le web et le courriel au sein du réseau	Visibilité et contrôle des données en mouvement via le web et le courriel au sein du réseau	Visibilité et maîtrise des données dans les applications et services personnalisés internes
Où sont les données découvertes/ protégées quand elles se trouvent au repos ?	Terminaux Windows Terminaux MacOS	OneDrive, SharePoint Online, Exchange Online, Google Drive, Box, DropBox, Salesforce, ServiceNow	Serveurs de fichiers sur site et stockage réseau : SharePoint, Exchange, Bases de données comme Microsoft SQL Server, Oracle et IBM Db2				
Où sont protégées les données en transit ?	E-mail, Web: HTTP(S), imprimantes, supports amovibles, serveurs de fichiers / NAS	Chargements, téléchargements et partage pour Office 365, Google Apps, Salesforce. com, Box, Dropbox & ServiceNow via API et TOUTES les autres applications majeures via un proxy	HTTP(S)		Courriel, imprimantes, FTP, Web : Http(S), ICAP	Courriel	Applications et services personnalisés internes
Où sont protégées les données en cours d'utilisation ?	Zoom, Webex, Google Hangouts, IM, partage de fichiers VOIP , Partage M365 Teams, applications (clients de stockage dans le cloud), presse-papiers OS	Pendant les activités de création, de modification et de collaboration utilisant les applications cloud					Applications et services personnalisés internes

Annexe B : comparaison des fonctionnalités de la solution DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Risk-Adaptive Protection	Module complémentaire		Module complémentaire actuellement pris en charge avec les tunnels GRE/IPSec avec Forcepoint Web Security	Module complémentaire	Module complémentaire	Module complémentaire	
Reconnaissance optique de caractères				Inclus	Inclus	Inclus	
Classification des données et intégrations d'étiquetage	Forcepoint Data Classification and Microsoft Purview Information Protection.						
Sur quelles données peut-on relever les empreintes ?	Structurées (bases de données), Non structurées (documents), Binaires (fichiers non textuels)						
Gestion unifiée des politiques	Configuration et application des politiques via une console unique allant des terminaux aux applications cloud						
Importante bibliothèque de politiques	Découverte et mise en application à partir de la plus grande bibliothèque de politiques de conformité du secteur.						