Forcepoint Data Loss Prevention

Protection des données dans un monde sans périmètre

Forcepoint

Brochure

forcepoint.com/fr

Forcepoint Data Loss Protection (DLP)

La sécurité des données partout où vos employés travaillent et résident

Assurer la sécurité des données est aujourd'hui un problème majeur pour les entreprises de tous les secteurs types et de toutes les tailles. D'une part, les entreprises d'informatique sont tenues de respecter les réglementations et de protéger les informations personnelles identifiables (PII), les données de santé et d'autres types d'informations réglementées contre les attaques malveillantes ciblées et les pertes accidentelles de données. De plus, elles doivent s'adapter aux profonds bouleversements qui perturbent le paysage informatique, comme l'adoption des applications cloud, les environnements cloud hybrides et les tendances PAP (utilisation de l'équipement personnel) : tout cela génère une augmentation des facteurs de fuite des données de votre entreprise.

Cette expansion de la surface d'attaque pose un défi majeur à ceux qui ont pour mission de protéger les données critiques. Les équipes chargées de la sécurité des données doivent tenir compte de l'explosion du mouvement des données depuis « l'intérieur » de l'entreprise, et de tous les endroits et canaux où les données résident et se déplacent désormais. Il est indispensable de pouvoir visualiser toutes les données, dans le cloud aussi bien que sur site. Les équipes chargées de la sécurité des données doivent également disposer d'une visibilité et d'un contrôle sur tous les canaux (terminaux, trafic web, réseau, courrier électronique et cloud) via un point de gestion unique.

Forcepoint DLP est la solution la plus fiable du secteur. Elle vous donne les outils nécessaires pour gérer facilement des politiques globales sur tous vos principaux canaux, qu'il s'agisse des terminaux, des réseaux, du cloud, du web ou des courriels. Nous pouvons simplifier votre travail grâce à nos modèles, politiques et classificateurs prédéfinis les plus nombreux de tous les fournisseurs DLP du secteur. Vous pouvez ainsi rationaliser considérablement votre gestion des incidents et vous concentrer sur l'essentiel, à savoir éliminer les risques et augmenter la productivité de vos salariés. Forcepoint DLP s'attaque aux risques en vous apportant visibilité et contrôle, partout où vos employés travaillent et partout où résident vos données.

La protection des données doit :

- **Assurer la sécurité des données réglementées** avec un point de contrôle unique par lequel transitent toutes les applications avec lesquelles les utilisateurs créent, sauvegardent et déplacent les données.
- **Protégez vos données sensibles** avec un DLP avancé qui analyse la façon dont les données sont utilisées, qui apprend à vos utilisateurs À bien gérer les données et qui hiérarchise les incidents par risque.

Protection des canaux importants

- **Applications personnalisées**
- **Applications cloud**
- **Applications privées**
- **Terminal**
- **Réseau**
- **Discovery**
- **Web**
- **Courriel**

Accélérez votre mise en conformité

Donnez à chacun le pouvoir de protéger les données

Détection et contrôle avancés

Intervenez et agissez selon les risques

Accélérez votre mise en conformité

Les environnements IT modernes posent un défi colossal aux entreprises souhaitant être en conformité au niveau mondial. Elles doivent respecter des dizaines de réglementations de sécurité, 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, mais inconsistantes pour les terminaux, les applications cloud et les réseaux. Forcepoint DLP accélère vos efforts de conformité en fournissant plus de 1600 classifieurs, politiques et modèles prédéfinis. Cela permet d'accélérer le déploiement initial du DLP et simplifie sa gestion courante. Le DLP Forcepoint permet de sécuriser efficacement les informations clients confidentielles et les données réglementées, afin que vous puissiez prouver en toute confiance votre respect des normes en cours.

- → **Régulez** la couverture afin de satisfaire et de maintenir la conformité avec plus de 1600 modèles, politiques et classifieurs prédéfinis applicables aux exigences réglementaires de 83 pays et de plus de 150 régions.
- → **Repérez et intervenez** sur les données réglementées avec la découverte sur le réseau, le cloud et les terminaux.
- → **Contrôle centralisé** et politiques cohérentes sur tous les canaux, y compris le cloud, les terminaux, le réseau, le web et le courriel.

Donnez à chacun le pouvoir de protéger les données

Un DLP proposant uniquement un contrôle préventif risque de frustrer les utilisateurs, ce qui les poussera à contourner les mesures pour pouvoir terminer une tâche. Contourner les mesures de sécurité fait prendre des risques superflus et peut générer une fuite des données survenant par inadvertance.

Le DLP Forcepoint part du principe que vos salariés sont en première ligne face aux cybermenaces.

- → **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.
- → **Enseignez aux employés** la prise de bonnes décisions, en diffusant des aides à la décision, des informations sur les politiques et validez les intentions des utilisateurs lors de ses 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** Avec l'intégration de Forcepoint Data Classification et Microsoft Purview Information Protection.

Détection et contrôles avancés qui suivent les données

Les fuites de données accidentelles et malveillantes représentent des incidents complexes et ne sont pas de simples événements. Forcepoint DLP est reconnu par Forrester, Gartner, Radicati Group et Frost & Sullivan comme un leader du secteur des solutions DLP. L'une des fonctionnalités clés est la capacité de Forcepoint DLP à identifier les données au repos, en mouvement et en cours d'utilisation. L'identification des données clés comprend:

- → **La reconnaissance optique de caractères (OCR)** identifie les données présentes dans les images, statiques ou en mouvement.
- → **Une identification renforcée** 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'intégration à Forcepoint Data Classification,** en exploitant des modèles d'IA/ML hautement qualifiés pour fournir une classification très précise des données utilisées.

- → **L'apprentissage machine**, qui permet de former les utilisateurs à identifier des données pertinentes, mais jamais vues auparavant.Les utilisateurs alimentent le moteur avec des exemples positifs et négatifs pour marquer des documents commerciaux identiques, du code source et autres.
- → **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.
- → **Les analyses**, qui 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. Avec la Protection dynamique des données, le DLP Forcepoint devient encore plus efficace en tirant parti des analyses comportementales 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.Cela permet aux équipes de sécurité de déployer des politiques dynamiques individualisées, plutôt que de s'appuyer sur des politiques globales statiques.

Identifier, gérer et résoudre les risques de protection des données.

La plupart des autres solutions DLP n'ont pas la robustesse d'une solide bibliothèque de classification prédéfinie et n'ont pas la visibilité sensible de toutes vos données, ce qui surcharge les utilisateurs de faux positifs tout en oubliant de protéger les données à risque. En plus de rendre les équipes de sécurité moins efficaces, cela frustre le personnel ou les utilisateurs, car ils considèrent les solutions de sécurité comme une entrave à leur productivité. Grâce à l'analyse et à la plus grande bibliothèque de modèles et de politiques prédéfinis du secteur, Forcepoint DLP réduit considérablement les faux positifs, ce qui renforce l'efficacité des activités de sécurité. Pour accroître la sensibilisation des employés à la sécurité, le DLP forme le personnel et promeut l'intégration de solutions de classification 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.
- → **Sensibilisez les employés** à à la manipulation des données sensibles et de propriété intellectuelle avec un coaching des employés sur Windows et macOS, en plus de permettre aux employés d'intégrer des solutions de classification comme Forcepoint Data Classification et Microsoft Purview Information Protection.
- → **Mettez en œuvre de 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.

Une visibilité omniprésente, y compris de vos données sur site et dans le cloud.

Les entreprises d'aujourd'hui doivent affronter des environnements complexes, au sein desquels les données sont omniprésentes et nécessitent protection dans des endroits qui ne sont pas gérés ou détenus par l'entreprise. Forcepoint ONE CASB, SWG et ZTNA étend les politiques d'analyse et de DLP aux applications cloud critiques, au trafic Web et aux applications privées basées sur le Web afin que vos données soient protégées, en tout lieu. Les API REST telles que Forcepoint DLP App Data Security API apportent visibilité et mise en application de la DLP aux applications développées en interne.

- → **Concentrez les efforts des équipes d'intervention pour identifier et protéger** les données transitant dans les applications cloud, les stockages de données en réseau, les bases de données et les terminaux 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 courriel
- → **Déployez une solution hébergée par Forcepoint** qui étend les fonctionnalités des politiques DLP, comme la prise d'empreintes digitales et l'apprentissage machine, aux applications cloud, tout en ayant la possibilité de conserver les données d'incidents et les indices au sein de votre centre de données.
- → **Visualisez les incidents et gérez-les dans des outils d'enquête tiers** par le biais d'API REST vulnérables. 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.

Le DLP Forcepoint inclut des modèles d'analyse et de politiques de réglementation avancés, à partir d'un point de contrôle unique, et lors de chaque déploiement.

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

Forcepoint DLP Endpoint	Forcepoint DLP – Terminaux 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 statiques (découverte), en transit et en cours d'utilisation. Il s'intègre avec Microsoft Azure Information Protection pour analyser les fichiers cryptés et appliquer des contrôles DLP appropriés à ces données. 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 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 d'autres clients de courriel
Forcepoint ONE CASB	Basé sur Forcepoint ONE 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 ONE SWG	Forcepoint ONE SWG 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 ONE ZTNA (à venir 2e semestre 2023)	Forcepoint ONE ZTNA offre un accès à distance Zero Trust simple, sûr et évolutif aux applications cloud internes et privées sans avoir besoin d'un VPN sur les appareils gérés et non gérés.
Forcepoint DLP —Discover	Forcepoint DLP – Discovery identifie et sécurise les données sensibles sur les serveurs de fichiers, SharePoint (sur site et dans le cloud), Exchange (sur site et dans le cloud), et la détection dans les bases de données telles que SQL Server et Oracle. Des empreintes digitales de pointe identifient les données réglementées et les propriétés intellectuelles inactives, et protègent ces données en appliquant un cryptage et des contrôles appropriés. Discovery inclut également l'analyse OCR qui permet de visualiser des données dans les images.
Forcepoint DLP – Network	Forcepoint DLP – Network permet d'arrêter le vol de données qui transitent via les messageries ou le web. La solution aide à identifier et empêcher l'exfiltration de données et les pertes de données accidentelles découlant d'attaques externes ou de menaces internes. La reconnaissance optique de caractères (OCR) permet de repérer des données dans une image. Analytiques inclut 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	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. Il 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
API de sécurité des données Forcepoint DLP	L'API de sécurité des données Forcepoint DLP 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 applique les actions de DLP telles qu'autoriser, bloquer, demander la validation avec une fenêtre pop-up personnalisée, chiffrer, annuler le partage et mettre 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 plateforme.

Annexe B : aperçu des composants de la solution DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP— DISCOVER	FORCEPOINT DLP— NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	API DE SÉCURITÉ DES DONNÉES FORCEPOINT DLP	FORCEPOINT ONE ZTNA (À VENIR 2e 2023)
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.	Decouverte des donnees et application de politiques dans le cloud ou avec des applications fournies par le cloud	Découverte, analyse et correction les données au repos dans les centres de données et autres environnements sur site	Visibilité et contrôle des données en mouvement via le web et le courriel au sein du réseau	Visibilité et contrôle des données en transit via les courriels sortants	Visibilité et contrôle des données en mouvement via le web (mais pas dans le réseau)	Visibilité et maîtrise des données dans les applications et services personnalisés internes	Visibilité et application des politiques de protection pour les données en mouvement (uploads et téléchargements) dans une application privée d'entreprise
Où se trouvent toutes les données découvertes et protégées quand elles sont 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 ?	Email, Web : HTTP(S), Imprimantes, Medias 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		Courriel, imprimantes, Web : HTTP(S) ICAP	Courriel	HTTP(S)	Applications et services personnalisés internes	Uploads et téléchargements via ZTNA Connector vers les applications privées
Où sont protégées les données en cours d'utilisation ?	Zoom, Webex, Google Hangouts, IM, partage de fichiers VOIP, partage d'équipe M365, applications (clients de stockage sur cloud), presse-papiers OS	Pendant les activités collaboratives via des applications Cloud						

Annexe B : comparaison des fonctionnalités de la solution DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP— DISCOVER	FORCEPOINT DLP— NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	API DE SÉCURITÉ DES DONNÉES FORCEPOINT DLP	FORCEPOINT ONE ZTNA (À VENIR 2e 2023)
Risk-Adaptive Protection	Module complémentaire		Module complémentaire	Module complémentaire	Module complémentaire	Module complémentaire actuellement pris en charge avec les tunnels GRE/IPSec avec Forcepoint ONE SWG		
Reconnaissance optique de caractères			Inclus	Inclus	Inclus			Prise en charge OCR pour l'amélioration DLP (2e semestre 2023)
Classification des données et intégrations d'étiquetage	Forcepoint Data Classification et Microsoft Purview Information Protection.							
Sur quelles données peut-on relever les empreintes ?*	Structurées (bases de données), Non structurées (documents), Binaires (fichiers non textuels)							Disponible au 2e semestre 2023
Gestion unifiée des politiques	Configuration et application des politiques via une console unique allant des terminaux aux applications cloud							Disponible au 2e semestre 2023
Importante bibliothèque de politiques	Découverte et mise en application à partir de la plus grande bibliothèque de politiques de conformité du secteur.							

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifie la sécurité des entreprises et des gouvernements à l'échelle mondiale. CLa plateforme tout-en-un de Forcepoint, de conception 100 % cloud, facilite l'adoption de Zero Trust et empêche le vol ou la perte des données sensibles et des propriétés intellectuelles, où que les gens travaillent. Basé à Austin, Texas, Forcepoint créé des environnements sûrs pour ses clients et leurs employés dans plus de 150 pays. Retrouvez Forcepoint sur www.forcepoint.com/fr, Twitter et LinkedIn.