# Forcepoint Data Loss Prevention (DLP)

La protection des données dans un monde sans périmètre

Forcepoint

Brochure

# Forcepoint DLP

## La sécurité orientée vers l'humain

Préserver la sécurité des données est un challenge sans fin. Les entreprises du secteur IT doivent maintenir leur niveau de respect des réglementations et protéger leurs propriétés intellectuelles contre les attaques ciblées et les failles accidentelles. 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 BYOD (apportez votre propre 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 en charge de la sécurité des données adoptent l'approche la plus logique pour suivre les données en les rassemblant, en les répertoriant et en les contrôlant. Mais aujourd'hui, les approches traditionnelles contre les pertes de données ont perdu leur efficacité, car elles ne prennent pas en compte la variable la plus importante en sécurité des données : les humains, le personnel avec lequel vous travaillez.

Plutôt que de se concentrer uniquement sur les données, la sécurité devrait commencer et finir par le facteur humain : le comportement des utilisateurs. Le point clé est d'acquérir une plus grande visibilité sur les interactions entre les utilisateurs, les données et les applications. Une fois cet objectif atteint, vous accédez à un niveau de contrôle basé sur le risque spécifique posé par l'utilisateur et le degré de confidentialité ou d'importance des données.

Le programme de protection des données d'une entreprise doit tenir compte du facteur humain – le point d'intersection vers le quel convergent utilisateurs, données et réseaux. De plus, l'entreprise doit maintenir sa vigilance sur la sécurité des données au cours de leurs divers transits dans l'entreprise et clairement identifier les membres du personnel qui peuvent créer, avoir accès, ou déplacer ces données.

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 attribués à chaque utilisateur pour se centrer sur les événements qui sont les plus significatifs, et pour accélérer la mise en conformité avec les réglementations mondiales touchant aux 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.
- **Protéger les propriétés intellectuelles** avec une solution DLP avancée qui analyse l'utilisation des données par le personnel, enseigne aux utilisateurs la prise de bonnes décisions quant au traitement de leurs données, et priorise les incidents par catégorie de risque.

## Visibilité et contrôle partout où votre personnel travaille et où vos données résident

- **Applications Cloud**
- **Terminal**
- **Réseau**
- **Discovery**

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 avec 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 mise en conformité en proposant une couverture générique respectant des réglementations mondiales, combinée à un contrôle central élargi à l'ensemble de votre environnement informatique. 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.

- → **Prise en charge de réglementations** respectant les exigences de conformité de plus de 370 politiques, pour couvrir les exigences légales dans 83 pays.
- → **Repérez et intervenez** sur les données réglementées en allant les découvrir dans le réseau, dans le cloud et sur les terminaux.
- → **Un contrôle centralisé** et des politiques cohérentes sur l'ensemble de l'environnement informatique.

## Donnez à chacun le pouvoir de protéger les données

Un DLP proposant uniquement un contrôle préventif risque de frustrer 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 survenant par inadvertance.

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

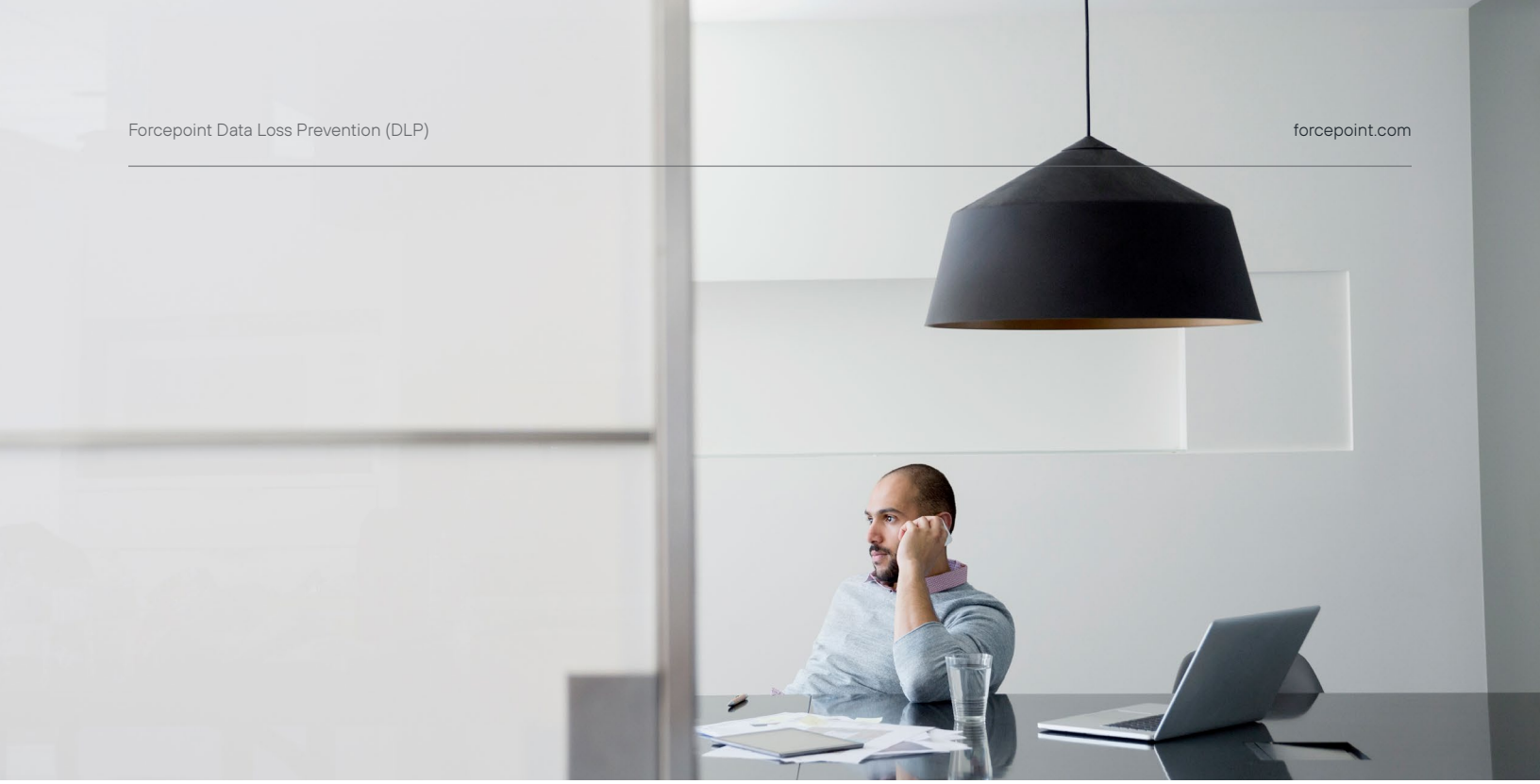
- → **Découvrez et contrôlez les données** où qu'elles se trouvent, qu'elles soient dans le cloud, sur le réseau, dans les courriels et sur le point d'accès.
- → **Enseignez aux employés** la prise de bonnes décisions, en diffusant des aides à la décision, des informations sur les politiques et validez les intentions des utilisateurs lors de ses interactions avec les données critiques.
- → **Collaborez en toute sécurité** avec des partenaires de confiance en utilisant 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 Azure Information Protection, Titus, Boldon James).

## Détection et contrôles avancés qui suivent les données

Les fuites de données accidentelles et malveillantes correspondent à des incidents complexes, et ne sont pas de simples événements. Le DLP Forcepoint est une solution éprouvée que des analystes comme Gartner, Radicati et d'autres identifient comme étant le leader de ce secteur. Les solutions DLP Forcepoint sont disponibles en deux versions : DLP pour la Conformité et DLP pour la Protection des propriétés intellectuelles (IP)

DLP pour la Conformité de Forcepoint 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 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)
- → **Intégration avec Microsoft Azure Information Protection** pour analyser les fichiers cryptés et appliquer les contrôles DLP appropriés à ces données.



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

- → **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 (comme les bases de données) et non structurées (comme 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 avec 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 des politiques adaptatives au risque posé. 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.

Les approches DLP traditionnelles submergent les utilisateurs de faux positifs, tout en omettant des données en situation de danger réel. En plus de rendre les équipes de sécurité moins efficaces, cela frustre le personnel ou les utilisateurs, qui considèrent alors les solutions de sécurité comme une entrave à leur productivité. En s'appuyant sur des analyses, Forcepoint DLP réduit les faux positifs, ce qui facilite les opérations 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 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 des solutions de classification comme Boldon James et Microsoft Azure 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 le contexte aux données** aux analyses élargies du comportement des utilisateurs avec une intégration en profondeur de Forcepoint Insider Threat et Forcepoint Behavioral Analytics.

## Une visibilité totale où que le personnel se trouve, un contrôle total sur vos données, où qu'elles résident

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 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 protégées en permanence, où qu'elles se trouvent.

- → **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, Salesforce, Box, Dropbox, Google Apps, Amazon 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 sur tous les canaux – cloud, réseaux et terminaux.
- → **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.

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. Les entreprises peuvent choisir les options de déploiement en fonction de leur environnement informatique.

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

| | |
|---|---|
| **Forcepoint DLP - Terminal** | 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 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 autorisées, notamment Office 365, Salesforce, Google Apps, Box, Dropbox, ServiceNow Amazon AWS, Zoom, Slack et plus encore. |
| **DLP Forcepoint – Discovery** | 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. |
| **DLP Forcepoint – Réseau** | Forcepoint DLP – Réseau 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. Un système DLP analyse et identifie les pertes de données pour stopper le vol de données au niveau de chaque fichier, et détecte les anomalies et autres comportements d'utilisateurs présentant un risque élevé. |

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

| | FORCEPOINT DLP – TERMINAL | FORCEPOINT DLP – CLOUD APPLICATIONS | FORCEPOINT DLP – DISCOVER | FORCEPOINT DLP – NETWORK |
|---|---|---|---|---|
| **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 ?** | Collection 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 services de messagerie |
| **Où se trouvent toutes les données découvertes et protégées quand elles sont au repos ?** | Terminaux Windows, MacOS et Linux | 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, Médias ou appareils mobiles amovibles, Serveurs de fichiers/NAS | Chargements, téléchargements et partage pour Office 365, Google Apps, Amazon AWS, Salesforce.com, Box, Dropbox & ServiceNow via API et toutes les autres applications majeures via proxy | | Email, proxy ActiveSync, Web : HTTP(S) ICAP |
| **Où sont protégées les données en cours d'utilisation ?** | Avec Zoom, Webex, Google Hangouts, IM, dans le partage de fichiers via VOIP, les applications (clients de stockage cloud), et le presse-papiers du système d'exploitation | Pendant les activités collaboratives via des applications Cloud | | |
| **Protection dynamique des données*** | Module complémentaire | | | Module complémentaire |
| **Reconnaissance optique de caractères** | | | Inclus | Inclus |
| **Classification des données & intégrations d'étiquettes** | Microsoft Azure Information Protection, Boldon James, Titus | | | |
| **Quelles sont les données dont on peut prendre 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 via les centres de données et les clouds publics | | | |
| **Importante bibliothèque de politiques** | Découverte et application depuis une large bibliothèque de politiques | | | |

# Bienvenue à l'ère de la Cybersécurité centrée sur l'humain

Forcepoint

**forcepoint.com/contact**

## À propos de Forcepoint

Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données ; son objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Les solutions personnalisées de Forcepoint s'adaptent en temps réel à la façon dont les usagers interagissent avec les données, et offrent un accès sécurisé tout en permettant aux employés de créer de la valeur. Basé à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables protégeant des milliers de clients dans le monde entier.