Forcepoint

Fiche technique

Forcepoint Data Security Posture Management

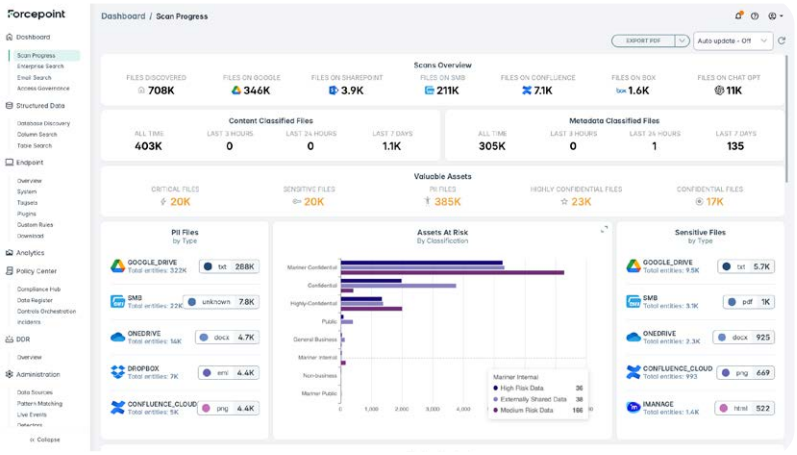
Avantages et fonctions clés :

- **AI Mesh Classification** – L'inspection complète du contenu permet une classification hautement précise et efficace grâce à GenAI, à l'apprentissage automatique et aux meilleurs classificateurs de données de Forcepoint.
- **Découverte rapide** – Exécutez Forcepoint DSPM dans le cloud et les emplacements de stockage sur place, aussi souvent que vous le souhaitez.
- **Évaluation des risques en temps réel** – Contrôlez les autorisations d'accès et autres risques liés aux données.
- **Orchestration des flux de travail** – Mettez en œuvre les priorités de l'entreprise pour les parties prenantes.

La transformation numérique a évolué vers une transformation par l'IA, portée par l'intégration des technologies d'IA dans les processus métier, notamment les applications GenAI et l'Agentic AI. Les organisations sont confrontées à une difficulté constante : savoir où se trouvent leurs données sensibles, qui peut y accéder, et comment en contrôler l'usage, alors qu'elles migrent applications et données entre systèmes sur site et cloud tout en développant l'usage de l'IA. La croissance exponentielle des "dark data", dissimulées dans des dépôts basés sur le cloud ou dispersées sur des appareils individuels et désormais dans les applications GenAI, représente un risque considérable. On estime que jusqu'à 80 % des données d'une organisation existent dans cet état "dark" échappant à toute surveillance traditionnelle.

Les conséquences de ce paysage de données obscurci peuvent être désastreuses. Sans visibilité ni gestion claires, les organisations s'exposent à des risques accrus de violations de données, aux conséquences potentiellement dévastatrices, aussi bien dans les secteurs commercial, associatif que gouvernemental. À l'ère actuelle de la transformation par l'IA, l'impératif de reprendre le contrôle des informations sensibles n'a jamais été aussi urgent. La seule façon de résoudre ce problème tout en suivant le rythme accéléré des affaires est l'automatisation, alliée à la précision et à l'explicabilité.

Forcepoint DSPM découvre et classe rapidement les données sensibles à grande échelle, couvrant aussi bien les données structurées que non structurées. Son AI Mesh unique assure une inspection complète du contenu, rapide et explicable, grâce à un modèle de langage restreint (SLM) hautement performant et à plus de 20 ans de classificateurs de données soigneusement élaborés par Forcepoint. Cet AI Mesh permet également une personnalisation sans nécessiter de réentraînement approfondi du modèle, garantissant une classification rapide et précise pour une confiance et une conformité renforcées.

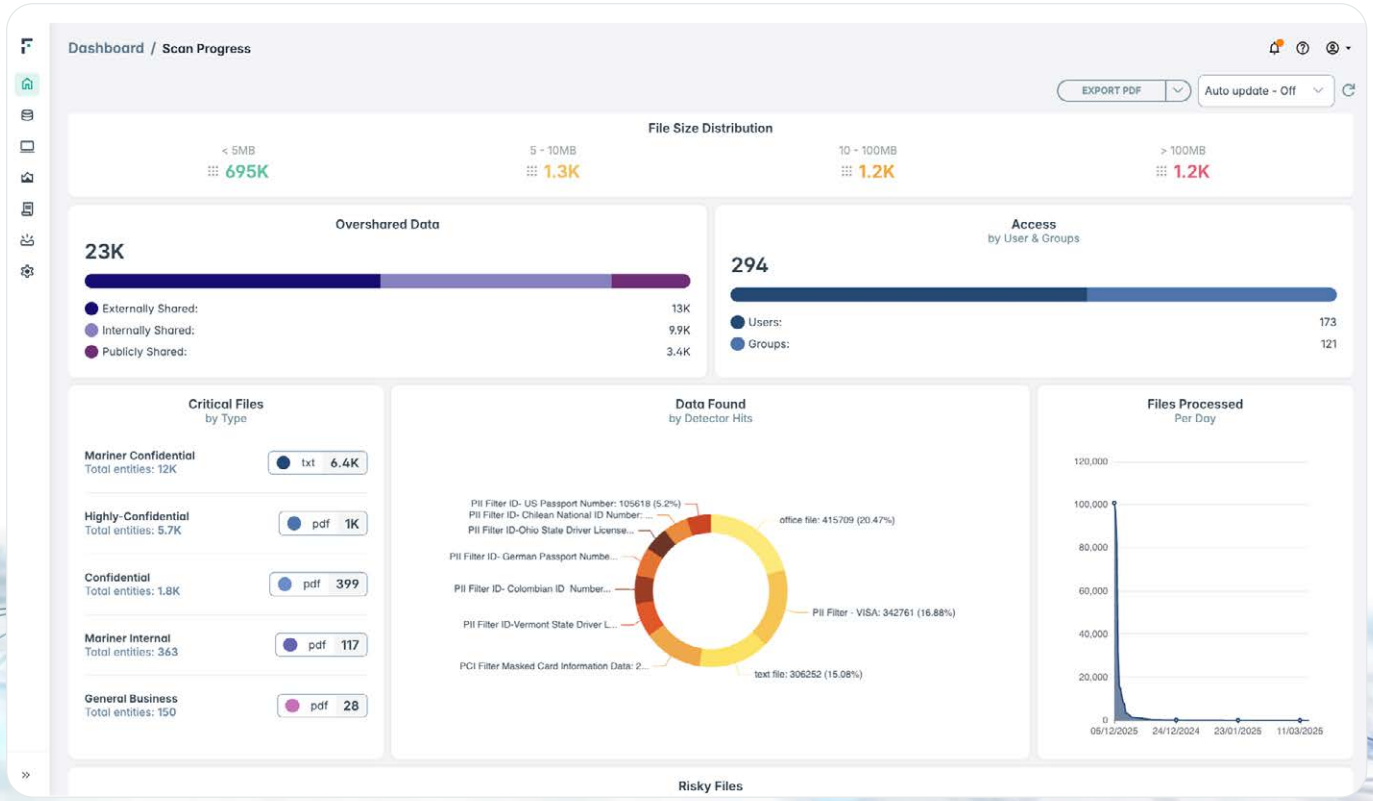


Découverte rapide et complète

Grâce à une multitude de connecteurs, Forcepoint DSPM localise et classe efficacement les données sensibles à l'aide d'une inspection complète du contenu, dans divers environnements de stockage, que ce soit dans le cloud ou sur site, pour des données structurées ou non structurées, en analysant les principales plateformes telles qu'Amazon (AWS S3 et IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) et Google (Google Drive et IAM), ainsi que les systèmes locaux LDAP et SharePoint.

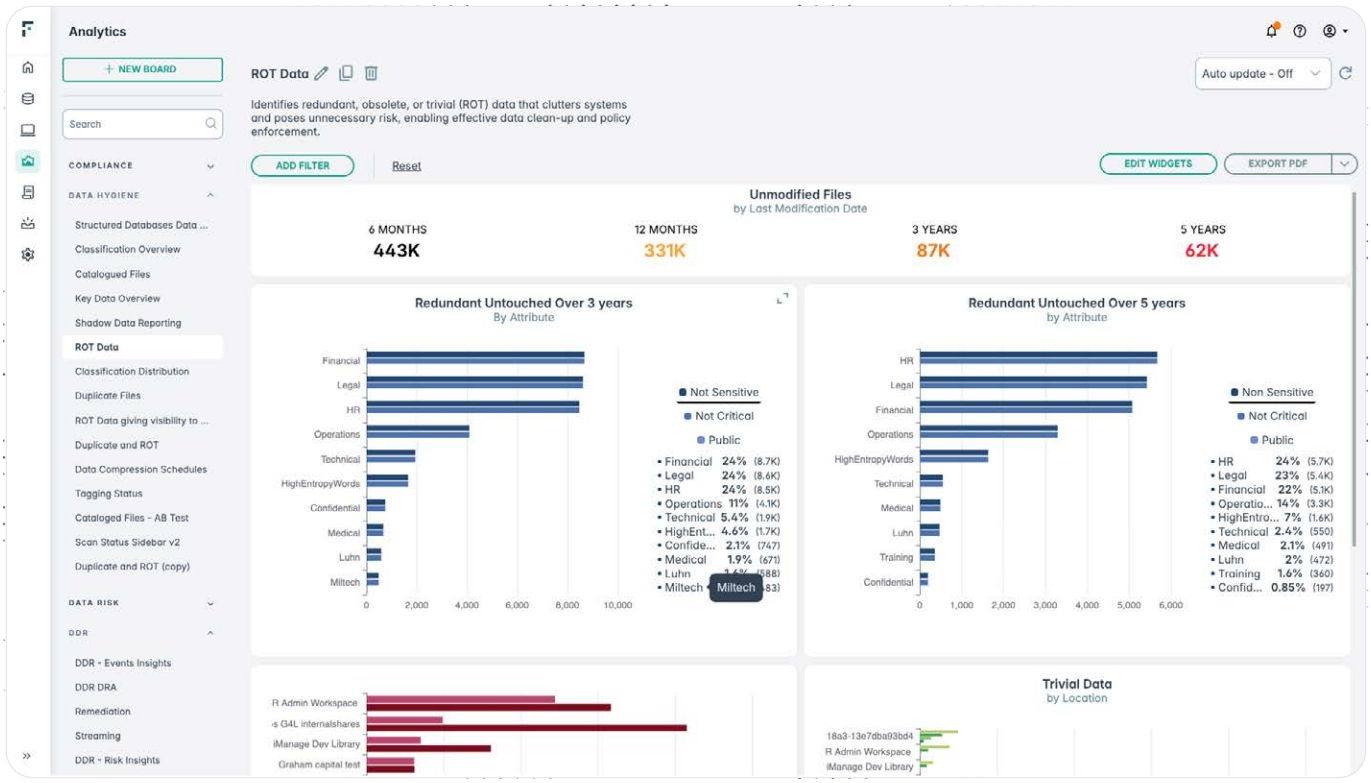
La précision activée par AI Mesh

La fonctionnalité AI Mesh de Forcepoint DSPM excelle à donner aux entreprises d'aujourd'hui une précision de classification des données supérieure. À la différence des autres solutions DSPM, elle offre une architecture d'IA reliée à plusieurs noeuds, tirant parti d'une SLM GenAI et d'un réseau de données et de composants d'IA avancés. Cette structure capture efficacement le contexte et transforme le texte en classifications précises de documents. L'AI Mesh est personnalisable, en fonction des besoins du secteur et des environnements réglementaires. Elle fonctionne efficacement sur les ressources de calcul standard sans nécessiter de GPU tout en fournissant une classification haute performance. Une précision accrue est obtenue sans formation approfondie au ML, ce qui réduit les coûts de maintenance. L'explicabilité de l'AI Mesh améliore la confiance et la conformité, en garantissant une posture de données hautement sécurisée et le respect des réglementations en matière de protection de la vie privée.



Surveillance des performances élevées et évaluation des risques liés aux données

Au fur et à mesure que Forcepoint DSPM analyse et découvre les données, elle fournit des informations détaillées telles que le nombre de fichiers partagés en interne qui renferment des informations critiques, la quantité de fichiers PII à risque et le nombre de fichiers redondants, obsolètes et triviaux (ROT).



Orchestration des flux de travail

Rationalisez la gouvernance de la sécurité des données sans effort avec Forcepoint DSPM. Son orchestration intuitive des flux de travail assure un suivi efficace de la propriété et de la responsabilité des données. En éliminant les silos et en facilitant la collaboration entre les parties prenantes, elle aligne les responsabilités, améliore l'efficacité opérationnelle et favorise la clarté au sein de l'organisation.

La mise en oeuvre d'une solution DSPM robuste est cruciale pour les organisations qui cherchent à sécuriser leur posture de données et à protéger les informations sensibles dans les emplacements de stockage cloud et sur site. En utilisant Forcepoint DSPM, les organisations peuvent stimuler la productivité en améliorant la fiabilité de l'accès aux données et du partage, en favorisant l'innovation, en facilitant l'adoption de l'IA et en encourageant la collaboration. Simultanément, elles peuvent atténuer les risques en identifiant et en traitant de manière proactive l'utilisation inappropriée des données sensibles, prévenant ainsi les violations de données. En fin de compte, les organisations peuvent rationaliser leurs efforts de conformité en obtenant une visibilité et un contrôle réels sur les données sensibles dans tous les environnements.

Découverte robuste

CARACTÉRISTIQUES	AVANTAGES
Découverte et catalogage rapides	La solution analyse plusieurs sources, traitant un plus grand nombre de fichiers par minute ou par heure, et synthétise les données structurées et non structurées dans un format clair et exploitable.
Se connecte à des sources de données importantes	Forte visibilité sur les données structurées et non structurées grâce à une gamme de connecteurs de sources de données.
Analyses de données surexposées	Identifiez les données surexposées qui sont partagées publiquement, partagées en externe avec des tiers et surpartagées en interne.
Afficher et corriger les autorisations	Affichez l'accès à chaque fichier et prenez des mesures correctives pour établir une sécurité Zero Trust selon le principe du moindre privilège (POLP).
Éliminez les risques dus aux données ROT (redondantes, obsolètes, triviales)	Identifiez et éliminez les fichiers redondants, obsolètes ou triviaux (ROT).
Visibilité sur l'accès et les autorisations	Les intégrations avec Active Directory et d'autres solutions IRM améliorent la sécurité de l'accès au sein des entreprises.

AI Mesh Data Classification

CARACTÉRISTIQUES	AVANTAGES
Classification AI Mesh des données structurées et non structurées	Classification hautement précise par IA des données structurées et non structurées.
Formation personnalisée des modèles	Les organisations peuvent adapter le modèle AI Mesh pour répondre à leurs besoins en données uniques (par exemple, IP, secrets commerciaux, etc.), pour une classification des données très précise, ce qui réduit les faux positifs/négatifs DSPM et DLP.
Capable de mapper les balises à l'étiquetage IP Microsoft Purview.	Fournit une couche supplémentaire de granularité de classification, en complément des balises MIP. Capacité de corriger le marquage MIP.
Balisage des données	Marque tous les fichiers numérisés et classifiés avec des étiquettes persistantes lisibles par DLP avec le marquage standard (confidentiels, hautement confidentiels, publics) et prend également en charge le catalogage/marquage d'entreprise (RH, marketing, finance, devops avec des sous-balises telles que CV, bon de commande, etc.).
S'intègre à Forcepoint DLP	Peut être intégré à Forcepoint DLP pour utiliser le marquage des fichiers DSPM AI Mesh pour créer des politiques solides.

Surveillance en temps réel et évaluation des risques liés aux données

CARACTÉRISTIQUES	AVANTAGES
Évaluation des risques liés aux données (DRA)	Le tableau de bord intégré d'évaluation des risques liés aux données analyse la posture actuelle de sécurité des données d'une organisation selon plusieurs catégories.
Tableau de bord interactif détaillé	Visualisez l'ensemble des détails de vos fichiers et bases de données dans une solution unique. Parcourez les données cruciales des fichiers, comme le niveau de risque, les autorisations et les emplacements (adresse IP, chemin).
Fonction de rapport	Générer des rapports qui montrent à la fois la préparation générale en matière de conformité et des réglementations spécifiques en matière de protection de la vie privée.
Système d'alerte avancé	Fournit des commandes de données sophistiquées et des alertes détectées lors des analyses pour détecter toute anomalie ou violation potentielle.
Recherche de demande d'accès aux données (DSAR)	Simplifiez la génération d'une DSAR pour vous conformer rapidement en matière de réglementation sur la confidentialité.
Suite d'analytiques	Découvrez une suite d'analytiques avancées pour un accès facile aux informations de sécurité et de classification en un coup d'oeil. Sélectionnez parmi divers tableaux de bord prédéfinis ou créez les vôtres, et exportez facilement les instantanés PDF en un seul clic. Les tableaux de bord prédéfinis incluent la surexposition et l'analyse de ransomwares, la duplication des données critiques, la détection des utilisateurs à risque, la rétention des données, les données égarées, l'évaluation des risques liés aux données, la souveraineté des données, le suivi des incidents pour les violations de contrôle des données et bien plus encore.
Analyses d'exposition aux ransomwares	Identifiez les données critiques qui pourraient être exposées à une attaque de ransomware.
Générateur de rapports et d'analyses sans code	Créez facilement des cas d'utilisation personnalisés et des rapports d'analyse ne nécessitant aucune compétence en codage.
Identification des utilisateurs à risque	Identifiez les utilisateurs ayant des profils de risque élevés qui ont accès à des quantités importantes d'informations critiques.
Incident de contrôle des données	Fournit une vue claire sur les violations du contrôle des données et une résolution de l'état des incidents.

Remediación

CARACTÉRISTIQUES	AVANTAGES
Correction des autorisations	Recevez des notifications des incidents de gouvernance de la sécurité des données ou des problèmes de conformité. Simplifiez leur suivi et leur gestion grâce aux outils ITSM et de productivité existants.
Correction par déduplication des données	La fonctionnalité de déduplication de DSPM identifie et élimine les données redondantes, réduisant les besoins de stockage et les coûts, tout en optimisant l'allocation des ressources. La suppression peut être automatisée conformément à des règles de gouvernance configurables.
Déplacer les fichiers	Utilisez DSPM pour déplacer les fichiers situés dans des emplacements à risque ou trop exposés vers des dépôts plus sécurisés, avec la possibilité de créer automatiquement un stub de fichier.
File Stubbing	Création automatique de stubs de fichiers pour maintenir les processus métier en documentant les changements d'emplacement des fichiers lors de leur déplacement via DSPM.

© 2026 Forcepoint. Forcepoint et le logo FORCEPOINT sont des marques déposées de Forcepoint. Toutes les autres marques déposées utilisées dans ce document sont la propriété de leurs propriétaires respectifs. [FP-DSPM Datasheet-FR] 19Aug2026