

# Forcepoint Data Security Posture Management

## Avantages et fonctions clés :

- › **AI Mesh et ML** – Le catalogue AI Mesh offre une précision et une efficacité inégalées, évoluant en permanence grâce à l'apprentissage machine pour des améliorations continues.
- › **Découverte rapide** – Exécutez Forcepoint DSPM dans le cloud et les emplacements de stockage sur place, aussi souvent que vous le souhaitez.
- › **Surveillance en temps réel et évaluation des risques** – Vérifiez les autorisations d'accès et les 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 la transformation de l'IA, entraînée par l'intégration des technologies d'IA, notamment les applications GenAI, dans les processus d'entreprise. Couplées à l'étalement de données des entreprises qui migrent des applications et des données de l'on-premise vers le cloud et qui utilisent des outils GenAI tels que ChatGPT, Co-pilote et Gemini, elles doivent faire face à la lutte permanente pour savoir où se trouvent leurs données sensibles, qui peut y accéder et comment elles sont utilisées. La croissance exponentielle des « données obscures », cachées dans les référentiels basés sur le cloud ou réparties sur des appareils individuels et désormais sur les applications d'IA de la génération précédente présente un risque substantiel. On estime que jusqu'à 80 % des données d'une entreprise existent dans cet état obscur « sombre », échappant à la surveillance traditionnelle.

Le résultat de ce paysage de données obscurcies est critique. Sans visibilité et sans gestion claires, les entreprises sont exposées à des risques accrus de violations qui ont des répercussions potentiellement dévastatrices dans les secteurs commerciaux, à but non lucratif et gouvernementaux. À l'ère de la transformation digitale, l'impératif de regagner le contrôle des informations sensibles n'a jamais été aussi urgent.

L'AI Mesh de Forcepoint DSPM permet aux organisations de bénéficier d'une précision supérieure en matière de classification des données. Son architecture d'IA en réseau, qui s'appuie sur un petit modèle de langage GenAI (SLM) et des composants de données et d'IA avancées, capture efficacement le contexte à partir de textes non structurés. Personnalisable et efficace, elle garantit une classification rapide et précise sans formation approfondie, améliorant ainsi la confiance et la conformité.

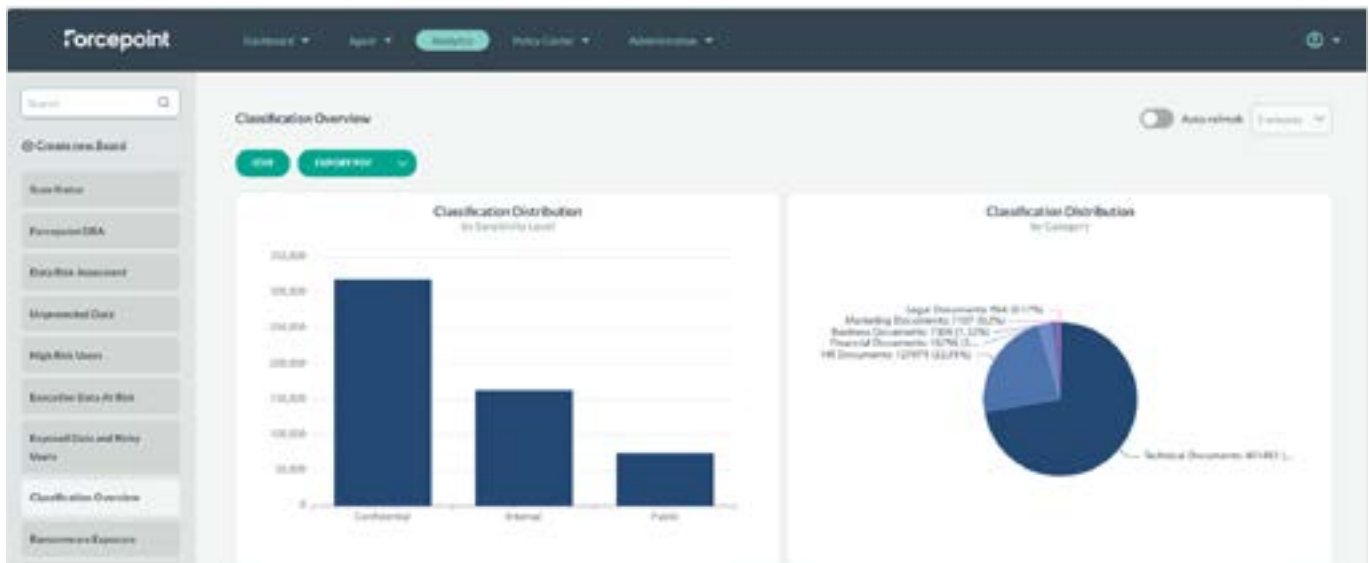


## Découverte rapide et complète

Avec une multitude de connecteurs, Forcepoint DSPM localise efficacement les données sensibles sur divers environnements de stockage, que ce soit dans le cloud ou sur site, en analysant environ un million de fichiers par heure sur 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 LDAP et SharePoint locaux.

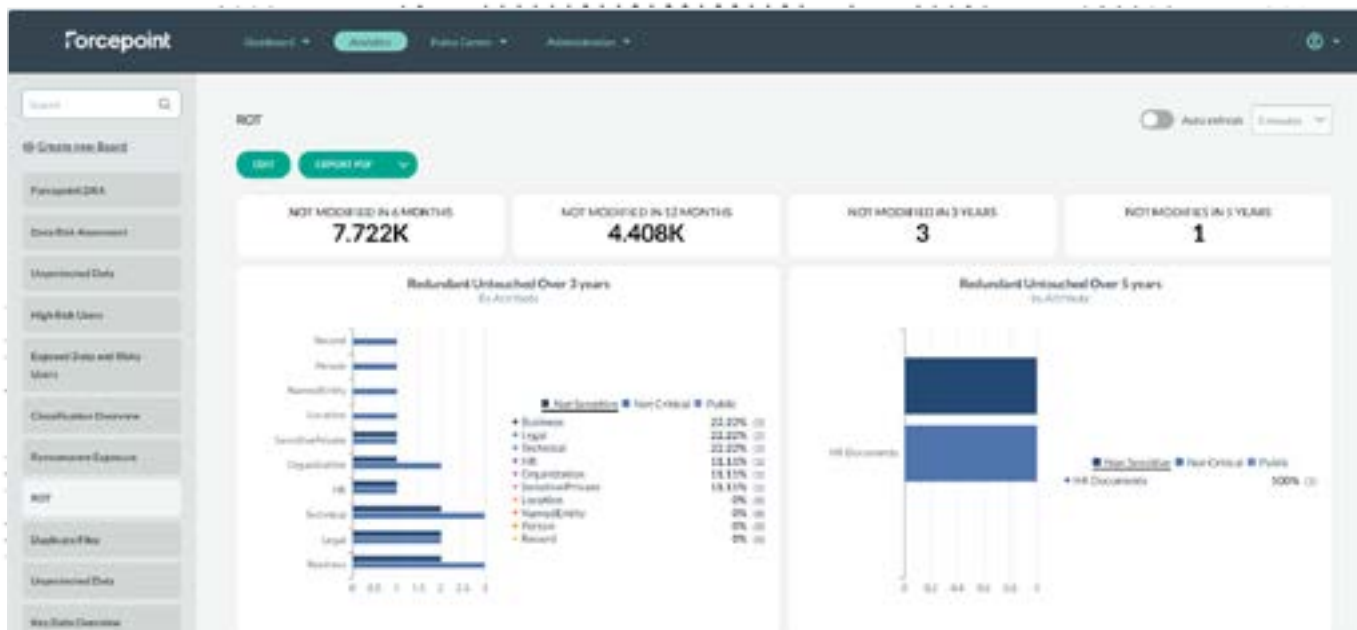
## La précision activée par AI Mesh

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 nœuds, 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 non structuré en classifications de documents précises. 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 en temps réel 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 œuvre d'une solution DSPM robuste est cruciale pour les entreprises qui souhaitent rationaliser leur parc de données et protéger les informations sensibles sur les sites de stockage de données cloud et sur site. En utilisant Forcepoint DSPM, les entreprises peuvent augmenter leur productivité en améliorant la fiabilité de l'accès et du partage des données, en favorisant l'innovation et en encourageant la collaboration. Simultanément, elles peuvent atténuer les risques en identifiant de manière proactive et en corrigeant l'utilisation incorrecte des données sensibles, prévenant ainsi les violations de données. En fin de compte, les entreprises peuvent rationaliser leurs efforts de conformité en obtenant une véritable visibilité et un contrôle sur les données sensibles dans tous les environnements.

## Découverte robuste

CARACTÉRISTIQUES	AVANTAGES
Découverte et catalogage rapides	Elle fonctionne sur plusieurs sources pour analyser de plus grands volumes de fichiers par minute/heure et synthétise les détails sur les assortiments de données non structurées, en les organisant dans un format facile à digérer.
Connecteurs de sources de données extensifs	Visibilité robuste sur des données non structurées en offrant une large 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.
Affichez les autorisations pour chaque fichier de données non structurées	Affichez l'accès individuel des utilisateurs pour chaque fichier et découvrez les utilisateurs ayant accès à la plupart des fichiers.
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.

## Data Classification AI Mesh

CARACTÉRISTIQUES	AVANTAGES
Classification AI Mesh et ML des données non structurées existantes	Des suggestions de classification très précises recommandées pour les données non structurées existantes qui sont analysées.
Formation personnalisée des modèles	Les entreprises peuvent adapter le modèle AI Mesh pour qu'il réponde à des besoins de données uniques (par exemple, la propriété intellectuelle, les secrets commerciaux, etc.), et grâce à l'apprentissage machine, il peut s'améliorer au fil du temps pour une meilleure précision.
Capable de mapper les balises à l'étiquetage IP Microsoft Purview.	Fournit une couche supplémentaire de granularité de classification, en complément des balises MPIP. Capable de corriger le marquage MPIP.
Balises des données	La rationalisation du déploiement DLP améliore l'efficacité de la DLP en marquant tous les fichiers scannés et classifiés avec des étiquettes lisibles par la DLP avec des étiquettes typiques (classifié, hautement classifié, public) ainsi qu'avec le catalog/marquage des entreprises (RH, marketing, finance, devops - avec des sous-étiquettes telles que des CV, des PO, etc.).
S'intègre à Forcepoint DLP	Peut être intégré pour utiliser le marquage des fichiers DSPM AI Mesh (classification) pour créer des politiques fortes.

## Surveillance en temps réel et évaluation des risques liés aux données

CARACTÉRISTIQUES	AVANTAGES
Évaluation des risques liés aux données (DRA)	Des évaluations gratuites des risques liés aux données sont disponibles pour analyser la posture actuelle des risques liés aux données d'une entreprise dans plusieurs catégories.
Tableau de bord interactif détaillé	Affichez les détails complets du dossier sur un seul écran. 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 répondre rapidement aux demandes des réglementations en matière de protection de la vie privée.
Suite d'analytiques	Découvrez une suite d'analytiques avancées pour un accès facile aux informations de sécurité et de classification en un coup d'œil. 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 comprennent la surexposition et l'analyse des ransomwares, la duplication des données critiques, la détection des utilisateurs à risque, la rétention des données, les données égarées, l'évaluation des risques des données, la souveraineté et le suivi des incidents pour les violations de contrôle des données.
Analyses d'exposition aux ransomwares	Identifiez les données critiques qui sont exposées à une attaque de ransomware.
Générateur de rapports et d'analyses sans code	Créez facilement des rapports d'utilisation et d'analyses personnalisés sans codage requis.
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.

## Orchestration des flux de travail

CARACTÉRISTIQUES	AVANTAGES
Propriété des données	Définit la responsabilité avec facilité et atteint l'alignement des parties prenantes.
Gestionnaire des tâches	Assigne les tâches aux dépositaires et aux propriétaires des données, en permettant le suivi des statistiques DSPM (telles que les tickets ouverts, résolus et fermés, le temps de résolution).