
Forcepoint DSPM

Optimisée par GetVisibility



Forcepoint

Brochure

La transformation par l'IA est la prochaine évolution de la transformation numérique

Vos données sont-elles en sécurité dans cette nouvelle ère ?

La plupart des organisations ayant procédé à la transformation numérique se préparent désormais à la prochaine évolution, la transformation par l'IA. Cette nouvelle ère de l'IA est portée par les nombreux avantages offerts par les applications GenAI telles que ChatGPT, Copilot, Gemini, et d'autres. Tirant parti de leur expérience en matière de transformation numérique, les organisations ont appris que la sécurité des données doit être une priorité absolue. Cependant, pour de nombreuses organisations, les données sont aujourd'hui comme un iceberg géant, dont la plus grande partie est enfouie sous la surface. Souvent appelées « données obscures » ou « données fantômes », elles restent invisibles et inconnues, alors qu'elles contiennent des quantités substantielles d'informations sensibles pour lesquelles les organisations portent une responsabilité directe. À présent, les organisations se demandent comment permettre aux utilisateurs d'exploiter en toute sécurité les applications GenAI afin d'améliorer la productivité et l'efficacité, tout en garantissant la protection de leurs données sensibles.



DSPM (Data Security Posture Management) offre une approche complète pour protéger vos informations contre l'accès non autorisé, la divulgation, l'altération ou la destruction de données. À la différence d'autres types de méthodes de sécurité des données qui mettent l'accent sur les systèmes et les appareils, DSPM met l'accent sur l'ensemble des données d'une organisation elle-même, en assurant le respect et en atténuant le risque de violations de données.



Selon IDC, 80 % des données globalement sont non structurées et 90 % de ces données ne sont pas examinées, également appelées « données obscures »¹



94 % des organisations stockent des données dans plusieurs environnements cloud.²



Equifax règle un litige de 1,4 milliard de dollars pour sa violation de données³ exacerbée par les pirates accédant à un lecteur partagé stockant plusieurs copies des noms d'utilisateur et des mots passe des employés. La société manquait d'outils pour détecter et identifier les fichiers redondants et périmés.

¹ The Unseen Data Conundrum, Forbes, février 2022

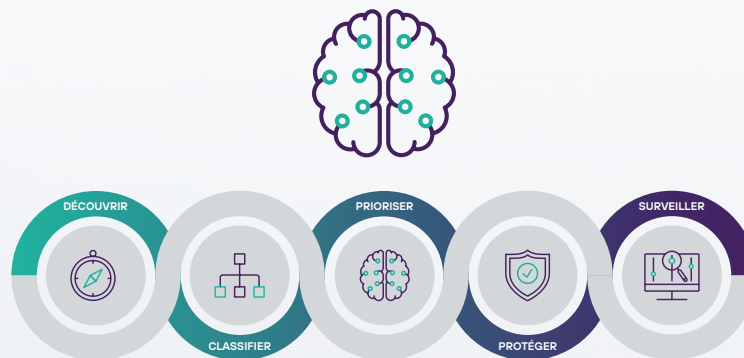
² Dark Data: The Cloud's Unknown Security and Privacy Risk, Forbes, juin 2023

³ Equifax agrees \$1.38bn data breach lawsuit settlement, Finextra, janvier 2020

De quoi traite DSPM ?

- **Cheminement de la transformation par l'IA :** Libérez le potentiel de l'IA avec Forcepoint DSPM, en protégeant vos données partout grâce à notre technologie avancée AI Mesh. Grâce à la visibilité centralisée de Forcepoint DSPM et au contrôle de Forcepoint ONE Data security, nous sécurisons vos informations sensibles sur les canaux clés, y compris les applications GenAI telles que ChatGPT, Copilot, Gemini, et bien d'autres- favorisant une innovation audacieuse tout en stimulant la productivité et en réduisant les risques.
- **Identification des données sensibles :** DSPM aide les organisations à identifier les données sensibles dans plusieurs environnements et services cloud ainsi que dans des emplacements sur site. Il s'agit notamment de comprendre où se trouvent les données sensibles, comment elles sont accessibles et qui dispose des autorisations pour interagir avec elles.
- **Analyser la vulnérabilité et le risque :** DSPM évalue la vulnérabilité des données sensibles aux menaces de sécurité et le risque de non-respect de la réglementation. En examinant la posture de sécurité des données, les organisations peuvent aborder de manière proactive les risques potentiels.
- **Mettre l'accent sur les données à la source :** à la différence des autres outils de sécurité des données qui sécurisent principalement les appareils, les systèmes et les applications, DSPM met l'accent sur la protection de l'ensemble des données d'une organisation. Elle vise à prévenir les violations de données et à assurer la conformité en sécurisant les données à sa base.
- **Traiter les données obscures et les données ROT :** DSPM traite directement les données obscures (données actuellement non vues ou utilisées dans les processus commerciaux normaux). De même, DSPM peut traiter les données ROT (redondantes, obsolètes et triviales) qui ont également tendance à proliférer dans les organisations lorsque les entreprises maintiennent de grandes quantités de données pour diverses raisons, pensant que cela les aidera à rester conformes. Cela crée en fait encore plus de risques liés aux données, et DSPM aide à gérer ce risque.
- **Traite les données surautorisées/surexposées :** en raison de la prolifération des données par la copie et l'édition de nouvelles versions de données, les autorisations d'accès aux données peuvent également s'étendre aux utilisateurs, aux groupes et même à l'ensemble de l'organisation. DSPM aide à appliquer le « principe du moindre privilège » Zero Trust qui réduit considérablement les données surautorisées afin de prévenir les violations de données.
- **Environnements multicloud et cloud hybride :** à mesure que les organisations adoptent des environnements multicloud et cloud hybride, le risque de violations de données augmente de manière considérable. DSPM offre visibilité et contrôle sur les données sensibles dans ces environnements informatiques diversifiés en plus des emplacements sur site.

Forcepoint DSPM est pensé pour l'organisation moderne qui a besoin d'une forte visibilité et d'un contrôle de ses données sensibles. Il fournit une visibilité sur divers environnements et serveurs cloud pour prévenir les violations de données et réduire les risques de non-conformité avec les réglementations régissant la confidentialité. Forcepoint offre une visibilité et un contrôle complets sur l'ensemble du cycle de vie des données, offrant une sécurité des données en tout lieu en combinant **la découverte proactive des risques liés aux données** (DSPM) avec **des contrôles actifs sur la façon dont les données sont utilisées** (DLP et SSE) tout en **s'adaptant continuellement aux actions de chaque utilisateur** (Risk-Adaptive Protection).



Découverte, classification et orchestration alimentées par l'IA



Unifier la visibilité et la maîtrise de votre paysage de données avec Forcepoint DSPM

La gestion et la sécurisation des données de votre organisation n'ont jamais été aussi complexes. Forcepoint DSPM offre une solution puissante pour obtenir une visibilité et une maîtrise complètes de vos données, quel que soit leur emplacement. Avec des vitesses de découverte à la pointe de l'industrie et des capacités avancées de classification des données AI Mesh, Forcepoint DSPM vous permet de prendre des décisions éclairées sur votre posture de sécurité des données et de faire face de manière proactive aux risques éventuels.

Les principaux avantages de Forcepoint DSPM comprennent :

Découverte rapide et complète : Forcepoint DSPM est capable d'analyser rapidement les fichiers de plusieurs clouds et sur site. Il n'est pas rare que des organisations disposent de nombreux téraoctets, pour certaines ce sont des pétaoctets, et les très grandes organisations ayant même des exaoctets de données à gérer. Grâce à cette découverte haute performance, Forcepoint permet aux organisations d'obtenir une vue rapide des données à travers un paysage de données massives, y compris ChatGPT Entreprise. À la différence des autres fournisseurs de DSPM, Forcepoint ne facture pas les analyses de découverte : les clients peuvent effectuer ces analyses aussi souvent qu'ils le souhaitent, sans frais supplémentaires.

Précision activée par AI Mesh : Forcepoint DSPM découvre les données à travers les sources cloud et réseau et les classe automatiquement, en utilisant un moteur de classification IA avancé. 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. Personnalizable et efficace, elle garantit une classification rapide et précise sans formation approfondie, améliorant ainsi la confiance et la conformité. En fin de compte, cette grande précision a permis aux organisations qui avaient des difficultés avec d'autres méthodes de classification populaires de réduire radicalement les faux

positifs/négatifs, protégeant avec succès leur propriété intellectuelle et d'économiser des sommes importantes en termes de temps et de ressources.

Visibilité des données dans votre paysage de données : Forcepoint DSPM vous permet d'inspecter les autorisations pour tous les fichiers et utilisateurs. Les administrateurs de données peuvent voir quelles personnes ont accès à un fichier ou au partage de fichier dans l'organisation. En un seul clic, vous pouvez immédiatement afficher les autorisations pour tous les fichiers numérisés. Forcepoint DSPM fournit des rapports en temps réel ainsi qu'un tableau de bord avec de nombreux détails donnant une vue d'ensemble des données obscures, ainsi qu'une évaluation des risques liés aux données pour vous aider à comprendre les domaines présentant le risque de données le plus élevé.



Orchestration de flux de travail : Définissez facilement la propriété et la responsabilité des différents ensembles de données afin de rationaliser le processus d'alignement des parties prenantes. Cela permet de mettre en place des flux de travail plus efficaces autour des actions effectuées sur chaque source de données et chaque actif. Une mesure corrective efficace nécessite une large adhésion et une collaboration au-delà de l'organisation

de la sécurité, avec le groupe CDO/Gouvernance, Risques et Conformité (GRC), ainsi que des fonctions telles que le marketing, la finance, DevOps et bien d'autres. Forcepoint DSPM considère la sécurisation de la posture des données non pas seulement comme une question de sécurité, mais comme une priorité commerciale.



Ne laissez pas les risques de données paralyser votre entreprise. Forcepoint peut vous aider !

À l'ère numérique d'aujourd'hui, les données sont l'ensemble le plus précieux d'une organisation, mais elles peuvent également être une responsabilité importante si elles ne sont pas gérées correctement. Forcepoint DSPM offre une approche proactive pour sécuriser vos données sensibles, atténuer les risques de violations de données et assurer le respect de la réglementation. En mettant en œuvre Forcepoint DSPM, vous pouvez obtenir une visibilité complète de votre paysage de données, identifier et traiter les vulnérabilités, et de protéger de manière proactive votre organisation des dommages financiers et de réputation causés par les violations de données et la non-conformité réglementaire, tout en sécurisant vos données dans les applications GenAI. Maîtrisez votre posture de sécurité des données dès aujourd'hui. Explorez comment la DSPM peut protéger vos précieuses informations. Rendez-vous sur www.forcepoint.com/fr/dspm pour demander une démonstration, ou pour vous inscrire à une évaluation gratuite des risques liés aux données au cours de laquelle un ingénieur en sécurité vous fournira un échantillon de vos propres données afin de déterminer les types de risques auxquels vous êtes actuellement confronté.

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint simplifie la sécurité pour les entreprises et les gouvernements dans le monde. La plate-forme tout-en-un de Forcepoint, véritablement native dans le cloud, facilite l'adoption de Zero Trust et empêche le vol ou la perte de données sensibles et de propriété intellectuelle, quel que soit le lieu de travail. Basée à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables pour les clients et leurs employés dans plus de 150 pays. Engagez-vous avec Forcepoint sur www.forcepoint.com, Twitter et LinkedIn.