Forcepoint DSPM



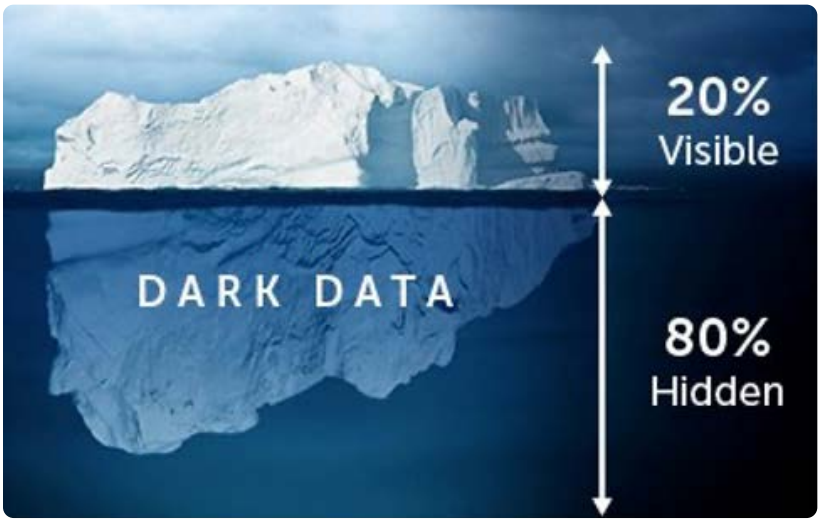
Forcepoint

Brochure

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

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

Les organisations de tous les secteurs sont aux prises avec la transformation de l'IA, portée par la promesse d'une augmentation considérable de la productivité. Cette ère marquée par l'IA se caractérise par des initiatives visant à intégrer des services d'IA d'entreprise, à gérer l'utilisation non autorisée de l'IA et à atténuer les risques liés à l'activité de l'IA agentique. De manière générale, une priorité clé sous-tendant ces efforts est la visibilité et le contrôle de l'utilisation des données sensibles. Cependant, pratiquement toutes les organisations peinent à obtenir une visibilité cohérente, et encore moins un contrôle, de leurs données à grande échelle. C'est comme un iceberg, dont nous ne voyons qu'une petite fraction à la surface, la grande majorité restant imperceptible sous l'eau. C'est ce que l'on appelle souvent les « données obscures » (dark data) : elles restent invisibles et inconnues, tout en contenant des quantités importantes d'informations sensibles dont l'organisation est directement responsable. Désormais, les organisations cherchent à déterminer comment permettre à leurs utilisateurs de tirer parti de l'IA en toute sécurité tout en assurant la protection de leurs données sensibles, mais l'utilisation de l'IA elle-même aggrave le problème en contribuant à créer davantage de données à une vitesse sans précédent.



La gestion de la posture de sécurité des données Data Security Posture Management (DSPM) offre une approche complète pour protéger vos informations contre les accès non autorisés, la divulgation, l'altération ou la destruction des données. Contrairement à d'autres méthodes de sécurité des données axées sur des applications et des appareils spécifiques, le DSPM permet de voir et de contrôler l'intégralité des données d'une organisation, que ce soit dans le cloud ou sur des réseaux privés, garantissant ainsi la conformité et réduisant le risque de violations de données.



Part des organisations ayant signalé une violation liée à l'IA et ne disposant pas de contrôles d'accès à l'IA appropriés[1].



Économies réalisées grâce à une utilisation intensive de l'IA dans les opérations de sécurité. Les équipes de sécurité utilisant intensivement l'IA et l'automatisation ont réduit leurs délais de confinement des violations de 65 jours et diminué leurs coûts moyens de 1,93 million de dollars US, par rapport à celles n'utilisant pas ces solutions[1].



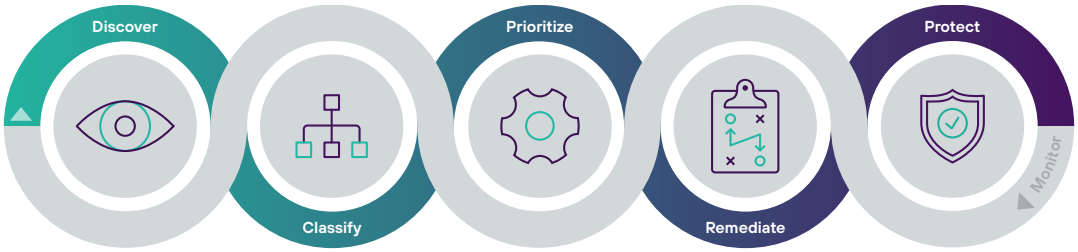
AT&T a accepté de verser 177 millions de dollars dans le cadre d'un règlement de recours collectif lié à deux violations survenues en 2024. La première a exposé des données, y compris des numéros de sécurité sociale, de 73 millions de clients actuels et anciens, tandis que la seconde a impliqué un accès non autorisé à un espace de travail contenant des informations sensibles sur les clients, hébergé dans un environnement cloud sans surveillance adéquate[2].

1 IBM's Cost of a Data Breach Report 2026
2 Top Class Actions **règlement du recours collectif relatif à la violation de données d'AT&T**

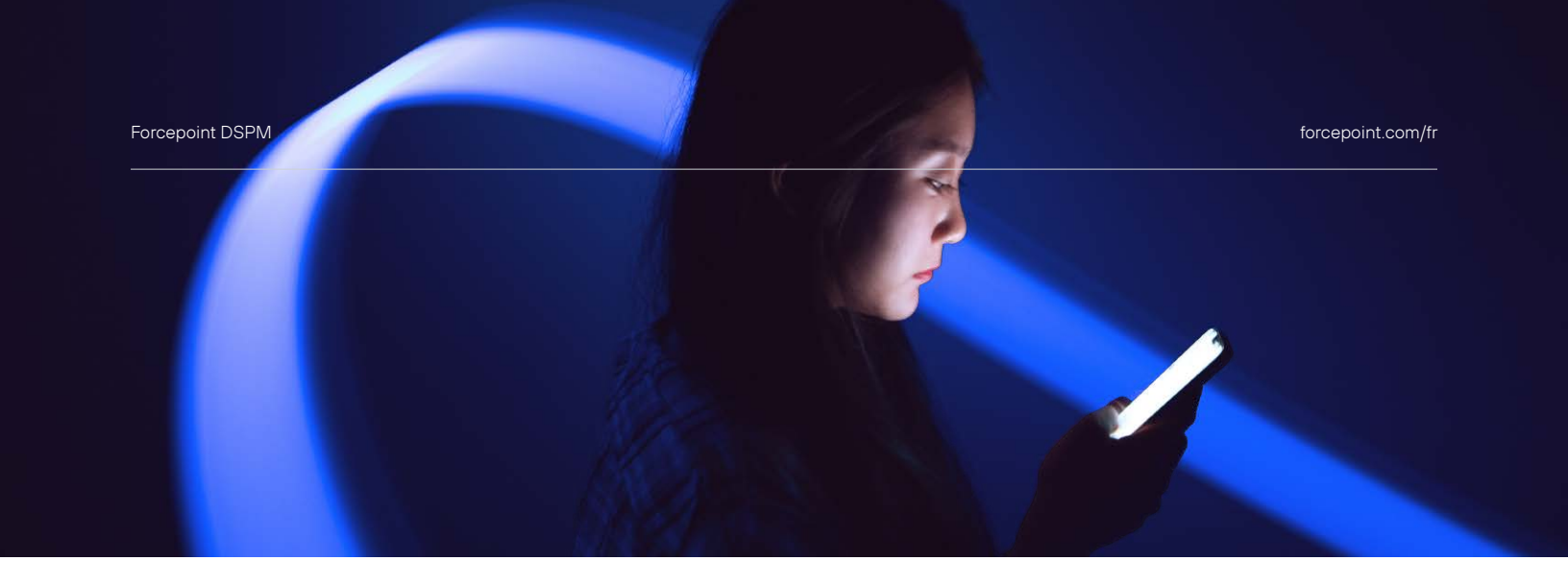
De quoi traite DSPM ?

- **Parcours de transformation de l'IA :** libérez le potentiel de l'IA avec Forcepoint DSPM, en protégeant vos données en tout lieu grâce à notre technologie avancée de maillage d'IA (AI Mesh). Grâce à la visibilité centralisée et à la capacité de remédiation de Forcepoint DSPM, ainsi qu'aux contrôles de blocage en temps réel de Forcepoint DLP, nous protégeons vos informations sensibles sur les principaux canaux, y compris les applications d'IA générative comme ChatGPT, Copilot, Gemini et bien d'autres, tout en favorisant une innovation audacieuse, en améliorant la productivité et en réduisant les risques.
- **Identification des données sensibles :** le DSPM aide les entreprises à identifier les données sensibles sur plusieurs environnements et services cloud, ainsi que sur les sites locaux, qu'il s'agisse de données structurées ou non structurées. Cela inclut l'identification de l'emplacement des données sensibles, des modes d'accès et des autorisations associées.
- **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.
- **Traite 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.
- **Surveillance continue des risques :** le module complémentaire Forcepoint Data Detection and Response (DDR) permet à Forcepoint DSPM de détecter les nouveaux risques liés aux données et d'y remédier dès qu'ils se produisent. Inutile d'attendre la prochaine analyse DSPM complète pour identifier de manière dynamique les risques liés à la sécurité de vos données à corriger.

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 le cycle de vie des données, fournissant la sécurité des données en tout lieu en combinant **la découverte proactive des risques liés aux données** (DSPM) à **des contrôles actifs sur la façon dont les données sont utilisées** (DLP), tout en **s'adaptant en permanence aux actions de chaque utilisateur grâce à une protection adaptative aux risques** (Risk-Adaptive Protection). Obtenez la découverte dynamique des risques liés aux données grâce à une surveillance continue (Forcepoint DDR) pour prévenir les violations des données et protéger votre stratégie de sécurité des données.



Découverte, classification et orchestration alimentées par l'IA



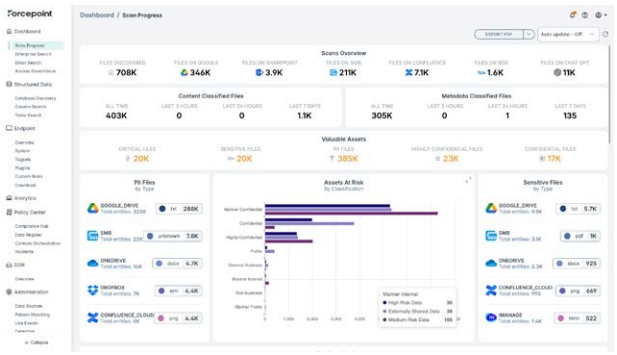
Unifier la visibilité et la maîtrise de votre paysage de données avec Forcepoint DSPM

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 un contrôle complets sur vos données, quel que soit leur emplacement. Grâce à une classification des données de pointe reposant sur une inspection complète du contenu, alimentée par l'AI Mesh de Forcepoint et des classificateurs DLP avancés, Forcepoint DSPM vous permet de prendre des décisions éclairées concernant votre posture de sécurité des données et de traiter les risques potentiels de manière proactive.

Les principaux avantages de Forcepoint DSPM comprennent :

Découverte rapide et exhaustive : Forcepoint DSPM assure une analyse rapide et performante des fichiers et des bases de données dans des environnements multicloud et sur site, en procédant à une inspection complète du contenu plutôt qu'en se limitant à un simple étiquetage des métadonnées ou à des approches par échantillonnage. Ce niveau d'analyse garantit une identification précise des données sensibles, et non une simple estimation. La découverte et la classification hautes performances de Forcepoint permettent aux organisations d'obtenir rapidement une visibilité complète sur leur paysage de données à grande échelle, couvrant aussi bien les référentiels structurés que non structurés, y compris les données hébergées sur des plateformes d'IA générative telles que ChatGPT Enterprise, Anthropic Claude et Microsoft Copilot, afin d'aider les équipes de sécurité à anticiper les risques émergents d'exposition des données liés à l'IA

Précision optimisée par l'AI Mesh : Forcepoint DSPM détecte les données à travers les sources cloud et réseau, puis les classe automatiquement à l'aide d'un moteur de classification IA avancé. L'AI Mesh de Forcepoint DSPM offre aux organisations une précision de classification des données supérieure. Son architecture d'IA en réseau, s'appuyant sur un modèle de langage restreint (Small Language Model, SLM) GenAI et sur les classificateurs DLP de Forcepoint, éprouvés et rigoureusement sélectionnés, capture efficacement le contexte à partir de texte non structuré. Personnalisable et efficace, elle garantit une classification rapide et précise sans nécessiter d'apprentissage approfondi, renforçant ainsi la confiance et la conformité. En définitive, cette grande précision a permis à des organisations rencontrant des difficultés avec d'autres méthodes de classification courantes de réduire considérablement les faux positifs/négatifs, protégeant ainsi efficacement leur propriété intellectuelle tout en réalisant d'importantes économies de temps et de ressources.



Visibilité des données dans votre paysage de données : Forcepoint DSPM vous permet d'inspecter les autorisations de tous les fichiers et de tous les utilisateurs. Les administrateurs de données peuvent voir quelles personnes ont accès aux fichiers et aux bases de données dans toute l'organisation. En un seul clic, vous pouvez immédiatement afficher les autorisations pour tous les fichiers numérisés. Forcepoint DSPM fournit un tableau de bord avec des détails nombreux donnant une vue d'ensemble des données non exploitées, ainsi qu'une évaluation globale des risques pour les données pour vous aider à comprendre les domaines les plus exposés aux risques les plus élevés.

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.

Forcepoint DDR: puissant module complémentaire à Forcepoint DSPM, est une solution clé pour s'attaquer aux violations des données. Il fournit une détection continue des menaces et une visibilité améliorée des risques liés aux données, en veillant à ce que les entreprises puissent effectivement voir les changements apportés aux données susceptibles d'entraîner des violations des données au moment où ils sont susceptibles de se produire. En s'appuyant sur les réponses basées sur l'IA, Forcepoint DDR (Dynamic Data Risk) offre une neutralisation précise des menaces, en aidant les entreprises à maintenir des mesures de sécurité robustes. Sa visibilité étendue sur le cloud et les terminaux, combinée au suivi du cycle de vie des données, en fait un outil essentiel pour la protection des informations sensibles, la réduction des pertes financières et le maintien de la confiance des clients.



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 oeuvre 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. Découvrez comment le DSPM peut protéger vos informations les plus précieuses. Rendez-vous sur www.forcepoint.com/fr/dspm pour demander.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint propose Self-Aware Data Security, une approche native de l'IA qui aide les entreprises et les administrations à connaître leurs données où qu'elles se trouvent, à s'adapter en temps réel à l'évolution des risques et des réglementations, et à assurer une protection à grande échelle grâce à un cadre de politique unique et unifié. Basée à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables pour ses clients et leurs collaborateurs dans plus de 150 pays. Retrouvez Forcepoint sur www.forcepoint.com, LinkedIn, Instagram et YouTube.

© 2026 Forcepoint. Forcepoint et le logo FORCEPOINT sont des marques commerciales de Forcepoint. Toutes les autres marques déposées utilisées dans ce document sont la propriété de leurs propriétaires respectifs. [FP-DSPM-Brochure-FR] 21Aug2026