proofpoint.

FICHE SOLUTION

Proofpoint Data Security Posture Management

Découvrez et sécurisez les données sur les plates-formes SaaS, l'infrastructure cloud et les environnements sur site

Principaux avantages

- **Les classificateurs d'IA** identifient les données sensibles et propres à l'entreprise sans règles manuelles dans les environnements SaaS, cloud et sur site.
- **Data Risk Map** priorise les risques en fonction de la sensibilité, de l'accès, de l'impact métier et du mouvement des données.
- **La gouvernance de l'accès sensible aux processus métier** rationalise la correction directe et déléguée, ainsi que la création de règles DLP.
- **La sécurité des données intégrée, optimisée par l'IA,** identifie les données sensibles exposées aux applications d'IA ainsi qu'aux pipelines d'apprentissage IA.
- **Les tableaux de bord de conformité** assurent le suivi de la posture de sécurité par rapport à plus de 25 cadres de référence, avec des rapports exploitables.
- **La sécurité unifiée des données** partage les informations pertinentes entre les solutions DSPM, DLP, Data Security for AI et de gouvernance de l'accès.

L'explosion des données d'entreprise

L'essor de l'IA, des plates-formes DBaaS (Database as a Service) et du stockage dans le cloud a accéléré la prolifération des données à la fois sur site, dans le cloud et dans les applications SaaS. Les équipes peinent à déterminer l'emplacement exact de ces données sensibles dès lors qu'elles sont éparpillées dans de multiples systèmes et pipelines. Le phénomène entraîne des angles morts de sécurité, augmente le risque d'exposition et complique la mise en conformité.

Les enjeux d'un accès non contrôlé

Cette dispersion des données est amplifiée par un manque de contrôle sur qui (et quoi) peut accéder aux informations sensibles. Les utilisateurs bénéficiant de privilèges excessifs, les outils non autorisés et les partages risqués créent un risque d'origine humaine. Les modèles d'IA, les agents et les workflows automatisés ajoutent de nouveaux vecteurs non humains. Sans gouvernance rigoureuse, les erreurs de configuration, les autorisations excessives et une supervision insuffisante peuvent provoquer des fuites de données, un usage inapproprié et des violations de la conformité.

55 %

des entreprises considèrent que 21 % à 40 % de leurs données sont sensibles.

Source : Proofpoint

68 %

des entreprises affirment que l'usage inapproprié de l'IA a exposé des données sensibles.

Source : Proofpoint

Découvrir, classifier, gouverner et protéger les données

Proofpoint Data Security Posture Management (DSPM) aide les équipes à reprendre le contrôle des données éparpillées et à réduire les accès à risque, qu'ils soient opérés par des utilisateurs ou par l'IA. La solution découvre et classifie les données sensibles, indique quels utilisateurs ou entités peuvent y accéder et priorise les risques. Les équipes peuvent ainsi corriger plus rapidement les vulnérabilités et renforcer la sécurité des données.

Fonctionnalités uniques

Dans le cadre de la sécurité des données de Proofpoint, la solution DSPM avec gouvernance de l'accès intégrée partage son cadre de classification avec Proofpoint Enterprise DLP et Proofpoint Data Security for AI. Les classificateurs d'IA identifient les catégories de documents sensibles en fonction du contexte et de la signification, pas uniquement à partir de modèles. La découverte et la classification en sont optimisées. La solution aide également les équipes à gérer l'accès, à créer des règles DLP et à protéger les données dans les environnements cloud, SaaS, sur site et IA.

Proofpoint DSPM repère les autorisations excessives, les accès à risque, les erreurs de configuration, les données obsolètes et les chemins d'attaque. La vue Data Risk Map indique où se situent les données sensibles, dans quelle mesure elles sont exposées, ainsi que les utilisateurs, applications et outils d'IA qui peuvent y accéder. Les workflows de gouvernance de l'accès aux données prennent en charge la correction en masse et déléguée. Les résultats DSPM peuvent être convertis en règles DLP en quelques clics, pour que les équipes puissent réduire l'exposition et faire respecter le principe du moindre privilège plus facilement.

Proofpoint DSPM permet une adoption plus sécurisée de l'IA. La solution détecte les données sensibles exposées aux copilotes, aux grands modèles de langage (LLM) et aux applications d'IA.

Allié à la gouvernance de l'accès aux données, à Enterprise DLP et à Data Security for AI, DSPM offre un moyen unique de découvrir, de gouverner et de protéger les données sensibles tout au long de leur cycle de vie.

Classification autonome de documents stratégiques

Proofpoint DSPM offre une classification des données de premier plan. Il utilise les expressions régulières, le traitement du langage naturel et les LLM pour améliorer les performances et réduire la consommation de ressources.

Proofpoint Autonomous Custom Classification (ACC) identifie les documents propres à l'entreprise sans règles manuelles ni apprentissage particulier. Les équipes peuvent découvrir des données propriétaires, éliminer les angles morts dans la visibilité et améliorer la détection des risques ainsi que l'application des règles.

La solution DSPM peut également appliquer des étiquettes de confidentialité Microsoft Information Protection (MIP) basées sur des classificateurs d'IA. Ces étiquettes aident à appliquer les règles de gouvernance, à appuyer la conformité et à protéger les données Microsoft contre tout accès non autorisé ou toute utilisation abusive.

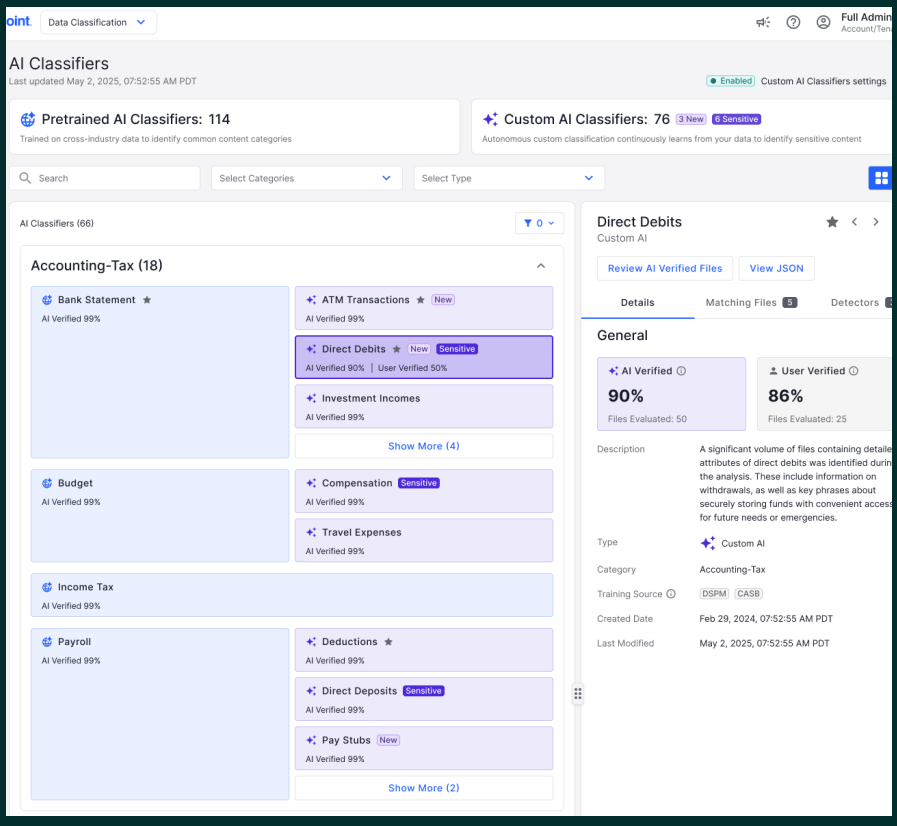

Figure 1. Les classificateurs d'IA pré-entraînés et autonomes de DSPM identifient les documents standard et propres à l'entreprise, dont les contrats, les dossiers financiers, le code source et les dossiers des employés.

Cartographie des risques d'accès aux données

La vue Data Risk Map indique où se situent les données sensibles dans les systèmes SaaS et sur site. Elle illustre le périmètre de partage des données ainsi que les utilisateurs, applications ou outils d'IA qui peuvent y accéder. Elle associe la classification de l'IA avec des informations sur l'accès et l'utilisation.

Les équipes de sécurité peuvent identifier les données surexposées, prioriser les risques, valider les correctifs et contrôler la pertinence des accès à mesure que l'utilisation de l'IA prend de l'ampleur. Les résultats de l'analyse de risques tiennent compte de la sensibilité des données, des tendances d'accès et de l'exposition. Ces renseignements aident les équipes à se concentrer sur les données à forte valeur et à haut risque tout en réduisant les coûts et la surface de risque de l'entreprise.

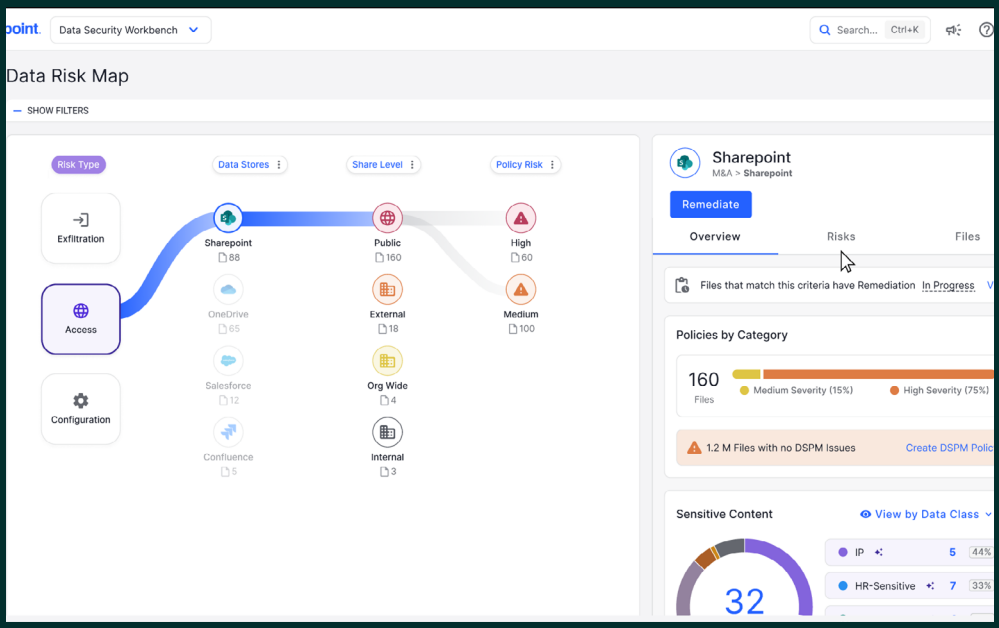

Figure 2. La vue Data Risk Map montre quels référentiels contiennent des données sensibles, l'étendue du partage des données et l'accès par les utilisateurs, les applications et les outils d'IA.

Prioriser les risques en fonction de la valeur monétaire des données

Les équipes de sécurité des données sont appelées à protéger de nombreuses banques de données. Cela étant, tous ces référentiels ne possèdent pas la même valeur ni le même niveau de risque. DSPM utilise une technologie de valorisation des données pour estimer le coût d'une compromission pour chaque banque de données. Les équipes peuvent ainsi se concentrer sur les ressources prioritaires. DSPM comprend également plus de 200 résultats d'analyses prédéfinies sur les accès et l'exposition, avec détection de combinaisons toxiques. Cette matrice des risques met en évidence les banques de données à haut risque et à fort impact financier.

Réduire les données obsolètes

Dans les systèmes SaaS et sur site, DSPM trouve et supprime les fichiers qui n'ont pas été consultés récemment. Les classificateurs d'IA aident les équipes à conserver les données stratégiques nécessaires. Dans les environnements IaaS (Infrastructure as a Service), DSPM identifie les banques de données inutiles. Il s'agit par exemple des données fantômes, dupliquées et abandonnées telles que les sauvegardes et les instantanés obsolètes.

Cette approche diminue les coûts de stockage, réduit la surface d'attaque et simplifie la gestion des données. Les équipes ne conservent que des données pertinentes et actives.

Veiller au respect du principe du moindre privilège

Proofpoint DSPM prend en charge l'accès selon le principe du moindre privilège en identifiant les utilisateurs dotés d'autorisations excessives, les accès inutilisés et les comptes à risque pour les diverses banques de données. La gouvernance de l'accès aux données et la stratégie Zero Trust de l'entreprise s'en trouvent renforcées.

La solution analyse les rôles relatifs à la gestion des identités et des accès (IAM), les autorisations, les droits d'accès aux bases de données et d'autres contrôles d'accès pour les identités humaines et machines. Elle indique qui peut accéder aux données sensibles en temps quasi réel. Les équipes peuvent supprimer les autorisations inutiles et réduire ainsi l'exposition.

Proofpoint DSPM signale également les comptes sous-protégés dans les environnements SaaS et PaaS (Platform as a Service). Par exemple, les utilisateurs ayant accès à des données sensibles sans authentification multifacteur (MFA), les comptes inactifs, ou encore les applications dotées de privilèges d'administration excessifs.

Détecter les chemins d'attaque dans les environnements cloud

Proofpoint DSPM collecte des informations sur les ressources de calcul et réseau, ainsi que sur les services PaaS et SaaS, pour les divers fournisseurs cloud. Il détecte les erreurs de configuration et les vulnérabilités dans ces ressources. Un graphique montre les chemins qu'un attaquant pourrait emprunter pour atteindre des données sensibles. La surveillance en temps quasi réel aide les équipes à repérer les changements qui augmentent l'exposition.

Des informations sur la sensibilité des données, les tendances d'accès et les risques viennent soutenir les outils DLP et DDR (Data Detection and Response).

Gouverner les accès directement ou par délégation

Dans les systèmes SaaS et sur site, les workflows DSPM transforment les renseignements sur les expositions de données en actions concrètes. Étant donné que des outils d'IA tels que Microsoft Copilot accentuent l'impact du partage excessif, la réduction de ces accès trop étendus devient essentielle. Les administrateurs peuvent révoquer les liens publics, les partages externes et l'accès au niveau du domaine sur Google Workspace et Microsoft 365. Cette action permet une correction à l'échelle de l'entreprise.

Les équipes de sécurité sont incapables d'estimer à elles seules le niveau d'accès approprié pour chaque fichier. Les workflows de gouvernance de l'accès aux données leur permettent d'attribuer des évaluations des accès aux propriétaires de contenu. Les campagnes automatisées, les rappels et le suivi facilitent la pérennité de la gouvernance.

L'intégration avec Enterprise DLP étend les protections au-delà des données au repos. Les données sensibles classifiées et les risques priorisés par DSPM peuvent être associés à des règles DLP. Cela favorise une protection cohérente et une correction automatisée sur l'ensemble de la messagerie, des endpoints, du cloud et des canaux de collaboration.

Dans les environnements IaaS et PaaS, des informations et des recommandations exploitables aident les équipes à réduire rapidement les expositions. Les intégrations avec les plates-formes de gestion des tickets, de notification et d'automatisation aident les opérateurs de sécurité à collaborer avec les équipes DevOps et d'ingénierie de plate-forme via les workflows existants.

Alignement sur les cadres de conformité

Proofpoint DSPM peut identifier des lacunes de conformité en matière de confidentialité et de sécurité pour plus de 25 cadres réglementaires (loi européenne sur l'IA, RGPD, HIPAA, NIST, CMMC, SOC 2, etc.).

Les violations sont marquées à la fois par cadre et par contrôle, de sorte que les analystes peuvent observer l'impact sur la conformité.

Les rapports montrent l'état de conformité dans l'ensemble de l'infrastructure, avec des vues par compte, ressource et cadre. Il est ainsi plus facile de corriger les vulnérabilités, de se préparer aux audits et de maintenir la conformité.

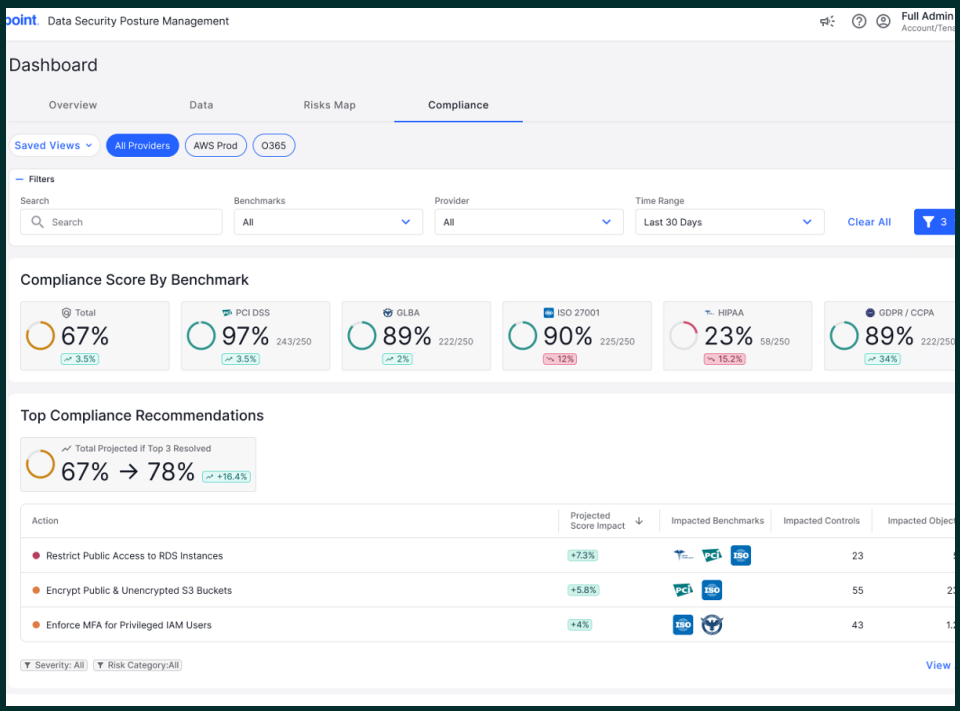

Figure 3. Tableau de bord affichant la posture de conformité.

Réduire les risques d'exposition des données à l'IA

Proofpoint DSPM aide les entreprises à maîtriser la présence de l'IA en identifiant les données sensibles exposées aux applications et workflows de l'IA.

La solution alimente le tableau de bord Proofpoint Data Security for AI en informations sur l'exposition. Ce tableau de bord propose une vue centrale des risques liés aux données dans les applications d'IA approuvées et non approuvées. DSPM surveille également les erreurs de configuration des applications d'IA et aide les équipes à les corriger, ce qui réduit le risque de fuites, renforce la gouvernance des données d'IA et favorise l'adoption sécurisée.

Proofpoint DSPM sécurise les LLM personnalisés et les applications d'IA sur des plates-formes telles qu'AWS Bedrock et Azure ML. Il détecte les données sensibles introduites dans les modèles de base, les modèles personnalisés et les workflows de génération augmentée par récupération (RAG).

DSPM fournit également des API spécialisées pour la sécurisation des LLM. En plus d'analyser en temps réel les données sensibles entrant et sortant des LLM, ces API assurent la gouvernance et la visibilité de l'utilisation des données et s'intègrent aux workflows clients.

Plates-formes et technologies prises en charge

Proofpoint DSPM découvre et classifie les données pour de nombreux services et plates-formes. Il prend en charge un large éventail de banque des données — des bases de données relationnelles aux magasins NoSQL et key-value. Les équipes disposent d'une visibilité sur les données structurées, non structurées et semi-structurées.

La solution prend en charge les principales plates-formes cloud et SaaS. AWS, Azure, Google Cloud Platform (GCP), Snowflake, Salesforce, ServiceNow, Workday, LLM et copilotes en sont des exemples.

Le cadre commun de découverte et de classification permet à Proofpoint d'ajouter rapidement la pris en charge de nouvelles banques de données.

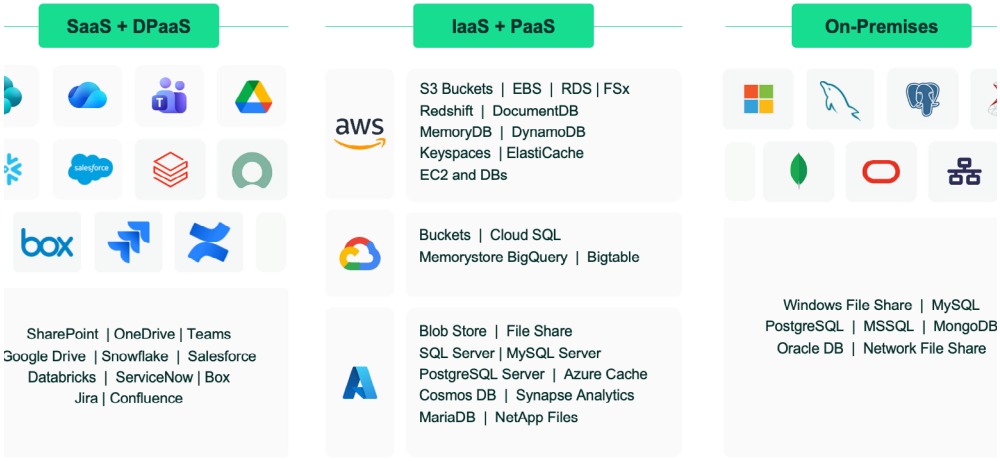

Figure 4. DSPM découvre et classifie les données pour une large gamme de plates-formes et de services.

Conclusion

Alors que les entreprises adoptent l'IA et gèrent davantage de données, elles doivent savoir où se trouvent les données sensibles, qui peut y accéder et comment elles sont utilisées. Proofpoint DSPM réduit l'exposition en classifiant les données sensibles, en priorisant les risques, en identifiant les niveaux d'accès excessifs et en appliquant le principe du moindre privilège dans les environnements cloud, SaaS, sur site et IA.

Dans le cadre du dispositif de sécurité des données de Proofpoint, la solution Proofpoint DSPM collabore avec Proofpoint Enterprise DLP. Ensemble, ils aident les équipes à découvrir, à classifier, à gouverner et à protéger les données sensibles. Les entreprises peuvent renforcer leur conformité, sécuriser l'adoption de l'IA, réduire les risques et protéger leurs informations les plus précieuses.

proofpoint.