proofpoint.

FICHE SOLUTION

Sécurité des données pour l'IA générative

Garantissez une utilisation sécurisée de l'IA générative.

Principaux avantages

- Obtention d'une visibilité sur l'utilisation non autorisée d'outils d'IA générative
- Prévention de l'exposition de données sensibles grâce à des outils d'IA générative d'entreprise et à un développement à l'aide de LLM
- Application de règles d'utilisation acceptable de l'IA générative dans le cloud et sur les endpoints
- Surveillance des menaces internes grâce à des règles dynamiques permettant de détecter toute utilisation dangereuse de l'IA
- Formation des collaborateurs à l'utilisation acceptable d'outils d'IA générative

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.

L'IA générative offre un immense potentiel, dans la mesure où elle stimule la productivité, l'innovation et les informations sur les données. Toutefois, son adoption présente également des défis, surtout en matière de sécurité des données, de confidentialité et de conformité. Lorsqu'ils se servent d'outils publics d'IA générative, les utilisateurs risquent d'exposer des données sensibles et des éléments de propriété intellectuelle. Par ailleurs, une gouvernance médiocre peut conduire à un accès non autorisé aux données par des outils d'entreprise comme Microsoft 365 Copilot et à la classification incorrecte des résultats sensibles. Les grands modèles de langage (LLM) personnalisés entraînés avec des données client peuvent divulguer des données personnelles, engendrant ainsi des risques de non-conformité à des réglementations telles que le RGPD et les lois HIPAA et CCPA. Sans gouvernance robuste, les entreprises risquent de faire l'objet de compromissions de sécurité et d'amendes pour non-conformité réglementaire.

Proofpoint garantit une utilisation acceptable des outils et modèles d'IA générative grâce à une approche complète et centrée sur les personnes qui allie visibilité, contrôle et formation. Proofpoint Data Loss Prevention (DLP) surveille l'utilisation de l'IA générative sur les endpoints, en fournissant des informations sur les interactions utilisateur et en identifiant les outils non autorisés. Pour prévenir les fuites de données, Proofpoint applique des règles qui bloquent la saisie de données sensibles ou masquent celles-ci dans les invites d'IA générative. Proofpoint Data Security Posture Management (DSPM) prévient l'exposition de données via des outils d'IA générative et des LLM en classant les données sensibles et en les protégeant contre les accès non autorisés. En outre, Proofpoint ZenGuide propose des formations de sensibilisation à la cybersécurité personnalisées pour apprendre aux collaborateurs à utiliser l'IA générative en toute sécurité, ce qui favorise une culture d'utilisation responsable.
En intégrant ces stratégies, Proofpoint protège les données sensibles des entreprises dans le paysage de l'IA générative en constante évolution.

Bénéficiez d'une visibilité sur l'utilisation non autorisée d'outils d'IA générative

Proofpoint aide les entreprises à comprendre qui utilise quels outils d'IA générative et si des données sensibles sont exposées via ces outils ou des LLM personnalisés. Notre rapport sur la sécurité des données dans un contexte d'utilisation de l'IA met en avant les types de données sensibles envoyés à des outils publics d'IA générative, les utilisateurs les plus actifs, les principaux sites par activité, etc. (figure 1).

Grâce à des API cloud, vous pouvez identifier les autorisations d'applications

Principaux avantages

- Prévention de l'exposition de données sensibles grâce à des outils d'IA générative d'entreprise et à un développement à l'aide de LLM

d'IA tierces telles qu'OpenAI et générer des alertes connexes. Vous pouvez également identifier les déploiements d'IA dans AWS Bedrock et Azure OpenAI qui utilisent des données sensibles.

Prévenez l'exposition de données sensibles via des outils d'IA générative et des LLM

Proofpoint DSPM identifie et classe les données sensibles dans les workflows d'IA, de manière à prévenir toute exposition susceptible de conduire à des compromissions. Il protège également les données auxquelles accède Microsoft Copilot en appliquant des étiquettes Microsoft Information Protection (MIP), qui sont utilisées pour mettre en œuvre des règles de protection telles que le chiffrement et des contrôles d'accès. Il sécurise en outre les LLM personnalisés et les applications d'IA sur des plates-formes telles qu'AWS Bedrock et Azure OpenAI en détectant les données sensibles qui alimentent les modèles de base ou personnalisés ainsi que les workflows RAG (Retrieval-Augmented Generation).

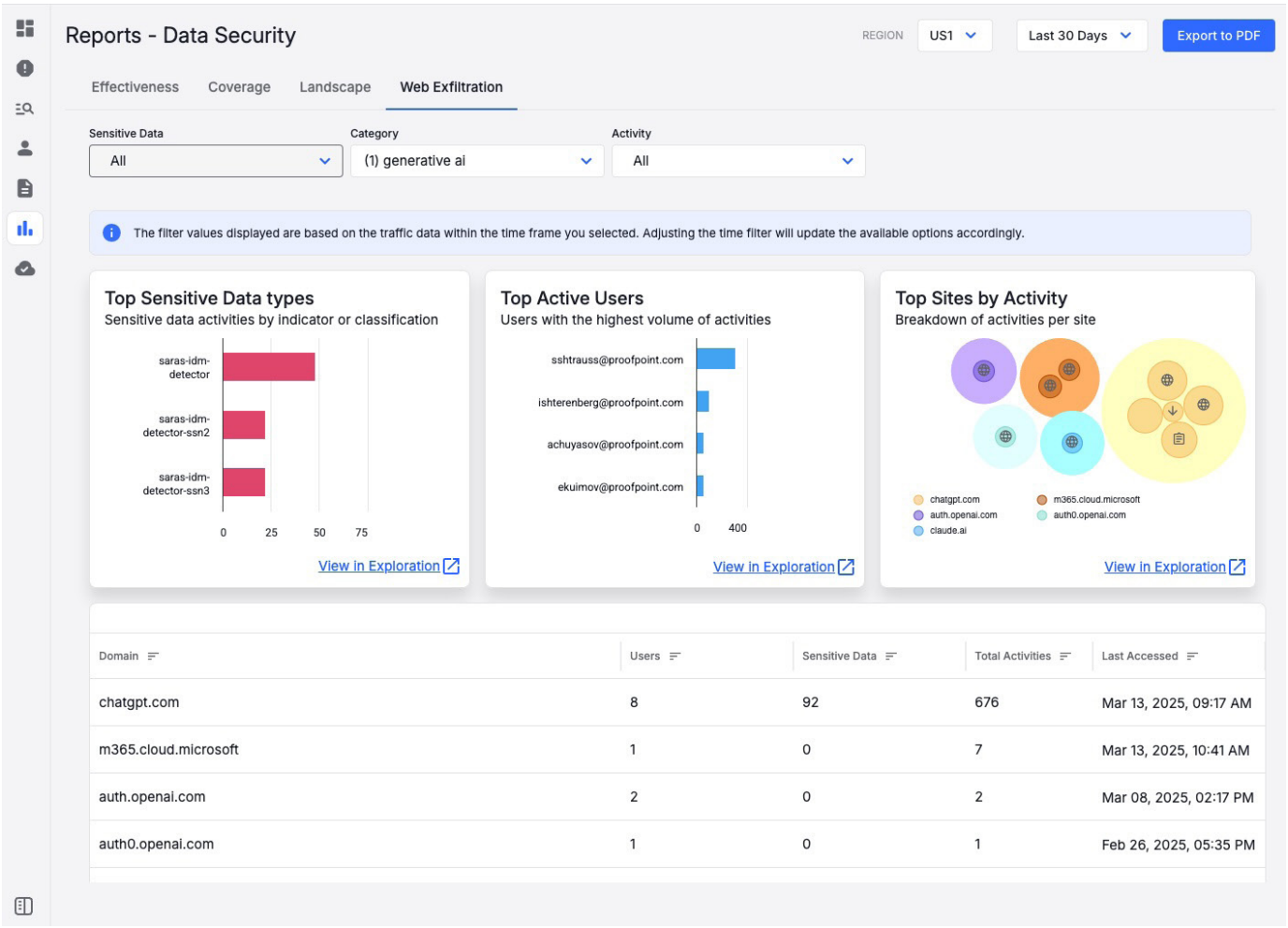

Figure 1. Rapport mettant en avant les principaux risques d'exfiltration de données via l'IA générative

Principaux avantages

- Application de règles d'utilisation acceptable de l'IA générative dans le cloud et sur les endpoints
- Surveillance des menaces internes grâce à des règles dynamiques permettant de détecter toute utilisation dangereuse de l'IA
- Formation des collaborateurs à l'utilisation acceptable d'outils d'IA générative

Proofpoint propose des API spécialisées pour la sécurité des LLM, ce qui permet d'analyser en temps réel la sensibilité des données transitant via les LLM. Ces API offrent une gouvernance et une visibilité totales sur l'utilisation des données grâce à une intégration fluide aux workflows client pour un déploiement efficace.

Prévenez les fuites de données et les menaces internes associées à l'utilisation de l'IA générative

Sur les endpoints, vous pouvez surveiller les utilisateurs qui naviguent sur des sites d'IA générative à l'aide de la catégorisation Web ou générer des alertes en cas d'installation d'applications d'IA non autorisées. Nos règles dynamiques peuvent renforcer la surveillance des endpoints pour les utilisateurs présentant des comportements à risque. Par exemple, vous pouvez capturer des métadonnées et des captures d'écran avant et après l'envoi par des utilisateurs de contenus sensibles à des sites d'IA générative non autorisés. Cela vous permet de consacrer moins de temps à l'analyse des interactions utilisateur avec les outils d'IA générative.

Avec Proofpoint DLP, vous pouvez appliquer des règles DLP au niveau des endpoints pour plus de 600 outils d'IA générative par utilisateur, groupe ou département, ainsi que bloquer les chargements Web vers des plates-formes d'IA générative ou masquer les données sensibles saisies dans les invites. Pour préserver la productivité des utilisateurs, notre solution peut également les encourager à respecter les règles d'utilisation de l'IA générative ou leur demander une justification au lieu d'appliquer des règles de prévention.

Via des API cloud, nous offrons une visibilité sur les fichiers partagés de manière excessive exposés à Microsoft 365 Copilot et avertissons votre équipe de sécurité lorsque des utilisateurs se servent de Copilot de façon abusive pour localiser des fichiers contenant des informations sensibles.

Par exemple, Proofpoint détecte quand un utilisateur interne à risque a recours à Copilot pour accéder à de nombreux fichiers contenant des données sensibles en un court laps de temps. Par ailleurs, notre solution classe, étiquette et protège les contenus générés par l'IA dans les applications cloud. Qui plus est, elle révoque ou bloque les autorisations d'applications d'IA tierces non approuvées.

Formez les collaborateurs à l'utilisation acceptable d'outils d'IA générative

Proofpoint apprend aux utilisateurs à se servir de l'IA générative en toute sécurité dans votre entreprise. Proofpoint ZenGuide forme les utilisateurs grâce à des vidéos, des posters, des modules interactifs et des newsletters sur la gestion sécurisée des données. Il vous permet de tirer parti d'informations sur vos utilisateurs à haut risque et d'automatiser l'apprentissage personnalisé basé sur le niveau de risque pour des groupes ciblés, par exemple les développeurs, ou pour vos utilisateurs les plus vulnérables.

Les activités de formation encouragent les comportements positifs par le biais d'évaluations, d'avertissements personnalisés et d'expériences de coaching. Ces activités incluent des évaluations des connaissances, des attributions de formations, des notifications et des confirmations d'adhésion à des règles, tous conçus pour améliorer la sensibilisation et encourager une utilisation sécurisée et acceptable des outils d'IA générative.

Boostez votre entreprise grâce à l'utilisation sécurisée de l'IA générative

Proofpoint propose une solution centrée sur les personnes pour relever les défis modernes en matière de sécurité des données. Nous fournissons des informations sur les risques d'exposition et de fuite de données liés aux outils d'IA générative et aux LLM.

Avec Proofpoint, vous pouvez trouver facilement le juste équilibre entre productivité des utilisateurs et sécurité des données en adoptant des stratégies qui permettent aux utilisateurs d'accéder à des outils et modèles d'IA générative grâce à des formations, à une surveillance renforcée et à des contrôles adéquats des données.

proofpoint.

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises du classement Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

Suivez-nous : LinkedIn

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →

0207-017-03-01 03/25