

Proofpoint Data Security for AI

Surveillez et contrôlez l'utilisation des données sensibles dans les applications d'IA approuvées et non approuvées

Principaux avantages

- Réduction des risques induits par l'IA qui pèsent sur les données
- Amélioration de la visibilité sur l'activité de l'IA à l'échelle de l'entreprise
- Surveillance et gouvernance de l'utilisation d'applications d'IA non approuvées
- Protection des données sensibles dans les requêtes et les téléchargements
- Accélération de l'adoption en toute sécurité de l'IA
- Soutien de la conformité et de la préparation aux audits

Le défi : l'exposition des données induite par l'IA

Les applications d'IA générative (GenAI) transforment l'entreprise, en aidant les collaborateurs à travailler plus rapidement et plus efficacement. Les entreprises éprouvent toutefois des difficultés à contrôler la manière dont les données sensibles sont partagées avec les outils d'IA, les copilotes et les applications optimisées par l'IA.

Bien souvent, les collaborateurs téléchargent des fichiers et envoient des requêtes contenant des informations métier sensibles à des applications d'IA approuvées et non approuvées. Or, les technologies traditionnelles de protection des données n'ont pas été conçues pour surveiller les requêtes, les téléchargements et les réponses de l'IA en temps réel. Les entreprises disposent ainsi d'une visibilité limitée sur la manière dont les systèmes d'IA accèdent aux données sensibles et les exposent.

De plus, les utilisateurs internes peuvent utiliser les outils d'IA de manière abusive — intentionnellement ou non — pour localiser, résumer, réécrire ou exfiltrer des informations sensibles, y compris des documents confidentiels, du code propriétaire et des éléments de propriété intellectuelle. Les utilisateurs internes malveillants peuvent utiliser l'IA pour accélérer le vol de données, échapper aux contrôles traditionnels ou automatiser l'extraction de données sensibles à grande échelle.

Sans les contrôles adéquats, les entreprises risquent de faire l'objet de fuites de données, de violations de la conformité et d'une exposition non autorisée d'informations réglementées ou confidentielles. Les équipes de sécurité ont besoin d'une visibilité continue sur l'utilisation et l'exposition des données par l'IA, d'une application plus stricte des règles et d'une auditabilité complète pour soutenir l'adoption de l'IA en toute sécurité.

La solution : Proofpoint Data Security for AI

Proofpoint aide les entreprises à adopter l'IA en toute sécurité grâce à une visibilité sur l'utilisation des données par les applications d'IA approuvées et non approuvées. Il unifie la surveillance, les contrôles des données spécifiques à l'IA et les informations sur l'activité de l'IA afin de réduire les risques et de favoriser une adoption sécurisée et évolutive de l'IA.

Fonctions essentielles

Visibilité sur l'utilisation des données par l'IA et le niveau de sécurité des applications d'IA

Proofpoint offre une visibilité sur la manière dont les collaborateurs et l'IA interagissent avec les données de l'entreprise. Les équipes de sécurité peuvent ainsi identifier les utilisateurs à haut risque, détecter les interactions non sécurisées avec l'IA et comprendre quelles données et documents sensibles sont exposés par l'utilisation d'applications d'IA approuvées et non approuvées.

Les classificateurs personnalisés autonomes de la solution identifient les données sensibles propres à l'entreprise qui sont partagées via des requêtes de l'IA, des téléchargements et des réponses générées par l'IA, notamment la propriété intellectuelle, le code source, les données financières et les documents stratégiques. Ce contexte permet de détecter, de masquer et de protéger les données avec plus de précision dans les applications d'IA approuvées et non approuvées.

Proofpoint surveille en permanence les environnements d'IA et SaaS afin de détecter les erreurs de configuration, les autorisations excessives au niveau du site et les intégrations non sécurisées. La mise au jour des droits d'accès excessifs et des lacunes de la configuration permet aux entreprises de remédier aux risques, de réduire leur surface d'attaque et d'éviter que des données sensibles ne soient exposées aux utilisateurs et aux applications d'IA.

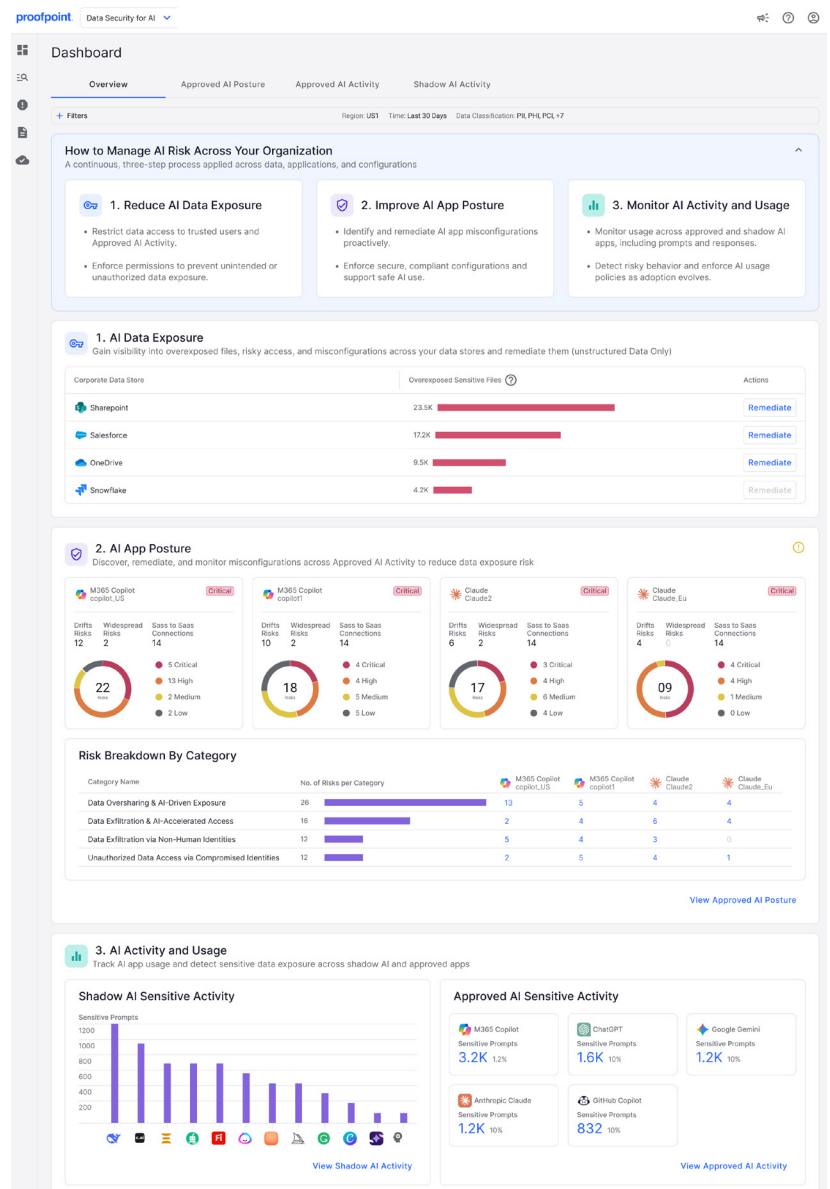


Figure 1. Proofpoint offre aux équipes de sécurité une visibilité approfondie sur la manière dont les collaborateurs et les outils d'IA interagissent avec les données sensibles.

Surveillance et remédiation des applications d'IA approuvées

Proofpoint surveille en continu les requêtes, les téléchargements et les réponses générées par l'IA au sein des applications d'IA approuvées afin d'identifier l'exposition de données sensibles et toute activité inhabituelle de la part d'utilisateurs internes, notamment un nombre excessif de requêtes ou le téléchargement de gros volumes de données. La capture complète des requêtes et des réponses facilite les investigations et la préparation aux audits. Les workflows de remédiation intégrés aident quant à eux les administrateurs et les propriétaires de fichiers à intervenir rapidement en cas de partage excessif de données.

Protection des données dans les applications d'IA non approuvées

Les entreprises peuvent réduire l'exposition des données par l'IA en surveillant et en contrôlant l'utilisation de celles-ci par les applications d'IA Web et de bureau non approuvées. Proofpoint aide à prévenir les fuites de données via des requêtes, des téléchargements et des actions de collage. Il masque également les données sensibles présentes dans les requêtes avant qu'elles ne soient partagées avec des outils d'IA. Les entreprises peuvent ainsi étendre l'adoption de l'IA en toute sécurité sans bloquer complètement les applications d'IA.

Impact opérationnel

Réduction des fuites de données induites par l'IA

Prévenez l'exposition de données sensibles dans des applications d'IA approuvées et non approuvées.

Amélioration de la visibilité et de la gouvernance de l'IA

Bénéficiez d'une visibilité centralisée sur la manière dont les collaborateurs et les outils d'IA interagissent avec les données de l'entreprise.

Adoption plus sûre de l'IA en entreprise

Autorisez une utilisation productive de l'IA générative tout en maintenant en place les contrôles de la sécurité, de la gouvernance et de la conformité.

Accélération des investigations et des réponses

Capturez l'activité de l'IA, les requêtes et les réponses afin de faciliter les investigations, la remédiation et la préparation aux audits.

Renforcement du niveau de conformité

Adaptez-vous à l'évolution des exigences en matière d'IA, de confidentialité et de protection des données en appliquant des règles aux informations réglementées, confidentielles et propriétaires utilisées avec des outils d'IA.

Réduction des risques liés aux applications d'IA non approuvées

Mettez au jour et gouvernez l'utilisation d'applications d'IA non approuvées et les comportements utilisateurs à risque tout en minimisant l'impact sur la productivité de l'entreprise.

En savoir plus

Pour plus d'informations, visitez notre site à l'adresse: proofpoint.com/fr.

À propos de Proofpoint. Inc. Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et en toute confiance. Pour en savoir plus, consultez le site proofpoint.com/fr.

Suivez-nous : [LinkedIn](#)

Proofpoint est une marque déposée ou un nom commercial de Proofpoint, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.