

Accélérez l'adoption de l'IA grâce à une sécurité intrinsèque

L'IA est désormais là et le modèle de sécurité traditionnel perd sa primauté

98 %

des entreprises disposent d'applications non autorisées au sein de leur parc applicatif, notamment liées à l'IA fantôme. Ces angles morts entraînent un risque d'exposition des données et de violations de la conformité.¹

50 %

Les attaques par injection d'invites (prompts) affichent un taux de réussite de 50 %. Il s'agit donc de la plus grande menace envers la sécurité selon le Top 10 de l'OWASP consacré aux applications LLM.²

97 %

des entreprises ayant subi des incidents de sécurité liés à l'IA ne disposaient pas de mesures adéquates en termes de contrôle des accès à l'IA.³

93 %

des collaborateurs reconnaissent avoir saisi des informations sans autorisation au sein d'outils IA.⁴

Sécurisez le cycle de vie de l'IA grâce à Cloudflare

sur l'ensemble des outils d'IA générative et agentique

Sécurité humain-IA



Sécurité de l'IA agentique



La sécurité est intégrée lors de vos efforts de développement d'IA sur Cloudflare



Études de cas clients

indeed

Premier site web consacré à l'emploi du monde

Identifie et contrôle l'IA fantôme

en parallèle de son projet de modernisation de l'accès à distance.

Cloudflare

Entreprise SaaS soutenue par IA

Protège les PII en empêchant les clients d'envoyer des informations sensibles aux points de terminaison d'IA générative accessibles par le public.

Cyndx

Entreprise de technologies financières soutenue par IA

Réduit les coûts d'inférence de 95 %

en adoptant Cloudflare pour mettre en cache et exécuter les réponses des fournisseurs de modèles d'IA.

Découvrez comment Cloudflare peut sécuriser votre adoption de l'IA

Découvrir les scénarios d'utilisation

1. Varonis, 2025 State of Data Security (État des lieux 2025 de la sécurité des données)

2. Liu, S., Wang, Z., Chen, Y., Deng, G., Liu, Y. et Liu, Y. (2024). Automatic and Universal Prompt Injection Attacks against Large Language Models (attaques par injection automatique et universelle d'invites à l'encontre des grands modèles linguistiques)

3. IBM, 2025 Cost of a Data Breach Rapport sur le coût d'une violation de données en 2025

4. ManageEngine, The Shadow AI Surge in Enterprises (L'explosion de l'IA fantôme au sein des entreprises)

© 2025 Cloudflare, Inc. Tous droits réservés. CLOUDFLARE® et le logo Cloudflare sont des marques commerciales de Cloudflare. Tous les autres noms d'entreprises et de produits peuvent être des marques commerciales des entreprises auxquelles ces noms sont associés.

01 73 01 52 44 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr

RÉV. : BDES-8274.2025OCT1