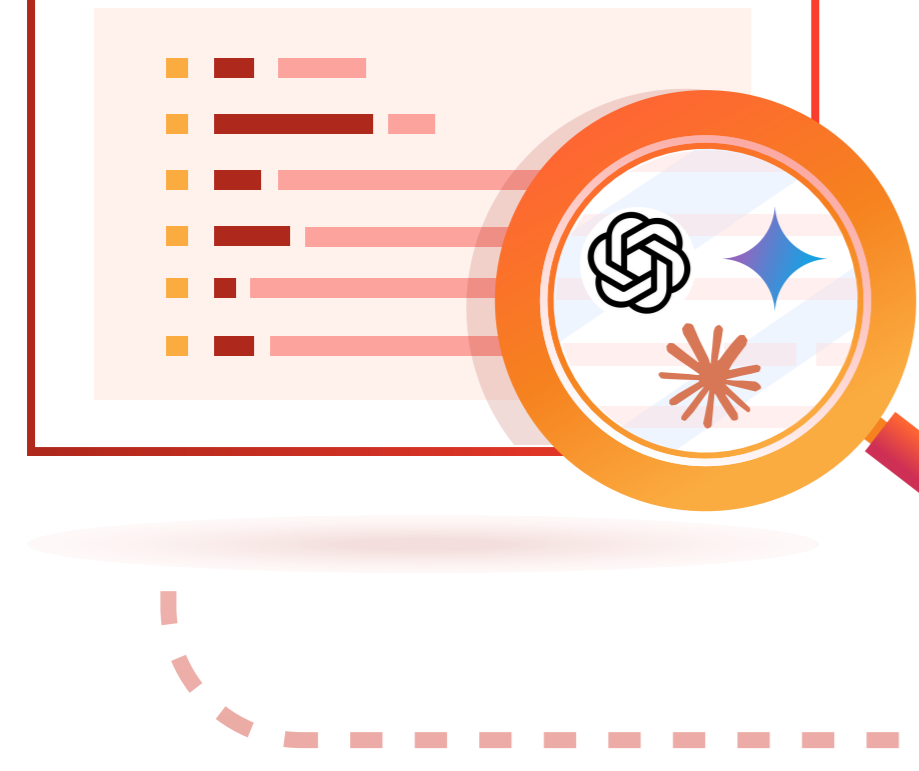


Accélérez l'adoption de l'IA grâce à une sécurité intrinsèque

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

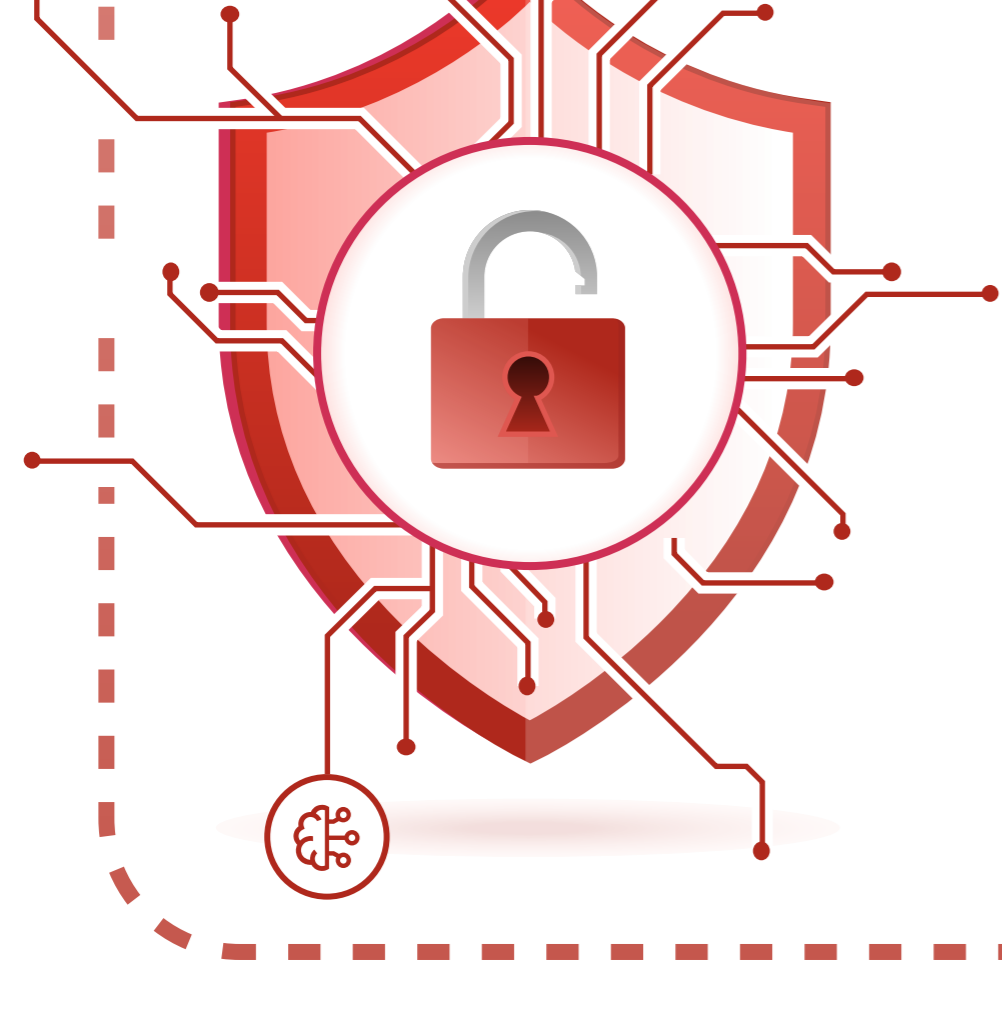
50 %

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

Sécurisez la manière dont vos collaborateurs utilisent l'IA générative

- Identifiez l'IA fantôme
- Évaluez les risques posés par les applications IA
- Gérez le niveau de sécurité des applications IA
- Limitez les saisies de données sensibles
- Appliquez des garde-fous aux invites et aux réponses

Protégez vos applications et vos workloads soutenus par IA

- Identifiez les points de terminaison des outils d'IA fantôme
- Protégez vos modèles IA et vos données d'entraînement contre les abus
- Empêchez l'exposition d'informations d'identification personnelle (PII) dans les invites et les réponses
- Appliquez des politiques de modération du contenu



Sécurisez ce que vous développez

- Concevez des serveurs MCP disposant de fonctions d'authentification/autorisation intégrées
- Journalisez et limitez les requêtes/réponses des modèles IA, l'utilisation des jetons et les coûts
- Empêchez les épisodes d'interruption de service grâce à des modèles de secours et au contrôle du volume des requêtes



La différence Cloudflare

Protection complète du cycle de vie de l'IA

Une plateforme unique permettant de sécuriser la communication humain-IA et IA-ressources, du développement au déploiement.

Sécurité de l'IA, en inline et en temps réel

Sécurisez les invites et les réponses de l'IA en temps réel grâce à des mesures de contrôle couvrant les environnements IA publics et privés.

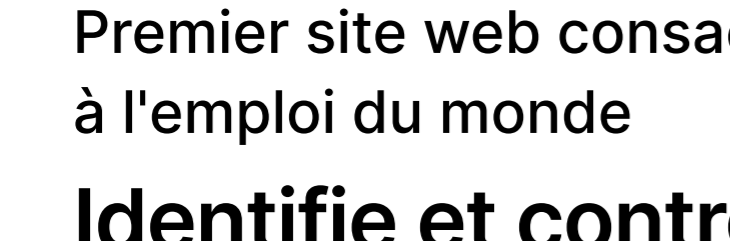
Architecture IA mondiale et pérenne

Tirez parti de notre réseau mondial pour assurer la disponibilité cohérente à la périphérie, à l'échelle et avec les performances exigées par l'IA.

Déploiement agnostique vis-à-vis des modèles

Les mesures de contrôle de la sécurité fonctionnent pour l'ensemble des modèles IA de votre environnement et assurent une approche unifiée de la gouvernance des déploiements d'IA.

Études de cas clients



Premier site web consacré à l'emploi du monde

Identifie et contrôle l'IA fantôme

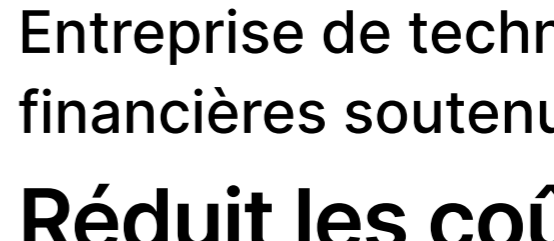
en parallèle de son projet de modernisation de l'accès à distance.



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.



Entreprise de technologies financières soutenues 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 Report (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)