CLOUDFLARE

PRÉSENTATION DE SOLUTION

Cloudflare AI Security Suite

Sécurisez vos interactions avec l'IA en contrôlant les données et en gérant les risques tout au long du cycle de vie de vos outils IA.

Faites évoluer l'IA en toute confiance

Les risques liés à l'IA nécessitent une sécurité moderne

Vos équipes font appel à l'IA afin d'innover plus rapidement, mais cette utilisation entraîne des risques critiques envers la sécurité. L'ancienne stratégie consistant à bloquer l'IA ou à ajouter davantage de solutions dédiées et complexes échoue, car elle entrave l'innovation et ignore la réalité :

- **85 % des collaborateurs** utilisent des outils IA avant que le service IT ne puisse les autoriser.[1]
- **93 % des collaborateurs reconnaissent** avoir saisi des informations sans approbation au sein d'outils IA.[2]
- **63 % des entreprises victimes de violations de données** ne disposent d'aucune politique de gouvernance en matière d'IA.[1]

Apprenez à donner du pouvoir à vos équipes et à permettre à ces dernières de tirer parti des avantages proposés par l'IA en termes de productivité, tout en préservant la sécurité et le degré de contrôle nécessaires à votre entreprise.

Une plateforme unifiée pour sécuriser l'IA agentique et générative

La plateforme unique proposée par Cloudflare permettra à votre entreprise d'adopter l'IA en toute confiance. Nous permettons aux responsables de la sécurité de disposer de tous les moyens nécessaires pour gérer les risques, aux équipes technologiques de gagner en productivité et aux ingénieurs chargés de la plateforme de développer en toute sécurité afin de veiller à ce que chaque pôle puisse innover ensemble, de manière sécurisée.

Lancez-vous dans l'aventure Cloudflare AI Security Suite

La Cloudflare AI Security Suite propose une plateforme unifiée permettant de sécuriser l'utilisation des outils IA et des applications publiques au sein de l'espace de travail. Identifiez l'IA fantôme (Shadow AI), protégez vos modèles contre l'utilisation abusive, sécurisez l'accès de vos agents et empêchez l'exposition de vos données dans les invites (prompts) afin de permettre à votre entreprise d'innover en toute sécurité et de manière plus efficace grâce à une visibilité accrue et à des mesures de contrôle renforcées.

Étendez la visibilité

à l'ensemble de vos applications IA, de vos points de terminaison d'API et des connexions de vos agents IA.

Atténuez les risques

à l'aide de garde-fous, ainsi que de mesures de contrôle du niveau de sécurité et d'atténuation des menaces en temps réel.

Protégez vos données

grâce à des mesures rapides de protection et de contrôle de l'utilisation pour vos collaborateurs et vos agents IA.

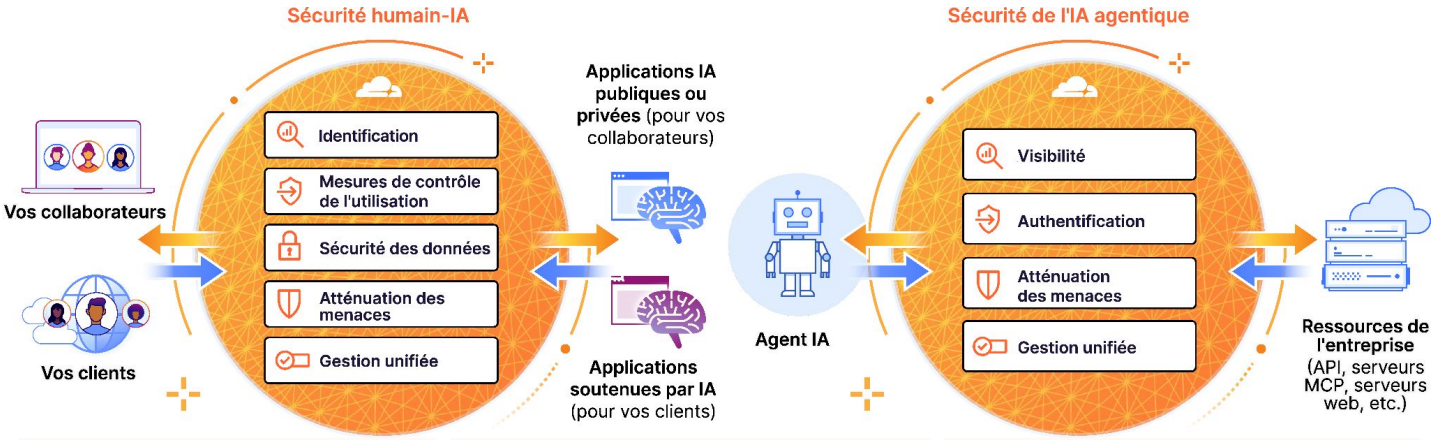
La sécurité est intégrée
lorsque vous développez des outils IA sur Cloudflare.

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

RÉV. : PMM-OCT2025

Sécurisez vos communications avec l'IA générative et agentique grâce à la Cloudflare AI Security Suite

Protégez toutes vos communications avec l'IA en contrôlant les données que vos collaborateurs utilisent dans les outils d'IA générative et en gérant les risques envers la sécurité posés par les agents autonomes.

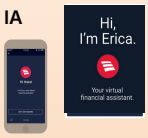


- **Vos effectifs :** collaborateurs, sous-traitants, développeurs, etc.
- **Vos clients :** visiteurs de vos sites web et utilisateurs de vos applications

- **Applications d'IA générative :** autonomes ou incorporées

Gemini Claude ChatGPT Copilot

- **Applications soutenues par IA** Exemple : Erica, le chatbot IA déployé par Bank of America



- **API** et **serveurs MCP** pour toutes les applications.

Google Workspace

- **Serveurs web** pour l'inférence et la génération augmentée par récupération (RAG, Retrieval-Augmented Generation)

Accélérez l'adoption de l'IA grâce à une sécurité intrinsèque, tout au long du cycle de vie de l'IA.

Sécurisez la manière dont vos collaborateurs utilisent l'IA

Mettez en œuvre des mesures de contrôle de l'utilisation de l'IA et de gestion de la posture de sécurité de l'IA (AI-SPM) afin d'atténuer les risques et de protéger vos données.

Protégez vos applications soutenues par IA

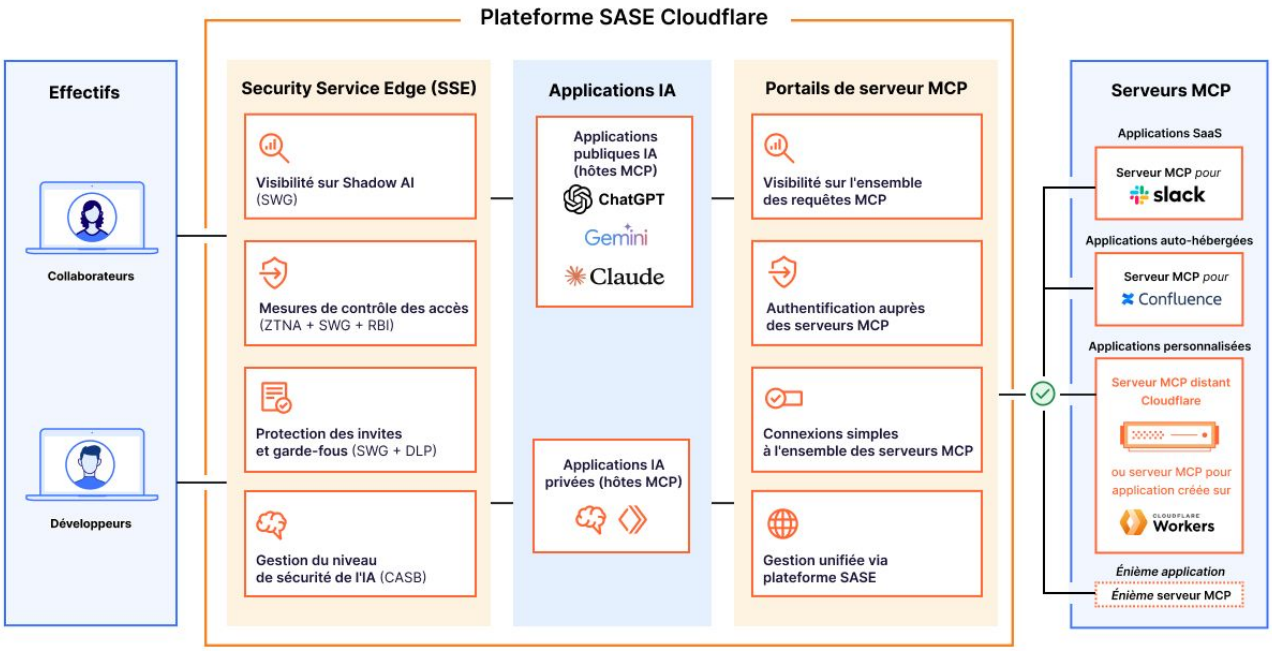
Protégez vos applications et vos API soutenues par IA contre l'injection d'invites et les fuites de données, en temps réel.

Développez des outils IA en toute sécurité

Donnez à vos développeurs tous les moyens nécessaires pour sécuriser les applications IA grâce à des fonctions d'observabilité intégrées, au contrôle du volume des requêtes et à des garde-fous internes (in-line) supervisant l'IA.

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

Sécurisez la manière dont vos collaborateurs utilisent les applications et les workloads IA grâce à la plateforme SASE de Cloudflare.



Le SSE au service de la protection de la communication entre les humains et l'IA

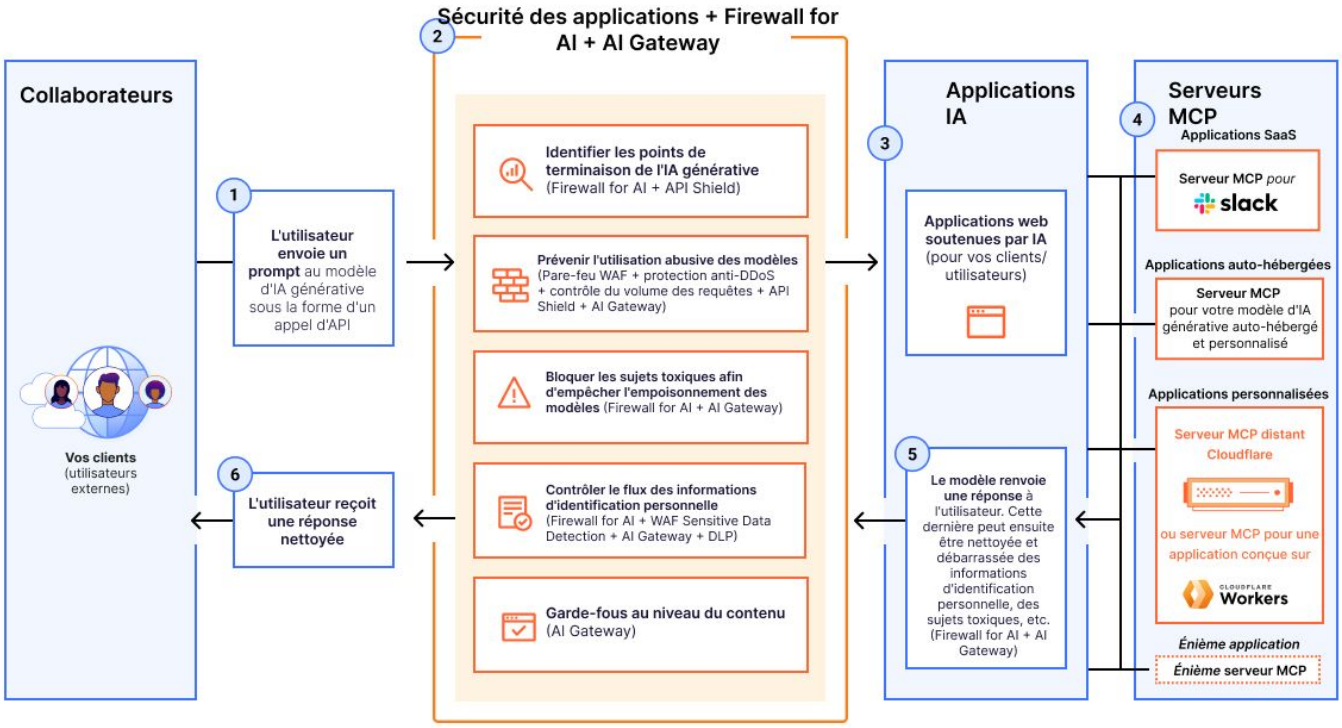
- **Visibilité :** identifiez et analysez l'utilisation du Shadow AI (IA fantôme) grâce à l'inspection du trafic en interne (in-line). Évaluez les risques présentés par ces applications à l'aide d'une notation transparente.
- **Contrôles des accès :** bloquez, isolez, redirigez ou autorisez les connexions utilisateur. Appliquez des règles Zero Trust basées sur l'identité et spécifiques à chaque application.
- **Protection des invites et garde-fous** : détectez et bloquez les invites des utilisateurs en fonction de leur intention (p. ex., tentatives de piratage, utilisation abusive du code, demandes d'informations d'identification personnelle).
- **Sécurité des données :** empêchez l'exposition des données sensibles grâce à des mesures de détection soutenues par IA et proposées dans le cadre de la prévention des pertes de données (DLP) pour les informations d'identification personnelle (PII, Personal Identification Information), le code source et plus encore.
- **Gestion du niveau de sécurité de l'IA :** intégrez les outils d'IA générative par API afin de rechercher les erreurs de configuration à l'aide de notre CASB (Cloud Access Security Broker, agent de sécurité des accès au cloud). Cette fonctionnalité est désormais disponible pour ChatGPT, Claude et Google Gemini.

Des portails pour les serveurs MCP afin de protéger la communication IA-ressources

- **Visibilité :** agrégez l'ensemble de vos journaux de requêtes basées sur le protocole MCP (Model Context Protocol) à des fins d'audit et d'analyse. Vérifiez et approuvez chaque serveur MCP avant de l'ajouter au portail.
- **Authentification :** authentifiez l'accès des utilisateurs aux portails en fonction de leur identité. Limitez l'accès aux serveurs MCP en fonction du principe du moindre privilège.
- **Connexions :** connectez tous les serveurs MCP accessibles à l'aide d'une URL unique plutôt que de configurer chaque serveur MCP de manière indépendante.
- **Gestion unifiée :** appliquez les mêmes politiques d'accès granulaires à vos connexions IA que celles que vous utilisez pour vos utilisateurs humains.

Remarque : les portails des serveurs MCP prennent en charge n'importe quel serveur MCP, y compris (sans s'y limiter) les serveurs MCP distants que vous développez ou déployez sur Cloudflare. Cette fonctionnalité est disponible sous forme de mesures de contrôle de l'accès réseau Zero Trust (ZTNA, Zero Trust Network Access).

Protégez vos applications et vos workloads soutenus par IA grâce à la sécurité intégrée (in-line) et agnostique du point de vue des modèles proposée par Cloudflare.



Protégez vos outils IA en contact avec le public grâce aux solutions de sécurité des applications et au service Firewall for AI pour :

- **Identifier les points de terminaison de l'IA générative :** identifiez automatiquement tous les modèles IA et toutes les API soutenues par IA figurant sur vos propriétés web.
- **Protéger vos modèles d'IA contre les abus :** utilisez notre service spécifique Firewall for AI pour bloquer l'injection d'invites, l'empoisonnement de modèles, l'utilisation excessive et les autres menaces susceptibles de contourner les mesures de protection traditionnelles.
- **Contrôler le flux des informations d'identification personnelle :** analysez les invites des utilisateurs et les réponses du modèle pour empêcher l'exposition des données sensibles et vous aider à entretenir la conformité.
- **Mettre en place des garde-fous au niveau du contenu :** bloquez les invites dangereuses ou toxiques à l'aide de modèles intégrés, comme Llama Guard. Concevez des règles WAF personnalisées pour bloquer ou journaliser facilement les interactions suspectes avec l'IA.

Protégez les outils IA que vous développez grâce à la plateforme pour développeurs Cloudflare et au service AI Gateway

- **Une interface de contrôle de l'IA unifiée :** gérez l'ensemble de vos applications IA à l'aide d'un tableau de bord unique. Acheminez vos requêtes, mettez en cache vos réponses, maîtrisez les coûts et surveillez vos performances.
- **Protéger vos identifiants en périphérie :** stockez en toute sécurité vos clés API et vos secrets en périphérie du réseau afin de prévenir l'exposition côté client et de simplifier la rotation des clés entre les fournisseurs.
- **Appliquer des garde-fous quant à la sécurité du contenu :** identifiez et bloquez/expurgez automatiquement les contenus malveillants et les informations d'identification personnelle figurant au sein des invites et des réponses.

Cloudflare est le seul fournisseur qui sécurise à la fois vos environnements IA publics et privés

Mettez en place les mesures de protection adéquates pour adopter l'IA en toute confiance afin de vous assurer que votre sécurité accélère bien le processus d'innovation au lieu de le freiner.

- **Une protection unifiée de l'écosystème IA :** les complexités au niveau des piles de sécurité augmentent les risques. Faites appel à une plateforme unique pour protéger vos données et assurer votre conformité tout au long du cycle de vie de l'IA.
- **Une architecture mondiale et pérenne :** anticipez dès aujourd'hui les difficultés de demain grâce à un réseau à sécurité post-quantique capable d'évoluer pour accueillir tous les volumes de trafic et de s'adapter en permanence aux nouvelles menaces, tout en restant programmable pour de nouveaux scénarios d'utilisation.
- **Une sécurité renforcée par IA :** nos mesures de protection soutenues par IA inspectent les invites et les réponses afin de détecter les menaces en temps réel.
- **Un leadership éprouvé en matière d'IA :** innovez en toute confiance sur une plateforme approuvée par 80 % des 50 principales entreprises du secteur de l'IA générative.
- **Un déploiement agnostique du point de vue 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 en matière de déploiements d'IA.

Ce que nos clients en disent

indeed

Premier site web consacré à l'emploi du monde
Lire l'étude de cas

Identifier et contrôler l'IA fantôme

en parallèle d'un projet de remplacement du VPN

APPLIED

Technologies d'assurance
Lire l'étude de cas

Isoler les outils d'IA générative publics type ChatGPT

afin d'empêcher le copier-coller de données sensibles

Une entreprise SaaS soutenue par IA

Protéger les informations d'identification personnelle

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

Cyndx

Technologies financières soutenues par IA

Réduction de 95 % des coûts d'inférence

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

Vous vous sentez prêts à discuter de vos besoins en matière de sécurité de l'IA ?

Contacter un expert

1. Recherche ManageEngine 2025 : source
2. IBM, Cost of a Data Breach Report 2025 (Rapport IBM sur le coût d'une violation de données en 2025) : source

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