CLOUDFLARE

APERÇU DE LA SOLUTION

Sécuriser l'utilisation de l'IA générative et agentique par les employés

Donnez à vos équipes les moyens d'utiliser n'importe quel outil d'IA en toute sécurité grâce aux mesures de protection mises en œuvre par la plateforme SASE de Cloudflare.

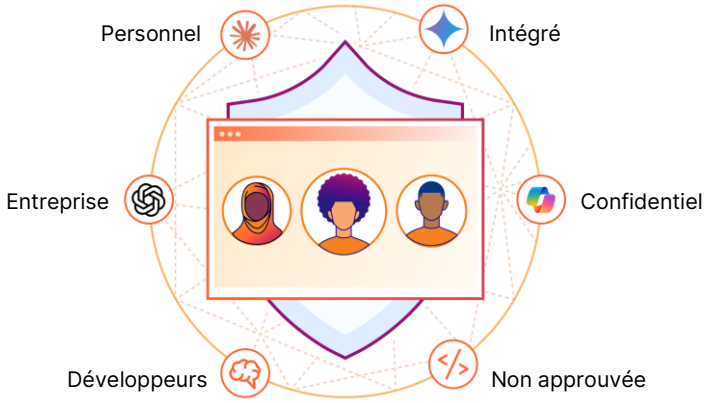
Reprenez le contrôle, gagnez en productivité

L'adoption de l'IA dans la précipitation donne lieu à une accumulation de risques, notamment des fuites de données, des violations réglementaires et l'élargissement de la surface d'attaque. L'interdiction de l'IA par principe se fera au détriment de votre avantage concurrentiel, et si vous en faites l'expérience avec des solutions dédiées vous ne ferez qu'ajouter de la complexité.

Cloudflare protège votre organisation dans son utilisation de l'IA par l'amélioration de la visibilité, l'atténuation des risques et la protection des données de manière holistique dans tous les environnements d'IA :

- **Découvrez l'IA fantôme** et gérez les politiques pour tous les outils d'IA autorisés et non autorisés.
- **Renforcez la gouvernance de l'IA** grâce à des contrôles d'accès basés sur l'identité et à la gestion du niveau de sécurité.
- **Empêchez les pertes de données** en bloquant les informations sensibles dans les invites utilisateur, en appliquant des garde-fous thématiques et en recherchant les erreurs de configuration dans les outils d'IA.

Déployez plus largement Cloudflare pour adopter l'IA en toute sécurité, qu'il s'agisse d'en limiter l'utilisation à des applications spécifiques ou d'en faire l'expérience avec un éventail plus large d'outils.



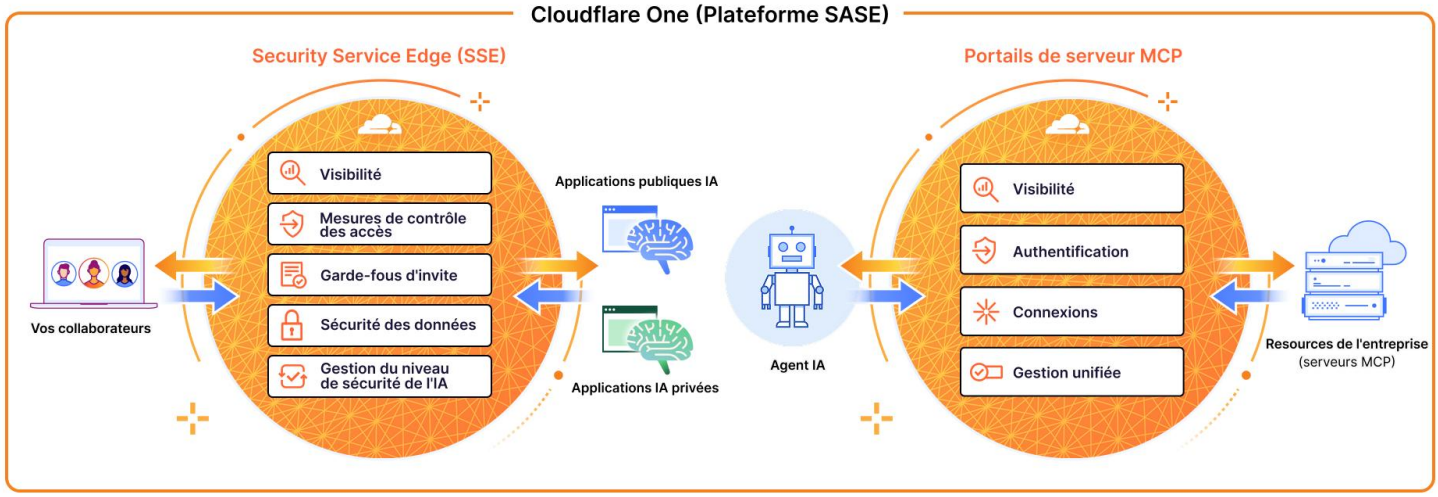
Pourquoi choisir SASE pour sécuriser l'utilisation de l'IA par les employés ?

La plateforme SASE (Service d'accès sécurisé en périphérie) de Cloudflare est placée entre vos équipes et les outils d'IA. Le modèle SASE constitue donc un point de départ idéal pour de nombreuses personnes souhaitant commencer à utiliser l'IA en toute sécurité.

Que les employés discutent avec ChatGPT ou que les agents d'IA collectent des informations sur les ressources de l'entreprise, la plateforme SASE de Cloudflare applique des contrôles de sécurité systématiques.

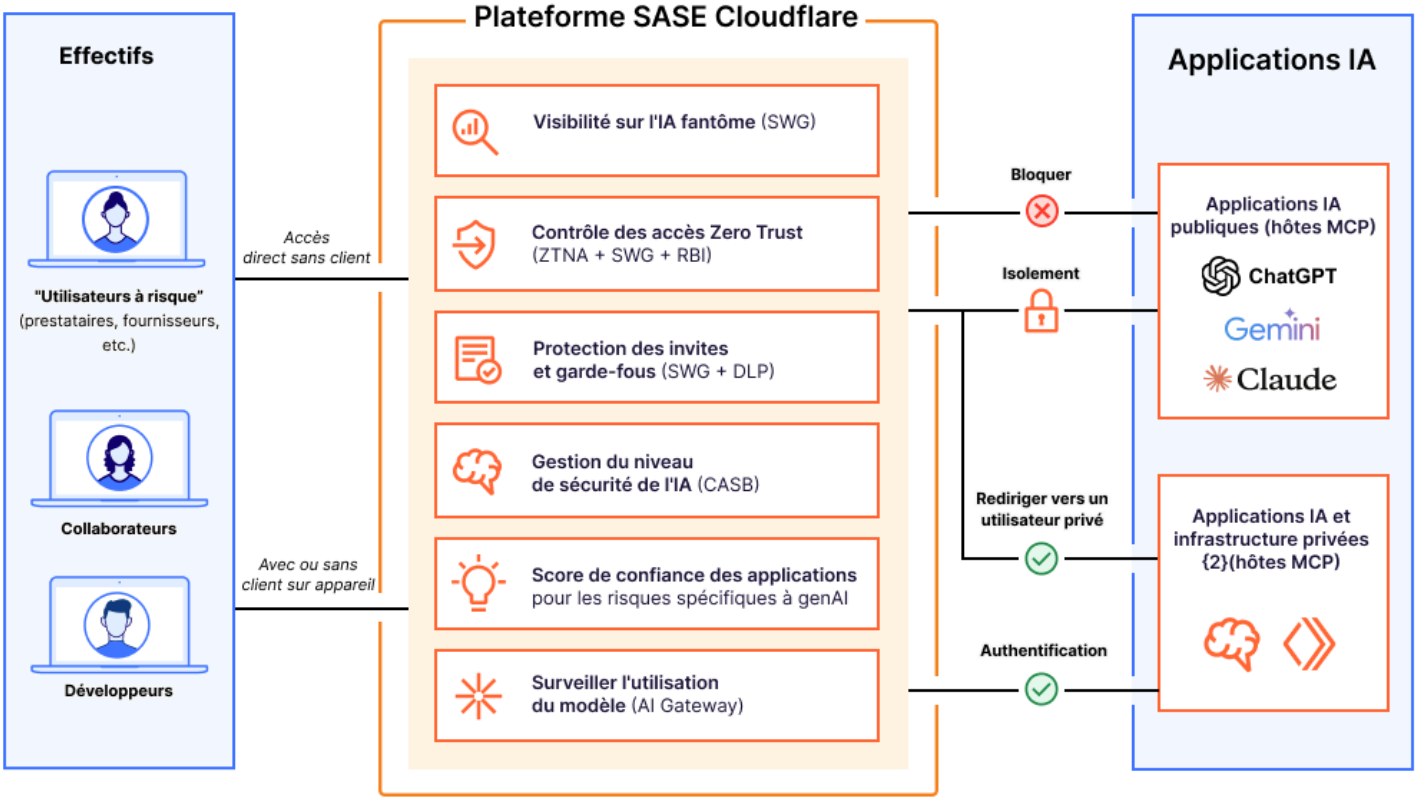
Sécuriser la communication de l'IA générative et agentique

La plateforme SASE de Cloudflare fournit un tableau de bord et un plan de contrôle unifiés pour gérer les interactions homme-IA et machine-machine au sein de votre organisation.



Contrairement aux autres fournisseurs SASE, Cloudflare aide également à connecter et à protéger les applications et les charges de travail basées sur l'IA et accessibles au public (comme le chatbot IA ou les moteurs de recommandation de votre site web).

Protégez les communications des utilisateurs avec les applications d'IA générative avec les contrôles d'utilisation de l'IA sur la plateforme SASE de Cloudflare



- **Visibilité :** découvrez et analysez l'utilisation de l'IA fantôme grâce à l'inspection du trafic en ligne. Évaluez les risques qui accompagnent ces applications d'IA grâce à une notation transparente.
- **Contrôles d'accès :** bloquez, isolez, redirigez ou autorisez les connexions utilisateur. Appliquez des règles Zero Trust basées sur l'identité par application.
- **Protection des invites et garde-fous :** détectez et bloquez les invites des utilisateurs en fonction de l'intention (par exemple, tentatives de piratage, abus de code, demandes d'informations d'identification personnelle).
- **Sécurité des données :** empêchez l'exposition des données sensibles grâce aux détections de la prévention des pertes de données (DLP) basées sur l'IA pour les informations d'identification personnelle, le code source, et plus encore.
- **Gestion du niveau de sécurité de l'IA :** intégrez les outils GenAI via API (disponible dès maintenant pour ChatGPT, Claude, Google Gemini) pour rechercher les erreurs de configuration à l'aide de notre Cloud Access Security Broker (CASB).

Résultats pour les clients

indeed

Premier site web consacré à l'emploi du monde

Identifier et contrôler l'IA cachée

en parallèle du projet de remplacement des VPN

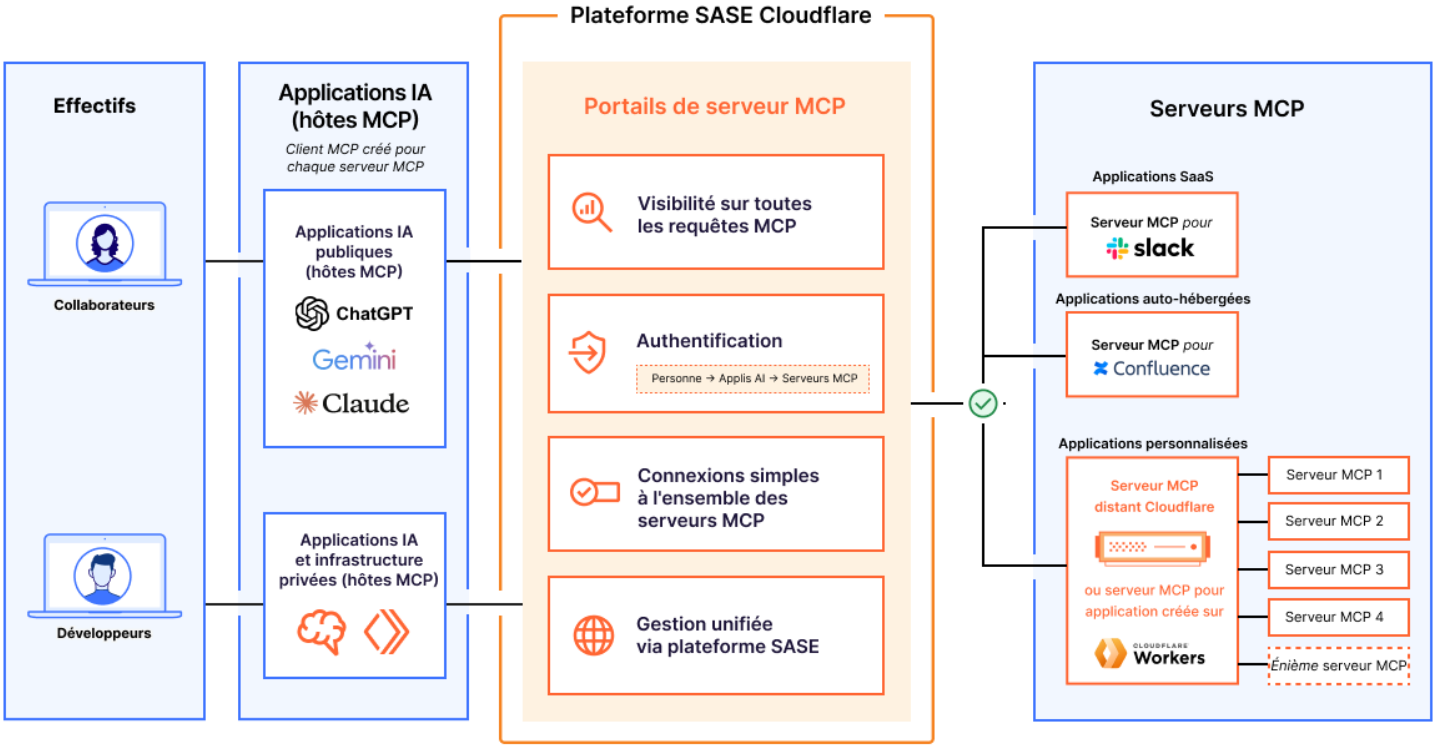
APPLIED

Technologies d'assurance

Isolez les outils d'IA générative publics, comme ChatGPT,

afin de bloquer le copier-coller de données sensibles

Sécuriser la communication IA agentique (IA-vers-ressource)
avec les portails de serveur MCP sur la plateforme SASE de Cloudflare



- **Visibilité :** regroupez tous les journaux de requêtes MCP pour l'audit et l'analyse. Vérifiez et approuvez chaque serveur MCP avant de l'ajouter au portail.
- **Authentification :** authentifiez l'accès des utilisateurs au portail en fonction de l'identité. Limitez l'accès aux serveurs MCP selon le principe du moindre privilège.
- **Connexions :** connectez tous les serveurs MCP accessibles avec une seule URL, au lieu de configurer chaque serveur MCP individuellement.
- **Gestion unifiée :** appliquez les mêmes politiques d'accès strictes pour les connexions IA que pour les utilisateurs humains.
- **Personnaliser les outils par portail** : choisissez les outils spécifiques et les modèles d'invite mis à la disposition de chaque utilisateur.

Remarque : les portails de serveur MCP de Cloudflare prennent en charge n'importe quel serveur MCP, y compris (mais sans s'y limiter) tout serveur MCP distant construit ou déployé sur Cloudflare. Cette fonctionnalité est disponible en tant que contrôle d'accès réseau Zero Trust (ZTNA).

Apprenez-en davantage sur notre vision dans ce blog.

Prêt à découvrir comment Cloudflare peut sécuriser votre utilisation de l'IA ?

Demander un atelier