CLOUDFLARE

PRÉSENTATION
DE SOLUTION

Protégez vos données sensibles

Une meilleure architecture réseau pour une protection des données plus efficace, plus productive et plus agile.

Une protection unifiée pour vos données, partout et sur tous les fronts

La protection des données n'est pas vraiment un nouvel impératif, mais le passage aux architectures cloud hybrides et l'adoption rapide de l'IA entraînent de nouvelles problématiques :

- **93 % des collaborateurs** reconnaissent avoir saisi des informations au sein d'outils IA qui n'avaient pas fait l'objet d'une autorisation préalable.[1]
- **79 % des pays du monde** disposent de dispositifs législatifs sur la confidentialité des données.[2]

Cloudflare applique des mesures de contrôle cohérentes tout au long du cycle de vie de vos données :

- **Sécurisez vos ressources partout et à tous les niveaux :** appliquez des mesures de contrôle cohérentes à l'ensemble de votre trafic (web, SaaS, e-mail et cloud).
- **Bloquez l'exfiltration par l'IA :** analysez les invites (prompts) saisies dans les outils d'IA générative afin d'empêcher les fuites de données sensibles et de régir l'utilisation de l'IA.
- **Maîtrisez les risques liés aux données :** identifiez et gérez l'informatique et l'IA clandestines (Shadow IT/AI), tout en analysant vos applications SaaS/cloud à l'aide de notre CASB.

« L'utilisation grandissante des outils IA non autorisés nous incite à reconsidérer notre approche de la sécurité. Nous sommes actuellement en train de nous intéresser au SASE. »
— *Head of Infosec,* ***AllSaints***

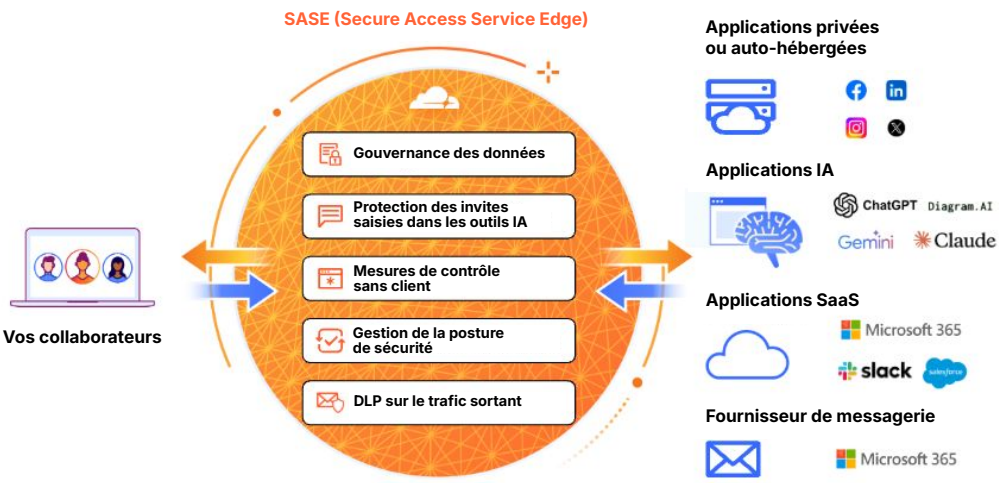
Pourquoi choisir le SASE plutôt qu'un service DLP pour entreprises ?

La plateforme SASE (Secure Access Service Edge, service d'accès sécurisé en périphérie) proposée par Cloudflare est conçue pour se placer entre vos équipes et l'ensemble de vos applications et de vos sources de données. Le modèle SASE constitue donc un point de départ idéal pour les nombreuses entreprises qui souhaitent commencer à assurer la sécurité de leurs données.

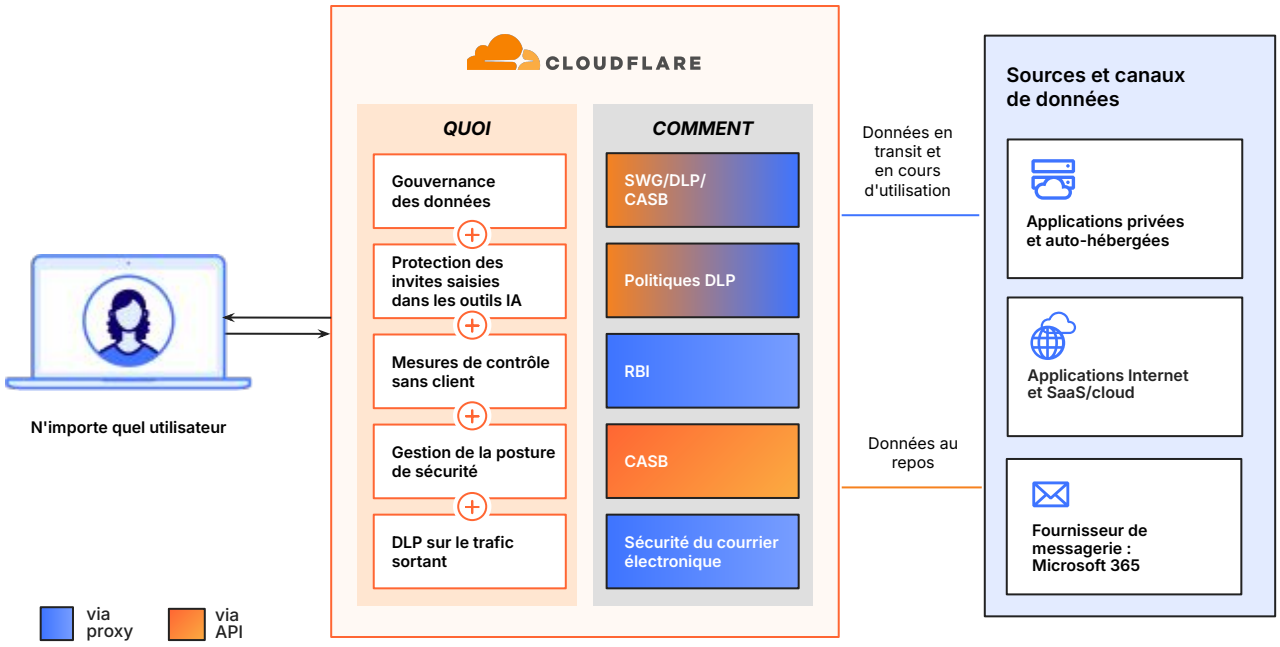
La plateforme SASE de Cloudflare applique des mesures de contrôle de la sécurité cohérentes à toutes les interactions avec vos données, que vos collaborateurs accèdent à des données au sein d'applications SaaS, téléchargent des fichiers sensibles ou discutent avec des outils d'IA générative.

Fonctionnement

La plateforme SASE de Cloudflare s'intègre (en mode in-line) entre vos collaborateurs et vos ressources afin d'unifier la visibilité sur vos données et les mesures de contrôle de ces dernières.



Une protection des données soutenue par IA et la plateforme SASE de Cloudflare
sur l'ensemble de vos canaux : web, SaaS, e-mail et cloud



Protection des données, en in-line et en temps réel

- **Service DLP granulaire :** empêchez l'exposition de vos données sensibles grâce à des mesures de détection contextuelles pour vos informations d'identification personnelle (PII), votre code source et vos données clients, parmi bien d'autres exemples.
- **DLP sur le trafic e-mail sortant :** signalez automatiquement les données sensibles contenues dans vos e-mails sortants afin d'éviter les fuites accidentelles de données.
- **Protection des invites :** détectez et bloquez les invites à risque saisies dans les outils IA et les réponses de ces derniers en fonction de l'intention (p. ex., tentatives de piratage, abus de code, demandes d'informations personnelles).

Accès sécurisé et mesures de contrôle des clients

- **Accès sécurisé aux applications :** appliquez des règles d'accès réseau Zero Trust, comme l'analyse DLP granulaire des connexions de l'IA agentique, à l'ensemble des applications de votre entreprise.
- **Niveau de sécurité des appareils :** contrôlez les accès à l'aide de mesures de contrôle granulaires de la posture de sécurité, comme le chiffrement du disque et l'activation de la DLP sur les points de terminaison.
- **Mesures de contrôle sans client :** appliquez des mesures de contrôle des données basées sur le navigateur afin de protéger les politiques régissant l'accès des tiers et les pratiques BYOD suivies par vos collaborateurs.

Risques liés à l'informatique clandestine et à la posture de sécurité

- **Identification de l'informatique et de l'IA clandestines :** identifiez et gérez le Shadow IT et le Shadow AI sur l'ensemble de votre environnement. Quantifiez les risques à l'aide de scores de confiance envers les applications et d'indicateurs sur les transferts de données afin d'atténuer rapidement l'exposition.
- **Gestion de la posture de sécurité :** analysez vos applications SaaS et vos environnements cloud à la recherche de risques envers la posture de sécurité. Prenez des mesures correctives pour corriger les lacunes détectées au sein de votre sécurité.
- **Contrôle des tenants :** bloquez les instances personnelles (tenants) d'applications SaaS afin d'empêcher l'exfiltration de vos données.

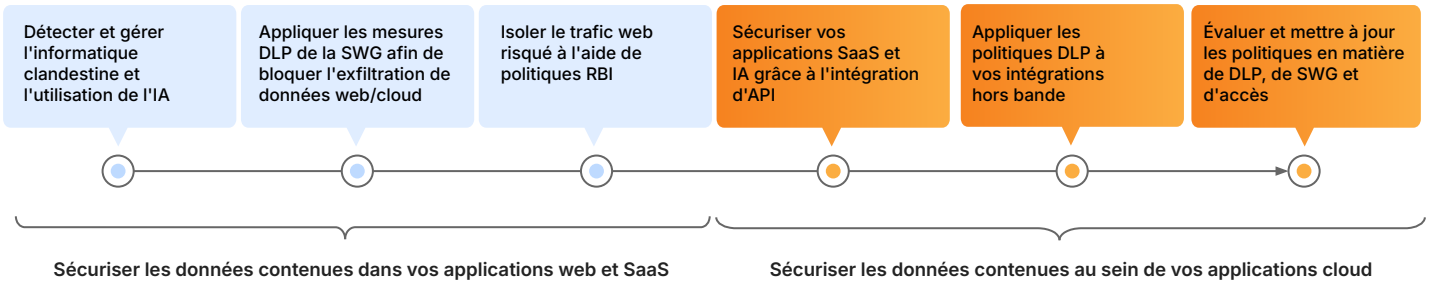
Intégrations et reporting

- **Intégrations CASB :** intégrez en toute fluidité les principales plateformes SaaS et IA (comme Microsoft 365, Google Workspace et ChatGPT) afin de mettre en place un processus d'analyse CASB basé sur API.
- **Intégration des MIP Microsoft :** synchronisez-vous en permanence avec les étiquettes Microsoft Information Protection (MIP, étiquettes Microsoft pour la protection des informations) afin de mettre en place des politiques DLP cohérentes.
- **Observabilité et analyses post-incident** : journalisez les données de manière sécurisée vers le SIEM de votre choix à des fins d'audit ou analysez instantanément les journaux par le biais du tableau de bord ou de l'API.

Exemple de parcours de protection des données

Commencez par identifier l'utilisation de l'informatique et de l'IA clandestines pour plus de visibilité sur votre surface d'attaque. Configurez des politiques DLP fondamentales sur notre passerelle SWG (Secure Web Gateway, passerelle web sécurisée) afin de bloquer les fuites de données à haut risque provenant d'applications cloud non gérées et déployez une solution d'isolement de navigateur à distance (RBI, Remote Browser Isolation) pour le trafic web non approuvé.

Vous pourrez ensuite déployer le CASB pour sécuriser vos applications SaaS et IA autorisées en corrigeant les erreurs de configuration et en appliquant des politiques de partage internes. Affinez et intégrez des politiques granulaires en matière de DLP et d'accès sur l'ensemble de vos solutions (SWG, courrier électronique et CASB) afin d'assurer une protection automatisée et unifiée sur l'ensemble des principaux vecteurs de données.



Exemples de scénarios d'utilisation pour bien démarrer

- **Bloquez l'exfiltration en temps réel des PII/PHI** sur l'ensemble des canaux de communication et de stockage non approuvés.
- **Protégez votre code source et votre propriété intellectuelle (PI)** contre le vol et la diffusion non autorisée par des éléments internes.
- **Appliquez des politiques de protection des invites** aux applications d'IA générative afin d'empêcher l'exposition de vos données sensibles et la contamination des modèles.
- **Prévenez les erreurs de configuration** et appliquez des mesures granulaires de contrôle des accès à l'ensemble de vos applications (SaaS et IA).

Résultats pour les clients

EESTI RAUDTEE

Fournisseur d'infrastructure
Lire l'étude de cas

Atténuer les pertes de données et les vulnérabilités du SaaS

en identifiant les fuites de données et les erreurs de configuration.

APPLIED

Technologies d'assurance
Lire l'étude de cas

Isoler les outils d'IA générative publics comme ChatGPT

afin d'empêcher le copier-coller de données sensibles.

Flo

Application phare consacrée à la santé
Lire l'étude de cas

Protéger les données des patientes

et assurer la conformité grâce à la sécurité du courrier électrique et au Zero Trust.

CREDIT SAISON INDIA

Organisme de prêt non bancaire
Lire l'étude de cas

Protéger les informations d'identification personnelle et assurez la conformité

afin d'empêcher les sorties de données indésirables.

Vous souhaitez parler de vos besoins en matière de protection des données ?

Demander un atelier

1. Recherche ManageEngine 2025 : source
2. Conférence des Nations unies sur le commerce et le développement 2025 : source

