CLOUDFLARE

PRÉSENTATION DE SOLUTION

Cloudflare One for Data Protection

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

Une protection unifiée pour les données, sur tous les fronts

Les risques envers la sécurité les plus modernes exigent une sécurité moderne, elle aussi

Le volume, la variété et la vélocité des données continuent de croître, de sorte que les entreprises font face à une escalade des risques posés par :

Les environnements cloud et SaaS tentaculaires
↳ dont les outils IA émergents et opaques, comme ChatGPT,
↳ qui conduisent à l'exposition du précieux code source.

La Cloudflare One Data Protection Suite est conçue pour rester à l'avant-garde de ces risques résolument modernes.

En unifiant les solutions dédiées sous une même plateforme et un même réseau, Cloudflare assure une protection des données :

- **Plus efficace**, en simplifiant la gestion de la connectivité et des politiques.
- **Plus productive**, en assurant une expérience utilisateur rapide, fiable et cohérente, sur tous les fronts.
- **Plus agile**, en innovant rapidement afin de répondre à l'évolution des exigences en matière de sécurité.

Une solution SSE (Security Services Edge) conçue pour protéger les données sur l'ensemble des environnements applicatifs (web, SaaS et privés)

Adoptez progressivement Cloudflare au sein de votre parcours SSE afin de :

1. Sécuriser l'accès aux données grâce au Zero Trust.
2. Bloquer les menaces, comme le phishing et les rançongiciels.
3. Détecter et verrouiller vos informations les plus sensibles.

Échappez à l'escalade des risques envers les données...

Une empreinte SaaS étendue

82 %

des violations impliquaient des données stockées au sein d'environnements cloud.[1]

Et bien entendu, les coûts des violations de données continuent de s'accroître, avec une augmentation de 15 % au cours des trois dernières années. [1]

Une diversité de nouvelles réglementations

71 %

des pays du monde disposent d'une législation permettant de garantir la protection des données et de la confidentialité.[2]

Aux États-Unis, **11 États** disposent désormais de lois complètes sur la protection des données, alors qu'ils n'étaient que 3 en 2021.[3]

La transformation numérique

89 %

des RSSI déclarent qu'aller trop vite sur les initiatives de transformation numériques introduit des risques imprévus concernant la sécurisation des données de l'entreprise.[4]

Scénario d'utilisation 1 : sécuriser le code développeurs

Problème
Le code peut être exposé ou ciblé à des fins de vol sur de nombreux outils pour développeurs, y compris dans des emplacements situés à la vue de tous, comme les référentiels publics.

Solution
Identifiez et corrigez les référentiels publics (comme GitHub) mal configurés et confrontés au risque de fuites de code. Détectez le code source dans les téléchargements/importations et appliquez-lui des mesures de contrôle.

→ GitHub
→ GitLab
→ Bitbucket

Scénario d'utilisation 2 : visibilité sur l'exposition des données et gestion des risques

→ OpenAI
→ Bard
→ GitHub Copilot

Problème
Les données couvrent divers environnements SaaS et cloud, l'informatique fantôme (Shadow IT) non autorisée et les outils IA émergents (comme ChatGPT), qui multiplient les risques de fuites.

Solution
Analysez les suites SaaS à la recherche d'erreurs de configuration et de données sensibles à l'aide de mesures de détection DLP intégrées. Bénéficiez d'une visibilité sur l'utilisation non autorisée des applications, avant d'autoriser, de bloquer, d'isoler ou d'appliquer des contrôles Zero Trust concernant l'accès à ces dernières.

Scénario d'utilisation 3 : conformité aux règlements

Problème
Des exigences juridiques plus strictes et plus extensives conçues pour contraindre les entreprises à préserver la sécurité et la confidentialité des données, avec des amendes de plus en plus lourdes en cas de non-conformité.

Solution
Identifiez et appliquez des mesures de contrôle aux classes de données régulées (PII, informations médicales, données financières). Entretenez des pistes d'audit détaillées par l'intermédiaire de journaux et d'analyses SIEM supplémentaires. Réduisez votre surface d'attaque à l'aide d'une stratégie de sécurité Zero Trust exhaustive.

✓ RGPD ✓ DPDP
✓ CCPA ✓ CPRA
✓ GLBA ✓ PCI DSS
✓ HIPAA ✓ ISO
✓ Et bien d'autres !

Fonctionnement

Une plateforme unifiée

Cloudflare fait converger la visibilité et les mesures de contrôle de ses solutions de DLP, de CASB, de ZTNA, de SWG, de RBI et de sécurité du courrier électronique vers une seule plateforme afin de simplifier la gestion.

Un réseau programmable

Un plan de contrôle disposant de services intégrés sur notre propre plateforme pour développeurs afin d'appliquer des mesures de contrôle aux données en transit, en cours d'utilisation et au repos sur l'ensemble des points d'application (environnements applicatifs web, SaaS ou privés).

Exemples de mesures de contrôle avec services composables

Appliquez la DLP aux données en transit et sécurisez l'accès

- Recherchez des données sensibles dans le trafic et les fichiers, puis configurez des politiques de blocage à l'aide de la DLP.
- Identifiez et gérez l'informatique fantôme (Shadow IT) grâce au CASB.
- Sécurisez l'accès aux données dans les applications grâce au ZTNA.
- Bloquez les instances personnelles d'applications SaaS afin d'empêcher l'exfiltration de données.

Isolez les applications pour sécuriser les données utilisées

- Bloquez les fonctions de copier/coller, téléchargement/importations, d'impression et de saisie clavier, le tous sans client sur appareil.
- Le déploiement sans client est idéal pour les appareils non gérés, les utilisateurs tiers et les outils IA, tels que ChatGPT.
- Appliquez des politiques DLP au sein des applications isolées.

Protégez les données au repos dans les applications SaaS

- Analysez les applications SaaS à la recherche d'activités suspectes, d'erreurs de configuration et de données sensibles.
- Prenez des mesures correctives pour réduire les risques à l'aide de politiques SWG.

Intégrez afin de rationaliser la conformité et les contrôles

- Transférez les journaux vers votre SIEM préféré à des fins de corrélation et d'audit.
- Intégrez-vous à 18 des suites SaaS les plus populaires afin de procéder à des analyses CASB basées sur API.
- Synchronisez-vous en permanence avec les étiquettes Microsoft Information Protection (MIP) dans le cadre de vos politiques DLP.

Une meilleure protection des données grâce à Cloudflare

Plus d'efficacité *grâce à la réduction de la complexité*

Simplifiez la connectivité à l'aide de nombreuses options flexibles afin d'envoyer du trafic vers Cloudflare à des fins d'exécution de nos solutions.

Utilisez des analyses basées sur API pour les suites SaaS ou des modes sans clients pour le ZTNA et le RBI afin de sécuriser l'accès aux applications. Pour placer du trafic en proxy de transfert, utilisez un client sur appareil ou des accès directs (on-ramps) sur réseau étendu pour l'ensemble de vos services de sécurité.

Plus de productivité *grâce à l'amélioration de l'expérience utilisateur*

Notre réseau se situe partout dans le monde, afin de vous assurer que les mesures de contrôle sont appliquées selon le principe de l'inspection en une seule passe, à proximité des utilisateurs finaux et des données, peu importe leur position géographique.

Une expérience fiable et non intrusive pour l'utilisateur final implique que l'application des mesures de contrôle des données ne perturbe jamais les flux de travail. Notre solution a été prouvée plus rapide que celles de nos concurrents dans le secteur du SSE.

Plus d'agilité *en innovant avec rapidité*

Notre architecture réseau programmable nous permet de développer rapidement de nouvelles fonctionnalités, afin que votre entreprise puisse s'adapter aux nouveaux risques avec agilité.

Nous adoptons rapidement les nouvelles normes et les nouveaux protocoles de sécurité (comme les connexions uniquement IPv6 ou le chiffrement HTTP/3) afin de vous assurer que votre solution de protection des données reste à jour.

Ce que nos clients en disent

« À l'heure actuelle, Cloudflare One empêche nos utilisateurs de partager les données sensibles et le code avec les outils de type ChatGPT et Bard, afin de nous permettre de tirer avantage de l'IA en toute sécurité. Nous sommes impatients de découvrir les futures innovations de Cloudflare en matière de protection des données, notamment leur vision et leur roadmap concernant les services DLP et CASB. »

Tanner Randolph
Responsable de la sécurité des systèmes d'information (RSSI)

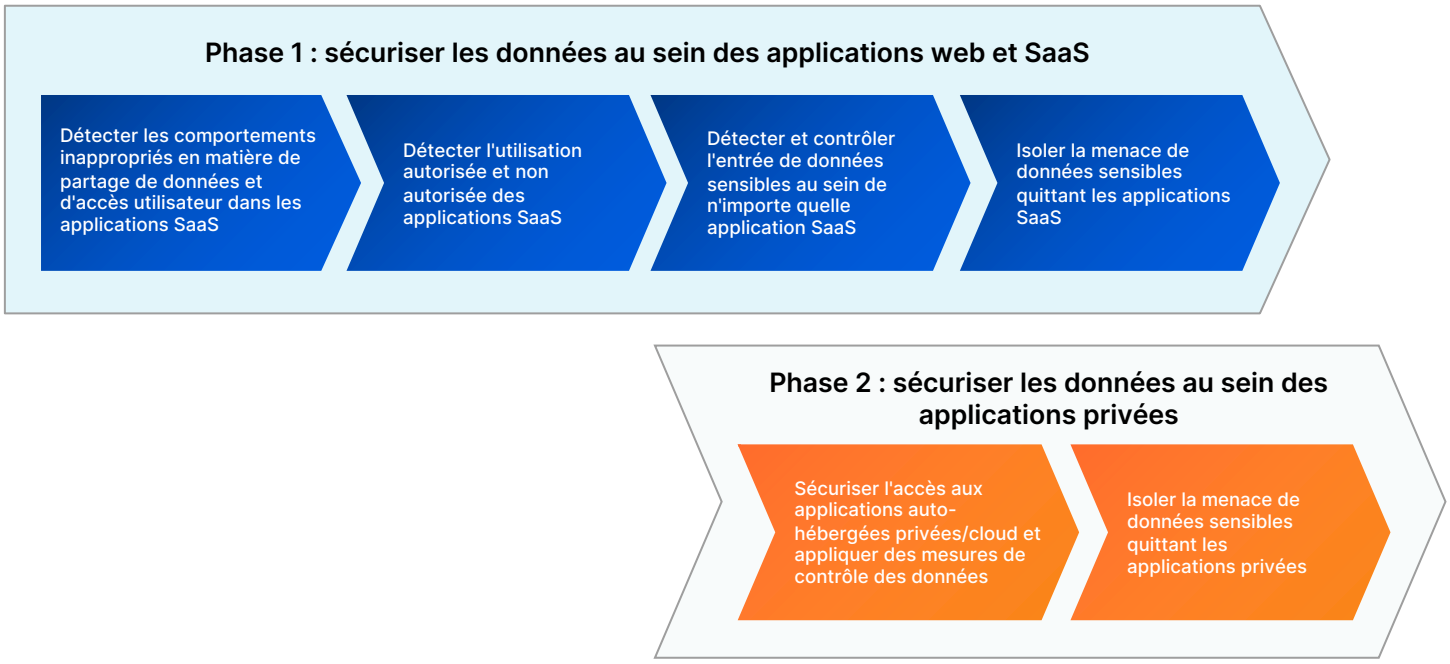
Applied Systems

Lire l'étude de cas

Autres scénarios d'utilisation

- **Une entreprise gazière classée au Fortune 500** cherchant à protéger l'accès aux données de ses sous-traitants.
- **Un important site d'offres d'emploi américain** cherchant à sécuriser son code et ses informations personnelles.
- **Une compagnie aérienne régionale américaine** cherchant à atténuer les risques d'exposition de ses données clients.
- **Une entreprise australienne spécialisée dans la santé** cherchant à protéger des informations médicales régulées.
- **Un fabricant d'appareils médicaux américain** cherchant à rationaliser sa conformité HIPAA

Parcours d'adoption courants



Premiers pas

DÉCOUVRIR...

l'escalade des risques envers les données dans cette infographie.

INTERAGIR...

avec la manière dont la plateforme fonctionne dans cette démo.

ÉPROUVER...

la valeur en demandant un atelier consultatif.

1. Rapport Cost of a Data Breach 2023, IBM
2. United Nations Conference on Trade & Development
3. International Association of Privacy Professionals (IAPP)
4. Rapport « State of the CISO » 2023