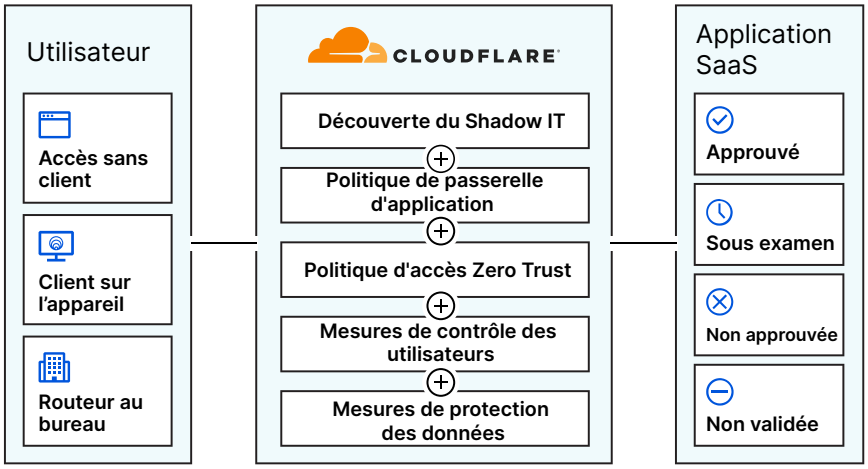
PRÉSENTATION DE SOLUTION

Contrôle et visibilité Zero Trust sur chaque application Saas

Les applications Saas confèrent à vos équipes les moyens nécessaires pour décupler leur productivité. Toutefois, la souplesse et la liberté qu'elles accordent à vos effectifs s'accompagnent de divers risques et difficultés en matière de sécurité, de visibilité et de contrôle des accès pour votre entreprise.

Cloudflare vous offre les outils dont vous avez besoin pour protéger vos données et vos collaborateurs, tout en permettant à ces derniers de continuer à utiliser les solutions qui les aideront à optimiser leurs tâches.



Découvrir et contrôler le Shadow IT

Si vous ne disposez pas d'une visibilité optimale sur les applications que vos collaborateurs utilisent, vous ne pouvez pas contrôler la manière dont les données sensibles sont stockées, partagées ou exposées à des tiers. Cloudflare vous aide à découvrir, catégoriser et contrôler toutes les applications (approuvées ou non) de votre entreprise, en journalisant chaque connexion et chaque requête dans un emplacement centralisé.

Appliquer une politique d'accès Zero Trust

Les applications SaaS sont hébergées en dehors du réseau de l'entreprise. Elles n'offrent à vos équipes de sécurité qu'un contrôle limité sur la manière dont les utilisateurs accèdent aux applications et manipulent les flux de données (entrants et sortants) de ces dernières. Les mesures de sécurité Zero Trust de Cloudflare sont disposées en plusieurs couches en amont de vos applications Saas. Elles permettent ainsi d'authentifier les utilisateurs et d'empêcher les utilisateurs non autorisés ou les appareils à risque d'accéder à vos fichiers et à vos données.

Appliquer des mesures de protection des clients et des données

Si vos collaborateurs accèdent à une mauvaise instance de vos applications, ils risquent de partager et de stocker vos données au mauvais endroit. Cette situation peut entraîner de potentielles fuites de données, et notamment des risques pour la sécurité en général. Cloudflare vous assure un meilleur contrôle du partage et du stockage de données, qu'elles soient en transit sur notre réseau ou en cours d'utilisation au sein de notre navigateur distant. Vous pourrez désormais concevoir et déployer des politiques de navigation Zero Trust, afin de protéger les données présentes au sein de n'importe quelle entité SaaS. Ces politiques permettront également d'éviter que vos collaborateurs accèdent aux mauvaises applications ou à de mauvaises instances d'applications approuvées.

Découvrir et contrôler le Shadow IT

Évaluez les applications utilisées par vos collaborateurs

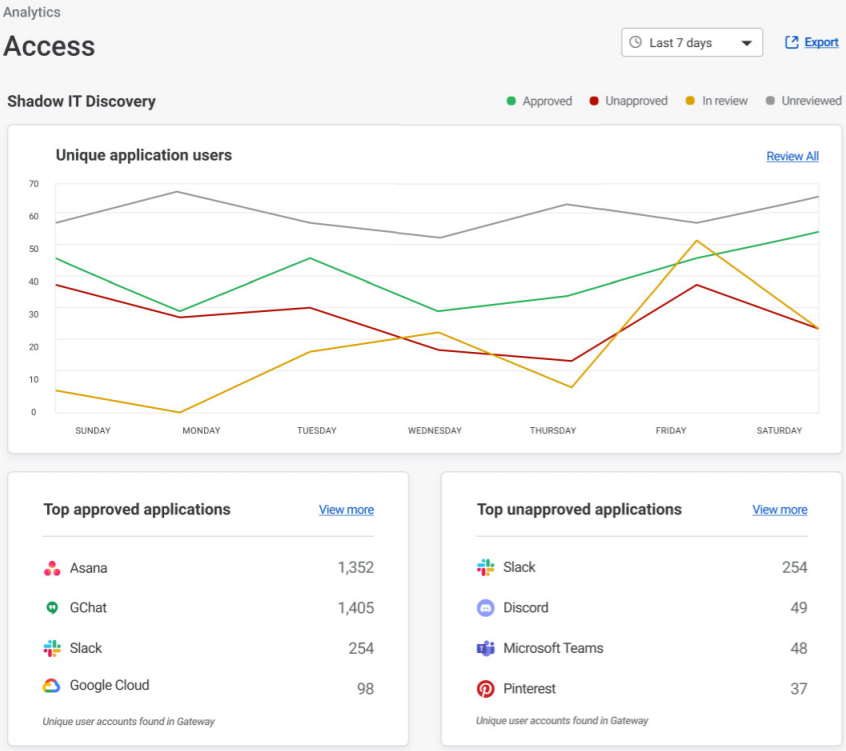
Si votre équipe informatique n'est pas en mesure de voir les applications utilisées par vos collaborateurs, elle ne pourra pas contrôler les flux de données au sein de ces applications. Cloudflare regroupe et répartit l'ensemble des requêtes HTTP sous différentes catégories dans notre journal d'activité, et ce par type d'application. Vous pouvez alors définir le statut et suivre l'utilisation des applications (approuvées ou non) au sein de votre entreprise.

Journalisez chaque connexion et chaque requête

Cloudflare contribue à atténuer les risques introduits au sein de votre entreprise lorsque vos collaborateurs accèdent à des applications non autorisées ou utilisent des appareils non gérés pour accéder à des informations sensibles. Chaque connexion et requête est ainsi journalisée dans un emplacement centralisé, afin de vous permettre de voir quelles applications sont en cours d'utilisation, ainsi que les actions effectuées au sein de ces dernières. Les administrateurs disposent également de la possibilité de bloquer ou d'autoriser les requêtes envoyées aux applications SaaS, afin d'éviter que les utilisateurs puissent contourner les contrôles de sécurité importants. Ces mesures permettent également d'empêcher les utilisateurs d'accéder de manière non autorisée aux applications, ressources et données de votre entreprise.

Fonctionnalités essentielles

- Gardez automatiquement une trace des applications déjà sécurisées par Cloudflare.
- Conservez les journaux jusqu'à 6 mois au sein du réseau Cloudflare.
- Transférez les journaux vers un ou plusieurs de vos services SIEM et emplacements de stockage de journaux dans le cloud.



Appliquer une politique d'accès Zero Trust à vos applications SaaS

Assurez un accès SaaS sécurisé grâce au proxy d'identité de Cloudflare

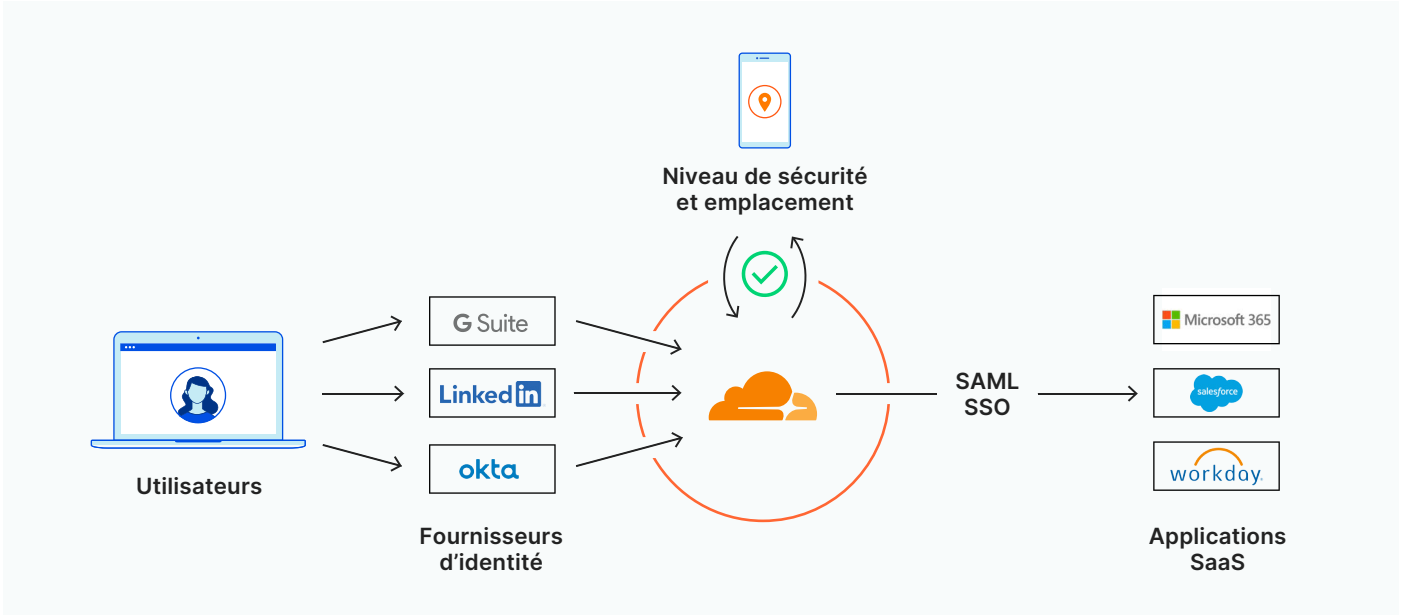
Les applications SaaS sont hébergées par des tiers et souvent gérées par des entités commerciales. Votre équipe informatique n'a donc pas souvent son mot à dire concernant la manière dont les utilisateurs accèdent à ces applications. Cloudflare s'insère entre le fournisseur d'identité et vos applications Saas, afin de vous permettre de développer et d'appliquer des règles Zero Trust adaptées au contexte et aux identités dans le cadre du processus de connexion. Le tout sans interruption de l'expérience utilisateur.

Déterminez les autorisations d'accès aux applications dont bénéficient les appareils des utilisateurs

Votre service informatique doit pouvoir exercer un contrôle précis sur la manière dont les appareils gérés par l'entreprise se connectent aux applications SaaS. Cloudflare intègre des règles Zero Trust au sein d'une procédure d'authentification unique, pour toutes les applications prenant en charge le SAML. Les utilisateurs commencent par s'authentifier à l'aide de leur fournisseur d'identité, puis Cloudflare vérifie la requête par rapport au niveau de sécurité et à la position géographique de l'appareil, avant d'autoriser l'accès à une application SaaS. La gestion des sessions reste souple, de manière à permettre la vérification en continu. Les administrateurs sécurité peuvent également créer des politiques spécifiques aux appareils, afin que les utilisateurs ne puissent accéder aux applications qu'à l'aide d'appareils conformes aux exigences de sécurité pré-établies, comme les certificats mTLS.

Fonctionnalités essentielles

- Intégrez plusieurs fournisseurs d'identité ou plusieurs instances du même fournisseur.
- Vérifiez l'identité des utilisateurs à l'aide de règles définies par application (la MFA exige une clé physique, par exemple).
- Vérifiez le niveau de sécurité des appareils en fonction de règles définies par application (application de politiques SWG, installation d'une protection EPP, activation d'un certificat mTLS ou du chiffrement du disque, par exemple) et de la position géographique.
- Le portail de lancement d'applications de Cloudflare permet aux utilisateurs de voir et d'accéder à toutes les applications Saas approuvées.



Appliquer des mesures de protection des clients et des données à n'importe quelle application SaaS

Limitez l'accès aux instances d'applications extérieures à l'entreprise

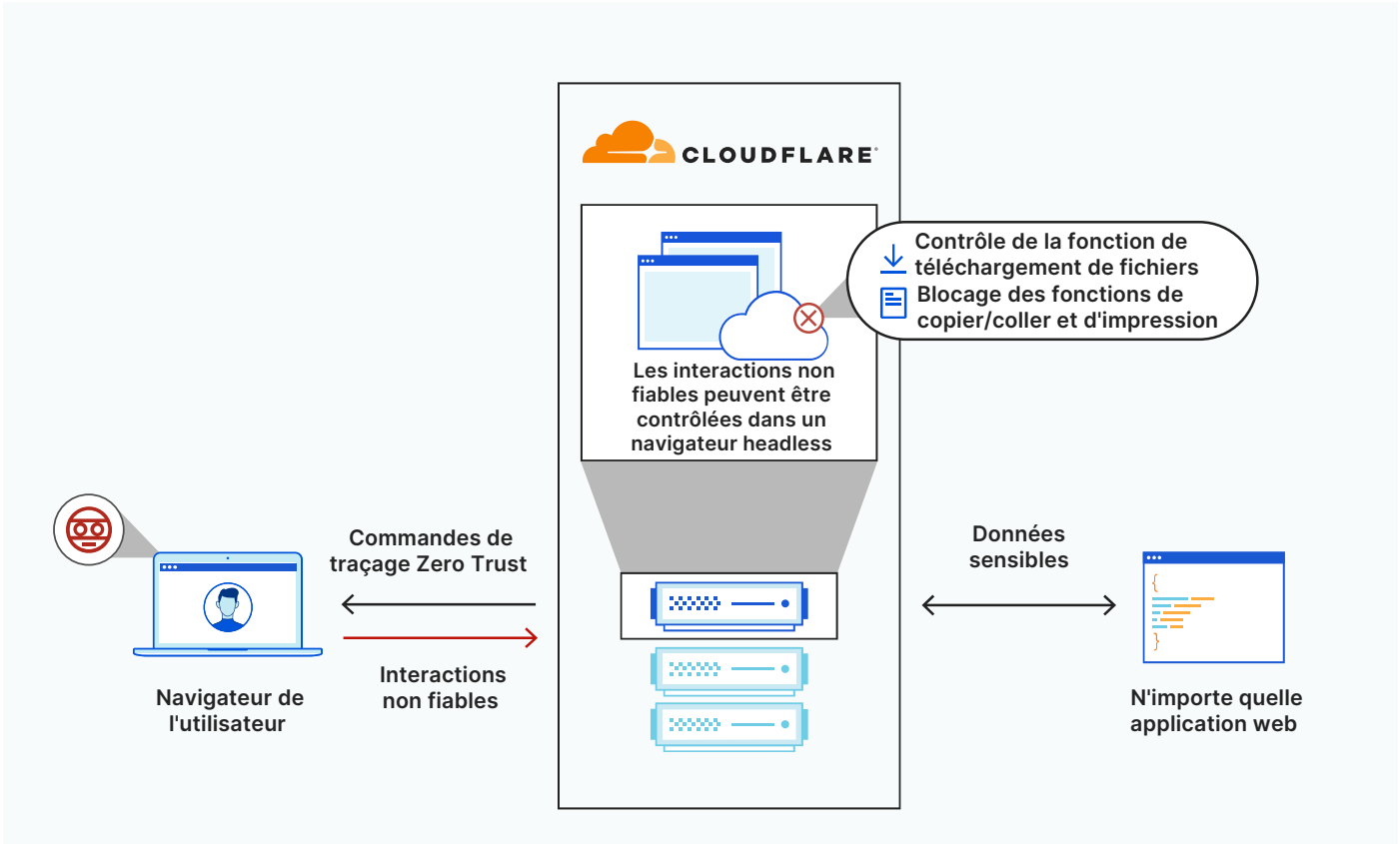
Cloudflare permet d'assurer un contrôle des clients à l'aide de politiques de passerelle HTTP. Ces dernières peuvent être configurées de manière à empêcher l'accès aux versions grand public des applications. Au lieu d'appliquer ces politiques à l'aide de serveurs proxy sur site, par l'intermédiaire de VPN d'entreprise, Cloudflare filtre et examine le trafic et les requêtes à l'aide de son vaste réseau mondial de datacenters. Vos utilisateurs ne connaissent ainsi jamais de problèmes de latence ou de dégradation des performances.

Empêchez les données d'entreprise de quitter vos clients

Cloudflare facilite la création et le déploiement de politiques de navigation Zero Trust permettant de contrôler et de protéger les données qui résident au sein de vos applications web. Le code de l'application s'exécute dans son intégralité au sein d'un navigateur headless sécurisé et distant sur notre vaste réseau mondial, pas au sein d'appareils constituant des points de terminaison. En conséquence, les données sensibles sont protégées contre les appareils compromis ou non fiables, ainsi que contre les menaces zero-day. Les administrateurs gardent en outre le contrôle sur la manière dont les utilisateurs accèdent aux données et les partagent, afin de vous permettre de minimiser le risque de perte accidentelle, voire de violation plus substantielle des données.

Fonctionnalités essentielles

- Autorisez ou bloquez certains comportements du navigateur en fonction de différents critères, comme l'application, le type d'application, le nom d'hôte, l'identité de l'utilisateur et le risque envers la sécurité.
- Contrôlez les actions des utilisateurs au sein du navigateur, comme l'utilisation des fonctions de téléchargement, d'importation, de copier/coller, de saisie et d'impression.



La différence Cloudflare

L'étendue de notre plate-forme

Cloudflare place les mesures de contrôle de l'accès Zero Trust (ZTNA), de la passerelle (SWG) et du navigateur (RBI) en amont de vos applications Saas. Votre équipe informatique n'a ainsi nullement besoin de configurer ou d'exécuter un produit CASB dédié.

Une solution 100 % maison

Les capacités CASB de Cloudflare fonctionnent en parfaite harmonie avec nos services ZTNA, SWG et RBI, dans la mesure où toutes ces solutions sont intégralement développées par nos soins. Vous n'aurez donc plus besoin de jongler avec plusieurs produits distincts pour protéger vos applications et vos équipes.

Une interface de contrôle unique

Cloudflare permet aux entreprises de définir des politiques et de gérer l'accès aux applications (de même que leur utilisation) à l'aide d'un tableau de bord unique. Vous pouvez ainsi surveiller toutes les requêtes et les autorisations d'un seul coup d'œil.

Cloudflare aide vos équipes à surveiller, protéger et contrôler vos applications Saas à l'aide d'une suite de fonctionnalités de sécurité Zero Trust intégrée nativement.

En savoir plus