CLOUDFLARE

PRÉSENTATION DE SOLUTION

Cloudflare Browser Isolation Le modèle Zero Trust intégré pour l'Internet

Étendre le Zero Trust à l'Internet

Vaste surface d'attaque, contrôles limités

De nos jours, le navigateur web est l'application d'entreprise la plus utilisée ; ce qui représente une surface d'attaque très vaste.

Cependant, la protection des utilisateurs des menaces provenant du web n'a jamais été satisfaisante. Et il n'a jamais été aussi difficile d'appliquer des contrôles pour protéger la manière dont les utilisateurs interagissent avec des données sensibles.

Parfaire le modèle Zero Trust

L'application du Zero Trust à l'activité de navigation implique qu'aucune opération (code ou interaction) ne doit être exécutée sur les appareils par défaut.

Le service d'isolation de navigateur Cloudflare Browser Isolation exécute l'ensemble du code à la périphérie de notre réseau. Il isole ainsi les utilisateurs du contenu web non fiable et protège les données lors des interactions du navigateur avec des utilisateurs et des appareils non fiables.

Un navigateur à distance pas comme les autres

- La compatibilité fonctionne avec toutes les pages web, sur tous les navigateurs.
- Les performances fournissent un flux à faible latence de la page web.

Sécurisez les données en cours d'utilisation qui proviennent d'utilisateurs ou d'appareils non fiables, et protégez les appareils et utilisateurs des attaques par rançongiciel ou hameçonnage, même celles de type zero-day.

Essayez dès maintenant, aucune procédure d'installation nécessaire

Une sécurité intégrée, pas ajoutée a posteriori

Conçue sur Cloudflare

Notre service a été intégralement développé par nos soins en même temps que nos autres services Zero Trust et a été conçu pour s'exécuter sur l'intégralité de notre réseau, qui compte plus de 275 emplacements.

Les sessions de navigation web sont servies aussi près que possible des utilisateurs, afin d'assurer une expérience ultrarapide.

intégré de manière native

À la différence des autres fournisseurs, l'isolation de navigateur de Cloudflare est nativement intégrée à l'ensemble de nos services Zero Trust.

Utilisation d'une interface de gestion unique pour :

- Passerelle web sécurisée (SWG)
- Accès réseau Zero Trust (ZTNA)
- Agent de sécurité des accès au cloud (CASB)
- Sécurité des e-mails dans le cloud (En prévision)
- .....et plus encore

Réduisez la surface d'attaque
La navigation Zero Trust empêche le code malveillant présent sur les sites non classés, à risque ou même à faible risque d'infecter les appareils des utilisateurs.

Simplifiez le déploiement
Définissez des politiques de navigation Zero Trust depuis la même interface que celle dans laquelle vous gérez l'accès aux applications.

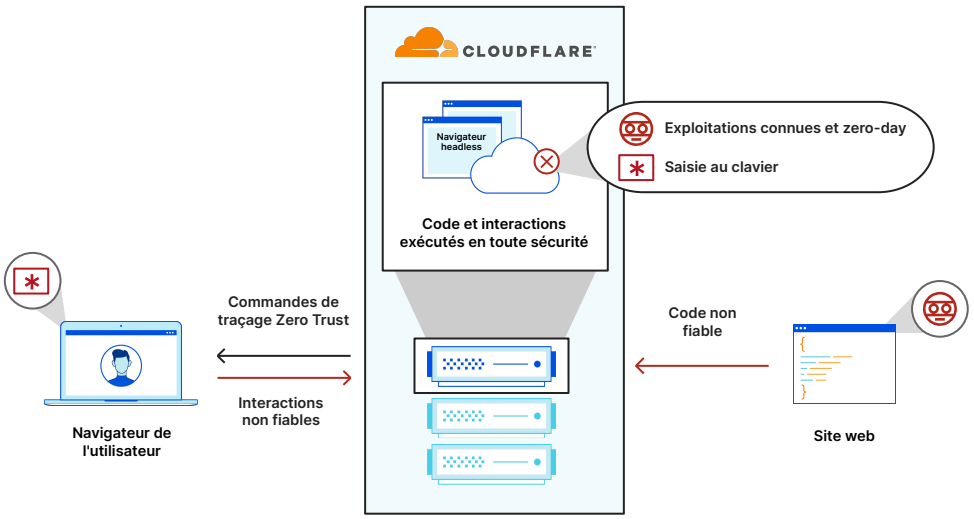
Protégez les données
Empêchez la perte de données et le hameçonnage en contrôlant les actions des utilisateurs (saisie clavier, copie, impression, transfert et téléchargement) dans les applications ou sur les sites à risque.

Réduisez votre surface d'attaque sans compromettre l'expérience utilisateur

Vérification :
Aucune équipe informatique ne peut continuellement appliquer des correctifs pour protéger tous les navigateurs contre les vulnérabilités connues. Qui plus est, soyons réalistes, les filtres et inspections ne pourront jamais détecter 100 % des menaces même avec les meilleures informations. Le blocage de tous les sites n'est pas non plus une bonne solution : un excès de restrictions risquerait d'être plus dommageable en raison de la perte de productivité induite pour l'utilisateur.

Solution :
Notre solution d'isolation du navigateur exécute une version headless de Chromium, qui rend l'ensemble du code du navigateur à la périphérie de notre réseau plutôt que sur vos points de terminaison, afin d'atténuer les menaces connues et inconnues, comme les logiciels malveillants. Cette expérience à faible latence est invisible pour les utilisateurs finaux et s'apparente à celle d'un navigateur local.

Fonctionnement



Déploiement *avec* un client sur l'appareil
Envoyez le trafic utilisateur des appareils vers le réseau global de Cloudflare pour une inspection et un filtrage complet des couches 4-7.

Déploiement sans client
Envoyez les utilisateurs vers un hyperlien isolé sans exposer leur adresse IP publique ou leur appareil à du code malveillant potentiellement présent sur le site.

Scénarios d'utilisation principaux

Rançongiciel

L'isolement protège efficacement contre les infections par des rançongiciels. Toutefois, même pour les sites non isolés, cette défense est renforcée par des intégrations natives à différents services, comme notre passerelle web sécurisée, pour bloquer les sites et les domaines à risque, ou notre accès réseau Zero Trust, pour réduire les mouvements latéraux des menaces.

Hameçonnage et sécurité des e-mails

L'isolation n'empêche pas uniquement le code malveillant contenu dans un lien d'hameçonnage de s'exécuter localement, mais empêche également la saisie d'informations sensibles au clavier. En outre, les administrateurs pourront bientôt activer le filtrage des e-mails en un seul clic, via la solution Area 1.

Attaques zero-day

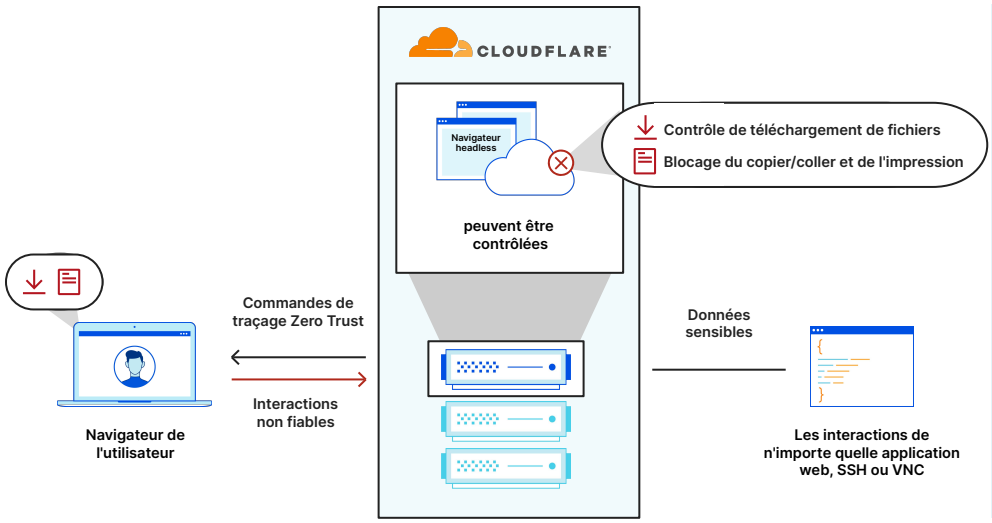
Lorsqu'un correctif est disponible pour combler une vulnérabilité zero-day, Cloudflare le déploie automatiquement sur l'ensemble des navigateurs distants situés sur notre réseau. Les administrateurs peuvent ainsi protéger les appareils, tout en évitant les interruptions de service. Ils n'ont plus besoin non plus d'interrompre les utilisateurs dans leurs tâches pour forcer les mises à jour.

Sécurisez les données utilisées au sein des navigateurs web

Vérification :
L'essor des logiciels SaaS ont fait du navigateur web le premier angle d'accès aux données pour les utilisateurs. Mais traditionnellement les administrateurs bénéficiaient de contrôles limités sur les données une fois qu'elles arrivent dans le navigateur. Généralement les utilisateurs peuvent copier, coller ou imprimer les données sensibles ou les données à caractère personnel dans d'autres sites Web, applications ou emplacements. Ces actions courantes augmentent le risque de violation de données.

Solution :
L'exécution d'un navigateur isolé redonne le contrôle aux administrateurs afin de leur permettre de protéger les données sensibles sur n'importe quel site web ou application SaaS. En tout juste quelques clics, les administrateurs peuvent définir des règles précises empêchant les actions risquées de la part des utilisateurs au sein du navigateur. Il peut ainsi s'agir de limiter les fonctions de téléchargement, mais aussi l'importation, le copier/coller, la saisie clavier et l'impression.

Fonctionnement



Déploiement *avec* un client sur l'appareil
Bénéficiez d'une visibilité totale et créez des politiques tenant compte du niveau de sécurité pour régir la manière dont les utilisateurs d'appareils gérés interagissent avec les données.

Déploiement sans client
Isolez les applications comportant des données sensibles (telles qu'un CRM) auxquelles les utilisateurs d'appareils non gérés sont le plus susceptibles d'accéder régulièrement.

Scénarios d'utilisation principaux

Accès sécurisé pour les fournisseurs

Isolez les connexions vers des hyperliens spécifiques, sans installer de logiciel sur les appareils des utilisateurs.

Appuyez-vous sur ce modèle sans client pour protéger les données avec lesquelles vos sous-traitants interagissent sur des appareils non gérés, le tout sans configuration supplémentaire.

Contrôlez les informations saisies sur les sites suspects

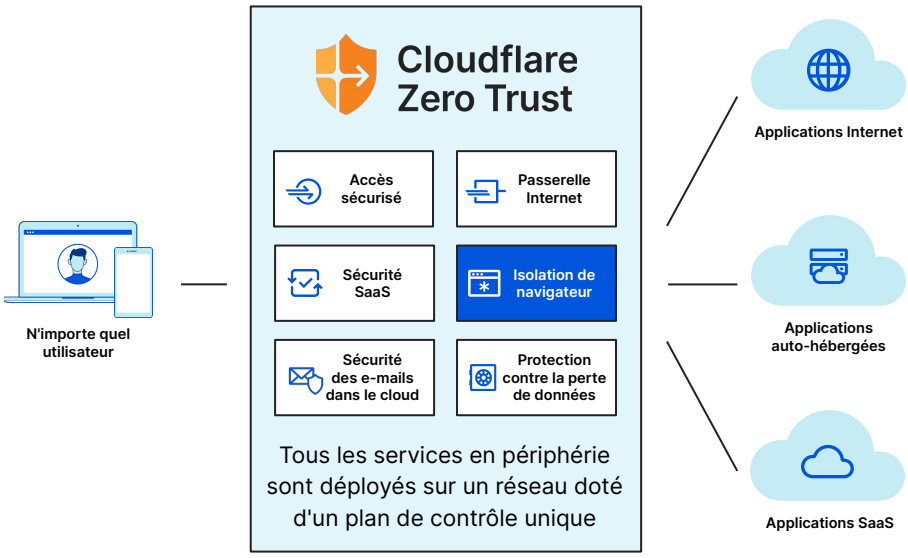
Les administrateurs peuvent protéger les équipes en isolant les sites web à haut risque, comme les sites de « typosquatting » et les « domaines » souvent utilisés pour le hameçonnage. Cloudflare diffuse le site en mode lecture seule et désactive les fonctions de transfert, de téléchargement et de saisie clavier.

Intégrez notre produit aux solutions tierces

Grâce à notre déploiement sans client, les administrateurs peuvent intégrer Cloudflare à des passerelles web ou e-mail existantes afin de profiter d'une transition plus graduelle lors de l'abandon de leurs anciens services. Envoyez les clics à haut risque vers notre navigateur distant et appliquez un blocage de page personnalisé ou d'autres formes de protection.

Isolation du navigateur : essentielle au Zero Trust

L'isolation est au cœur de l'architecture Zero Trust. Quelques clics dans la plateforme Zero Trust de Cloudflare suffisent pour étendre la visibilité et les contrôles au navigateur.



L'isolation désormais réalisable
Par le passé, l'isolation du navigateur n'était possible que dans le cadre de solutions autonomes dont seules les grandes entreprises pouvaient justifier l'achat étant donné le coût et la complexité.

Avec Cloudflare, les intégrations natives avec ZTNA, SWG et d'autres services SSE facilitent le lancement du processus de modernisation de la sécurité là où c'est pertinent, avant d'étendre plus largement le modèle Zero Trust avec l'isolation du navigateur.

Navigation locale ou à distance

Navigation locale
Le code des pages web non fiables et les sites d'hameçonnage s'exécutent localement sur l'appareil du point de terminaison. Les utilisateurs peuvent librement saisir des données sensibles sur des sites d'hameçonnage, et leurs appareils et leurs données sont directement exposés à des menaces non corrigées ou de type zero-day.

Navigation à distance
Du code ou des sites non filtrés peuvent être exécutés dans un navigateur distant, continuellement mis à jour. Les interactions de l'utilisateur sont contrôlées afin de bloquer les logiciels malveillants et les attaques par hameçonnage, et les attaques de type zero-day sont isolées de l'appareil de l'utilisateur final.

La méthode de Cloudflare

Network Vector Rendering (NVR)
Contrairement à la technique Pixel-Pushing, qui consomme une grande quantité de bande passante, ou à la technique Content-Disarm and Reconstruction, la technologie NVR transmet en continu des commandes de dessin sûres à l'appareil, sans transmettre de code de page web malveillant et sans affecter l'expérience de l'utilisateur final.

Notre réseau mondial
D'autres fournisseurs hébergent des navigateurs distants sur des fournisseurs de Cloud public. Cloudflare positionne les navigateurs plus près de vos utilisateurs, proposant ainsi une expérience qui ne diffère pas de la navigation locale, quel que soit l'endroit.

Fonctionnalités principales

- Exécution de l'ensemble du code du navigateur dans le cloud, loin des utilisateurs
- Pas de pixel-pushing
- Réseau ultra-rapide (à 50 ms de 95 % des utilisateurs d'Internet du monde entier)
- Compatibilité avec tous les navigateurs modernes
- Déploiement avec ou sans client sur appareil
- Empêchez les données de quitter les applications de l'entreprise et gagnez en visibilité sur le Shadow IT.
- Bloquez les attaques par rançongiciel et l'hameçonnage grâce aux informations issues de notre pare-feu réseau et de nos règles Zero Trust.
- SLA avec garantie de disponibilité de 100 %

Faites l'expérience dès aujourd'hui d'une navigation plus rapide et plus sécurisée

Essayez dès maintenant l'isolation du navigateur