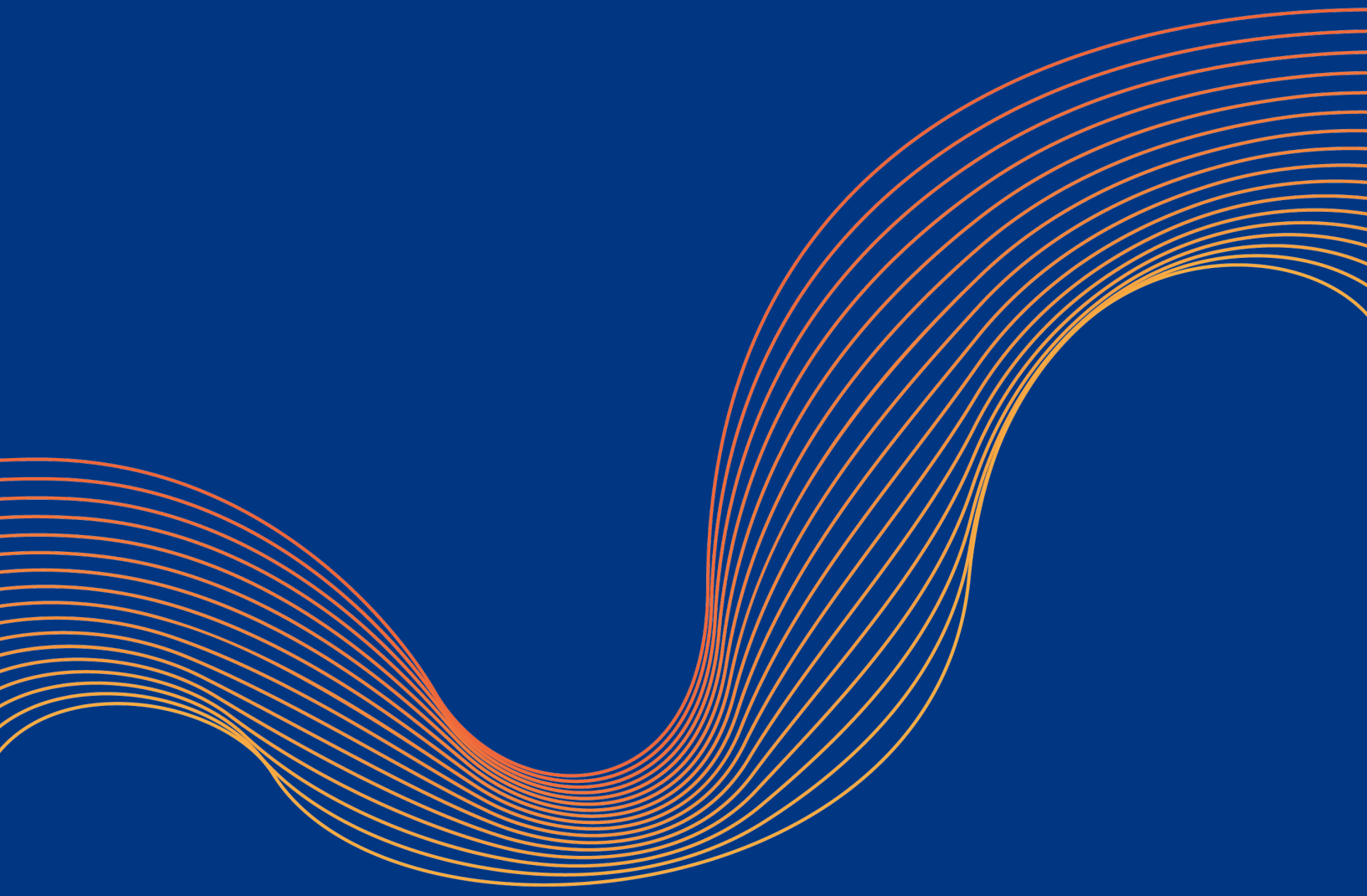
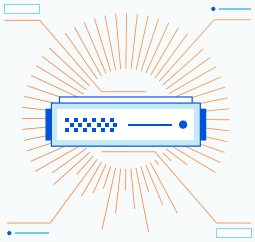
Les difficultés communes de l'isolation de navigateur, et comment les résoudre

L'intersection de la navigation sur Internet et de la sécurité Zero Trust



+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

INDEX



Introduction

Les équipes informatiques et de sécurité ont de bonnes raisons de ne pas faire confiance à l'Internet public. Un rapport de Verizon a déterminé que le phishing et les logiciels malveillants étaient à l'origine de 39 % de toutes les violations de données survenues en 2020, tandis qu'une étude de Forrester Consulting commandée par Cloudflare a révélé qu'en 2020, 61 % des entreprises de plus de 1000 employés ont constaté une augmentation des attaques par phishing par rapport aux années précédentes.

Tous les professionnels de l'informatique et de la sécurité veulent éviter que leur entreprise n'apparaisse dans ces statistiques. Plus précisément, ils cherchent à :

- **Bloquer les logiciels malveillants et le phishing**, qui adoptent continuellement de nouvelles tactiques afin d'échapper à la détection.
- **Empêcher les pertes de données en général**, qu'elles résultent d'appareils infectés ou d'interactions avec les utilisateurs.
- **Obtenir une meilleure visibilité de la navigation des employés sur Internet**, afin de comprendre l'environnement de menaces particulier auquel de leur entreprise et de réagir plus rapidement à d'éventuelles violations.

Ces scénarios d'utilisation sont des composantes importantes de la **sécurité Zero Trust**, selon laquelle les propriétés Internet et le code ne doivent pas bénéficier d'une confiance implicite et doivent donc être traités de manière sécurisée à chaque interaction avec l'utilisateur.

Pour atteindre ces objectifs, certaines organisations optent pour l'isolation de navigateur, dans laquelle la navigation du personnel sur Internet est séparée des réseaux et de l'infrastructure locaux. Mise en œuvre avec précision et efficacité, l'isolation de navigateur pourrait potentiellement devenir le moyen le plus efficace d'atténuer les attaques provenant d'Internet. Regrettablement, elle est jusqu'à présent restée une technologie de niche, en raison d'un certain de nombre de problématiques telles que **des coûts élevés, des expériences de navigation insatisfaisantes, des difficultés liées à la gestion logistique** et **des failles de sécurité.**

Ce document décrit ces difficultés dans le détail, afin d'aider les équipes informatiques et de sécurité à mieux comprendre leurs besoins en matière de sécurité de la navigation sur Internet. Il propose également une méthode permettant de résoudre ces difficultés et, pour conclure, explique comment Cloudflare a intégré cette méthode dans son réseau mondial.

Les difficultés des stratégies communes d'isolation de navigateur

Les logiciels malveillants, le phishing et les pertes de données affectent les organisations dans tous les secteurs et tous les domaines. L'isolation de navigateur est généralement déployée pour apporter une solution aux deux premiers types de menaces, afin de consolider les approches reposant sur les listes de blocage et la correspondance de fichiers et les approches comportementales utilisées par les passerelles web sécurisées.

Dans la pratique, toutefois, l'isolation de navigateur peine souvent à atteindre cet objectif.

Pourquoi cela ? Réfléchissez aux limites des méthodes d'isolation de navigateur les plus courantes :

Diffusion de captures d'écran de l'activité de navigation depuis le Cloud

Cette approche, parfois appelée « pixel-pushing », capture les événements dans le navigateur de l'utilisateur final et les transmet à un navigateur à distance hébergé dans le Cloud, qui exécute les actions de navigation et transmet une séquence d'images en pixels de la fenêtre du navigateur distant au navigateur de l'utilisateur final. Ainsi, tout code malveillant (qu'il ait été téléchargé automatiquement ou par l'action délibérée d'un utilisateur) est séparé de l'appareil de l'utilisateur final. Les sites de phishing potentiels, à l'image des pages contenant des champs de formulaire de saisie du nom d'utilisateur/mot de passe, peuvent être affichés en lecture seule ou avec l'ajout d'un message d'avertissement.

Cette approche permet d'isoler les terminaux des logiciels malveillants et du phishing. Cependant, elle comporte notamment les problèmes suivants :

Latence pour l'utilisateur final : lorsque l'isolation de navigateur à distance est hébergée dans le Cloud public (ou sur un réseau privé géographiquement restreint), les utilisateurs finaux peuvent constater de la latence lorsqu'ils sont physiquement éloignés des datacenters où est mise en œuvre d'isolation de navigateur. Ce phénomène empire lorsque le trafic des utilisateurs finaux transite par d'autres outils de sécurité, tels qu'une passerelle web sécurisée, qui ne sont pas hébergés dans les mêmes datacenters ou nécessitent plusieurs « passages » dans des conteneurs dotés d'une architecture inefficace.

Coûts élevés : l'encodage continu des flux vidéo de pages web à distance vers les terminaux des utilisateurs exige une grande capacité de traitement. Il nécessite également une bande passante importante, même lorsqu'il est fortement optimisé. Ces coûts sont généralement répercutés sur les clients.

Failles de sécurité : puisque le « pixel-pushing » entraîne fréquemment des expériences insatisfaisantes pour les utilisateurs finaux, de nombreuses organisations limitent son utilisation aux équipes ayant accès à des données particulièrement sensibles, à l'image des services financiers, des ressources humaines ou de la direction de l'entreprise. L'organisation peut également appliquer la navigation à distance à un pourcentage réduit de pages web considérées comme particulièrement dangereuses. Dans tous les cas, l'organisation reste exposée, que ce soit en raison de la présence d'employés non protégés ou de sites « de confiance » ayant été compromis.

Consommation élevée de bande passante : la diffusion d'images consomme une grande quantité de bande passante, ce qui peut surcharger l'infrastructure réseau et avoir un impact négatif sur l'expérience des utilisateurs finaux. Par ailleurs, la densité des pixels augmente exponentiellement avec la résolution, et certains éléments (les polices, en particulier) peuvent paraître flous ou imprécis lors des sessions de navigation à distance sur des appareils HiDPI.

Déconstruction des sites web dans le Cloud et élimination du code malveillant

Cette méthode est souvent appelée « manipulation du DOM ». Dans le développement d'applications front-end, le DOM (« Document Object Model », c'est-à-dire modèle objet du document) est la représentation sous forme de données des objets composant la structure et le contenu d'une page Web. Dans la manipulation du DOM, un navigateur à distance hébergé dans le Cloud examine le code HTML, le code CSS et les autres éléments d'une page web et tente d'éliminer le code actif tel que le code JavaScript, les codes malveillants connus et d'autres contenus potentiellement malveillants. Le navigateur distant transmet ensuite ce code au navigateur de l'utilisateur final, qui l'utilise pour reconstruire une version « propre » de la page. Par ailleurs, comme avec le « pixel-pushing », la manipulation du DOM peut également signaler certaines pages présentant un risque de phishing.

Puisque la manipulation du DOM transfère uniquement le code du site web, plutôt qu'un flux complet reproduisant l'expérience de navigation, cette approche consomme moins de bande passante et peut permettre de proposer des expériences utilisateur plus réactives.

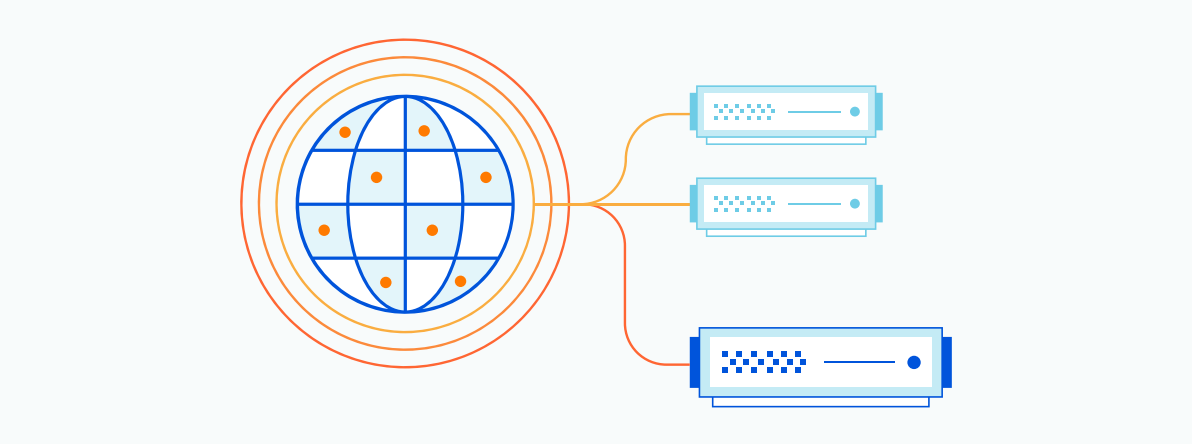
Cependant, elle comporte notamment les problèmes suivants :

Latence pour l'utilisateur final : à l'instar du « pixel-pushing », si l'isolation de navigateur par manipulation du DOM est exécutée dans le Cloud public (ou sur un réseau privé géographiquement restreint), les utilisateurs finaux peuvent constater de la latence lorsque les serveurs d'origine sont trop éloignés ou lorsque l'isolation de navigateur et d'autres outils de sécurité sont hébergés dans différents datacenters.

Dysfonctionnements de l'expérience de sites web : inévitablement, les tentatives de suppression de code malveillant actif, ainsi que la reconstruction du code HTML, du code CSS et des architectures de sites peu communes peuvent entraîner des dysfonctionnements de pages, qui ne s'affichent alors pas correctement, voire ne s'affichent pas du tout. Par ailleurs, des sites web qui fonctionnent aujourd'hui peuvent ne plus fonctionner demain, car les éditeurs de sites peuvent effectuer des modifications quotidiennes susceptibles de bloquer la fonctionnalité de reconstruction du DOM. La manipulation du DOM gère même difficilement la prise en charge de services communs à l'ensemble de l'entreprise, tels que Google G Suite ou Microsoft Office 365. Le résultat est une série infinie de problèmes accaparant d'importantes ressources informatiques dans une interminable partie de jeu de la taupe.

Coûts élevés : certains services de manipulation du DOM sont hébergés dans une infrastructure de Cloud public tiers, générant ainsi des coûts supplémentaires qui sont généralement répercutés sur les clients. Dans tous les cas, l'organisation reste exposée, que ce soit en raison de la présence d'employés non protégés ou de sites « de confiance » ayant été compromis.

Failles de sécurité : à l'instar des manipulations de type « pixel-pushing », l'expérience utilisateur que propose l'approche DOM est peu fiable ; c'est pourquoi les organisations ne l'utilisent que sporadiquement. Par ailleurs, bien que la manipulation du DOM soit une forme d'isolation de navigateur, elle transmet toujours du code tiers non fiable aux terminaux. Si le service ne parvient pas à identifier du code malveillant (ce qui est un risque permanent, compte tenu de l'évolution continue de l'environnement des menaces), des terminaux peuvent encore être victimes d'une attaque.



Isolation de l'activité de navigation sur une machine virtuelle exécutée sur le terminal

Dans cette approche, le logiciel installé sur un terminal crée une machine virtuelle isolée du reste du système d'exploitation de l'appareil. Toute l'activité de navigation se déroule sur cette machine virtuelle ; aussi, un logiciel malveillant téléchargé ne risque pas d'infecter le reste de l'appareil. Par ailleurs, comme d'autres approches, le logiciel permet d'identifier certaines pages présentant des risques de phishing.

Malheureusement, cette approche comporte également certaines difficultés :

- **Forte sollicitation des ressources processeur et de la RAM :** l'exécution d'une machine virtuelle distincte peut ralentir de nombreux ordinateurs personnels, entraînant des expériences de navigation lentes pour les utilisateurs finaux.
- **Difficultés de gestion des terminaux :** l'isolation de navigateur via un logiciel local nécessite que les équipes informatiques installent et mettent à jour le logiciel sur chaque terminal, ce qui constitue une tâche complexe dans les grandes entreprises. Cette complexité logistique devient encore plus problématique lorsque les organisations comptent un grand nombre de télétravailleurs ou lorsqu'elles emploient des sous-traitants qui n'utilisent pas les appareils fournis par l'entreprise.
- **Problèmes de compatibilité avec les appareils mobiles :** l'isolation de navigateur sur une machine virtuelle exécutée sur l'appareil nécessite des déploiements spécifiques au système d'exploitation. Souvent, de nombreux appareils mobiles ne sont pas pris en charge.
- **Défaillances de l'isolation :** les services d'isolation de navigateur local comportent périodiquement des vulnérabilités qui permettent à du code malveillant d'accéder au système d'exploitation principal. Dans ces circonstances, les équipes informatiques ou les utilisateurs finaux doivent installer manuellement des correctifs et des mises à jour. Cependant, si le correctif n'est pas correctement installé, le terminal peut rester vulnérable.
- **Expérience utilisateur insatisfaisante :** les déploiements sur des machines virtuelles nécessitent fréquemment que les utilisateurs finaux utilisent des navigateurs, des fenêtres ou des bureaux « virtualisés » distincts. Cette approche exige une formation adéquate du personnel et entraîne, pour le service informatique, un surcroît d'interventions d'assistance.

Ces difficultés immédiates en engendrent d'autres

Les conséquences immédiates telles que les coûts élevés, les expériences insatisfaisantes pour les utilisateurs finaux et les difficultés de gestion des terminaux ne sont pas les seules difficultés des approches courantes d'isolation de navigateur.

Une autre problématique est celle des conséquences à long terme de la compromission d'un appareil. Lorsque les utilisateurs finaux se connectent à des applications sensibles via un appareil compromis, un logiciel malveillant peut accéder aux données de cette application sans que l'utilisateur n'en ait conscience.

En outre, toutes ces approches d'isolation du navigateur peinent à prévenir certains types de perte de données. Des acteurs internes peuvent encore transférer et transmettre des informations sensibles par e-mail ou les saisir dans des formulaires en ligne.

Une meilleure approche de l'isolation de navigateur à distance

Malgré les problèmes mentionnés dans la section précédente, les organisations souhaitent encore adopter la navigation à distance.

Heureusement, certaines technologies peuvent être utiles :

Problème	Solution
Latence	**Utilisation d'un réseau périphérique étendu :** au lieu d'héberger l'isolation de navigateur dans un nombre limité de datacenters dans le Cloud public, hébergez plutôt le traitement sur un réseau périphérique mondial proche de l'utilisateur final, où qu'il se trouve. Par ailleurs, utilisez un logiciel d'isolation du navigateur qui réside dans les mêmes datacenters que les passerelles web sécurisées et autres outils de sécurité.
Consommation élevée de bande passante	**Pas de « pixel-pushing » :** la diffusion en continu d'images de l'activité du navigateur à distance est difficile à mettre en œuvre dans les grandes entreprises, tant du point de vue du coût que de celui de l'expérience de l'utilisateur.
Dysfonctionnement de l'expérience des sites web	**Optez pour une technologie native de navigateur :** les navigateurs à distance utilisant une technologie déjà intégrée dans les applications de navigateur pour terminaux répandues offrent une reconstruction plus fiable et précise de tous les types de sites.
Coûts de traitement élevés	**Cloud computing de nouvelle génération :** évitez les solutions d'isolation de navigateur à distance hébergée dans le Cloud public. Optez pour des techniques informatiques serverless performantes, qui améliorent la virtualisation et la conteneurisation en éliminant l'orchestration et la gestion des ressources de serveur sous-jacentes, utilisant ainsi plus efficacement ces ressources.
Failles de sécurité	**Optez pour une technologie de navigateur native :** au lieu d'essayer de déterminer quel code transmettre ou bloquer, la technologie de navigateur native permet d'éviter tout envoi de code. Au lieu de cela, elle peut uniquement envoyer la dernière étape du processus de rendu, qui trace la page.
Difficultés spécifiques au terminal	**Pas d'isolation de navigateur locale :** l'isolation de l'activité de navigation sur les terminaux est trop lente et difficile à gérer, ce qui rend cette approche complètement obsolète.

Pour découvrir comment ces technologies fonctionnent en pratique, prenez l'exemple de Cloudflare Browser Isolation, intégré nativement à notre plateforme Zero Trust.

Comment Cloudflare rend la navigation à distance rentable et moins perturbante pour l'utilisateur final

Sommairement, Cloudflare évite les difficultés spécifiques aux terminaux en s'exécutant simplement sur un réseau périphérique mondial, plutôt que sur les terminaux. Plus précisément, la technologie de Cloudflare élimine également les autres problèmes :

Problème	Solution	Déploiement de Cloudflare
 Latence	Utilisation d'un réseau périphérique mondial	L'isolation de navigateur à distance est exécutée dans chaque datacenter du réseau périphérique de Cloudflare, qui couvre plus de 200 villes dans 100 pays et s'étend à moins de 100 millisecondes de 95 % de la population mondiale connectée à Internet. Cette même infrastructure fournit des services DNS et de réseau CDN à très faible latence dans le monde entier. Par ailleurs, notre technologie de navigation à distance interagit de manière fluide avec notre proxy de transfert pour appliquer l'ensemble des autres filtres (tels que le blocage d'une partie d'une page) et inspections sans multiplier les passages et les transitions entre des solutions dédiées disparates.
 Consommation élevée de bande passante	Technologie de navigateur native	La technologie Network Vector Rendering de Cloudflare (plus d'informations ci-dessous) transmet des commandes de traçage, plutôt que des images à base de pixels ou du code « nettoyé ». Cette méthode ne nécessite qu'une infime quantité de la bande passante consommée par la navigation normale ou la manipulation du DOM, et bien moins encore que le « pixel-pushing ».
 Perturbation des expériences de sites web	Technologie de navigateur native	Le navigateur à distance de Cloudflare est basé sur le moteur open source Chromium, sur lequel reposent Google Chrome et 21 autres navigateurs répandus. L'investissement continu considérable consacré au moteur Chromium garantit des niveaux maximaux de compatibilité avec les sites web. Par ailleurs, puisque la technologie Network Vector Rendering de Cloudflare transmet des commandes de traçage plutôt que du code « nettoyé », elle préserve le bon fonctionnement des pages web, même les plus complexes.
 Coûts de traitement élevés	Cloud computing de nouvelle génération	Puisque la technologie Cloudflare Browser Isolation est exécutée sur notre réseau, nous n'avons pas besoin de répercuter les coûts du Cloud public sur les clients. Et puisque nous pouvons orchestrer et gérer très efficacement les ressources de serveurs, nous pouvons éviter les lenteurs du démarrage à froid qui affectent fréquemment les applications hébergées dans le Cloud public.
 Failles de sécurité	Technologie de navigateur native	En transmettant des commandes de dessin vectoriel légères, plutôt que le code d'origine d'un site web, Cloudflare élimine le risque qu'implique l'exécution de code non fiable sur le terminal. Les logiciels malveillants non détectés compromettent uniquement le navigateur à distance, sans affecter le terminal. Et puisque Cloudflare propose des expériences utilisateur performantes, les entreprises peuvent appliquer la navigation à distance à des scénarios d'utilisation moins risqués, qui pourraient autrement ne bénéficier d'aucune protection.
	Contrôle granulaire du comportement des utilisateurs finaux	Les outils de prévention des pertes de données protègent généralement les données pendant qu'elles transitent sur le réseau, en autorisant ou en bloquant la transmission. Cloudflare Browser Isolation offre aux administrateurs un contrôle granulaire sur : • L'autorisation d'utiliser les fonctions Copier/Coller/Imprimer • Les actions de transfert/téléchargement de fichiers • L'activité du clavier en général • Les autorisations de renseignement de formulaires • L'emplacement de stockage des fichiers téléchargés* *Disponible prochainement

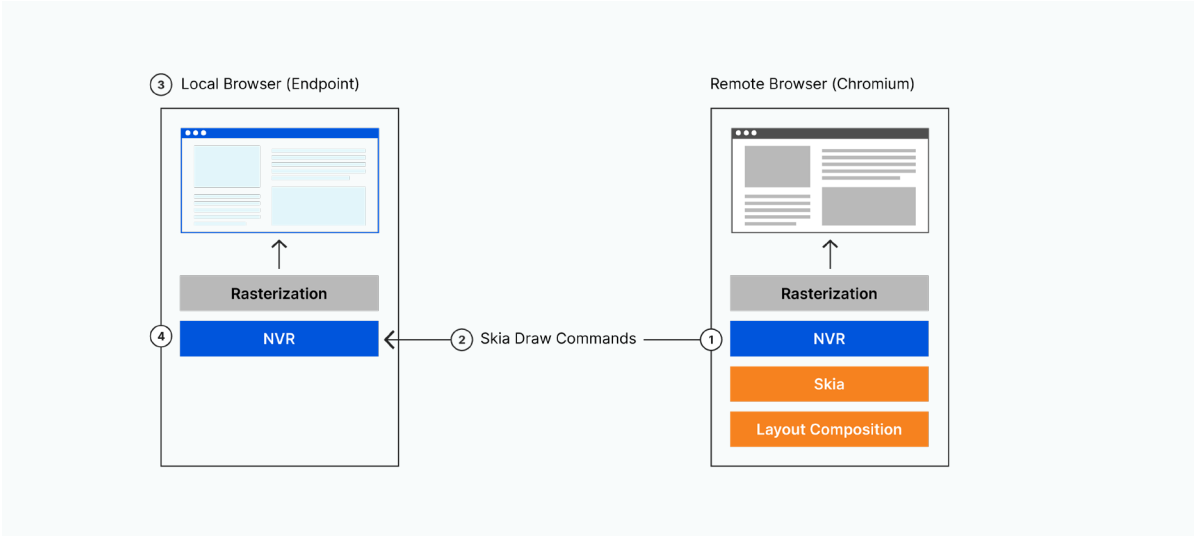
Lisez la suite pour découvrir une étude approfondie de la technologie NVR décrite ci-dessus :

La technologie Network Vector Rendering offre de meilleures expériences utilisateur et comble les failles de sécurité

Comme nous l'avons indiqué ci-dessus, le navigateur à distance de Cloudflare est conçu autour de Chromium. Une des principales caractéristiques architecturales du navigateur Chromium est l'utilisation de Skia, un moteur graphique multiplate-forme communément utilisé pour Android, Google Chrome, Chrome OS, Mozilla Firefox et de nombreux autres navigateurs. Tous les navigateurs compatibles HTML5 peuvent assurer le rendu de Skia. Le rendu de tout le contenu visible dans une fenêtre de navigateur Chromium est assuré par la couche de rendu Skia. Cela concerne l'interface utilisateur de la fenêtre d'application (les menus, par exemple), mais surtout, tout le contenu de la fenêtre de la page web est rendu par Skia. Cloudflare peut même isoler les fichiers téléchargés et les transférer vers différents emplacements, selon les besoins de l'utilisateur final.

La technologie Network Vector Rendering (NVR) de Cloudflare intercepte les commandes de traçage de Skia du navigateur à distance Chromium, les identifie avec un jeton et les compresse, puis les chiffre et les transmet à tout navigateur web conforme à la norme HTML5 exécuté localement sur le terminal (ordinateur de bureau ou appareil mobile). Les commandes de l'API Skia sont capturées par NVR avant rastérisation, et sont donc très compactes. Et puisque Skia est extrêmement répandu, la navigation à distance de Cloudflare est compatible avec tous les navigateurs web modernes.

La technologie Network Vector Rendering est également plus sécurisée. Comme nous l'avons mentionné plus haut, puisque Cloudflare transmet des commandes de traçage plutôt que le code du site web aux terminaux, le transport des données sous-jacentes ne constitue pas un vecteur d'attaque.



En savoir plus et vous lancer

Dès sa fondation, Cloudflare s'est donnée pour mission d'aider à bâtir un Internet meilleur et de démocratiser les technologies qui étaient jusqu'alors uniquement accessibles aux grandes entreprises possédant des réseaux sophistiqués, des équipes informatiques dédiées et des budgets colossaux. L'isolation plus performante des navigateurs à distance est une composante importante de cette mission.

En rendant l'isolation de navigateur plus rentable et en proposant des expériences utilisateur exceptionnelles, nous espérons permettre à un nombre croissant d'entreprises de découvrir la valeur réelle de cette technologie. Comme dans un passé pas si lointain, où le chiffrement HTTPS était réservé aux pages de connexion « sensibles » et aux pages de validation de commande des sites d'e-commerce, nous pensons que l'approche consistant à faire confiance au code d'un site web quelconque deviendra tout aussi archaïque que la création du nouveau paradigme de navigation Zero Trust.

Pour en savoir plus sur Cloudflare Browser Isolation et comment la solution peut vous aider à déployer une navigation Zero Trust, consultez le site web https://www.cloudflare.com/products/zero-trust/browser-isolation/