Sécuriser le travail hybride

Réduisez les risques et améliorez la visibilité pour tous les utilisateurs, à la fois sur le réseau et en dehors

Sécurisez n'importe quelle connexion, de n'importe quel utilisateur, sur n'importe quel appareil, sur n'importe quel site

Le travail nomade est notre avenir : quelques années après la pandémie et face à la récession à venir, le travail hybride semble parti pour s'installer durablement. Les équipes informatiques et de sécurité doivent assurer une protection et une expérience cohérentes à l'ensemble des utilisateurs et des appareils, que ces derniers se situent au domicile du collaborateur (en cas de télétravail) ou au bureau. De même, les outils traditionnels fondés sur l'emplacement géographique (comme les VPN et les mesures de contrôle basées sur l'adresse IP) manquent à leur mission.

Une sécurité moderne pour des effectifs modernes : en réponse, de nombreuses entreprises réimaginent ainsi leurs architectures informatiques et de sécurité, en adoptant un modèle de sécurité dans le cloud capable d'évoluer selon les besoins des effectifs distribués et en suivant les bonnes pratiques du Zero Trust.

Cloudflare facilite la sécurisation de n'importe quelle connexion, afin que les utilisateurs travaillant sur n'importe quel appareil ou de n'importe quel endroit restent sécurisés et productifs lorsqu'ils accèdent à vos applications ou à Internet.

Ce qu'en dit Gartner® :

D'ici à 2026, 75 % des employés continueront à répartir leur temps entre le bureau traditionnel et le télétravail, soit un chiffre en légère baisse depuis les 77 % lors du pic de la pandémie en 2021.[1]

Les modèles de sécurité réseau basés sur une collection d'équipements de sécurité périmétriques conviennent mal pour répondre aux besoins nomades et dynamiques d'une entreprise numérique moderne et de ses effectifs hybrides.[2]

Sommaire, par page

Opportunités de modernisation de la sécurité

Sécurisez l'accès aux applications sans VPN

Face à des utilisateurs aussi dispersés, la redirection du trafic (backhauling) via des équipements sur site, tels que les VPN, ralentit le système et engendre des risques de mouvements latéraux des menaces sur l'ensemble du réseau d'entreprise.

À la place, récupérez de la visibilité sur toutes les requêtes et appliquez des mesures de contrôle basées sur l'identité au plus près des utilisateurs afin de soutenir la productivité. Aucune redirection n'est nécessaire.

Simplifiez la sécurité SaaS

Les employés se reposent plus que jamais sur des applications SaaS situées en dehors de la sphère de contrôle des réseaux traditionnels.

En réponse, les entreprises ont besoin d'une meilleure visibilité et d'un degré de contrôle plus exhaustif sur leurs applications SaaS pour définir des politiques d'accès, appliquer des mesures de protection des données, atténuer le Shadow IT (informatique fantôme) et analyser leurs applications à la recherche d'erreurs de configuration.

Protégez les utilisateurs et les données des menaces Internet

Les attaques par rançongiciel, par phishing et les autres menaces Internet sont plus nombreuses que jamais et de plus en plus sophistiquées.

L'adoption d'une solution d'inspection et d'isolement basée sur le cloud pour le trafic sortant protège les utilisateurs contre les logiciels malveillants. En outre, les administrateurs peuvent appliquer des mesures de contrôle pour empêcher les données sensibles de rejoindre des appareils locaux, non gérés.

Travail hybride pour entreprises matures

Modernisez en toute confiance la sécurité des entreprises matures en vue du travail hybride

Problème: environnements traditionnels, complexes

Les entreprises expérimentent divers modèles de travail au bureau (sur site). Toutefois, la préservation de la cohérence, tant au niveau des protections que de l'expérience utilisateur, s'avère difficile dans les scénarios hybrides.

Ces entreprises ont tendance à être plus établies, ainsi qu'à disposer d'investissements pré-existants (sur site et traditionnels) plus lourds et souvent complexes. Le lancement d'un nouveau projet de sécurité peut paraître trop risqué et difficile face aux vents contraires de la récession.

Opportunité : une voie plus simple vers la modernisation

Les entreprises méritent de poursuivre le processus de transformation numérique à leur propre rythme, sans avoir besoin d'un budget infini, de démonstrations de faisabilité coûteuses, de phases de mise en œuvre complexes ni de chaînes de services liés.

Afin d'aider ces entreprises matures à répondre à leurs besoins en termes de travail hybride, les solutions Cloudflare sont conçues pour être plus simples et rapides à déployer que celles des autres fournisseurs de services Zero Trust, comme Zscaler.

Exemples de scénarios d'utilisation

Télécommunications

Situation : une entreprise de télécommunications européenne plus que centenaire (et affichant un chiffre d'affaires annuel de plus de 20 milliards) souhaitait disposer d'un fournisseur unique afin de déployer le filtrage Internet et d'authentifier l'accès à ses anciennes applications, récemment migrées vers plusieurs environnements cloud.

Solution : l'entreprise a sélectionné Cloudflare pour consolider ses services et utiliser une plateforme unifiée afin de sécuriser à la fois l'accès à ses applications et à Internet pour l'ensemble de ses collaborateurs (plus de 100 000).

Gouvernement fédéral

Situation : "l'U.S. Department of Homeland Security a réalisé des investissements en matière de protection contre les menaces Internet sur divers agences fédérales, emplacements et infrastructures.

Solution : le DHS a sélectionné Cloudflare et Accenture Federal Services afin de développer une solution commune visant à filtrer les requêtes DNS vers les destinations risquées et malveillantes. Cette solution sera ensuite utilisée par l'ensemble des agences fédérales.

Médias et publicité

Situation : un conglomérat d'entreprises du secteur des médias (plus de 10 milliards de chiffre d'affaires et plus de 100 000 collaborateurs à travers le monde) était confronté à des cyberattaques visant son infrastructure interne, dont une accompagnée d'une demande de rançon.

Solution : Cloudflare sécurise des centaines d'applications web et non web à l'aide de règles Zero Trust basées sur l'identité. L'entreprise a déployé une protection couvrant 50 000 collaborateurs en trois mois et prévoit d'élargir cette dernière à l'intégralité de ses effectifs sous neuf mois.

Électricité

Situation : un fournisseur de gaz naturel figurant au Fortune 500 cherchait une protection renforcée contre l'accroissement des cybermenaces visant le secteur, afin de sécuriser à la fois ses datacenters distribués et ses effectifs (plus de 1 500 collaborateurs).

Solution : l'entreprise a sélectionné Cloudflare pour remplacer Zscaler, citant une plus grande fiabilité et une meilleure cohérence en termes de protection des applications et de l'accès à Internet, ainsi qu'un parcours plus simple sur le long terme en matière d'adoption de mesures de contrôle avancées, dotées d'une fonctionnalité d'isolation des navigateurs distants.

TÉMOIGNAGES DE CLIENTS

Cloudflare agit comme un multiplicateur de puissance sur notre parcours Zero Trust.

John McLeod
RSSI, National Oilwell Varco

Cloudflare a permis à Ziff Media Group de mettre sa suite d'outils internes à la disposition de ses employés du monde entier de manière facile et sécurisée, indépendamment des appareils utilisés et ce sans devoir recourir à des configurations réseau complexes.

Josh Butts
SVP Product & Technology, Ziff Media Group

Grâce à Cloudflare, nous avons pu réduire notre dépendance aux VPN et à la mise sur liste d'adresses IP autorisées pour les environnements de développement.

Alexandre Papadopoulos,
Director of Cyber Security, INSEAD

Des effectifs principalement axés sur le télétravail pour les digital natives

Dans le cas des digital natives, privilégiez une sécurité agile afin de soutenir la flexibilité du télétravail

Problème : faire évoluer et automatiser la sécurité cloud

De nombreuses entreprises adoptent un modèle de recrutement principalement axé sur le télétravail. Elles ont tendance à être composées d'entreprises plus jeunes, primo-adoptantes en matière de cloud, à ne disposer que d'une infrastructure sur site limitée et à suivre des modèles commerciaux reposant sur des services numériques sûrs, rapides et fiables.

La prise en charge de la flexibilité en termes de travail nomade peut constituer un facteur de différenciation, mais exige des outils de sécurité tout aussi flexibles, capables de suivre les déplacements des utilisateurs et leur utilisation d'appareils personnels.

Opportunité : une sécurité composable, à l'échelle appropriée

Avec une quantité moindre de solutions informatiques à abandonner, les digital natives (natifs numériques) peuvent tirer parti de notre architecture native d'Internet et de notre flexibilité en matière de déploiement afin de rester agiles lors du processus de modernisation de leur sécurité.

Grâce à nos services composables, notre conception orientée API et nos possibilités de gestion à partir d'un panneau unique, vous pouvez facilement mettre en place et adapter votre sécurité. La vitesse, l'échelle et la fiabilité de notre réseau mondial répondent aux besoins des effectifs intégralement axés sur le télétravail.

Exemples de scénarios d'utilisation

SaaS B2B

Situation : Canva, une plateforme de design graphique australienne estimée à 40 milliards en 2021, a déployé Cloudflare avant la pandémie pour rationaliser l'accès des utilisateurs tiers et éviter les tracas liés à la mise en œuvre d'un VPN.

Solution : au fil du temps, Canva a déployé des politiques d'accès Zero Trust sur l'ensemble de ses effectifs en pleine croissance. L'entreprise a également étendu ses fonctionnalités de filtrage et d'inspection Internet.

Fintech et blockchain

Situation : BlockFi, une plateforme de gestion de patrimoine de série D soutenue par la technologie de la blockchain, avait besoin d'améliorer sa sécurité face aux cybermenaces visant son parc d'actifs en croissance gérés par des effectifs axés sur le télétravail.

Solution : Cloudflare a permis à BlockFi de passer à une authentification basée sur l'identité pour l'accès aux applications et de se détourner des mesures de contrôle basées sur l'adresse IP, particulièrement chronophages.

Réseaux sociaux

Situation : une plateforme de réseaux sociaux mondiale a fait les frais d'une violation à haute visibilité de sa sécurité. Cette dernière exploitait l'accès aux applications internes et la configuration des VPN.

Solution : en réponse, l'entreprise a décidé de repenser son approche de l'accès distant en adoptant la solution d'accès réseau Zero Trust (ZTNA) de Cloudflare pour ses 13 000 employés et sous-traitants, ainsi qu'en abandonnant ses déploiements de VPN.

E-commerce

Situation : une plateforme d'e-commerce mondiale (plus de quatre milliards de chiffre d'affaires et plus de 15 000 collaborateurs) cherchait une meilleure protection pour ses utilisateurs distants, à la fois pour leur activité de navigation sur Internet et l'accès à des applications SaaS sensibles, lorsqu'ils ne se trouvaient pas sur le réseau.

Solution : l'entreprise a déployé Cloudflare pour superposer des fonctionnalités de protection contre les menaces, comme le filtrage DNS, tout en assurant une visibilité améliorée sur l'utilisation des applications SaaS.

TÉMOIGNAGES DE CLIENTS

> *Chez Delivery Hero, nous nous efforçons de toujours offrir une expérience extraordinaire à nos clients. Cloudflare nous aide à faire de même pour nos équipes internes, en leur assurant un environnement de travail sécurisé dans le monde entier et un moyen simple de développer des applications rapides, fiables et respectueuses de la confidentialité.*

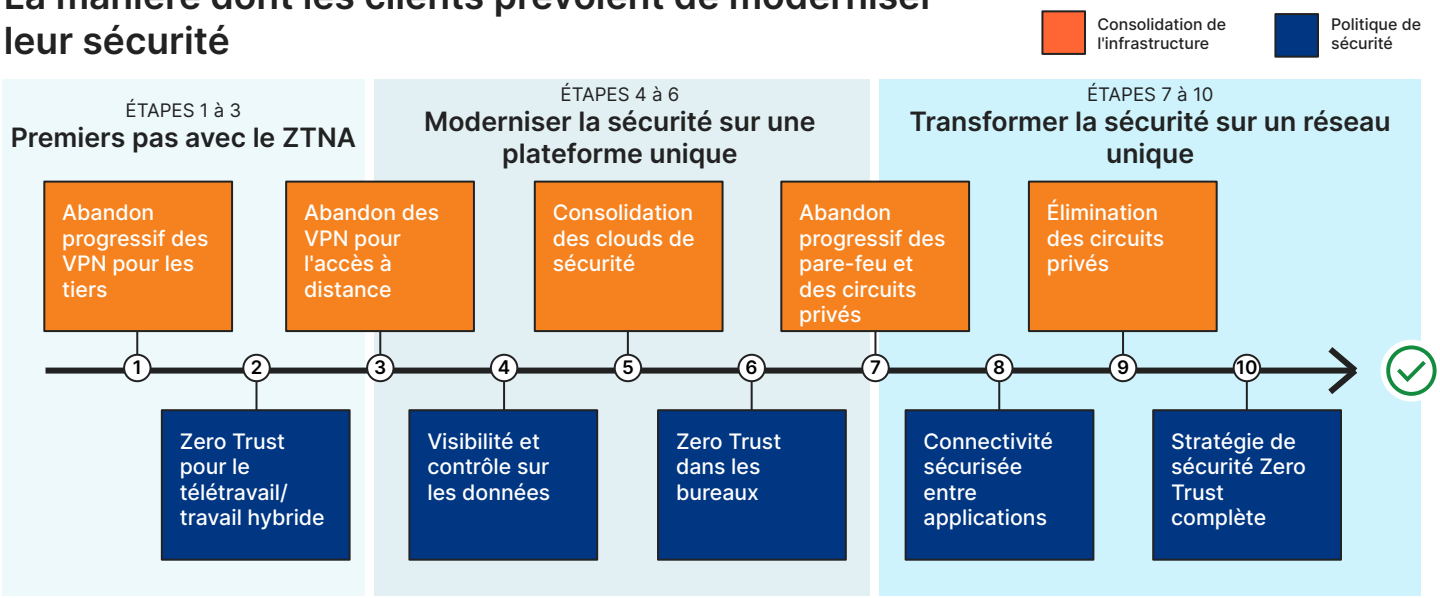
Christina von Hardenberg
CTO, Delivery Hero

> *Cloudflare est essentielle dans la manière dont nous sécurisons nos effectifs distants, en croissance rapide. L'adoption du Zero Trust pour l'accès aux applications a permis à nos administrateurs de profiter d'une visibilité renforcée et de mesures de contrôle plus précises dont ils n'auraient jamais pu bénéficier avec nos anciens outils, plus traditionnels.*

Marccio Alcaide
Head, IT Security, Facily

Feuille de route illustrative concernant le travail hybride

La manière dont les clients prévoient de moderniser leur sécurité



Feuille de route en matière de modernisation de la sécurité

La feuille de route ci-dessus illustre l'approche que nous voyons les entreprises suivre lors de la modernisation de leur sécurité afin de l'adapter au travail hybride. Cette feuille de route présente deux objectifs essentiels :

1) **Ligne supérieure (en orange) :** consolider la connectivité et l'infrastructure de sécurité, en se détournant des solutions ponctuelles et des équipements physiques au profit d'une plateforme unique et native du cloud.
2) **Ligne inférieure (en bleu) :** mettre en place la visibilité et les mesures de contrôle nécessaires à l'adoption de la sécurité Zero Trust entre les utilisateurs et les ressources, sur n'importe quel appareil et à n'importe quel endroit.

Phases 1 à 5 : sécurisation de l'accès aux applications et à Internet

Pour de nombreuses entreprises, l'adaptation au travail hybride implique en premier lieu de moderniser la manière dont leurs collaborateurs accèdent aux ressources de l'entreprise.

Phase 1 : la première étape des entreprises consiste souvent à commencer à décharger le trafic des VPN et à mettre en place des mesures de contrôle natives d'Internet pour une sélection d'utilisateurs, comme les sous-traitants, les développeurs, les partenaires ou les équipes nouvellement acquises. Cloudflare facilite particulièrement le processus de sécurisation des applications auto-hébergées accessibles par l'intermédiaire d'un navigateur, sans devoir déployer d'élément logiciel sur les points de terminaison.

Phase 2 : cet outillage moderne permet la visibilité nécessaire à la conception de politiques spécifiques à chaque application, basées sur le rôle, les exigences en matière de MFA et de clés physiques, ainsi que les stratégies de sécurité des appareils et de l'identité.

Phase 3 : à mesure que les équipes développent leur confiance envers cette approche, elles commencent à abandonner totalement leur VPN, ainsi qu'à protéger leurs réseaux privés traditionnels et non web à l'aide de mesures Zero Trust.

Phase 4 : l'accent passe alors sur l'amélioration de la visibilité et des mesures de contrôle pour les applications SaaS, en incluant notamment l'atténuation du Shadow IT (informatique fantôme), la gestion des tenants et la prévention de l'exfiltration de données.

Phase 5 : maintenant que leurs applications internes et SaaS sont gérées par une plateforme unique, les entreprises cherchent à étendre les mesures de contrôle concernant l'accès Internet sortant et à consolider leur protection contre les menaces à l'aide d'outils tels que des filtres DNS et des passerelles web sécurisées (Secure Web Gateways).

Phases 6 à 10 : migration de la connectivité vers le cloud

Les phases restantes de la feuille de route sont en voie de planification pour la plupart des entreprises, mais l'idée consiste à procéder à la migration de l'ensemble des fonctions de connectivité et de sécurité réseau vers un réseau cloud unique et unifié.

Phase 6 : à ce stade, les entreprises cherchent à étendre leur approche Zero Trust constante à tous les emplacements réseau, comme le siège, les bureaux régionaux, les datacenters et les postes satellites afin de prendre en charge le travail hybride.

Phase 7 : à mesure que le trafic des bureaux est envoyé de manière plus fréquente vers Cloudflare à des fins de sécurité, les entreprises peuvent abandonner progressivement leurs pare-feu traditionnels sur site et les autres équipements de leurs réseaux privés.

Phase 8 : ces scénarios d'utilisation avancés se concentrent sur la sécurisation de la connectivité entre applications au sein d'environnements hybrides multicloud, qui prépare l'équipe chargée de l'infrastructure réseau à mettre un terme aux contrats MPLS lors de la phase 9.

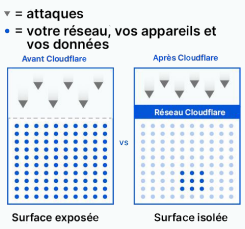
Phase 10 : bien que le processus de modernisation ne soit jamais vraiment terminé, l'idée derrière cette phase consiste à étendre le Zero Trust à l'ensemble des utilisateurs, des appareils, des données, des applications et des environnements.

Résultats opérationnels et en matière de sécurité

Cinq moyens par lesquels le Zero Trust permet à votre entreprise d'économiser du temps et de l'argent

Réduisez votre surface d'attaque de

91 %↓



Réduisez vos coûts de violation de

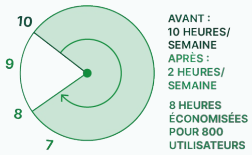
35 %↓

Accélérez le temps d'intégration des collaborateurs de

60 %↑

Réduisez le temps passé à traiter les tickets informatiques de

80 %↓



Réduisez la latence pour les utilisateurs de

39 %↓

Autres moteurs économiques

Libérer la productivité de vos effectifs

Pour les administrateurs

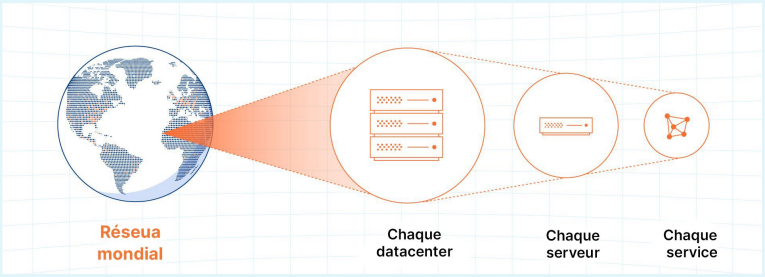
- Simplifiez la configuration à l'aide d'une interface de gestion unique afin de définir des politiques couvrant l'ensemble des accès aux applications et à Internet.
- Configurez toutes les intégrations à l'aide de fournisseurs d'identité, de solutions de protection des points de terminaison, de fournisseurs de cloud et d'accès réseau directs (on-ramps) depuis cette même interface de gestion.

Pour les utilisateurs finaux

- Profitez d'un processus d'authentification sans friction et d'expériences de navigation natives à l'aide d'une sécurité qui n'entrave pas vos activités.

Réduire le coût des services traditionnels

- Remplacez ou améliorez les équipements de votre réseau privé virtuel (VPN) et adoptez à la place l'accès réseau Zero Trust (ZTNA).
- Passez d'un proxy ou d'un pare-feu sur site à des services de sécurité des couches 3 à 7 natifs du cloud.
- Déchargez vos scénarios d'utilisation d'une infrastructure avec bureau virtuel grâce à la solution d'isolation du navigateur Remote Browser Isolation (RBI)
- Échangez votre passerelle web sécurisée traditionnelle contre une solution de sécurité des e-mails dans le cloud moderne.



Une vitesse et une échelle constantes pour protéger l'ensemble de vos utilisateurs, distants ou au bureau

Toutes les fonctions d'amélioration de la sécurité, des performances et de la fiabilité sont conçues pour s'exécuter sur chaque serveur dans chaque datacenter du réseau Cloudflare, qui s'étend aujourd'hui à plus de 275 villes.

Accélérez votre feuille de route Zero Trust

Essayer maintenant | Nous contacter

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : PMM-2022JJUL

[1] *Top Network Practices to Support Hybrid Work* (Meilleures pratiques réseau pour prendre en charge le travail hybride), Gartner, Karen Brown, Andrew Lerner, Mike Toussaint, 08/04/2022
[2] *2022 Strategic Roadmap for SASE Convergence* (Feuille de route stratégique 2022 pour la convergence SASE), Gartner, Neil MacDonald, Andrew Lerner, John Watts 24/06/2022