

# Cloudflare Zero Trust

La plateforme Zero Trust la plus rapide du marché en matière de navigation et d'accès aux applications

## Les risques situés au-delà du périmètre

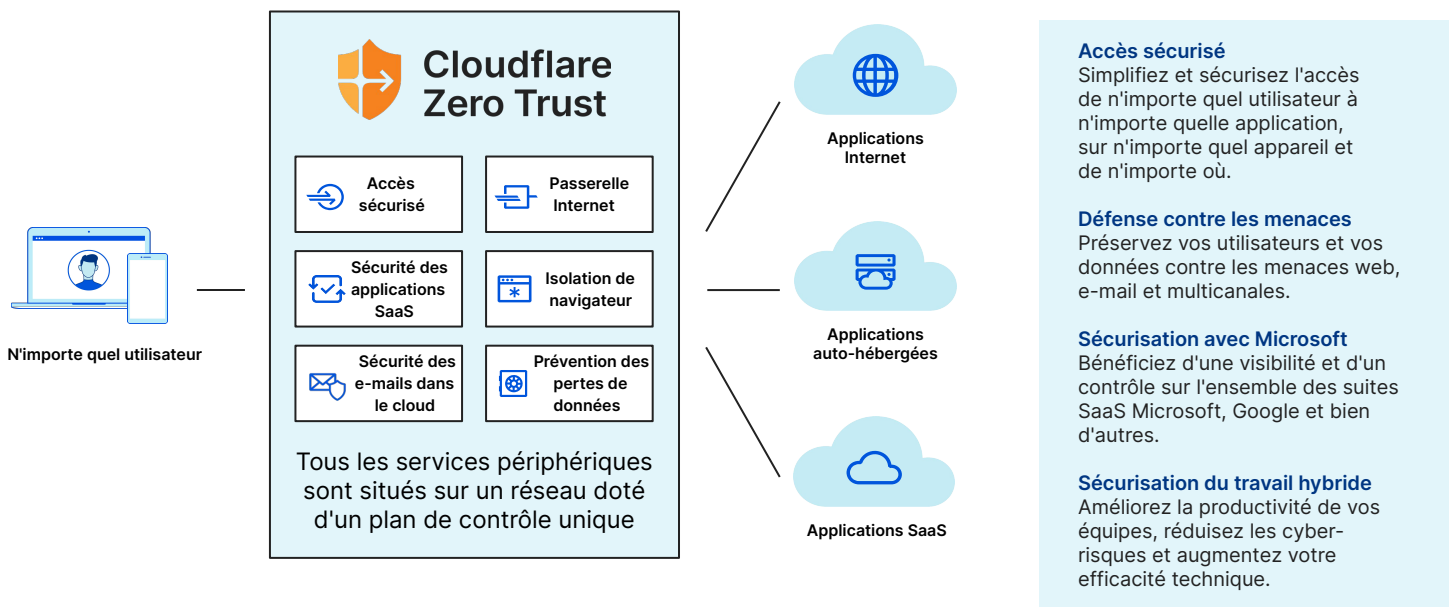
Lorsque les applications et les utilisateurs ont quitté le périmètre de l'entreprise, les équipes de sécurité ont dû faire des compromis sur la manière d'assurer la protection des données. Les méthodes de sécurisation du trafic axées sur la géolocalisation (comme les VPN, les pare-feu, et les proxys web) n'ont pas résisté à la pression. Les entreprises se sont ainsi retrouvées en proie à divers problèmes, tels qu'une visibilité limitée, des conflits de configuration et des risques excessifs.

Face à des risques désormais persistants partout dans le monde, les entreprises se tournent vers une approche Zero Trust dans le cloud pour s'adapter à ce nouveau contexte.

## Adoptez une solution Zero Trust native d'Internet

La plateforme de sécurité de Cloudflare Zero Trust améliore la visibilité, élimine les complexités et réduit les risques liés à la connexion aux applications ou à Internet de vos utilisateurs en télétravail ou au bureau. Bâtie sur le principe de l'architecture en une seule passe, la solution vérifie, filtre et inspecte le trafic avant de l'isoler des menaces.

Le service s'exécute sur l'un des réseaux Anycast les plus rapides du monde (couvrant plus de 275 villes dans plus de 100 pays) afin d'assurer un déploiement plus rapide et de meilleures performances que les autres fournisseurs.



## Avantages pour l'entreprise

### Réduire l'excès de confiance

Protégez vos applications à l'aide de règles Zero Trust basées sur l'identité et le contexte. Bloquez les rançongiciels, le phishing et les autres menaces en ligne. Isolez les points de terminaison des risques en conservant le code web non fiable loin des appareils et l'activité des utilisateurs non fiables loin des données.

### Éliminer la complexité

Réduisez la dépendance aux produits spécifiques d'ancienne génération et appliquez des mesures de contrôle de la sécurité standard à l'ensemble du trafic, quel que soit l'origine de la connexion ou l'endroit où elle réside au sein de la pile réseau.

### Restaurer la visibilité

Bénéficiez de journaux complets sur l'activité DNS, HTTP, SSH, l'activité réseau et l'informatique fantôme (Shadow IT). Surveillez l'activité des utilisateurs sur l'ensemble des applications. Envoyez les journaux vers plusieurs de vos solutions préférées en matière de stockage cloud et d'outils d'analyse.

## Accès sécurisé (ZTNA)

### Un moyen plus rapide, plus simple et plus sécurisé de connecter n'importe quel utilisateur à n'importe quelle application

#### Problème : un accès lent, complexe et risqué

Les mesures de contrôle traditionnelles basées sur le périmètre (comme les VPN) s'avèrent de plus en plus risquées. Les performances médiocres nuisent à la productivité des utilisateurs finaux, les administrateurs se retrouvent aux prises avec des processus de configuration complexes et les mouvements latéraux se révèlent difficiles à contenir.

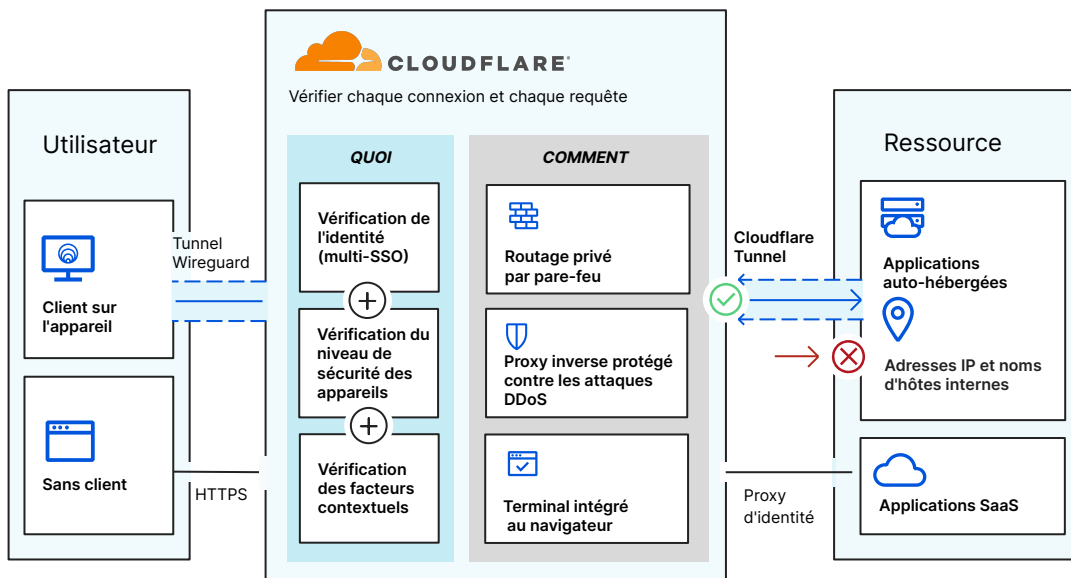
L'adoption accélérée du cloud et le travail hybride ont contribué à exposer davantage ces défauts, ainsi qu'à faire apparaître les VPN comme plus vulnérables.

#### Accès réseau Zero Trust (ZTNA)

Access, le service ZTNA de Cloudflare, améliore ou remplace les clients VPN en protégeant n'importe quelle application au sein de n'importe quel environnement, qu'il s'agisse d'un réseau sur site, d'un cloud public ou d'un environnement SaaS.

La solution ZTNA de Cloudflare fonctionne avec vos fournisseurs d'identité et vos plateformes de protection des points de terminaison afin d'appliquer des règles Zero Trust refusant l'accès par défaut, qui permettent de limiter l'accès aux applications, aux espaces IP privés et aux noms d'hôte de l'entreprise.

### Fonctionnement



**Un déploiement sans client** pour les applications auto-hébergées web, SSH ou VNC accessibles via un navigateur.

**Procédez au déploiement grâce au client sur appareil de Cloudflare** afin de vous connecter aux adresses IP et aux noms d'hôte internes, ainsi qu'aux applications non web.

### Scénarios d'utilisation principaux



#### Prendre en charge le télétravail et les initiatives BYOD

Vérifiez les accès pour tous les utilisateurs, peu importe leur position géographique, en fonction de l'identité, du niveau de sécurité de l'appareil, de la méthode d'authentification et d'autres facteurs contextuels.

Appliquez ces politiques Zero Trust à vos effectifs hybrides. Prenez en charge les initiatives BYOD (Bring Your Own Device, utilisez vos propres appareils) en sécurisant à la fois les appareils gérés et non gérés.



#### Rationaliser les accès tiers grâce à une meilleure flexibilité

Accélérez la configuration des accès pour les sous-traitants, les fournisseurs, les agences, les collaborateurs, etc.

Intégrez plusieurs fournisseurs d'identité (IDP, identity providers) à la fois. Définissez des règles de moindre privilège basées sur les IDP que vous utilisez déjà.

Évitez de provisionner des licences SSO, de déployer des VPN ou de créer des autorisations à usage unique.



#### Simplifier l'administration de la configuration et du support

Ajoutez de nouveaux utilisateurs, fournisseurs d'identité ou règles Zero Trust en quelques minutes.

Débridez votre productivité en réduisant le temps d'intégration des nouveaux collaborateurs ([eTeacher Group](#)) et en abandonnant la configuration d'accès basée sur l'adresse IP ([BlockFi](#)). Vous n'aurez plus besoin d'engager de personnel dédié pour la gestion de vos VPN ([ezCater](#)).

## Défense contre les menaces (SWG et RBI)

### Filtrez, inspectez et isolez le trafic Internet

#### Problème : un panorama des menaces évolutif

Il n'a jamais été aussi difficile de faire passer la sécurité au niveau supérieur, tout en maintenant la productivité des utilisateurs. Le télétravail implique qu'un plus grand nombre d'appareils non gérés stockent un plus grand nombre de données sensibles à l'échelon local. Pendant ce temps, les rançongiciels, le phishing, l'informatique fantôme et les autres menaces véhiculées via Internet ont véritablement explosé, tant en termes de volume que de sophistication.

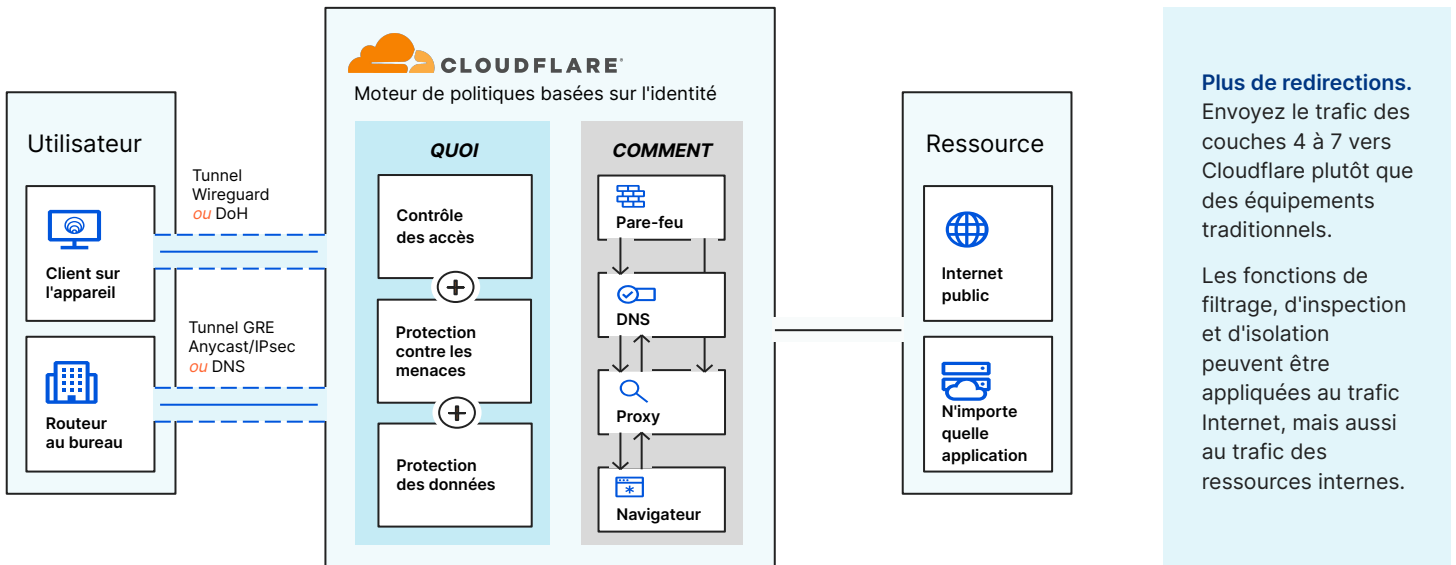
La stratégie visant à se reposer sur des solutions ponctuelles traditionnelles et des sauvegardes des données afin de se protéger contre les menaces multicanales s'avère des plus risquées.

#### SWG et navigation Zero Trust

Notre passerelle web sécurisée (SWG, Secure Web Gateway) Cloudflare Gateway protège les utilisateurs par le biais d'une fonction de filtrage web basée sur l'identité, en plus d'une solution d'isolation de navigateur à distance (RBI, Remote Browser Isolation) nativement intégrée.

Commencez par mettre en place un filtrage DNS afin d'atteindre un délai de rentabilisation rapide pour les utilisateurs distants ou sur site. Appliquez ensuite une inspection HTTPS plus complète et terminez en étendant les mesures de contrôle RBI, afin d'adopter l'approche Zero Trust sur l'ensemble de votre activité Internet.

### Fonctionnement



### Scénarios d'utilisation principaux



#### Arrêter les rançongiciels

Bloquez les sites et les domaines hébergeant des rançongiciels grâce aux informations issues de notre réseau mondial. Isolez l'activité de navigation des sites à risque afin de renforcer la protection.

Alliez le filtrage SWG et le RBI à une solution ZTNA refusant l'accès par défaut afin d'atténuer le risque qu'une infection par rançongiciel se répande horizontalement et procède à une escalade des privilèges sur l'ensemble de votre réseau.



#### Bloquer le phishing

Filtrez les domaines de phishing connus et « nouvellement observés ». Isolez la navigation afin d'empêcher les contenus malveillants de s'exécuter localement. Bloquez la saisie d'informations sensibles sur des sites de phishing suspects à l'aide de mesures de contrôle des entrées clavier de notre solution RBI.

En outre, les administrateurs pourront bientôt activer le filtrage des e-mails en un seul clic via la solution [Area 1](#).



#### Prévenir les fuites de données

Mettez en place une protection contre la perte de données permettant de contrôler les types de fichiers susceptibles d'être envoyés vers les sites par les utilisateurs.

Déployez une solution de navigation Zero Trust afin de contrôler et de protéger les données qui résident au sein de vos applications web. 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.

## Sécurisation avec Microsoft (CASB)

### Rationalisez la sécurité SaaS pour plus de visibilité et de contrôle, à moindre coût

#### Problème : la prolifération des applications SaaS

Les effectifs modernes s'appuient plus que jamais sur les applications SaaS, comme Microsoft 365. Or, chacune de ces dernières nécessite des considérations de sécurité différentes et fonctionne en dehors des mesures de protection du périmètre traditionnel.

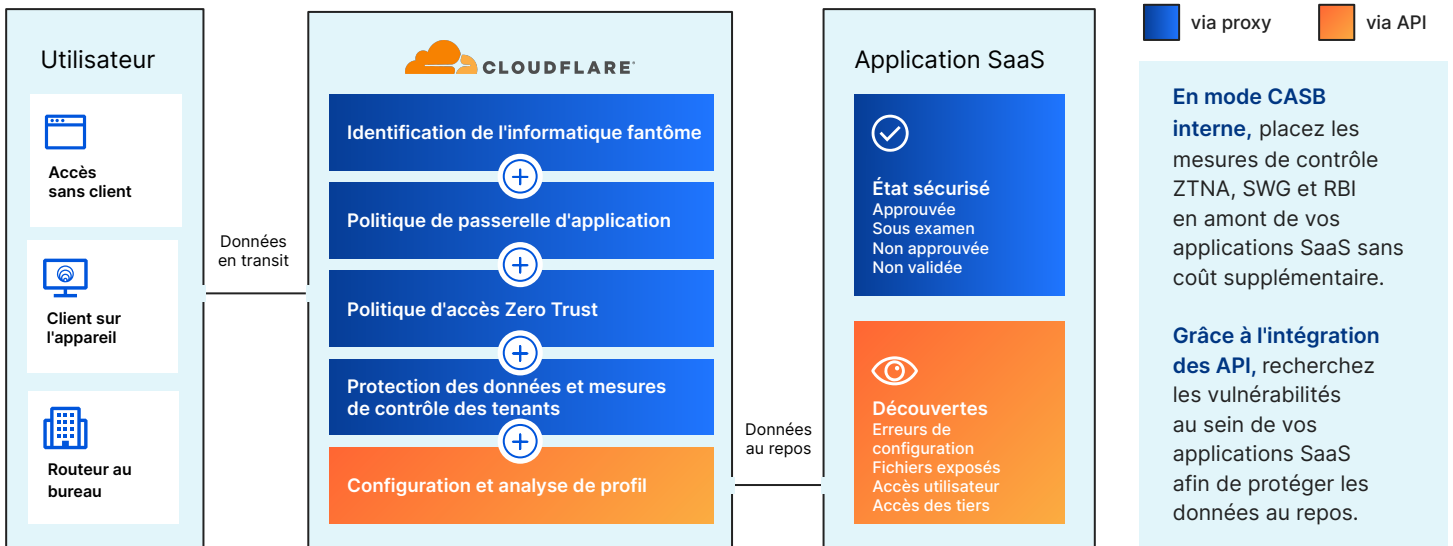
Alors que les entreprises adoptent des dizaines d'applications SaaS, la préservation de la cohérence en termes de sécurité, de visibilité et de performances devient de plus en plus difficile.

#### CASB (Cloud Access Security Broker)

Le service CASB (Cloud Access Security Broker, agent de sécurité des accès au cloud) de Cloudflare assure une visibilité intégrale et un contrôle total sur les applications SaaS, afin de vous permettre d'éviter facilement les fuites de données et les violations de la conformité.

Bloquez les menaces internes, les partages de données risqués et les acteurs malveillants. Journalisez chaque requête HTTP afin de révéler les applications non autorisées. Analysez les applications SaaS afin de détecter les erreurs de configuration et les activités suspectes.

### Fonctionnement



### Scénarios d'utilisation principaux



#### Appliquer des mesures de protection des clients et des données

Appliquez des mesures de contrôle des entités (tenants) par le biais de politiques de passerelle HTTP afin d'empêcher les utilisateurs d'accéder à vos données et de les stocker au sein de mauvaises versions d'applications SaaS populaires, par inadvertance ou de manière malveillante.

Contrôlez les actions des utilisateurs (p. ex. copier/coller, téléchargement, impression, etc.) au sein des applications SaaS web afin de minimiser le risque de perte de données.



#### Atténuer et contrôler l'informatique fantôme

Minimisez les risques introduits par les applications SaaS non approuvées.

Cloudflare regroupe et répartit l'ensemble des requêtes HTTP sous différentes catégories dans notre journal d'activité, et ce par type d'application. Les administrateurs peuvent alors définir le statut et suivre l'utilisation des applications (approuvées ou non) au sein de votre entreprise.



#### Identifier les nouvelles menaces et les erreurs de configuration

Connectez-vous aux applications SaaS populaires (Google Workspace, Microsoft 365, etc.) via API et analysez-les à la recherche de risques.

Renforcez les possibilités de vos équipes informatiques et de sécurité en leur assurant une visibilité sur les autorisations, les erreurs de configuration, les accès inappropriés et les problèmes de contrôle susceptibles de mettre les données et les collaborateurs en danger.

## Protection contre le phishing (CES)

### Étendre le Zero Trust aux e-mails pour une protection complète contre les menaces

#### Problème : le courrier électronique est le premier vecteur de menaces

Le courrier électronique constitue le moyen de communication principal des équipes, mais aussi le premier canal par lequel les acteurs malveillants lancent leurs attaques. Une étude récente a d'ailleurs conclu que **91 %** de l'ensemble des cyberattaques commencent par un e-mail de phishing.

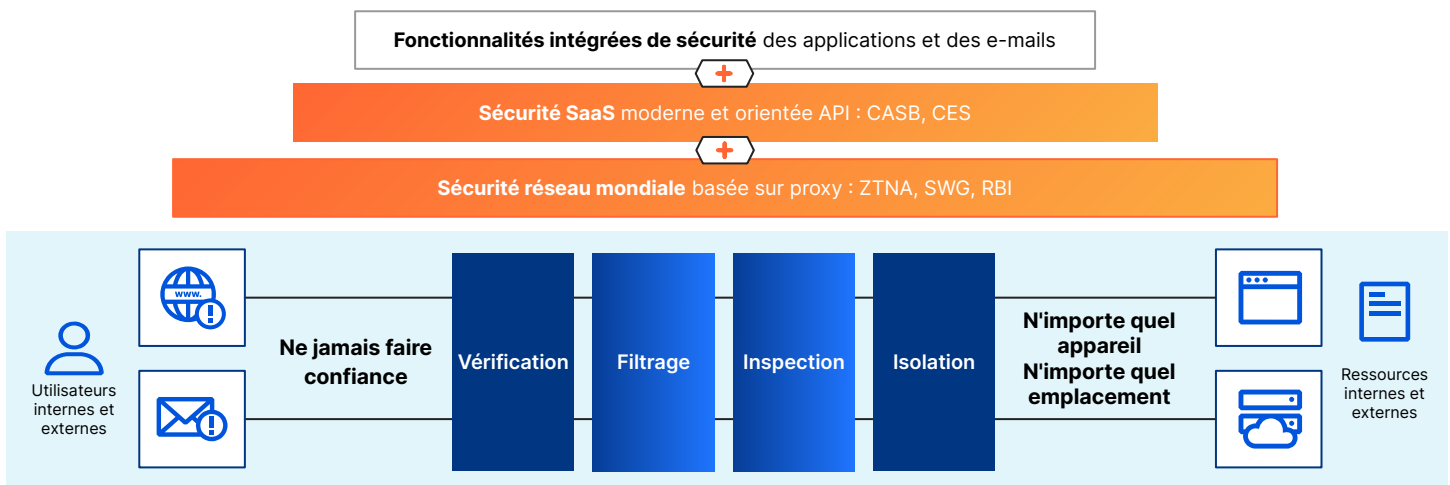
Les acteurs malveillants visent fréquemment et exploitent avec succès le haut degré de confiance bien souvent accordé aux communications par e-mail.

#### Intégrer une solution de sécurité des e-mails native du cloud

L'ajout de la solution de sécurité des e-mails dans le cloud (CES, Cloud Email Security) Area 1 en tant qu'élément d'une stratégie Zero Trust exhaustive élimine la confiance implicite entourant les e-mails afin de bloquer de manière préventive les attaques par phishing et la compromission du courrier électronique professionnel (BEC, Business Email Compromise).

L'ensemble du trafic utilisateur (dont les e-mails) est vérifié, filtré, inspecté et isolé des menaces connues, mais aussi inconnues. La solution Area 1 aide les clients à bloquer les menaces véhiculées par e-mail, à adopter une stratégie de sécurité proactive et à réduire de 90 % le temps de réponse aux incidents de phishing.

### Fonctionnement : Zero Trust pour l'ensemble du trafic e-mail, web et réseau



### Scénarios d'utilisation principaux

#### Empêcher les attaques BEC et la fraude basée sur les e-mails

Arrêtez les attaques BEC (Business Email Compromise, compromission du courrier électronique professionnel) sophistiquées et l'usurpation des comptes des fournisseurs grâce à l'analyse des sentiments, aux graphiques sociaux des partenaires, à la classification des messages et à l'analyse de la source des campagnes.

Bloquez, placez en quarantaine et faites remonter automatiquement les communications financières frauduleuses.

#### Se protéger contre les attaques multicanales

Bloquez sans effort les campagnes d'attaques visant les particuliers via plusieurs canaux de communication, comme les e-mails et Internet, en permettant aux utilisateurs de charger en toute sécurité les liens suspects ou inconnus au sein d'un navigateur distant et isolé.

Stoppez les attaques par phishing différé qui utilisent des liens comme moyens hostiles après distribution grâce à une classification des liens au moment du clic.

#### Accélérez le triage et les réponses au phishing

Libérez des cycles d'investigation de sécurité, bénéficiez de statistiques utiles sur votre environnement d'e-mails et réduisez le temps de réponse à l'aide de ressources dédiées qui améliorent les capacités de votre équipe existante afin de neutraliser rapidement les menaces véhiculées par phishing.

Profitez d'un support supplémentaire et d'une expertise en matière de sécurité grâce à nos services gérés de sécurité des e-mails.

# Sécurisation du travail hybride : la différence Cloudflare

## Une sécurité moderne pour des effectifs modernes

### Simplicité de déploiement

Cloudflare propose une plateforme uniforme et composable, pour plus de simplicité en matière de configuration et d'opérations. Grâce à leurs connecteurs uniquement logiciels et à leurs intégrations effectuées en une seule passe, les services périphériques de Cloudflare (de même que les services d'accès direct) fonctionnent tous en bonne intelligence.

Cette approche permet de proposer une meilleure expérience à vos collaborateurs et vos utilisateurs finaux.

### Résilience du réseau

Nos mesures d'automatisation du trafic de bout en bout assurent une connectivité réseau fiable, évolutive et dotée d'une protection constante depuis n'importe quel emplacement.

Avec Cloudflare, chaque service périphérique est conçu pour s'exécuter dans n'importe quel emplacement réseau, afin d'être disponible pour chaque client, contrairement aux solutions proposées par les autres fournisseurs de sécurité.

### Rapidité de l'innovation

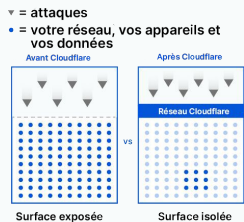
Notre architecture évolutive nous aide à développer et à proposer rapidement de nouvelles capacités de mise en réseau et de sécurité.

Qu'il s'agisse de notre adoption rapide des nouvelles normes applicables à Internet et à la sécurité ou du développement de scénarios d'utilisation à l'initiative de nos clients, notre historique de prouesses techniques parle pour lui. En outre, la fondation même de notre solution offre une liberté de choix absolue.

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

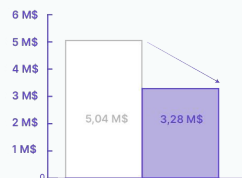
### Réduction de la surface d'attaque de

91 % ↓



### Réduction des coûts de violation de

35 % ↓



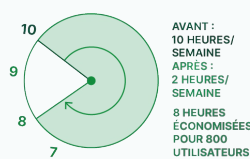
### Accélération du temps d'intégration des collaborateurs de

60 % ↑



### Réduction du temps passé à traiter les tickets informatiques de

80 % ↓



### Réduction de la latence utilisateur de

39 % ↓



## Une solution optimisée pour l'accessibilité

### Une interface de gestion unique

Simplifiez-vous la configuration grâce à un tableau de bord nativement intégré, conçu à la fois pour les politiques d'accès à Internet et aux applications.

Utilisez un tableau de bord unique pour intégrer vos fournisseurs d'identité, vos solutions de protection des points de terminaison et vos accès réseau directs (on-ramp).

### Une plateforme consolidée

Remplacez votre patchwork de clients VPN, de pare-feu sur site et d'autres solutions hétéroclites par une plateforme dotée d'un plan de contrôle unique.

Réduisez les coûts et la complexité en faisant migrer votre sécurité vers la périphérie.

### Une expérience inégalée pour l'utilisateur final

Cloudflare se situe plus près de vos utilisateurs et de vos services. Nous acheminons les requêtes plus rapidement grâce à un processus de routage optimisé et piloté par les informations sur l'ensemble de notre vaste réseau Anycast, couvrant plus de 275 emplacements dans plus de 100 pays à travers le monde.



Accélérez votre parcours Zero Trust

Essayer maintenant

Nous contacter