LIVRE BLANC

CLOUDFLARE

Débuter avec le modèle SASE : un guide pour sécuriser et rationaliser votre infrastructure de réseau

Le modèle SASE (Secure Access Service Edge) simplifie l'architecture traditionnelle en fusionnant les services réseau et de sécurité sur un réseau mondial unique. Ce livre blanc explore l'évolution en matière de sécurité des réseaux qui a abouti au modèle SASE, présente la portée des services intégrés à une solution SASE et propose les mesures concrètes à mettre en oeuvre pour adopter le modèle SASE.

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

INTRODUCTION

Inventé par Gartner en 2019, le terme SASE (Secure Access Service Edge) a été initialement proposé pour constituer une avancée majeure dans le processus de transformation numérique : des services réseau et de sécurité fortement personnalisables, intrinsèquement intégrés à la structure même d'une plate-forme cloud mondiale. Avec un taux d'adoption de 20 % attendu d'ici 2023, Gartner a affirmé que la demande de fonctionnalités SASE « redéfinirait le réseau d'entreprise et l'architecture en matière de sécurité réseau, tout en transformant radicalement le paysage concurrentiel. »[1]

Depuis, le terme s'est répandu comme une traînée de poudre dans le secteur de la sécurité informatique et des entreprises. Tandis que les fournisseurs de sécurité réseau et de réseaux SD-WAN se bousculent pour se positionner comme autant de leaders sur le marché du SASE, les entreprises se trouvent confrontées à un ensemble hétéroclite de services réseau et de sécurité qui rappelle l'infrastructure SASE, sans toutefois vraiment l'embrasser.

L'adoption du véritable modèle SASE nécessite plus qu'une accumulation de solutions ponctuelles existantes : elle exige de repenser intégralement l'infrastructure du réseau d'entreprise. Le maintien d'un strict périmètre réseau sur site ne suffit plus à protéger une main-d'œuvre toujours plus mobile et distribuée. De même, le recours à plusieurs services de sécurité pour protéger une infrastructure hybride peut s'avérer coûteux, faire du déploiement et de la gestion un véritable casse-tête pour les équipes informatiques et laisser d'immenses failles en matière de sécurité.

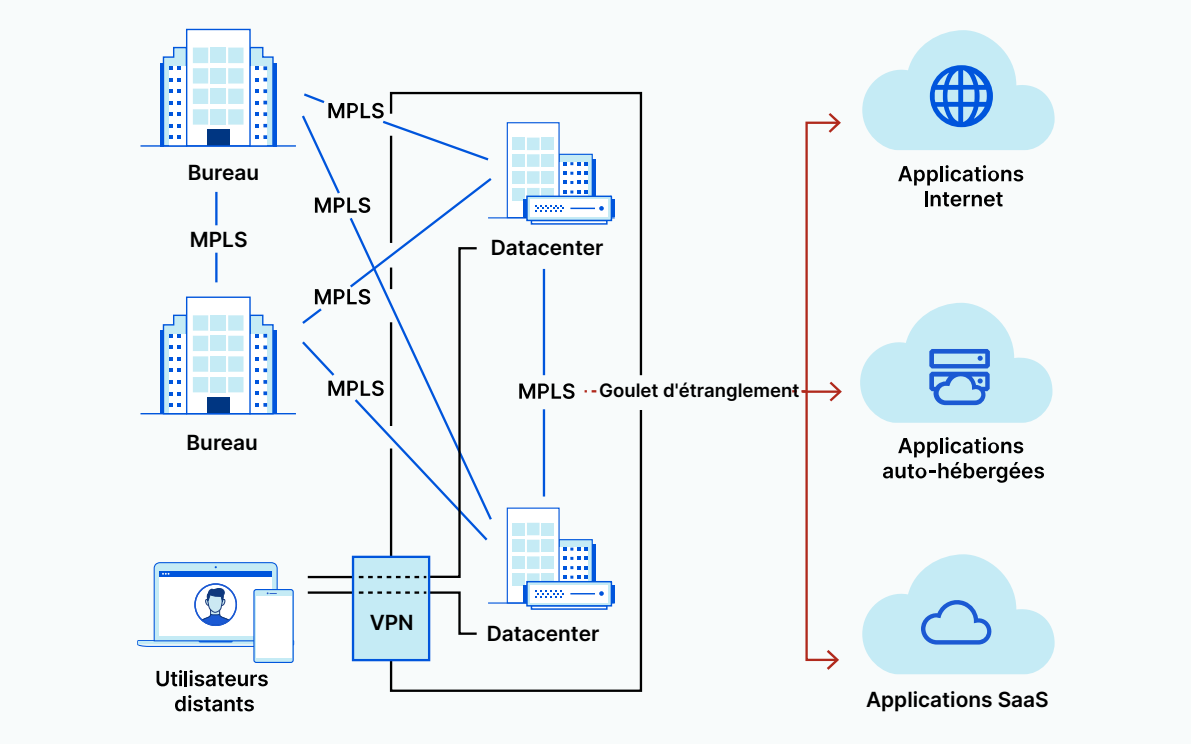
L'approche SASE relève ces défis en déplaçant le périmètre réseau des datacenters centralisés vers l'utilisateur. En consolidant la connectivité et les services de sécurité du réseau, ainsi qu'en déployant ces fonctionnalités depuis une plate-forme cloud-native unique et reposant sur les principes du Zero Trust, le modèle SASE élimine les failles de sécurité entre les services, assure une meilleure visibilité sur l'activité réseau aux équipes informatiques et simplifie le processus de migration vers le cloud.

LES ORIGINES DU SASE : ANCIEN MODÈLE

Pour comprendre le tournant décisif que représente le modèle SASE, il est important d'examiner l'évolution progressive des infrastructures et de la sécurité réseau.

Avant l'adoption généralisée du cloud, les ressources, les données et les applications des entreprises résidaient dans des équipements sur site, protégés par des pare-feu matériels et des solutions anti-DDoS physiques. Les employés présents au sein d'une agence accédaient aux ressources internes au moyen de connexions privées, filtrées par des pare-feu réseau. Les utilisateurs qui se connectaient depuis des sites distants le faisaient généralement via un VPN, un équipement sujet à la latence et présentant un coût élevé pour éviter les encombrements et corriger les vulnérabilités, tout en offrant des performances médiocres en termes d'expérience mobile.

À l'origine de cette configuration était la crainte de l'Internet ouvert : un outil initialement conçu dans une optique de résilience, sans toutefois tenir compte des besoins des entreprises en matière de performances et de sécurité. Internet s'étant révélé intrinsèquement vulnérable aux attaques, les organisations ont choisi d'établir leurs propres réseaux privés et de sécuriser (souvent, avec une efficacité limitée) leurs données, leurs applications et leurs ressources au moyen de pare-feu matériels et d'équipements anti-DDoS physiques. Le trafic entrant était acheminé vers des datacenters centralisés à des fins d'inspection et de filtrage, créant ainsi un phénomène de « hairpinning », également appelé « effet trombone ».



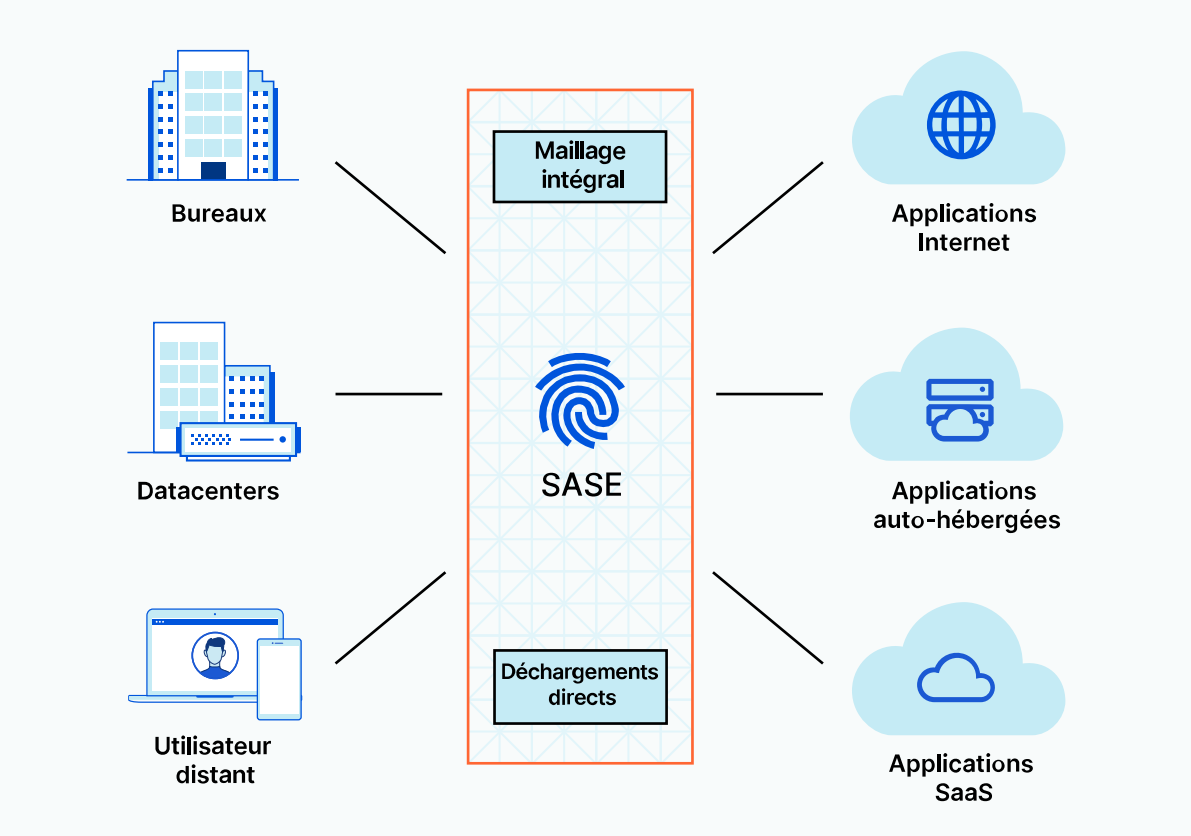
Ce modèle de sécurité réseau se montrait à la fois coûteux et complexe. En outre, les entreprises restaient vulnérables aux violations de données et aux menaces internes. Un pirate parvenant à franchir le périmètre réseau pouvait causer des dommages considérables au sein d'une entreprise en diffusant des rançongiciels, en usurpant le contrôle de comptes utilisateur[2] et en dérobant de précieuses données clients.[3]

Avec l'avènement du cloud et des services SaaS, les organisations ont désormais plus de liberté et de flexibilité pour repenser l'infrastructure de leur réseau, car les applications, les données et les collaborateurs n'ont plus nécessairement besoin de résider au sein d'équipements sur site.

LES ORIGINES DU SASE : NOUVEAU MODÈLE

Cette liberté s'accompagne toutefois de nouveaux défis en matière de sécurité. Les équipes informatiques ont la charge de protéger un ensemble hétérogène de services sur site et dans le cloud, tout en sécurisant une main-d'œuvre toujours plus mobile et distante.[4] Pour y parvenir, elles doivent souvent gérer du matériel coûteux et superposer les services de sécurité ponctuels de différents fournisseurs, dont la mise en œuvre et la gestion peuvent s'avérer fastidieuses et difficiles.

La prochaine évolution en matière de sécurité des réseaux ne ressemblera probablement pas à l'approche matérielle qui protégeait les infrastructures en étoile traditionnelles (hub-and-spoke) ni aux complexes solutions de contournement requises par une architecture cloud hybride. Elle prendra plutôt la forme d'une infrastructure SASE, capable de consolider les services réseau et de sécurité, avant de les déployer en tant que service intégré.



Plutôt que de dépendre d'équipements physiques inefficaces ou d'assembler des services de sécurité cloisonnés, le modèle SASE propose une approche rationalisée de la sécurité des réseaux. Il remplace les procédures de redirection complexes (backhauling) par la périphérie du réseau Internet, afin de permettre aux entreprises d'acheminer, d'accélérer, de vérifier, de filtrer, d'isoler et d'inspecter le trafic en une seule passe. Associé à une connectivité WAN à maillage intégral, des politiques d'accès Zero Trust et à une protection contre les menaces au niveau du réseau, le modèle SASE élimine la nécessité de déployer des solutions traditionnelles mettant en œuvre des VPN et des circuits MPLS, appuyées par des pare-feu matériels, un proxy et des équipements de protection anti-DDoS physiques. Les entreprises bénéficient ainsi d'une meilleure visibilité et d'un meilleur contrôle sur leurs configurations de sécurité réseau.

DÉFINIR LA PORTÉE DU SASE : FONCTIONNALITÉS ESSENTIELLES

Fondé sur le cloud, le modèle de sécurité SASE associe un réseau étendu défini par logiciel à des services de sécurité réseau essentiels déployés à la périphérie du cloud. La plupart des offres SASE se caractérisent par cinq fonctionnalités principales :

Construction et gestion de réseaux

L'utilisation d'un réseau étendu défini par logiciel (SD-WAN) permet aux entreprises d'établir des réseaux d'entreprise privés sans recourir à des routeurs physiques ou des circuits MPLS (Multiprotocol Label Switching). Malgré certaines vulnérabilités inhérentes en termes de sécurité, cette architecture logicielle virtuelle leur offre davantage de flexibilité en matière de création et de maintenance de leur infrastructure réseau.

Filtrage du trafic

Les passerelles web sécurisées (SWG) permettent de lutter contre les cybermenaces et les fuites de données en filtrant les contenus indésirables du trafic web, en bloquant les comportements non autorisés d'utilisateurs et en appliquant les politiques de sécurité de l'entreprise. Elles incluent généralement le filtrage des URL, la détection et le blocage des logiciels malveillants et le contrôle des applications, entre autres fonctionnalités.

Sécurisation des données

Un Cloud Access Security Broker (CASB) assure plusieurs tâches de sécurité pour les services hébergés dans le cloud (comme les applications SaaS, IaaS et PaaS). Les CASB standard sécurisent les données confidentielles par le biais de mesures de contrôle des accès et de prévention des pertes de données. Ils révèlent également les phénomènes de Shadow IT et garantissent le respect des réglementations en matière de confidentialité des données.

Connexion des utilisateurs aux applications

L'accès réseau Zero Trust (ZTNA) nécessite une vérification en temps réel de chaque utilisateur pour chaque application protégée, afin de protéger les ressources internes et d'offrir une défense contre les violations de données potentielles. Avec une approche Zero Trust, aucune entité n'est automatiquement approuvée tant que son identité n'a pas été vérifiée, même si elle se trouve déjà dans le périmètre d'un réseau privé.

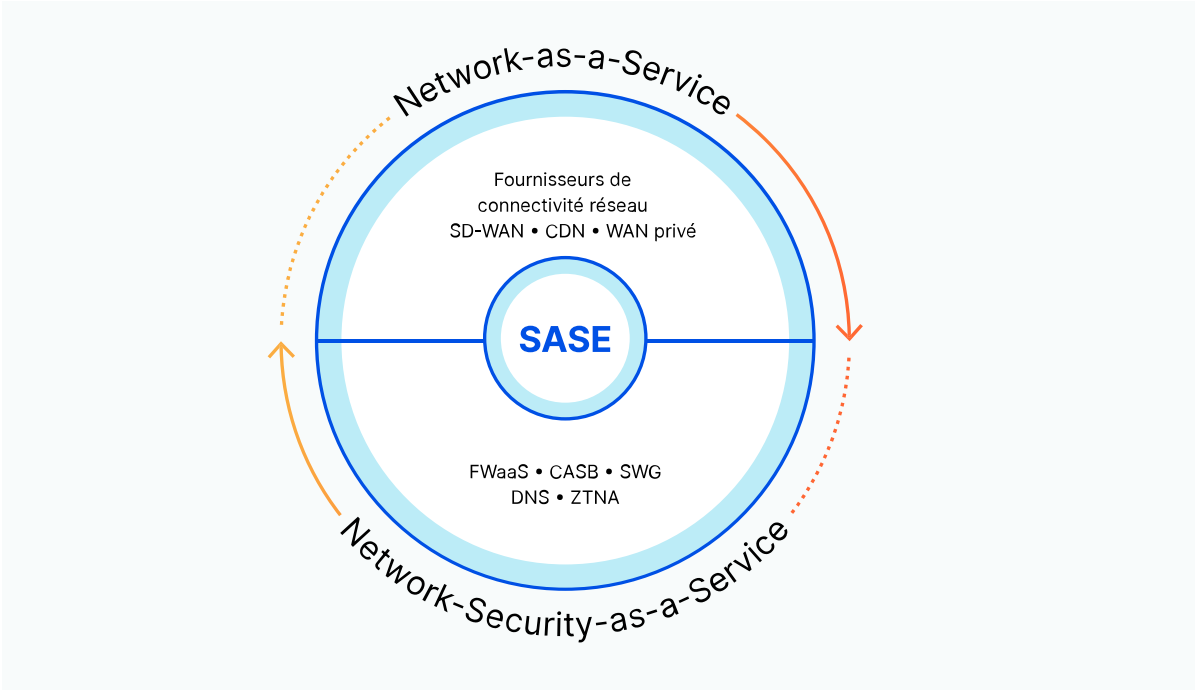
Protection des applications et de

l'infrastructure

Les pare-feu cloud (FWaaS) protègent l'infrastructure et les applications dans le cloud contre les cyberattaques grâce à un ensemble de fonctionnalités de sécurité, telles que le filtrage d'URL, la prévention des intrusions et la gestion uniforme des politiques.

DÉFINIR LA PORTÉE DU SASE : LES MEILLEURES FONCTIONNALITÉS DE LEUR CATÉGORIE

Bien qu'une solution SASE classique inclue les cinq services décrits ci-dessus, cette liste constitue davantage un point de départ qu'un ensemble d'exigences strictes. Fondamentalement, le modèle SASE repose sur la convergence de deux fonctionnalités fondamentales et distinctes : l'architecture réseau basée sur logiciel et les services de sécurité dans le cloud. Les fournisseurs peuvent ensuite ajouter ou supprimer des services, selon les besoins.



Si un réseau SD-WAN permet d'aider les clients à gérer le « dernier segment » en matière de connectivité réseau, il ne peut pas assurer directement la sécurité, les performances et la fiabilité du « segment intermédiaire », situé entre les utilisateurs et les applications. Au mieux, il pourra optimiser les connexions de bout en bout, en s'appuyant sur plusieurs réseaux mondiaux et en enchaînant plusieurs services de sécurité, selon un processus qui s'avère complexe et coûteux. Un fournisseur SASE disposant d'une solution WAN-as-a-Service intégralement construite par ses soins (avec ou sans SD-WAN) permet aux clients de n'avoir à gérer qu'un seul réseau mondial, tout en profitant de fonctionnalités d'amélioration de la sécurité, des performances et de la fiabilité intégrées par défaut. Employées conjointement, les solutions SWG, CASB et ZTNA permettent de réduire fortement les risques. Toutefois, cette combinaison laisse toujours de nombreuses failles ouvertes dans tous les scénarios d'utilisation, qu'il s'agisse de se prémunir contre les menaces ou de protéger les données. Un fournisseur SASE ayant développé son service d'isolement du navigateur dès le départ, afin d'intégrer nativement ces solutions au sein de chaque datacenter, permet d'éliminer ces vulnérabilités.

AVANTAGES DE L'APPROCHE SASE

Si le modèle SASE continue à évoluer, sa mise en œuvre peut varier considérablement d'un fournisseur à l'autre et d'une entreprise à l'autre. La plupart des solutions SASE partagent toutefois plusieurs avantages essentiels communs par rapport aux configurations de sécurité réseau sur site et hybrides :

Mise en œuvre simplifiée

En consolidant les services réseau et de sécurité, le modèle SASE élimine la nécessité d'incorporer des services fondés sur le, cloud, de déployer des équipements sur site et d'investir du temps, de l'argent et des ressources internes dans l'actualisation de ces composants afin de faire face aux nouvelles menaces.

Gestion simplifiée des politiques

Le modèle SASE permet aux entreprises de définir, surveiller, ajuster et appliquer des politiques d'accès sur l'ensemble des emplacements, utilisateurs, appareils et applications. Les attaques et les menaces entrantes peuvent être identifiées et atténuées depuis un portail unique, plutôt qu'être surveillées et gérées individuellement à l'aide de différents outils de sécurité dédiés.

Accès réseau basé sur l'identité

L'approche SASE repose largement sur le modèle de sécurité Zero Trust, dans lequel l'identité et l'accès des utilisateurs sont définis en fonction de différents facteurs, tels que la situation géographique de l'utilisateur, l'heure de la journée, les règles de sécurité de l'entreprise, les politiques de conformité et le processus d'évaluation continue des risques et de la confidentialité. Ce niveau de sécurité (qui constitue une avancée significative par rapport aux VPN, trop permissifs et intrinsèquement vulnérables) offre une protection contre les violations de données, tant externes qu'internes, ainsi que d'autres attaques.

Réduction de la latence

L'approche SASE permet de réduire la latence et **d'améliorer** les performances en acheminant le trafic réseau sur un réseau périphérique mondial, au sein duquel le trafic est traité au plus près de l'utilisateur. Les optimisations de routage peuvent contribuer à déterminer le chemin réseau le plus rapide en fonction de l'encombrement du réseau et d'autres facteurs.

Réseau mondial

La structure SASE s'appuie sur un réseau mondial unique, permettant aux entreprises d'étendre le périmètre de leur réseau à n'importe quel utilisateur, bureau régional, application ou appareil distant et de bénéficier d'une meilleure visibilité et d'un contrôle renforcé sur l'ensemble leur infrastructure de réseau.

DÉBUTER AVEC LE SASE

L'adoption du modèle SASE peut paraître décourageante pour les entreprises qui ont investi beaucoup de temps, de ressources et d'argent dans des configurations sur site élaborées, qui gèrent des ensembles complexes de services de sécurité dans le cloud ou qui s'adaptent encore à l'avenir du télétravail, mais cette impression ne doit pas constituer une fatalité.

Voici cinq mesures pratiques que vous pouvez prendre pour faire vos premiers pas dans l'univers du SASE :

1. Protégez vos effectifs en télétravail.

Déployez une solution ZTNA capable de réduire la dépendance à votre VPN (voire de le supprimer purement et simplement), mais aussi de protéger les données et les ressources de l'entreprise contre les menaces internes et externes, tout en améliorant l'expérience utilisateur. La migration de votre passerelle web sécurisée, de votre pare-feu et de vos navigateurs vers la périphérie vous permet de filtrer, isoler et inspecter le trafic sans le réacheminer vers un datacenter centralisé.

2. Placez les bureaux régionaux derrière un périmètre cloud.

Appliquez une architecture Zero Trust dans les bureaux régionaux. Elle vous permettra d'éliminer la nécessité de déployer des équipements de sécurité physiques sur site (gestion unifiée des menaces, etc.), qui peuvent s'avérer coûteux à entretenir et se révéler inefficaces au sein d'un paysage des menaces en évolution rapide.

3. Déplacez la protection anti-DDoS vers la périphérie.

Débarrassez-vous des équipements anti-DDoS physiques et protégez les réseaux d'entreprise contre les attaques grâce à une protection cloud-native contre les attaques DDoS visant la couche réseau, capable de détecter et d'atténuer les menaces en temps réel.

4. Faites migrer vos applications vers le cloud.

Afin de suivre les évolutions de votre entreprise, faites migrer les applications auto-hébergées de vos datacenters vers le cloud et assurez-vous d'appliquer des politiques de sécurité cloud cohérentes à l'ensemble du trafic.

5. Remplacez les équipements de sécurité physiques sur site par une application unifiée de politiques cloud-native.

Réduisez le coût et la complexité de la maintenance des équipements réseau en déplaçant l'application des politiques vers la périphérie, où vous pouvez surveiller et gérer l'ensemble du trafic, des schémas d'attaque et des politiques de sécurité en une seule passe et depuis une interface unique.

LA SOLUTION SASE DE CLOUDFLARE S'APPELLE CLOUDFLARE ONE

Cloudflare One, la solution SASE de Cloudflare, constitue une plate-forme de Network-as-a-Service (réseau en tant que service) Zero Trust qui connecte de manière dynamique les utilisateurs aux ressources de l'entreprise. Elle profite également de contrôles de sécurité basés sur l'identité et mis en œuvre à proximité des utilisateurs, peu importe leur situation géographique.

Grâce aux services réseau de Cloudflare One, les équipes chargées de l'infrastructure peuvent :	**Grâce aux services Zero Trust de Cloudflare One, les équipes chargées de la sécurité informatique peuvent :**
• Utiliser le réseau mondial de Cloudflare en tant que WAN. • Remplacer les équipements physiques traditionnels par un pare-feu réseau cloud-native. • Améliorer les performances des applications et la latence affectant l'utilisateur final.	• Connecter les utilisateurs aux ressources de manière simple et sécurisée, sans VPN. • Bloquer les mouvements latéraux, les rançongiciels, les logiciels malveillants et le phishing. • Améliorer l'expérience des utilisateurs finaux et les besoins d'administration, en particulier pendant l'intégration de nouveaux utilisateurs.

Pourquoi Cloudflare ?

Simplicité de déploiement et de gestion

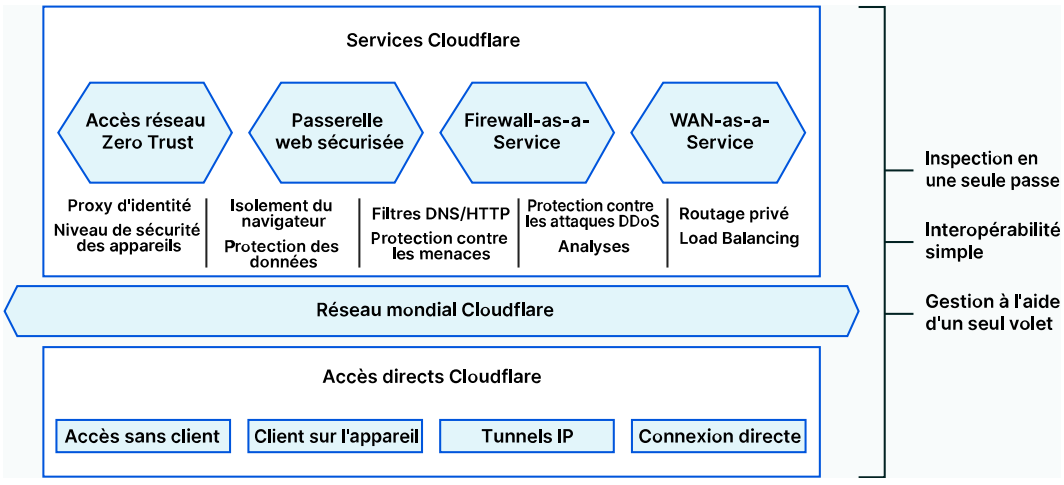
Chaque service Cloudflare One s'exécute dans chacune des plus de 250 villes couvertes par notre réseau à travers le monde. Nul besoin d'intégrer manuellement plusieurs produits spécifiques lorsque vous évoluez vers le modèle SASE.

Sécurité et vitesse constantes, partout dans le monde

Chaque datacenter Cloudflare assure l'inspection et le routage du trafic, et ce en une seule passe. Les utilisateurs bénéficient ainsi de la même protection partout dans le monde, sans perte de vitesse due à la latence ou au « hairpinning » (effet trombone).

Une solution qui se connecte à celles que vous utilisez déjà

Cloudflare exploite le réseau le plus puissant et le plus interconnecté du monde, et Cloudflare One prend en charge les fournisseurs d'identité, de points de terminaison et de cloud que vous utilisez déjà. Le tout au sein d'un produit facile à utiliser et ne nécessitant qu'une seule passe d'intégration.



LA SOLUTION SASE DE CLOUDFLARE S'APPELLE CLOUDFLARE ONE

La solution Cloudflare One vous propose les fonctionnalités de sécurité et de connectivité dont vous avez besoin pour connecter vos utilisateurs, applications et bureaux régionaux au sein d'un monde nomade.

<table>
<tr><th colspan="2">Cloudflare One</th></tr>
<tr><td>Accès réseau Zero Trust
Connectez n'importe quel utilisateur à n'importe quel réseau privé ou application, plus rapidement et avec plus de sécurité qu'un VPN, en limitant les mouvements latéraux et en appliquant des règles basées sur l'identité et le contexte.

Fonctionnalités SASE essentielles :
• Connexion des utilisateurs aux applications
• Sécurisation des données</td><td>WAN-as-a-Service
Déployez une connectivité point à point (« any-to-any ») dotée d'une plus grande rapidité, de mesures de sécurité intégrées et d'une résilience accrue en remplaçant votre ancienne architecture WAN par notre réseau d'infrastructure privé mondial.

Fonctionnalité SASE essentielle :
• Construction et gestion de réseaux</td></tr>
<tr><td>Passerelle web sécurisée
Bloquez les menaces Internet connues et inconnues (et contrôlez facilement les flux de données) en appliquant des règles DNS, HTTP, réseau et d'isolement du navigateur avec une inspection SSL illimitée.

Fonctionnalités SASE essentielles :
• Filtrage et inspection du trafic
• Sécurisation des données</td><td>Firewall-as-a-Service
Contrôlez les accès (et arrêtez les attaques DDoS et autres menaces) en appliquant des règles d'inspection dynamique à l'ensemble du trafic entrant et sortant, tout en préservant la rapidité de votre système.

Fonctionnalité SASE essentielle :
• Protection des applications et de l'infrastructure</td></tr>
<tr><td colspan="2">Réseau mondial Cloudflare
Présent à moins de 50 ms de 95 % de la population connectée à Internet, notre réseau couvre plus de 250 villes. Fort de sa capacité de plus de 100 Tb/s, il intègre plus de 10 000 interconnexions et présente une garantie de disponibilité de 100 % dans le cadre du SLA.</td></tr>
<tr><td>Accès sans client
Intégrez n'importe quel utilisateur ou appareil (notamment les utilisateurs tiers et les appareils personnels des utilisateurs) grâce à un accès sécurisé par navigateur aux applications auto-hébergées et SaaS, au-delà de la simple utilisation du protocole HTTP.</td><td>Tunnels IP
Intégrez des sous-réseaux IP publics et privés entiers via des annonces de routage BGP Anycast, par l'intermédiaire de tunnels GRE ou de notre connecteur Tunnel au sein d'environnements cloud ou sur site.</td></tr>
<tr><td>Client sur l'appareil
Intégrez les appareils Windows, macOS, iOS, Android, ChromeOS et Linux pour un accès client sécurisé à l'ensemble des réseaux privés, applications ou destinations Internet.</td><td>Connexion directe
Intégrez physiquement ou virtuellement votre infrastructure réseau sur plus de 1 600 sites de colocalisation, plutôt que sur l'Internet public, pour une expérience plus fiable et plus sûre.</td></tr>
</table>

RÉSULTATS OPÉRATIONNELS LIÉS À L'UTILISATION DE CLOUDFLARE ONE

↓91 %

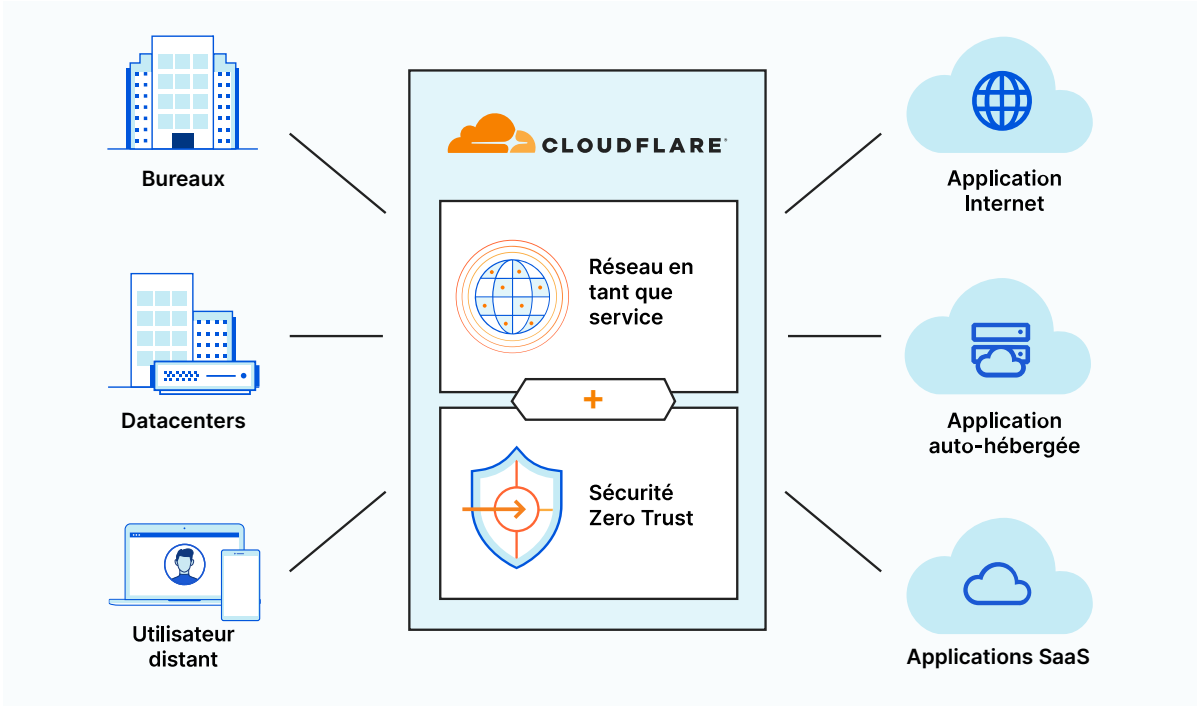
Réduisez la surface d'attaque de jusqu'à 91 % en isolant la navigation à haut risque des systèmes des utilisateurs finaux et en séparant l'accès aux applications des réseaux.

10 → 1

Réduisez le coût total de possession et accélérez votre activité en consolidant jusqu'à 10 produits spécifiques sur une plate-forme unique

↑60 %

Intégrez les nouveaux employés et les sous-traitants jusqu'à 60 % plus rapidement lorsque vous connectez des utilisateurs aux ressources par l'intermédiaire de Cloudflare plutôt que par un VPN.



En savoir plus sur Cloudflare One

Cliquez ici

RÉFÉRENCES

1. Gartner, « The Future of Network Security Is in the Cloud ». Analyste(s) : Neil MacDonald, Lawrence Orans, Joe Skorupa. 30 août 2019. Gartner.

2. Twitter Inc. « An update on our security incident ». Twitter. Accès le 27 octobre 2020.

3. Marriott International News Center. « Marriott International Notifies Guests of Property System Incident ». Marriott. Accès le 27 octobre 2020.

4. Bursztynsky, Jessica. « Dropbox is the latest San Francisco tech company to make remote work permanent ». CNBC. CNBC. Accès le 27 octobre 2020.