CLOUDFLARE

DOSSIER DE SOLUTION

Security Service Edge (SSE)

Planifier la consolidation de services de sécurité avec une adoption à votre rythme

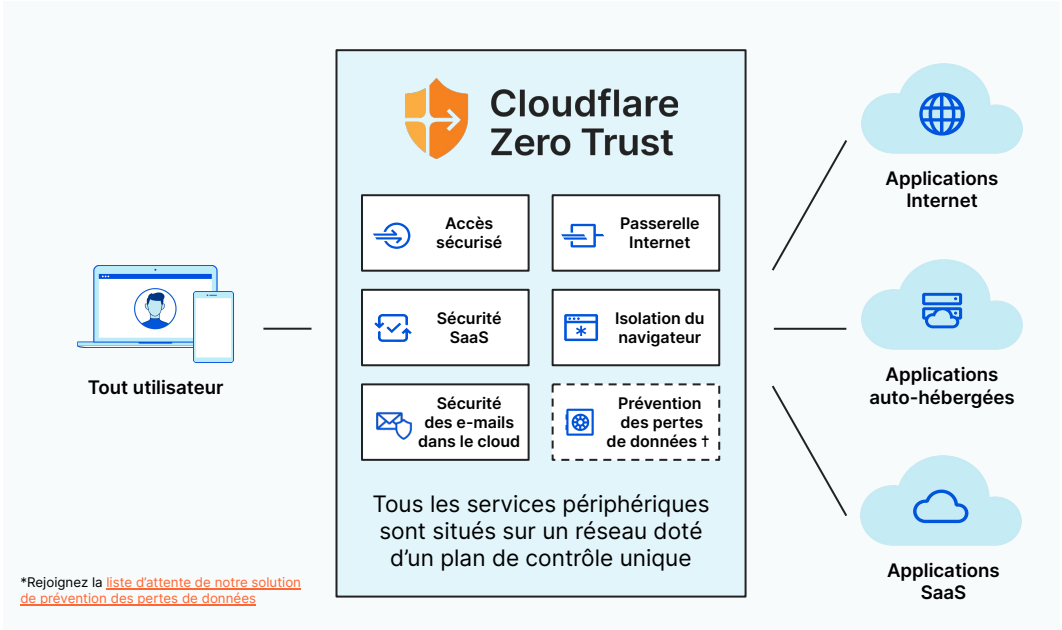
Convergence orientée cloud

La complexité inhérente à la gestion de plusieurs solutions dédiées pousse la plupart des organisations à consolider le choix de leurs fournisseurs préférés. Aujourd'hui, des capacités « inégalées dans leur catégorie » et des plateformes étendues ne sont pas forcément mutuellement exclusives. Tandis que la majorité des acheteurs informatiques optent pour la consolidation, les fournisseurs de solutions de sécurité répondent à l'appel en amplifiant la valeur de leurs plateformes de sécurité au-delà de ce que pourrait accomplir individuellement chaque service.

L'approche SSE, qui se situe entre les produits dédiés et la consolidation intégrale, se concentre davantage sur les capacités de sécurité que la plupart des offres Secure Access Service Edge (SASE), car elle n'est pas liée à l'infrastructure réseau. Selon nous, notre plateforme Zero Trust correspond à l'approche SSE de Gartner et permet la convergence de produits dédiés encore récemment distincts, à l'image des solutions ZTNA, VPN, SWG, CASB, RBI, Firewall as a service (FWaaS) et du filtrage DNS.

« Consolidez les fournisseurs et réduisez la complexité et les coûts lors du renouvellement des contrats de vos solutions SWG, CASB et VPN (en les remplaçant par une approche ZTNA). Tirez parti d'un marché convergent qui émerge en réunissant ces services. » [1]

Gartner



*Rejoignez la liste d'attente de notre solution de prévention des pertes de données

Remplacement du VPN

Simplifiez et sécurisez la connexion de n'importe quel utilisateur à n'importe quelle ressource

Sécurité SaaS

Visibilité et contrôle des applications, dont le courrier électronique

Protection Internet

Protégez vos données contre les menaces sur n'importe quels port et protocole

Modernisation de la sécurité

Productivité améliorée, opérations plus simples, surface d'attaque réduite

Le SSE en tant que passerelle vers le SASE

Si la convergence des services de sécurité et des services à la périphérie du réseau est l'objectif ultime de l'approche SASE, certaines entreprises n'aspireront jamais à consolider toutes leurs solutions auprès d'un revendeur unique, en raison de leur historique et de leur infrastructure actuelle. Quelle que soit votre stratégie SASE à long terme, Cloudflare peut vous aider à moderniser la sécurité, à transformer votre réseau d'entreprise ou les deux.

Solution SASE mono-fournisseur

Pour les entreprises qui aspirent à unifier entièrement la sécurité et les services à la périphérie du réseau auprès d'un fournisseur unique, notre plateforme SASE Cloudflare One propose une solution Network-as-a-Service Zero Trust bâtie sur notre réseau, qui couvre plus de 275 villes à travers le monde.

Solution SASE multi-fournisseurs

Pour les entreprises disposant de déploiements SD-WAN matures ou d' équipes disjointes chargées de la sécurité et des réseaux, Cloudflare Zero Trust peut aider à moderniser la sécurité et réaliser un déploiement SSE en tirant parti des partenariats SD-WAN pour une solution SASE multi-fournisseurs.

Adoption d'une solution SSE composable

L'évolution vers une solution SSE dans le cloud n'est pas envisageable du jour au lendemain ; Cloudflare Zero Trust aide les organisations à se débarrasser progressivement de leur matériel, à leur rythme. De nombreuses entreprises débutent leur évolution vers l'approche Zero Trust en complétant leur VPN avec une solution ZTNA, avant de remplacer entièrement leur VPN. La rationalisation de la sécurité SaaS est une deuxième priorité essentielle pour la plupart des entreprises, et les stratégies plus larges de lutte contre les menaces et de protection des données suivent de près.

Notre architecture uniforme et composable facilite l'adoption modulaire des services de sécurité. Les entreprises peuvent déployer des combinaisons personnalisées de services adaptées à leurs scénarios d'utilisation prioritaires ; une approche « tout ou rien » n'est pas nécessaire.

> « Inventoriez les équipements et les contrats pour mettre en œuvre une élimination progressive, sur plusieurs années, des équipements de sécurité périmétrique et des succursales en faveur du déploiement d'une approche dans le cloud. Ciblez la consolidation des équipements sur site, idéalement dans un appareil unique. » [1]
>
> Gartner

L'intégration soutient l'innovation

Tous les services de Cloudflare s'exécutent sur chaque serveur dans chaque datacenter composant notre immense réseau mondial, assurant une couverture sans faille ni incohérence. Ceci nous aide à assurer l'inspection en une seule passe et à garantir un niveau maximal de sécurité, de performances et de fiabilité.

Les services nativement intégrés offrent également des possibilités plus créatives d'associer les fonctionnalités de plusieurs services et de répondre aux scénarios d'utilisation souhaités par nos clients. À mesure que ces lignes de produits se rapprochent, l'interaction entre les services nous aide à résoudre des scénarios plus avancés et à moderniser véritablement la sécurité.

Renforcez la sécurité de l'accès d'utilisateurs tiers

- Les solutions ZTNA et RBI s'intègrent pour offrir un accès sécurisé aux utilisateurs tiers tels que les sous-traitants et les partenaires
- Vérifiez les informations contextuelles pour déterminer les autorisations et servez les applications dans des navigateurs isolés pour protéger les données
- Le fonctionnement sans client des deux services simplifie le déploiement, sans nécessiter de téléchargement

Visualisez et auditez les sessions SSH

- Les solutions ZTNA et SWG s'intègrent pour offrir une visibilité de l'ensemble des sessions SSH, permettant une surveillance des accès privilégiés
- Simplifiez l'accès SSH avec des sessions SSH sans client, dans un navigateur, avec un accès ZTNA
- Proposez une visibilité de la session SSH au niveau de la couche réseau ; enregistrez chaque commande en utilisant la passerelle SWG en tant que proxy

Simplifiez les flux de résolution SaaS

- Les solutions SWG et CASB s'intègrent pour déployer un flux de travail de « localisation et réparation » ; et bloquer une partie ou la totalité de l'activité SaaS suspecte directement depuis les résultats de sécurité du CASB
- Accroître la visibilité de la solution SaaS pour aider à détecter et corriger les problèmes pouvant entraîner des fuites de données ou des violations de la conformité

Déployez une meilleure protection contre le phishing

- Les solutions de sécurité des e-mails et RBI s'intègrent pour lutter contre les attaques par phishing sophistiquées et la compromission des adresses e-mail professionnelles (BEC)
- Aucune solution d'information prédictive sur les menaces n'est parfaite ; l'ouverture dans un navigateur isolé des liens contenus dans les e-mails offre une couche de protection supplémentaire

Commencez votre parcours vers un réseau plus rapide, plus fiable et plus sécurisé

Essayer maintenant

Pas encore prêt à l'essayer ? Apprenez-en davantage sur Cloudflare One

[1] *Gartner Hype Cycle™ for Network Security, 2021*