CLOUDFLARE

E-BOOK

Guide du RSSI : l'adoption du SASE

Évaluer les plateformes SASE à l'aune des scénarios d'utilisation prioritaires

La mission visant à réaliser la cyber-résilience

Le National Institute of Standards and Technology (NIST) définit la cyber-résilience comme la capacité à anticiper, résister, récupérer et s'adapter aux conditions difficiles, aux tensions, aux attaques ou aux compromissions des systèmes qui utilisent ou s'appuient sur des ressources informatiques.

Or, s'il permet de réduire le coût d'atténuation des violations, le renforcement de la cyber-résilience présente également plusieurs défis :

- **Les cybercriminels continuent de faire évoluer leurs tactiques :** le panorama des menaces devient de plus en plus difficile à sécuriser pour les entreprises à mesure que les acteurs malveillants développent davantage de techniques, de procédures et d'outils sophistiqués.
- **Les environnements informatiques gagnent en complexité :** du fait de l'abondance d'applications et d'appareils connectés sur les architectures multicloud, la sécurisation de ces environnements constitue un processus coûteux et compliqué.
- **Les équipes internes sont surchargées :** les entreprises peuvent se retrouver face à des contraintes en matière de ressources, lorsque les budgets se resserrent et que les équipes internes sont mises à rude épreuve.

Pour surmonter ces difficultés, de nombreux RSSI font appel à un cadre SASE (Secure Access Service Edge, service d'accès sécurisé en périphérie). À la différence des approches plus anciennes en matière de connectivité réseau, l'architecture SASE unifie la sécurité et les fonctions réseau sur une plateforme cloud unique, pour plus de cohérence dans la visibilité et le contrôle. Le SASE place les mesures de contrôle du réseau en périphérie du cloud (et non au sein du datacenter de l'entreprise) afin de permettre aux entreprises de proposer un accès simple et sécurisé à n'importe quel utilisateur, application, appareil ou réseau, indépendamment de sa position géographique.

Ce guide présente certains des scénarios d'utilisation du SASE les plus courants et décrit les étapes principales nécessaires au lancement de votre déploiement SASE, afin de vous permettre de renforcer votre cyber-résilience et d'obtenir des résultats rapides.

Scénario d'utilisation n° 1 :

Adopter l'accès réseau Zero Trust (ZTNA)

Le fait de se reposer sur une sécurité traditionnelle, basée sur le périmètre, pour l'organisation du travail hybride, des environnements multicloud et des appareils non gérés laisse les entreprises aux prises avec une visibilité limitée, des configurations conflictuelles et un risque excessif. Une approche Zero Trust (dans laquelle des mesures granulaires de contrôle des accès garantissent que les entités ne se voient accorder aucune confiance par défaut) peut vous aider à moderniser votre stratégie de sécurité de différentes manières :

Remplacement de la sécurité traditionnelle basée sur des équipements physiques

Les mesures de contrôle réseau périmétriques traditionnelles, comme les VPN (Virtual Private Network, réseau virtuel privé) peuvent être difficiles à faire évoluer. De même, elles ont une incidence sur la visibilité et compliquent la tâche aux équipes de sécurité qui tentent de repérer et de remédier aux attaques. Le modèle SASE propose une alternative sécurisée en mettant en place l'accès réseau Zero Trust (Zero Trust Network Access, ZTNA), tout en routant et en traitant le trafic réseau sur un réseau cloud mondial, afin de réduire à la fois les frictions au niveau de l'utilisateur final et les mouvements latéraux.

Gestion de l'accès des appareils

Le fait d'accorder un accès à des utilisateurs tiers, comme des sous-traitants, des agences et des fournisseurs, peut introduire des risques lorsque les entreprises surprovisionnent accidentellement des privilèges ou donnent un accès à des appareils non gérés. Le SASE permet aux entreprises de définir des politiques Zero Trust sans client, afin de s'assurer que les utilisateurs tiers n'ont accès qu'aux ressources dont ils ont besoin.

Prévention des attaques par rançongiciel

Les rançongiciels peuvent se propager rapidement sur l'intégralité du réseau et, dans certains cas, peuvent même se propager à plusieurs réseaux ou entreprises. Le SASE contribue à prévenir la propagation des rançongiciels en révoquant les accès aux réseaux et aux applications dès la détection de l'infection. Soutenue par le principe Zero Trust de « moindre privilège vis-à-vis du contrôle des accès », cette approche complique la tâche des acteurs malveillants qui tentent d'élever leurs privilèges et d'effectuer des mouvements latéraux au sein d'un réseau.

Limiter l'exposition des données

L'exposition et l'exfiltration de données peuvent représenter une menace sérieuse pour les entreprises lorsque les utilisateurs importent ou distribuent des informations sensibles sur des applications autorisées et non autorisées. Les politiques SASE Zero Trust peuvent empêcher l'exposition des données en limitant le nombre d'applications auxquelles chaque utilisateur a accès, tout en analysant les suites SaaS populaires à la recherche de données sensibles et d'erreurs de configuration.

ÉTUDE DE CAS

Adopter le Zero Trust

Un fournisseur de télécommunications figurant au Fortune 500 s'est servi de la plateforme SASE de Cloudflare pour sécuriser son environnement de travail hybride regroupant plus de 100 000 collaborateurs autour de centaines d'applications hébergées sur AWS, Azure et d'autres environnements cloud. Grâce à une architecture réseau Zero Trust basée sur l'identité, à une passerelle web sécurisée et à des mesures de contrôle des accès unifiées, l'entreprise a pu protéger ses utilisateurs contre les menaces sans avoir besoin de jongler avec plusieurs interfaces de définition de politiques, VPN et services de filtrage Internet.

Scénario d'utilisation n° 2 :

Protéger les surfaces d'attaque

La transformation numérique et le télétravail ont élargi la surface d'attaque. Davantage d'utilisateurs dispersés et d'appareils non gérés ont désormais besoin d'un accès aux ressources internes. Toutefois, l'extension des pare-feu sur site au cloud et la mise à l'échelle des réseaux par l'intermédiaire de VPN peuvent augmenter l'exposition aux menaces (internes et externes), tout en réduisant simultanément la visibilité. Grâce à une architecture SASE, les entreprises peuvent étendre leur visibilité et leur contrôle afin de soutenir un modèle « sans périmètre » et de mettre en place une protection cohérente de la manière suivante :

Éviter le phishing multicanal

Les acteurs malveillants lancent souvent des attaques de phishing via les canaux sur lesquels les utilisateurs ont tendance à relâcher leur garde concernant l'endroit où ils cliquent, notamment sur les outils qui ne sont généralement pas protégés par des mesures de contrôle de la sécurité du courrier électronique. Une plateforme SASE unifiée permet d'activer une protection complète sur l'ensemble de vos environnements afin d'atténuer le risque de vol d'identifiants, d'usurpation de compte et d'exfiltration de données.

Protéger les collaborateurs en télétravail

Le télétravail nécessite que les utilisateurs puissent se connecter depuis plusieurs positions géographiques et appareils, bien souvent au-delà du périmètre des entreprises qui les emploient. L'architecture SASE permet aux entreprises de sécuriser l'accès de leurs collaborateurs et des tiers aux données et aux environnements essentiels, afin d'assurer la protection et la productivité de cette approche hybride du travail.

Améliorer l'expérience utilisateur

Les approches traditionnelles en matière de nettoyage du trafic des entreprises nécessitent souvent de rediriger ce dernier vers des datacenters professionnels, qui ajoutent de la latence et nuisent à la productivité. Or, l'alternative (c'est-à-dire le fait d'accorder un accès Internet direct aux utilisateurs) introduit des risques en termes de sécurité et crée des incohérences au sein de l'expérience utilisateur. L'approche SASE gère et optimise intelligemment les connexions directes à n'importe quel cloud ou destination Internet. Elle permet également d'appliquer les politiques et les protections aussi près de l'utilisateur final que possible.

Sécuriser les réseaux étendus (WAN)

Certains WAN contournent la sécurité cloud pour le trafic circulant entre les bureaux régionaux, de sorte que les promesses d'intégration entre les services de sécurité et les WAN définis par logiciels ne sont parfois pas ce qu'elles paraissent être à l'origine. Le SASE permet aux entreprises de simplifier et de sécuriser la manière dont elles se connectent par WAN en filtrant et en inspectant le trafic circulant entre les bureaux, les datacenters, les clouds publics et les autres emplacements situés au sein et en dehors du périmètre d'Internet au sens large.

ÉTUDE DE CAS

Protéger des surfaces d'attaque en pleine expansion

Werner Enterprises a déployé des services SASE en toute fluidité au cours de sa migration vers le cloud, sans interruption critique de l'activité ou du service client. Après ce déploiement, l'entreprise a réduit de 50 % le nombre d'e-mails malveillants présents sur ses comptes, tout en minimisant les efforts de triage manuel des e-mails de plusieurs heures par jour, afin que son équipe de sécurité puisse se concentrer sur des objectifs métier plus stratégiques.

Scénario d'utilisation n° 3 :

Protéger vos données partout dans le monde

Plus les données s'étendent à de nouveaux environnements, plus les entreprises ont du mal à les suivre. Les données sensibles peuvent être exposées par le biais d'une utilisation non autorisée de l'intelligence artificielle générative et par l'informatique fantôme (Shadow IT), en entraînant ainsi une compromission ou des violations qui peuvent s'avérer coûteuses à corriger. Le SASE fait converger la visibilité et les mesures de contrôle sur les données sur l'ensemble des environnements applicatifs (web, SaaS et privés) afin d'aider les entreprises à atteindre les objectifs suivants :

Simplifier la conformité avec les réglementations sur la confidentialité des données

Face à l'essor des grands modèles linguistiques (Large Language Models, LLM) et des autres outils basés sur l'IA, les normes en matière de conformité doivent évoluer pour protéger les données des utilisateurs. Le SASE assure la sécurité et la confidentialité des données en unifiant les mesures de contrôle de ces dernières afin que les équipes de sécurité puissent verrouiller les classes de données régulées, réduire le risque de violations et assurer la continuité de la conformité à des exigences strictes en matière de données.

Gérer l'informatique fantôme

L'informatique fantôme (c'est-à-dire les applications non autorisées, qui ne sont ni gérées ni sécurisées par les entreprises qui les utilisent) peut introduire des risques lorsque des données sensibles circulent à travers les applications qui la composent. Le SASE permet de minimiser ces risques en mettant le trafic en proxy par l'intermédiaire de CASB (Cloud Access Security Brokers) in-line, qui journalisent chaque connexion et chaque requête afin de révéler la présence d'applications non autorisées. Les entreprises peuvent ensuite contrôler la manière d'accéder à ces applications et de les utiliser.

Utiliser l'IA générative en toute sécurité

Plus les entreprises adoptent l'IA, plus le risque d'exposer des données sensibles augmente. Grâce à une passerelle web sécurisée et à un CASB, l'approche SASE permet aux équipes de sécurité de détecter et d'approuver la manière dont les applications utilisent l'IA, analyser ces dernières à la recherche d'erreurs de configuration risquant de conduire à des fuites de données ou d'exécuter des applications basées sur l'IA au sein de navigateurs web isolés afin de limiter les entrées et les sorties de données.

Protéger les données sensibles

L'architecture SASE permet aux entreprises de détecter et de contrôler la manière dont les données sensibles entrent, circulent au sein et sortent de leurs environnements informatiques. Ce processus inclut l'analyse des applications et l'inspection du trafic à la recherche de données personnelles régulées et de données liées à la propriété intellectuelle, le blocage des menaces Internet (comme le phishing et les rançongiciels), de même que la mise en œuvre de protections supplémentaires contre le vol de données et les fuites involontaires.

ÉTUDE DE CAS

Protéger vos données partout dans le monde

Applied Systems a adopté les services SASE pour sécuriser l'accès de plus de 2 500 collaborateurs à ses applications auto-hébergées et à son infrastructure. Cette nouvelle approche offre à son équipe de sécurité la flexibilité nécessaire pour appliquer des mesures de contrôle rigoureuses afin de répondre à différents besoins des utilisateurs, tout en contrôlant la manière dont les données sont partagées avec les outils IA.

Choisir une solution SASE :

Consolidation à fournisseur unique ou plusieurs solutions dédiées ?

Un fournisseur de SASE à fournisseur unique fait converger les fonctions réseau et les fonctions de sécurité au sein d'un service unique, proposé via le cloud. Cette approche permet aux entreprises de consolider différents produits dédiés, d'éliminer les équipements et d'assurer une application cohérente des politiques. Alors qu'un déploiement SASE multi-fournisseurs peut permettre d'obtenir des résultats similaires à ceux obtenus en suivant l'approche à fournisseur unique, il accroît souvent la complexité et les coûts, tout en réduisant la visibilité interne et la flexibilité.

La consolidation de ces capacités sur une plateforme unique vous permet de tenir la véritable promesse du SASE : une infrastructure simplifiée et efficace en matière de réseau et de sécurité, capable de réduire votre coût total de possession (TCO) et de s'adapter facilement afin de répondre aux besoins de votre entreprise.

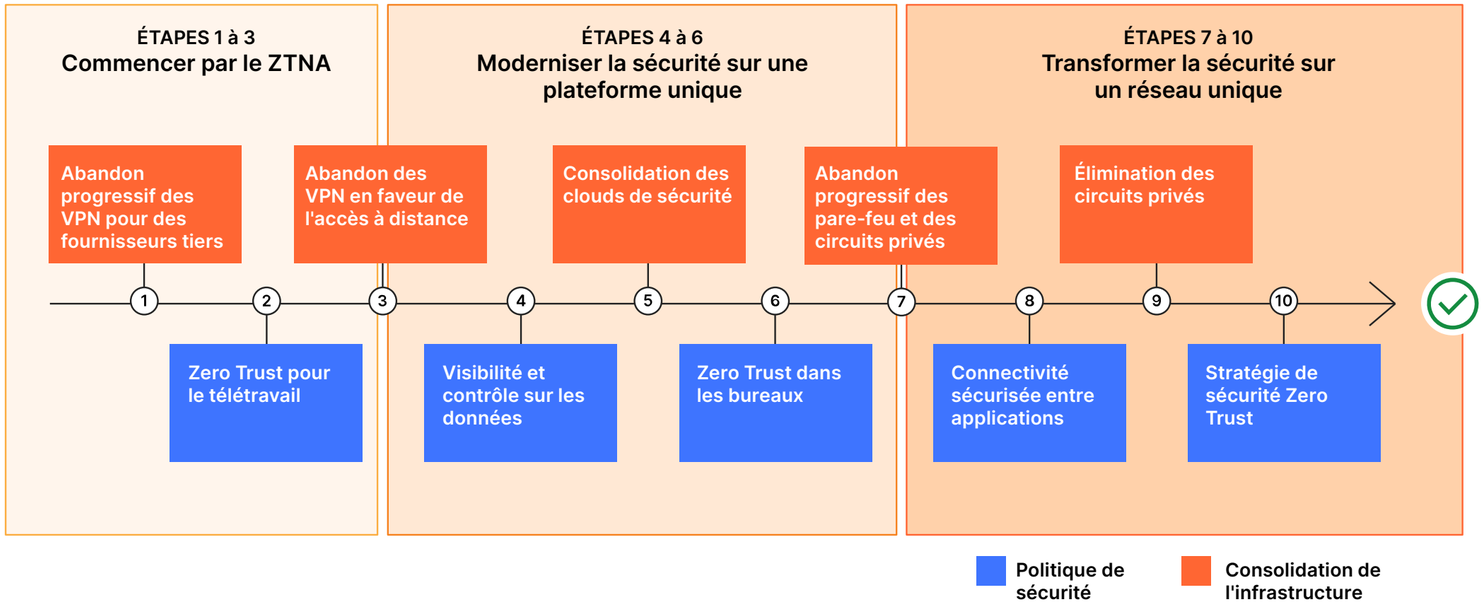
Lorsque vous évaluez de potentiels fournisseurs de SASE, veillez à garder les questions suivantes à l'esprit :

1. Le trafic des applications est-il déchiffré et inspecté en une seule par des moteurs de détections des menaces et des données sensibles ? Existe-t-il certaines mises à garde concernant le déploiement ?
2. Toutes les communications et tous les flux de données transitant par l'intermédiaire de suites SaaS sont-ils protégés sur chaque canal (in-line, web hors bande et e-mail) ?
3. L'isolement de navigateur à distance est-il activité pour chaque utilisateur et chaque application ? Comment ce service affecte-t-il la productivité ? S'accompagne-t-il de frais supplémentaires ?
4. Certaines fonctions de sécurité sont-elles contournables par un accès direct (on-ramp) au réseau ?
5. Est-il possible d'assurer l'isolement du trafic client et son caractère privé au sein d'une architecture cloud multi-tenant ?
6. Quelles capacités de régionalisation des données sont disponibles ? L'activation de la régionalisation des données ajoute-t-elle de la latence pour les utilisateurs distants qui se connectent depuis une autre région que votre espace régionalisé ?
7. Pouvez-vous intégrer vos flux d'informations sur les menaces à leur architecture ? Comment la plateforme réduit-elle le taux de faux positifs provenant de ces flux ?
8. Quelle sorte d'outils d'analyse et de notation des risques liés aux utilisateurs/appareils sont disponibles ? Les scores de risque peuvent-ils s'appliquer uniformément à l'ensemble des applications ?

Distribution de l’architecture SASE par Cloudflare

De nombreuses entreprises font confiance à Cloudflare pour finaliser leur parcours vers une plateforme SASE unifiée. Nous sommes le seul fournisseur de SASE à commencer avec une architecture réseau Zero Trust disposant d'une connectivité basée sur l'identité et le contexte intégrée de manière cohérente à l'ensemble de notre plateforme.

Votre feuille de route à long terme décrivant le déploiement complet d'une architecture SASE pourrait suivre un cheminement similaire à l'exemple ci-dessous :



Soutenue par son réseau mondial couvrant plus de 310 villes à travers le monde, Cloudflare aide les RSSI à bénéficier d'une sécurité, d'une résilience et de performances de niveau professionnel. Notre interface de contrôle unique fait converger les solutions dédiées réparties sur plusieurs domaines de sécurité, afin de permettre aux entreprises de simplifier leurs opérations de sécurité et d'assurer une protection cohérente contre des menaces en évolution constante.

Rendez-vous sur notre site web pour en savoir plus sur Cloudflare et la plateforme SASE de Cloudflare.

Téléphone : +33 7 57 90 52 73
E-mail : enterprise@cloudflare.com
Site : www.cloudflare.com/fr-fr/