citrix

Livre blanc

Comprendre les architectures Secure Access Service Edge (SASE)

Repensez les architectures réseau et sécurité pour répondre aux exigences d'aujourd'hui

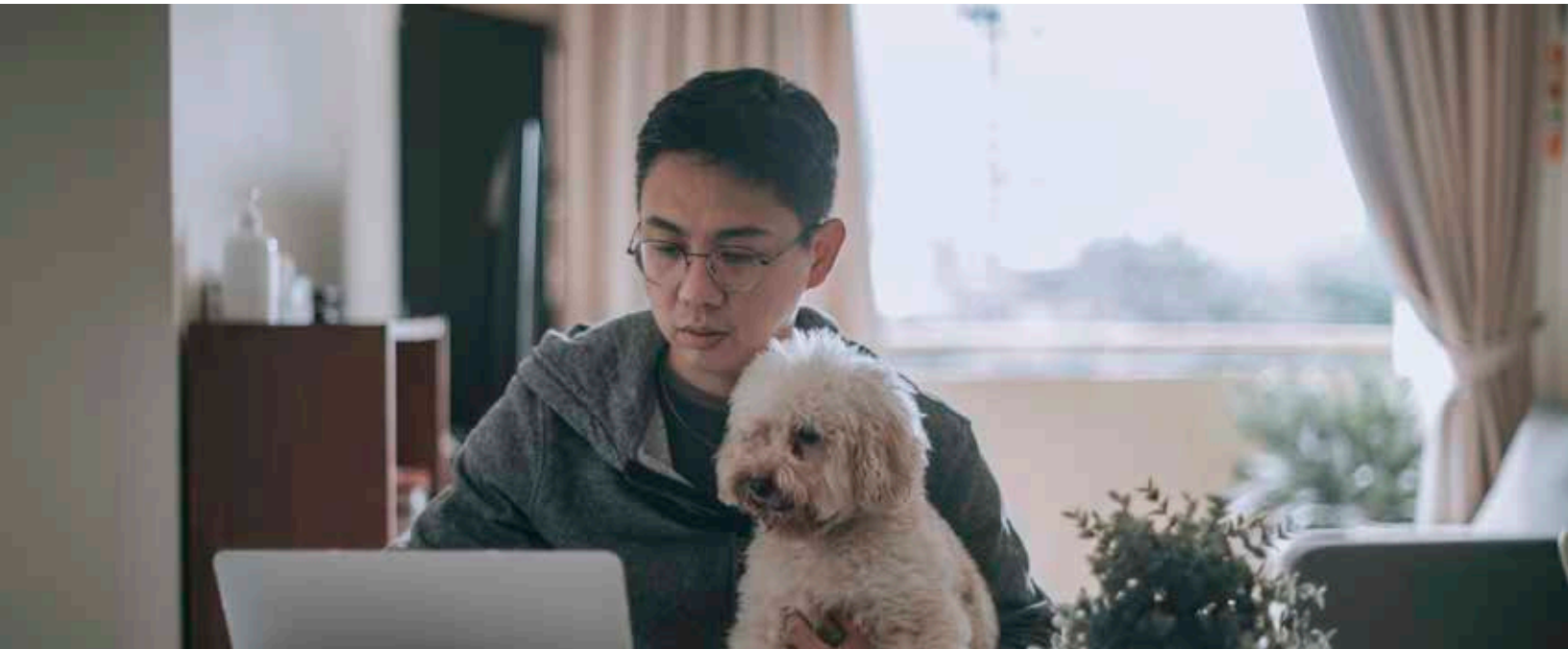
Évolution des modes de travail

Les modes de travail ont évolué. Les entreprises doivent tenir compte de ces évolutions pour planifier notamment les futurs investissements d'infrastructure, les architectures et les délais de mises à disposition de nouveaux services digitaux. Suivre le rythme de ces évolutions est impératif pour influencer positivement les indicateurs tangibles du succès métier, tels que les performances opérationnelles, les coûts financiers, l'engagement des collaborateurs et la satisfaction client.

- **Utilisation accrue de services et d'applications cloud :** Gartner estime à 34 % l'augmentation des dépenses pour des applications SaaS entre 2020 et 2022 dans le monde[1]. Ces applications SaaS sont adoptées pour une utilisation à la fois professionnelle et privée. Dans les deux cas, les utilisateurs attendent de ces applications une expérience de niveau consommateur : un accès rapide quels que soient l'application consultée ou l'endroit où se trouve l'utilisateur.
- **Nombre croissant de télétravailleurs :** Le COVID-19 a forcé employeurs et collaborateurs à essayer le télétravail. Selon un rapport réalisé en juin 2020, 72 % des collaborateurs aimeraient télétravailler au moins deux jours par semaine, même après la résolution de la crise du COVID-19[2]. Ceci étant dit, les télétravailleurs mentionnent également la difficulté à collaborer comme une raison majeure de la perte de productivité. Il n'est pas surprenant que 53 % des employeurs prévoient d'investir dans la fourniture d'une meilleure expérience mobile pour les données et les applications professionnelles[3].
- **Augmentation des menaces de sécurité létales :** 3,86 millions de dollars : c'est le coût total moyen d'une violation de données[4]. La plupart des violations de données sont orchestrées intentionnellement à des fins malveillantes (par rapport à des erreurs humaines ou des bugs du système). Il est impératif pour les entreprises de faire évoluer leurs architectures et systèmes de sécurité pour échapper aux acteurs malveillants. Ceci non seulement évite des pertes financières conséquentes mais aide également à conserver la confiance des clients et des collaborateurs.

Les équipes IT ont besoin d'une architecture réseau et sécurité sous-jacente capable de prendre en charge un accès rapide, homogène et sécurisé vers les applications cloud pour tous, y compris les télétravailleurs. Malheureusement, les architectures sécurité et réseau en étoile utilisées aujourd'hui ont été conçues pour l'ère des applications sur site et des travailleurs basés dans des succursales, connectés via des WAN privés. Il est nécessaire que ces architectures sous-jacentes évoluent pour pouvoir prendre en charge des tendances technologiques plus larges à même d'impacter de façon tangible le succès métier.

« 53 % des employeurs prévoient d'investir dans la mise à disposition d'une meilleure expérience mobile pour les applications et les données professionnelles »



Architectures pour l'ère du Cloud-First et du Mobile-First

Les défis des architectures traditionnelles

Voici les défis spécifiques qui doivent être relevés pour mettre à disposition des architectures adaptées à l'ère du Cloud-First et du Mobile-First.

- **Une expérience applicative médiocre pour les collaborateurs :**
  - *Défis liés à l'architecture :* les architectures en étoile forcent le trafic à transiter vers le datacenter pour des raisons de sécurité. Ce saut de trafic supplémentaire augmente les exigences WAN mais, plus important, ajoute une latence inévitable et détériore l'expérience collaborateur.
  - *Défis liés aux appliances :* lorsque les télétravailleurs collaborent et utilisent des applications cloud, notamment des applications chiffrées de partage de fichiers telles que Microsoft SharePoint et des applications de vidéoconférence telles que Microsoft Teams, la charge sur l'infrastructure sous-jacente (appliances basées dans le datacenter et liaisons WAN) augmente considérablement. Ces appliances matérielles ont des limites de traitement et l'augmentation de la charge venant d'applications cloud chiffrées détériore les performances et affecte l'expérience collaborateur.
- **Une sécurité non homogène pour les télétravailleurs :**
  Les collaborateurs attendent des performances applicatives similaires à celles des succursales, même lorsqu'ils télétravaillent. Pour atteindre cet objectif, les collaborateurs se déconnectent souvent de clients VPN lorsqu'ils accèdent à des applications web et SaaS. Ce qui les laisse sans protection et vulnérables face aux menaces. De la même manière, les collaborateurs qui accèdent à des données d'entreprise depuis des appareils BYO peuvent faire augmenter les risques pour l'entreprise. En fait, 61 % des CISO et des CIO disent qu'ils constatent une augmentation des risques liés à l'utilisation d'appareils et de logiciels n'appartenant pas à l'entreprise en raison de la progression du télétravail[5]. Par conséquent, les entreprises doivent trouver un moyen de sécuriser de façon homogène tous les utilisateurs et tous les appareils, en tout lieu et sans impacter l'expérience applicative des collaborateurs.
- **La complexité opérationnelle :**
  Les architectures traditionnelles sont souvent composées de solutions fragmentées, enchaînées à des services. Il est alors difficile d'apporter des changements à l'architecture sans « casser » un autre lot de configurations. Ainsi, mettre à l'échelle l'architecture selon des modèles de trafic changeants implique souvent de mettre à niveau des appliances physiques vers des limites de capacité supérieures. Ceci demande du temps et empêche l'équipe IT de se concentrer sur la mise à disposition de nouveaux services digitaux.

Fonctionnalités clés pour une architecture d'entreprise moderne

- **Accès direct à Internet :**
  Les collaborateurs ont besoin d'accéder à toutes les applications par un chemin direct, du collaborateur à l'application. Cette connexion doit cependant être sécurisée.
- **Une sécurité qui suit l'utilisateur :**
  La sécurité basée sur un datacenter ne permet pas l'accès direct à Internet. Il est ainsi nécessaire d'avoir une architecture de sécurité qui autorise que la sécurité soit placée sur le chemin entre l'application et le collaborateur, quel que soit l'endroit où celui-ci se trouve. Cela n'est possible qu'avec des services de sécurité mis à disposition dans le cloud. Comme on peut s'y attendre, 76 % des entreprises prévoient de déplacer leur sécurité dans le cloud[6].
- **Services WAN pour les performances applicatives :**
  L'accès direct à Internet raccourcit le chemin entre le collaborateur et l'application. Cependant, il ne fait rien pour atténuer les variations des performances applicatives résultant de l'imprévisibilité des ressources ou des connexions Internet métier. Par conséquent, les entreprises ont besoin de fonctions complètes, comme le SD-WAN (Software-Defined WAN) et l'optimisation WAN, pour garantir les performances applicatives sur des connexions d'accès direct à Internet.
- **Architecture à passage unique :**
  Pour supprimer la latence supplémentaire résultant des moteurs d'inspection enchaînés à un service dans une pile de sécurité typique, les entreprises doivent déployer une architecture à passage unique. Les architectures à passage unique ouvrent et inspectent le trafic une seule fois en vue de son traitement par plusieurs moteurs de stratégies. Par exemple, une architecture à passage unique ouvrira et inspectera un paquet chiffré une seule fois pour analyse par les moteurs de protection contre les malwares et de prévention contre les pertes de données.

- **Gestion unifiée :**
  L'intégration de panneaux de gestion sur le réseau et la sécurité doit simplifier les opérations sur le cycle de vie complet : provisioning, gestion basée sur des stratégies, visibilité et dépannage. Par exemple, les équipes d'administrateurs IT doivent avoir une vue holistique de l'ensemble de l'architecture d'entreprise pour le réseau et la sécurité, y compris l'emplacement des sites distants, les points de présence de sécurité, les tunnels et l'utilisation du réseau, le tout sur un tableau de bord unifié. Ceci supprime les angles morts et simplifie les configurations sur toute l'architecture, limitant les risques d'erreur humaine.

« 76 % des entreprises prévoient de déplacer leur sécurité dans le cloud »

Secure Access Services Edge

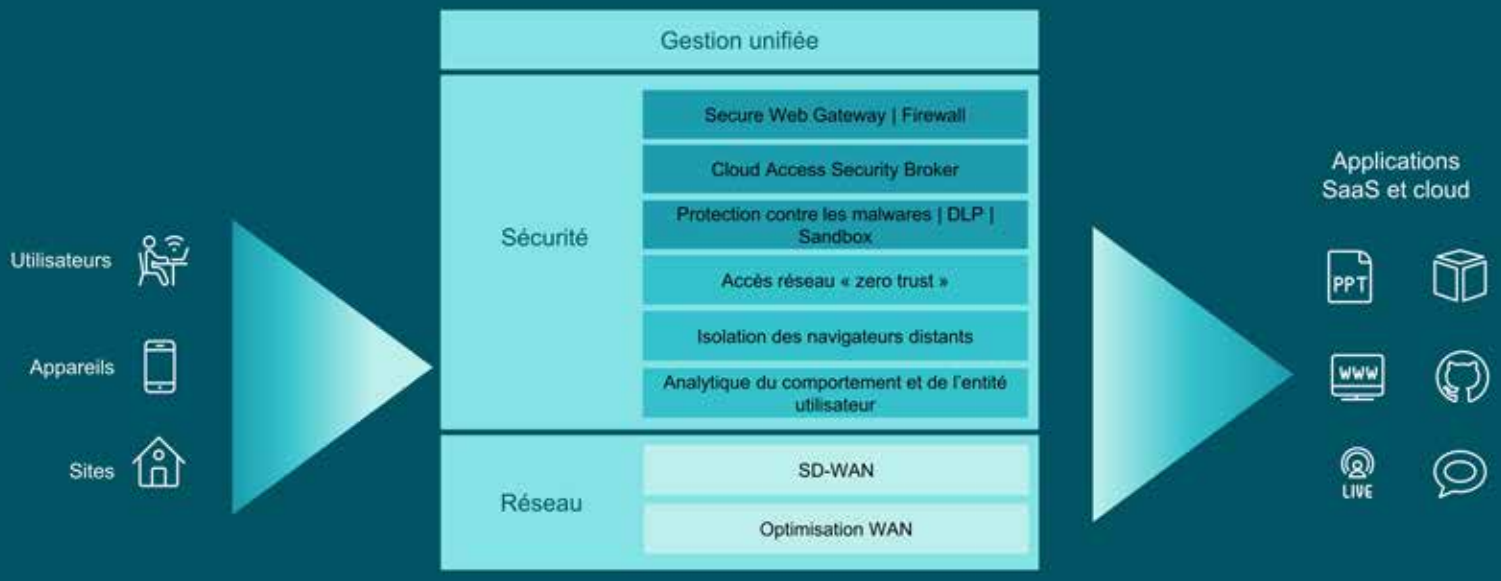
Secure Access Services Edge (SASE) est conçu pour remplacer les architectures traditionnelles en étoile par un accès direct à Internet. L'unification de la sécurité mise à disposition dans le cloud, l'accès « zero trust » et des fonctionnalités WAN complètes garantissent une expérience collaborateur sécurisée et homogène, quel que soit l'endroit où se trouve le collaborateur ou celui où est hébergée l'application.

Les services SASE sont appliqués en se basant sur l'identité de l'utilisateur et sur le contexte en temps réel. Par exemple, un cadre du service financier recevra un accès différent de celui d'un sous-traitant tiers en marketing. Les principaux services d'une architecture SASE comprennent :

- Les passerelles **Secure Web Gateways (SWG)** sont des solutions de sécurité d'entreprise conçues pour protéger les utilisateurs contre les cybermenaces basées dans le web. Elles proposent les fonctionnalités suivantes :
  - *Filtrage URL* – Autorise ou bloque l'accès à des sites web en comparant les URL demandées à une base de données de filtrage définie par une stratégie organisationnelle.
  - *Protection anti-malware* – Inspecte des contenus web chiffrés et non chiffrés pour identifier et bloquer toutes les menaces.
  - *Contrôle des applications* – Apporte de la visibilité sur les applications qui sont consultées et permet un contrôle granulaire pour garantir sécurité et conformité.

Les SWG sont en général mises en œuvre dans un service cloud en ligne, orchestrées sous la forme de piles de sécurité multi-locataires via des points de présence (PoP)

SASE fait converger le réseau et une sécurité complète mise à disposition dans le cloud avec une gestion unifiée



distribués mondialement. Le trafic venant des utilisateurs d'entreprise, aussi bien en télétravail que sur des sites distants, est transféré vers le cloud SWG où il est inspecté et sécurisé.

- Les brokers **Cloud Access Security Brokers (CASB)** aident à surveiller, sécuriser et gérer les accès vers des applications SaaS autorisées et non autorisées. Les fonctionnalités CASB sont construites autour de quatre piliers :
  - *Visibilité* – Vue consolidée sur toutes les applications, y compris les applications d'IT fantôme non autorisées, qui sont utilisées par les utilisateurs d'entreprise
  - *Sécurité des données* – Évite l'accès non autorisé à des données sensibles et leur exfiltration
  - *Protection contre les menaces* – Utilise des architectures proxy en ligne, des flux de menaces natifs ou intégrés et des analyses du comportement pour identifier et limiter les dommages causés par des malwares et des utilisateurs compromis
  - *Conformité* – Visibilité et reporting pour montrer que les réglementations du secteur et les stratégies sur la résidence des données sont respectées
- L'approche **Zero-trust Network Access (ZTNA)** vise à éliminer toute « confiance excessive » en fournissant un accès « juste à temps » et « juste suffisant » entre des utilisateurs autorisés et des applications approuvées. Contrairement aux solutions VPN traditionnelles qui autorisent un utilisateur avec une adresse IP spécifique à accéder à l'ensemble du réseau d'entreprise, le ZTNA permet un accès précis, adaptable, sensible à l'identité et au contexte. Les principales caractéristiques des solutions ZTNA sont :
  - *Sensibilité à l'identité* - L'accès est autorisé en se basant sur l'identité de l'utilisateur. Les solutions ZTNA intègrent en général des fournisseurs d'identité tels que Microsoft Azure Active Directory pour les informations sur l'identité.
  - *Sensibilité au contexte* - Les solutions ZTNA tiennent compte de paramètres contextuels en temps réel tels que l'identité de l'utilisateur, le lieu et l'appareil depuis lesquels l'accès est demandé, l'heure du jour, la sensibilité de l'application demandée et un calcul des risques en temps réel basé sur des entrées venant de services de sécurité et de surveillance.
  - Les niveaux d'accès sont adaptables : l'accès peut être autorisé/limité/refusé en fonction de l'évolution de ces paramètres.
  - *Accès au niveau applicatif* - Les utilisateurs autorisés se voient accorder l'accès à l'application spécifique et non au réseau sous-jacent. Ceci limite la possibilité d'une propagation latérale des malwares dans le réseau d'entreprise.
  - *Les applications restent cachées d'Internet* - Le transfert de données entre un utilisateur et une application est pris en charge par un « broker » au sein de l'architecture ZTNA, sans qu'il soit nécessaire que l'application expose son adresse IP à Internet. L'application reste donc cachée des acteurs malveillants qui pourraient vouloir lancer des attaques de type DDoS ou similaire.

Les solutions ZTNA limitent la surface d'attaque de l'entreprise en protégeant à la fois les utilisateurs et les applications. Comme les utilisateurs n'ont plus à se connecter à un VPN ni à transiter par la pile VPN, l'expérience utilisateur est améliorée. Enfin, les solutions ZTNA simplifient l'architecture de sécurité des entreprises en remplaçant la pile VPN requise dans les datacenters par un service mis à disposition dans le cloud, ce qui renforce l'agilité et l'efficacité.

- **Firewall-as-a-Service** – Les pare-feu agissent comme des gardiens ou des filtres entre le réseau d'entreprise et Internet, en proposant des contrôles bidirectionnels (entrée et sortie) pour n'autoriser que le trafic sécurisé et de confiance. Les pare-feu proposent en général des fonctionnalités telles que la prévention/détection des intrusions, la protection contre les malwares, la tenue de journaux et le reporting. De plus, la plupart des pare-feu modernes proposent également des fonctions de sandboxing, de géolocalisation et de détection des menaces (basée sur les anomalies) sans signature. Quelques-unes sont expliquées ici :
  - *Protection anti-malware* – Inspecte des contenus web chiffrés et non chiffrés pour identifier et bloquer toutes les menaces.
  - *Système de détection/prévention des intrusions (IPS/IDS)* – Le système IPS/IDS inspecte le trafic et le compare aux signatures de menaces connues pour identifier des fichiers malveillants. L'IDS est un outil de surveillance et de tenue de journaux qui crée une alerte lorsqu'un malware est détecté. L'IPS va un cran plus loin et bloque automatiquement le trafic potentiellement malveillant.

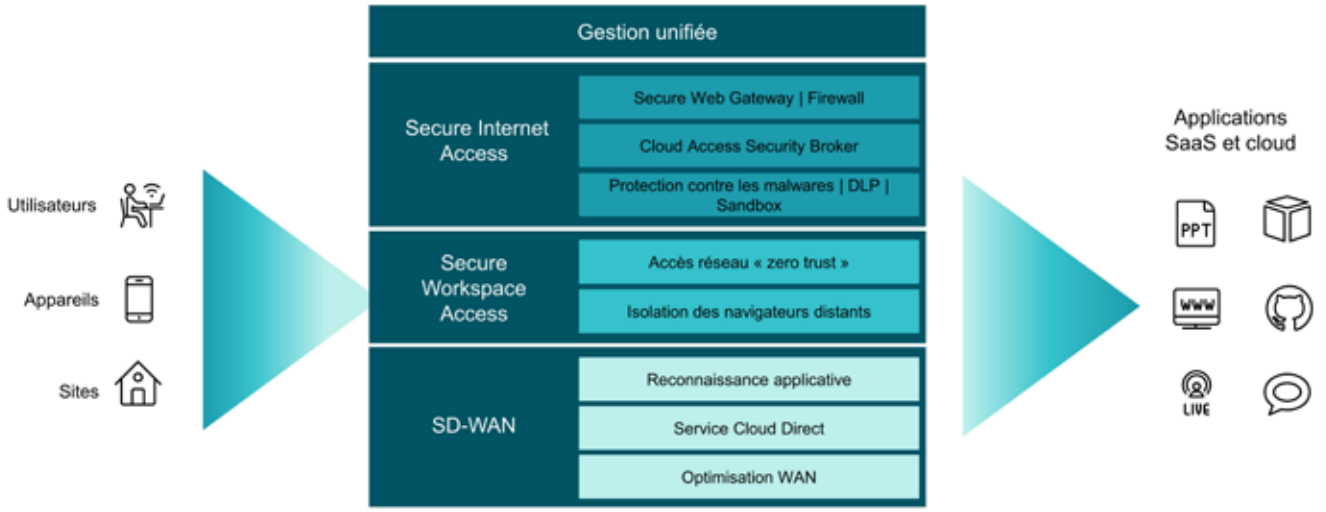
- *Détection des menaces basée sur les anomalies/sans signature* - La détection basée sur des anomalies implique de comparer le comportement réel ou potentiel d'un fichier (en inspectant le code contenu dans le fichier) par rapport à des données de base représentatives. Par exemple, un fichier récemment téléchargé qui essaie de désactiver des contrôles de sécurité doit probablement être mis en quarantaine.
- *Sandbox réseau* – Les fichiers suspects sont envoyés vers le « bac à sable » (sandbox) pour être exécutés dans un environnement isolé. Si les fichiers s'avèrent malveillants, l'information est envoyée au pare-feu pour bloquer ces fichiers.
- *Géolocalisation* – Attribution de certains types d'adresse IP à un emplacement géographique spécifique pour autoriser/limiter/bloquer l'accès en se basant sur cette attribution.

Des pare-feu sont utilisés pour protéger les sites distants, les datacenters et les instances cloud des entreprises contre les menaces. Ils sont souvent intégrés avec d'autres solutions (analytique) de sécurité et SecOps pour créer une « plateforme » de gestion des menaces plus complète et robuste.

- **SD-WAN :**
  Les solutions WAN Software-Defined fournissent une connectivité résiliente et à faible latence depuis des sites d'entreprise distribués vers des applications cloud et sur site, tout en surmontant la complexité générée par l'utilisation de solutions pour la mise en réseau traditionnelles basées sur des routeurs pour gérer des réseaux modernes. La fonctionnalité SD-WAN comprend des fonctions de périphérie WAN plus holistiques, notamment :

  - *Sélection du chemin* – Identification et orientation dynamique du trafic en se basant sur des stratégies définies par l'administrateur et sur l'état du WAN en temps réel (perte de paquets, instabilité, latence, etc.). Les fonctionnalités de sélection du chemin aident à garantir que les utilisateurs bénéficient d'une expérience applicative homogène, quelle que soit l'évolution des performances réseau.
  - *Routage* – Fonctionnalité qui permet de remplacer les routeurs de site distant (BGP, OSPF, prise en charge de multiples topologies).
  - *Sécurité native* – Fonctionnalité de sécurité au niveau des sites distants, y compris IPS/IDS, protection contre les malwares basée sur l'heuristique et les signatures et filtrage web. De plus, les solutions SD-WAN simplifient souvent la configuration des tunnels VPN entre les sites distants et les instances (IaaS/PaaS) cloud.
  - *Provisioning « zero-touch »* – Cette fonctionnalité permet d'effectuer à distance le provisioning et la configuration initiale des appliances SD-WAN des sites distants. Elle permet aux appliances SD-WAN d'être envoyées vers des sites distants et simplement branchées à un ou

L'approche unifiée SASE de Citrix



L'approche SASE de Citrix unifie les fonctionnalités d'un accès sécurisé et fiable aux applications, quels que soient le lieu, le moment ou l'appareil

plusieurs circuits WAN sans qu'aucune configuration complexe sur site ne soit nécessaire. Les appliances SD-WAN téléchargent les configurations depuis le panneau de contrôle SD-WAN et démarrent automatiquement la configuration du tunnel pour d'autres sites distants ou cloud compatibles SD-WAN.

Les fonctionnalités de sécurité ci-dessus, associées au SD-WAN, permettent à une entreprise de transformer ses architectures réseau et sécurité pour répondre aux besoins du cloud, de la mobilité et d'une main-d'œuvre de plus en plus diversifiée.

L'approche unifiée SASE de Citrix

Citrix propose une solution SASE entièrement unifiée qui intègre une pile de sécurité complète mise à disposition dans le cloud ainsi qu'un accès « zero trust » pour faire bénéficier les collaborateurs de la meilleure expérience de façon sécurisée, quels que soient l'appareil, le lieu ou l'application.

- **Sécurité complète, mise à disposition dans le cloud :** Citrix Secure Internet Access (SIA) propose des services de sécurité complets, mis à disposition dans le cloud. Ils comprennent une passerelle Secure Web Gateway, un pare-feu de dernière génération, un broker Cloud Access Security Broker, une intelligence anti-malware alimentée par plus de 10 moteurs de détection des menaces, des fonctions de prévention contre la perte de données et de sandboxing, une analytique alimentée par l'intelligence artificielle, etc. Distribué mondialement à travers plus de 100 points de présence (PoP), chacun proposant tous les services de façon homogène, SIA protège les collaborateurs avec une pile de sécurité complète, quel que soit l'endroit où ils se trouvent.

Citrix Secure Internet Access propose des services de sécurité complets mis à disposition dans le cloud

- **Accès « zero trust », sensible à l'identité :** Citrix Secure Workspace Access fournit un accès « zero trust » sensible à l'identité à toutes les applications d'entreprise autorisées dans un Digital Workspace conçu pour rationaliser l'expérience collaborateur sur n'importe quel appareil. L'isolation intégrée des navigateurs distants protège les terminaux et le réseau d'entreprise contre

les attaques basées sur des navigateurs. Les données des sites web ne sont pas transférées directement sur l'appareil utilisateur de sorte que l'expérience est sécurisée.

- **Expérience applicative rapide avec SD-WAN :** Citrix SD-WAN est une solution de périphérie WAN de nouvelle génération qui fournit une connectivité sécurisée, flexible et automatisée pour améliorer la performance des applications SaaS, cloud et virtuelles. Des fonctionnalités, telles que la priorisation du trafic au niveau du paquet, avec des basculements inférieurs à la seconde entre les liaisons WAN, et une qualité de service à deux extrémités, garantissent des performances applicatives d'une rapidité homogène, quelle que soit la disponibilité du réseau.
- **Analyse approfondie et recherche facile :** La tenue de journaux détaillés pour tous les utilisateurs, y compris les utilisateurs mobiles, et pour leur activité, notamment des informations complètes sur les URL (pas uniquement le nom de domaine) dans le trafic HTTPS fournit une visibilité unique et approfondie. Des moteurs de reporting alimentés par l'intelligence artificielle extraient des informations essentielles pour le reporting et les alertes. En plus des rapports intégrés, des journaux peuvent également être exportés en temps réel vers des solutions SIEM.
- **Gestion unifiée :** Citrix propose de gérer des intégrations approfondies, des automatisations et une vue unifiée sur SD-WAN et SIA pour simplifier les opérations sur le cycle de vie complet, de la configuration initiale jusqu'à la gestion continue et au dépannage.

  - Connectivité automatisée des connexions « double résilience » entre les sites Citrix SD-WAN et Citrix SIA
  - Vue singulière sur l'architecture complète couvrant les sites compatibles SD-WAN, les PoP SIA et les tunnels de connexion
  - Contrôle granulaire sur l'orientation du trafic et attribution de bande passante sur le SIA, les fournisseurs cloud et autres liaisons WAN, en fonction des besoins métier
  - Élimine les angles morts en intégrant un reporting sur l'architecture réseau et sécurité

Avantages de la mise en œuvre d'une architecture SASE

Les architectures SASE ont été conçues pour permettre un accès rapide, fiable et sécurisé aux applications cloud par les collaborateurs mobiles et distants, tout en améliorant l'agilité informatique. Si l'on suppose que les entreprises accordent de l'importance aux nuances proposées en termes de fonctionnalités (par exemple la gestion unifiée sur le réseau et la sécurité, une conception architecturale à passage unique et des fonctions SD-WAN puissantes), un déploiement SASE peut faire bénéficier les entreprises des avantages suivants :

- **Expérience, collaboration et engagement accrus des utilisateurs** – L'accès direct à Internet supprime la latence venant de connexions réacheminées. Cependant, les fonctionnalités SD-WAN et optimisation WAN sont nécessaires dans les solutions SASE pour garantir des performances homogènes, même si les performances Internet fluctuent. Les architectures à passage unique garantissent que les moteurs de stratégies et d'inspection eux-mêmes n'ajoutent aucune latence inutile.
- **Sécurité améliorée indépendamment de la localisation du collaborateur** – Un accès « zero trust » sensible à l'identité est accordé pour les applications autorisées. Ceci réduit la surface d'attaque et limite le déplacement latéral des malwares dans le réseau d'entreprise. Pour les applications web et non autorisées, une sécurité complète mise à disposition dans le cloud garantit une posture de sécurité homogène, quel que soit l'endroit où se trouve le collaborateur.
- **Des opérations simplifiées avec une agilité informatique améliorée** – Les architectures SASE peuvent aider à consolider les fournisseurs pour le réseau et la sécurité. Les solutions avec fournisseur unique proposent des intégrations plus profondes et une gestion unifiée qui simplifient le déploiement, la configuration, le reporting et les services d'assistance. Comme les architectures SASE nécessitent de déplacer la sécurité dans le cloud, l'empreinte matérielle globale est réduite ce qui, en retour, améliore la mise à l'échelle et l'élasticité de l'architecture.

Démarrage

Comme toute technologie disruptive, certaines entreprises adopteront les architectures SASE plus tôt que d'autres. Le remplacement d'architectures en étoile traditionnelles, le remplacement d'anciennes technologies VPN héritées (legacy), la migration d'applications dans le cloud, une sécurité homogène pour les télétravailleurs et le besoin d'améliorer l'engagement des collaborateurs ne sont que quelques sujets parmi d'autres pour engager la conversation.

La capacité à repenser et à réagencer les architectures réseau et sécurité donnera un avantage significatif aux adopteurs précoces, créant un impact positif sur les indicateurs du succès métier tels que les performances opérationnelles, les coûts financiers, l'engagement des collaborateurs et la satisfaction client. Pour permettre cette transformation, les entreprises doivent choisir judicieusement leur partenaire technologique.

Citrix unifie tous les services SASE, sur le réseau et la sécurité, en proposant une gestion des intégrations approfondies, des automatisations et d'une vue unifiée. Adopté par 400 000 entreprises pour créer une meilleure façon de travailler, Citrix peut vous aider à accélérer votre transformation réseau et sécurité.

Pour en savoir plus, consultez le site *www.citrix.fr/secure-internet*.

Notes de fin de page

1 Basé sur les propres calculs de Citrix. Communiqué de presse Gartner, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020, 23 juillet 2020. https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

2 PwC's US Remote Work Survey, juin 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

3 PwC's US Remote Work Survey, juin 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

4 Cost of a Data Breach Report 2020, IBM, https://www.ibm.com/security/data-breach

5 PwC's Workforce Pulse Survey, https://www.pwc.com/us/en/library/covid-19/workforce-pulse-survey.html

6 PwC's Global Digital Trust Insights 2021, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/global-digital-trust-insights/cyber-defense-technology.html

Ventes aux entreprises
Amérique du Nord | 800-424-8749
International | +1 408-790-8000

Sites
Siège social | 851 Cypress Creek Road Fort Lauderdale, FL 33309, États-Unis
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, États-Unis