HPE aruba networking

Brochure

GUIDE D'INTRODUCTION AU SASE UNIFIÉ

Vers une mise en œuvre simplifiée et plus rentable du SASE monofournisseur

HPE

66%

des responsables RH déclarent que leur entreprise applique un modèle de travail hybride[1], ce qui accroît la demande de solutions SASE.

65%

des entreprises interrogées indiquent avoir déployé ou prévoir de déployer le SASE.[2]

65%

« D'ici 2027, 65 % des nouveaux achats de SD-WAN feront partie d'une offre SASE auprès d'un fournisseur unique, soit une augmentation de 20 % par rapport à 2024. »[3]

[1] 9 Ways to Manage Hybrid Employees for Better Productivity, Gartner, March 2023

[2] 2025 Ponemon Institute report

[3] Magic Quadrant for single-vendor SASE, Gartner, July 2024

L'émergence du SASE unifié : une mise en œuvre simplifiée et plus rentable du SASE

Ces douze derniers mois, de nombreux responsables informatiques ont adopté un cadre SASE (Secure Access Service Edge) afin d'obtenir une connectivité plus rapide et plus sécurisée sur l'ensemble de leurs sites à l'échelle mondiale. Le SASE regroupe les solutions de réseau et de sécurité en un seul service cloud-native pour offrir une connectivité et une protection homogènes n'importe où.

Cette architecture n'est pas une simple tendance technologique, mais un impératif stratégique pour les entreprises modernes qui cherchent à prospérer à l'ère du numérique.

Toutefois, toutes les solutions SASE ne se valent pas. Certains fournisseurs SASE proposent des solutions multipoints mal intégrées ou qui nécessitent un routage entre les POP de différents fournisseurs, ce qui peut générer de la latence, des problèmes de performance et des frais de gestion.

D'autres solutions SASE fournissent toutes les fonctionnalités essentielles de SASE à partir d'une seule plateforme étroitement intégrée, permettant d'améliorer la politique de sécurité, la productivité des collaborateurs, les expériences utilisateur et admin, mais aussi les coûts.

C'est ce que l'on appelle le SASE unifié. Pour une mise en œuvre simplifiée et plus rentable du SASE, c'est la solution à privilégier.

Dans ce guide, vous découvrirez tout ce que vous devez savoir sur le SASE, notamment :

— Qu'est-ce que le SASE unifié ?

— Les avantages du SASE monofournisseur pour l'entreprise moderne

— Un SASE unifié puissant grâce à HPE Aruba Networking

— Démarrer votre parcours SASE

À la fin de ce guide, vous serez en mesure de comprendre comment l'architecture SASE peut vous aider à atteindre vos objectifs de sécurité plus rapidement et plus efficacement.

Les raisons majeures de l'adoption du SASE

Commençons par le commencement : pourquoi adopter une solution SASE ? La réponse peut être résumée en 3 points :

1. La **sécurité** qui auparavant était efficace ne l'est plus.
2. Les **réseaux** qui auparavant étaient faciles à gérer ne le sont plus.
3. Les **solutions** qui auparavant étaient performantes ne le sont plus.

Les architectures traditionnelles de réseau et de sécurité qui reposaient principalement sur une connectivité sécurisée basée sur le périmètre ne répondent plus aux besoins de l'environnement moderne des entreprises. L'adoption rapide des services cloud, des dispositifs mobiles, de l'Internet des objets, de l'OT et du travail hybride à distance a créé des équipes dynamiques et distribuées ayant besoin d'un accès sécurisé et fiable aux applications et aux données, n'importe où, à n'importe quel moment et sur n'importe quel appareil.

Or, face à ces besoins qui fortement évolué, continuer à exploiter des solutions traditionnelles de sécurité réseau expose les entreprises à de nouveaux défis et risques de connectivité, notamment les suivants :

— **Augmentation de la surface d'attaque et de la complexité :** avec la multiplication des utilisateurs, des appareils, des sites et des services cloud à protéger, les organisations doivent gérer un nombre croissant de points d'entrée exploitables par les pirates, et ont de plus en plus d'outils de sécurité à gérer et à mettre à jour. De plus, chaque point d'entrée (utilisateur ou appareil) dispose d'un accès direct au réseau d'entreprise, d'où un risque accru pour la sécurité.

— **Dégradation de l'expérience utilisateur et baisse de la productivité :** avec l'augmentation du trafic acheminé via le VPN et le réseau d'entreprise, les utilisateurs subissent plus de latence, de gigue, de perte de paquets et de limitations de bande passante. Résultat : une baisse de leurs performances, de leur productivité et de leur degré de satisfaction.

— **Coûts opérationnels et inefficacités élevés :** avec la multiplication des solutions de sécurité et de réseau à déployer, maintenir, mettre à jour et dépanner, les organisations doivent consacrer plus de temps et de ressources à la gestion de l'infrastructure et à la résolution des problèmes.

Affronter ces défis et ces risques peut sembler insurmontable. Toutefois, les responsables du réseau et de la sécurité peuvent éliminer ces problèmes en travaillant ensemble au sein d'un cadre SASE unifié.

Qu'est-ce que le SASE ?

Le Secure Access Service Edge, ou SASE, est un concept de cybersécurité introduit pour la première fois en 2019. Il s'agit d'un cadre informatique combinant les fonctionnalités de réseau et de sécurité sur une seule plateforme, ce qui permet de connecter de manière sécurisée tous les utilisateurs, dispositifs et applications entre les équipes distribuées à l'échelle mondiale.

Le SASE est constitué de deux « ensembles de technologie » incluant WAN Edge Services (SD-WAN) et Security Service Edge (ZTNA, SWG, CASB et DEM) qui permettent aux équipes de réseau et de sécurité d'autoriser n'importe quel utilisateur, dispositif ou serveur à se connecter de manière sécurisée depuis n'importe où via n'importe quelle méthode de transport. L'exploitation d'un large fabric SD-WAN et d'un SSE fourni via le cloud avec un réseau global de POP offre un accès Edge to Cloud rapide, qui permet de réduire la latence et d'améliorer la performance.

Les composantes du SASE

Deux ensembles de technologie de base constituent une offre de SASE unifié monofournisseur :

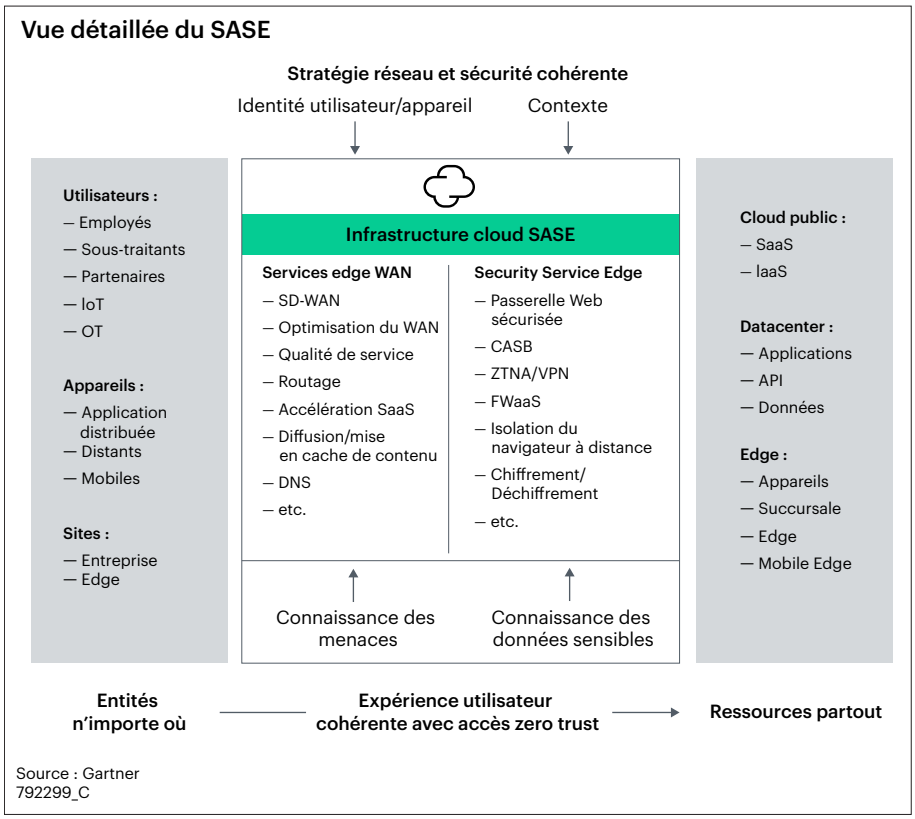

Figure 1. Secure Access Service Edge – vue détaillée, Guide du marché pour le SASE mono-fournisseur[4]

[4] Market Guide for Single-Vendor SASE, Gartner, December 2023

WAN Edge services (SD-WAN sécurisé)

— **Sécurité :** les SD-WAN sécurisés incluent des fonctionnalités NGFW, notamment la segmentation granulaire et IDS/IPS, permettant aux entreprises de remplacer les pare-feu de succursales et de sécuriser les dispositifs IoT. De plus, toutes les connexions sont chiffrées sur le fabric SD-WAN.

— **Réseau multicloud :** des instances virtuelles de solutions SD-WAN peuvent être déployées chez des fournisseurs de services cloud tels que AWS, MS Azure et Google Cloud, pour établir une connexion résiliente de la filiale au cloud. Le SD-WAN peut aussi diriger intelligemment le trafic des applications vers le cloud afin d'éviter le réacheminement du trafic vers le datacenter. De plus, il s'adapte dynamiquement aux changements associés aux modèles de trafic.

— **Agrégation de liens :** le SD-WAN combine de multiples liaisons de transport, notamment MPLS, l'Internet haut débit, la 4G/5G ou des liaisons satellite. Il sélectionne dynamiquement les meilleures liaisons en fonction des conditions du réseau et de l'intention commerciale.

— **Technologie Path Conditioning :** les solutions SD-WAN utilisent également des techniques tels que le Path Conditioning pour surmonter les effets négatifs des paquets perdus et dans le désordre, qui sont courants avec les connexions d'Internet haut débit et MPLS. Elles offrent une performance similaire à une ligne privée sur des liaisons Internet, ce qui permet aux organisations de limiter leur dépendance au MPLS et d'intégrer rapidement de nouveaux sites à leur réseau.

— **Optimisation WAN :** cette fonctionnalité accélère la transmission des données sur le réseau étendu en appliquant l'accélération du protocole TCP en plus de la déduplication des données et des algorithmes de compression.

— **Orchestration centralisée :** les politiques commerciales et de sécurité sont gérées de manière centralisée à partir d'une interface unique. Cela simplifie les opérations de réseau et la résolution des incidents, car les administrateurs peuvent effectuer des modifications et appliquer des politiques depuis un seul et même endroit.

Security Service Edge (SSE)

Accès réseau zero trust (ZTNA) | Accès sécurisé aux applications privées

— La technologie ZTNA fournit un accès zero trust granulaire, basé sur l'identité, aux applications et aux ressources privées, quel que soit l'endroit où elles sont hébergées ou l'endroit où les utilisateurs sont situés. Les solutions ZTNA modernes permettent aux équipes d'éliminer complètement les VPN à accès à distance pour les employés et les utilisateurs tiers, réduisant considérablement la surface d'attaque en permettant l'accès aux applications privées autorisées spécifiquement sans étendre l'accès au réseau sous-jacent.

Passerelle Web sécurisée (SWG) | Accès sécurisé à Internet

— La SWG protège l'entreprise distribuée face aux attaques avancées avec des fonctionnalités telles que le filtrage Web, l'inspection SSL et la détection et la prévention des programmes malveillants. Cette solution veille à ce que les utilisateurs autorisés bénéficient d'un accès rapide et sécurisé aux ressources Internet tout en protégeant l'entreprise contre tout danger.

Cloud Access Security Broker (CASB) | Accès sécurisé aux applications SaaS

— Le CASB permet au service informatique d'identifier, de gérer et de contrôler l'utilisation des services cloud. En plus d'assurer la médiation entre les utilisateurs et les applications SaaS sur le cloud, un service CASB aide à réguler le flux de données, empêche la perte de données et dévoile le shadow IT pour s'assurer que les données sensibles restent protégées.

Surveillance de l'expérience digitale (DEM) | Amélioration de l'expérience et de la productivité numérique

— La DEM offre une meilleure visibilité en ligne et une analyse dans les interactions, l'expérience et la performance des dispositifs, des applications et des réseaux. Elle aide les équipes informatiques à mieux utiliser leur temps en accélérant la résolution des incidents, pour des diagnostics ultra-précis des problèmes d'expérience.

Qu'est-ce que le SASE unifié ?

Le SASE unifié combine les deux ensembles de technologie (SD-WAN et SSE) en une solution monofournisseur qui permet aux entreprises d'atteindre une meilleure simplicité, des efficacités opérationnelles et des économies de coût. Une approche unifiée offre également une meilleure agilité et un déploiement plus rapide, ce qui réduit votre délai de rentabilisation. Gartner prédit que « d'ici 2027, 65 % des nouveaux achats de SD-WAN feront partie d'une offre SASE auprès d'un fournisseur unique, soit une augmentation de 20 % par rapport à 2024 ».[5]

Les avantages du SASE monofournisseur pour l'entreprise moderne

Le SASE unifié offre aux entreprises les nombreux avantages du SASE, tout en simplifiant l'adoption et en améliorant la rentabilité. La solution parvient à ce résultat grâce aux approches suivantes :

- **Unifier et améliorer la politique de sécurité :** le SASE unifié réduit la surface d'attaque et améliore la détection de menace ainsi que les temps de réponse en appliquant les règles de sécurité universelles et les contrôles d'accès centralisé sur l'ensemble du trafic et des sites.
- **Améliorer l'efficacité des équipes de réseau et de sécurité :** le recours à un fournisseur unique pour le SASE assure non seulement la consolidation, mais également l'unification des fonctions de réseau et de sécurité. On élimine ainsi les obstacles entre les équipes et on réduit la complexité et les coûts, tout en optimisant la collaboration et la mise en œuvre au-delà des cloisonnements fonctionnels. Les opérations de réseau et de sécurité sont simplifiées grâce à un système de gestion centralisée qui permet la visibilité, la configuration, la surveillance et la résolution des incidents.
- **Offrir une meilleure expérience utilisateur et administrateur :** le SASE unifié permet aux équipes de garantir aux utilisateurs des performances élevées et une connectivité à faible latence aux applications, et ce, en acheminant automatiquement le trafic via les chemins d'accès les plus rapides et en évitant le réacheminement du trafic vers le datacenter. Les utilisateurs finaux bénéficient d'une expérience d'accès optimisée, tandis que les administrateurs obtiennent des contrôles d'accès simples mais granulaires appliqués via des politiques zero trust universelles.
- **Réduire les coûts et augmenter la rentabilité :** le SASE réduit les dépenses d'immobilisation (CapEx) et les dépenses d'exploitation (OpEx) en supprimant le besoin de solutions multi-points et d'appareils matériels. Le SASE unifié est également extrêmement extensible, s'adapte rapidement aux besoins évolutifs de l'entreprise et fournit de multiples points de présence pour les entreprises distribuées géographiquement.

Comment démarrer le déploiement d'un SASE unifié

Déployer une solution SASE monofournisseur peut sembler une tâche insurmontable, mais ce n'est pas une fatalité. Avec le partenaire approprié et une feuille de route claire, les organisations peuvent effectuer une transition fluide et sécurisée vers le SASE, sans interrompre leurs opérations existantes ni compromettre leurs performances.

Les déploiements SASE les plus réussis suivent cinq étapes élémentaires :

- **Étape 1 : définir vos objectifs et exigences SASE.** Identifiez vos objectifs commerciaux, vos cas d'utilisation et vos exigences SASE. Évaluez votre architecture actuelle de réseau et de sécurité. Recherchez les lacunes, les défis et les ressources existantes.
- **Étape 2 : choisir un prestataire SASE monofournisseur.** Comparez les différents prestataires en fonction de leurs fonctionnalités, couverture, performances, évolutivité, fiabilité, support technique et tarifs. Recherchez une solution SASE monofournisseur bien conçue, qui soit intégrée, unifiée, flexible et facile à utiliser.
- **Étape 3 : concevoir et développer votre stratégie SASE.** Collaborez avec votre prestataire pour définir la topologie de votre réseau, les politiques de sécurité, les groupes d'utilisateurs, les profils d'applications et les options de connectivité en fonction des meilleures pratiques. Ce processus avec votre prestataire doit être collaboratif afin de garantir une réussite optimale pour votre entreprise.
- **Étape 4 : commencer le déploiement SASE avec une approche graduelle.** Déployez les composants nécessaires tels que les agents, les connecteurs, les dispositifs SD-WAN ou les points de référence privés par le biais d'une console de gestion centralisée. Migrez vos utilisateurs, dispositifs, sites et applications vers votre solution SASE en utilisant une approche par phases ou par lots. Le SASE peut fonctionner en tandem avec les solutions existantes, permettant un déploiement rapide ou lent, selon les besoins de votre équipe.
- **Étape 5 : exploiter le plein potentiel du SASE.** Avec la poursuite du développement, utilisez les outils et les tableaux de bord de votre prestataire pour obtenir une visibilité, des connaissances et des commentaires pour optimiser encore davantage votre solution SASE. Optimisez au maximum votre investissement et découvrez de nouveaux cas d'utilisation et des fonctionnalités où le SASE peut être également bénéfique à votre entreprise.

[5] Magic Quadrant para SASE de proveedor único, Gartner, julio de 2024

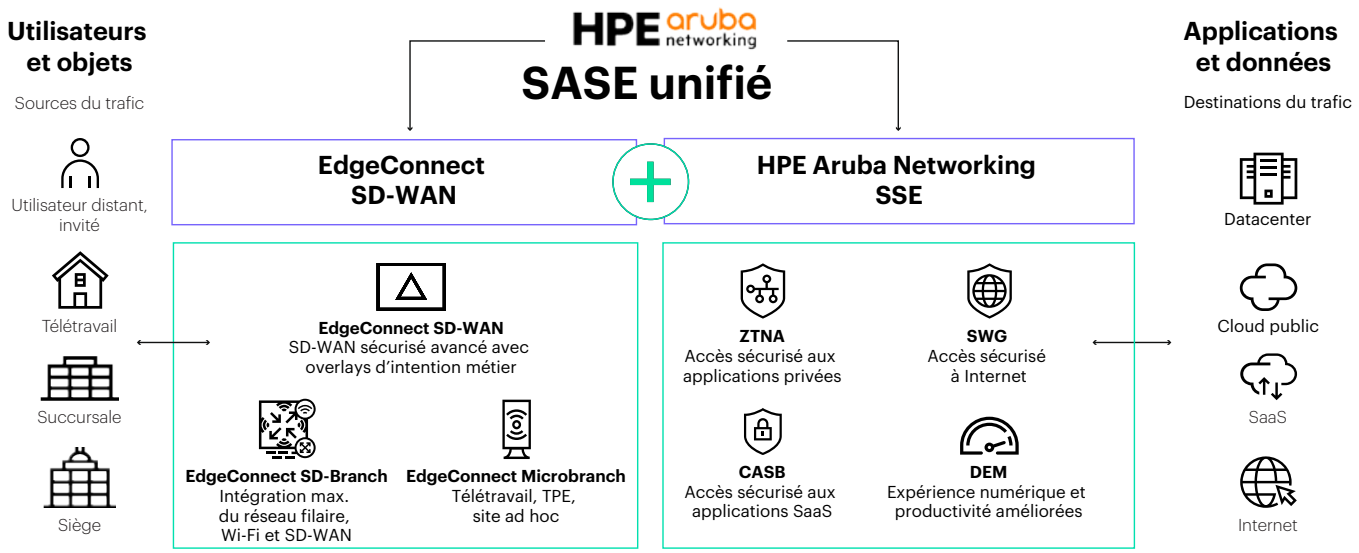

Figure 2. Plateforme de SASE unifié HPE Aruba Networking

Un SASE unifié, sûr et piloté par l'IA grâce à HPE Aruba Networking

Si vous recherchez une solution SASE monofournisseur et puissante qui offre un accès professionnel sécurisé et fiable depuis n'importe quel endroit, l'architecture SASE de HPE Aruba Networking peut être la solution. Avec son SD-WAN de pointe et SSE primé, HPE Aruba Networking offre une approche unifiée et complète au SASE conçu pour l'entreprise distribuée et dynamique moderne.

Produisez des résultats innovants pour votre entreprise grâce aux solutions HPE Aruba Networking complètes de réseau pilotées par l'IA et axées sur la sécurité, qui connectent et protègent votre entreprise de l'edge au cloud sans aucun compromis sur les hautes performances. Conçues selon les principes du zero trust, elles offrent aux entreprises de multiples avantages : visibilité accrue, gestion centralisée des politiques, protection des données, défense contre les menaces, contrôle des accès et automatisation intelligente. Les équipes informatiques peuvent fournir des contrôles de sécurité WAN et cloud directement sur l'application à l'edge du réseau grâce à HPE Aruba Networking EdgeConnect SD-WAN, plutôt que d'acheminer les données via le datacenter. De plus, le SSE veille à ce que les contrôles de sécurité zero trust puissent être appliqués à toutes les personnes et tous les dispositifs, quel que soit l'endroit de connexion : sur le campus, dans une filiale, à la maison ou en déplacement. Les informations sur le réseau et la sécurité obtenues grâce à l'IA vous aident à assurer la gestion et la protection à grande échelle, ce qui libère les équipes réseau et de sécurité, leur permettant de se concentrer sur les tâches plus stratégiques.

Démarrer votre parcours SASE

« 65 % des entreprises interrogées indiquent avoir déployé ou prévoir de déployer le SASE. »

– Rapport 2025 du Ponemon Institute[6]

Le SASE n'est pas une simple tendance technologique éphémère, mais un impératif stratégique pour les entreprises modernes qui cherchent à prospérer dans l'ère numérique. Ce cadre permet aux entreprises de surmonter les défis et les risques des architectures réseau et de sécurité axées principalement sur le contrôle du réseau, tout en améliorant leur politique de sécurité, l'expérience utilisateur, l'efficacité opérationnelle et leurs budgets.

Grâce au SASE unifié fourni par un seul prestataire SASE qui répond à vos objectifs et à vos exigences, vous pouvez y arriver encore plus rapidement.

Si le SASE unifié semble répondre aux besoins actuels de votre entreprise, une question reste en suspens : où souhaitez-vous démarrer votre implémentation ? Voici les deux voies les plus courantes suivies par les entreprises.

[6] 2025 Ponemon Institute report

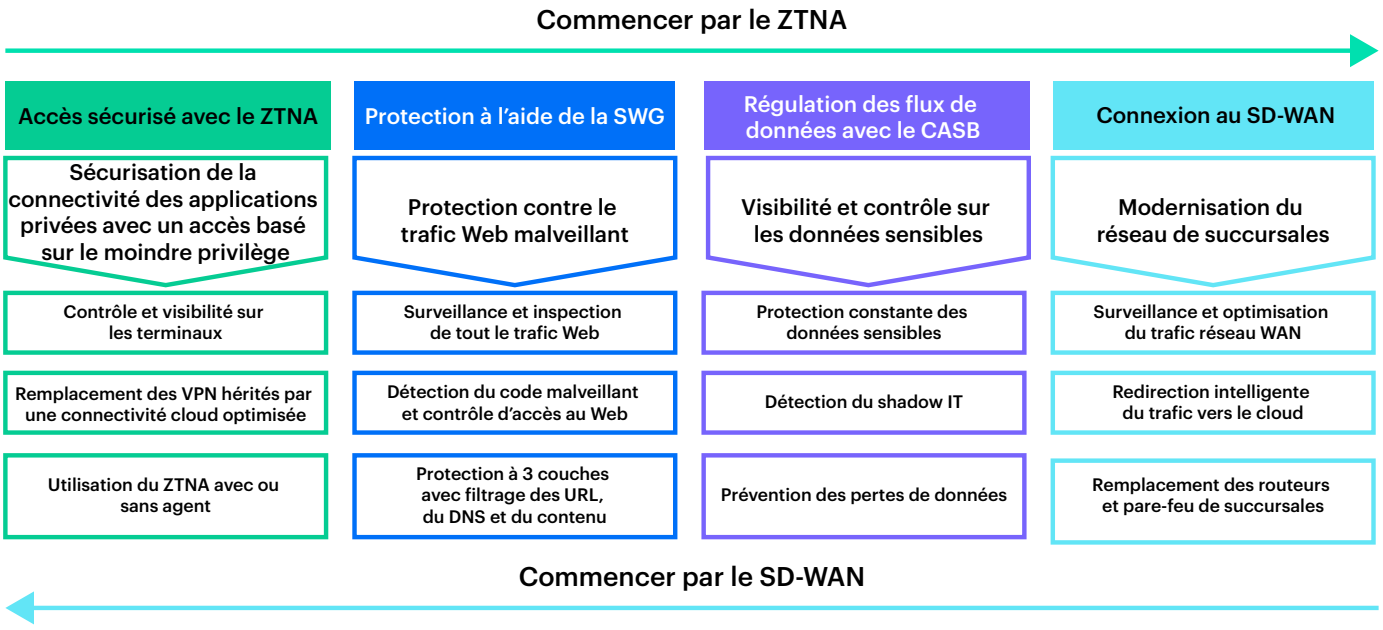

Figure 3. Parcours vers le SASE

1re possibilité : commencer par le SSE (et plus particulièrement par le ZTNA)

Le rapport 2024 d'adoption du SSE a conclu que 57 % des entreprises prévoyaient de lancer leur parcours SASE par la technologie SSE. Si cette approche vous parle, commencez par remplacer vos VPN par le ZTNA HPE Aruba Networking pour assurer un accès zero trust à vos applications privées, qu'elles soient hébergées dans votre datacenter, sur le cloud ou dans un emplacement intermédiaire.

En savoir plus sur HPE Aruba Networking SSE

2nde possibilité : commencer par le SD-WAN

Lancez votre parcours SASE en vous attaquant au SD-WAN. Complétez votre portefeuille d'edge sécurisé (TPE/bureaux à domicile, succursales, campus ou WAN) avec un fabric SD-WAN unique soutenu par la technologie HPE Aruba Networking EdgeConnect SD-WAN.

En savoir plus sur HPE Aruba Networking EdgeConnect SD-WAN

En savoir plus sur le SASE HPE Aruba Networking

Visit HPE.com

Live Chat Ventes

a00133570FRE, révision 3

HEWLETT PACKARD ENTERPRISE

hpe.com

infodium
L'art de la technologie

t/f : +213 28 23 11 31
m : +213 550 918 676/678
sales@infodium-dz.com | www.infodium-dz.com