Guide pratique

# Les secrets d'une migration SASE réussie

verizon business

# Sommaire




# Comment surmonter les obstacles à l'intégration SASE

De plus en plus d'entreprises se tournent vers le SASE (Secure Access Service Edge) pour optimiser leurs opérations, tout en renforçant la sécurité de leur réseau. Mais le processus de transition et d'intégration peut se révéler complexe. Quels sont les écueils à éviter ? Comment les entreprises peuvent-elles surmonter ces obstacles ? Les experts Verizon vous livrent leurs conseils pour négocier ce virage en toute sérénité.

Face à l'intensification des cybermenaces et à la sophistication croissante des attaques, les entreprises doivent se doter d'une sécurité réseau plus efficace que jamais. Mais, pour accéder à leurs applications et à leurs données, elles doivent aussi compter sur des environnements multicloud, qui ne cessent d'étendre leur surface d'attaque. Et bien que le travail en présentiel ait regagné du terrain, les modèles hybrides sont toujours d'actualité, ce qui ne fait qu'exacerber le problème.

Une architecture SASE désigne un SD WAN (Software Defined Wide Area Network) associé à des technologies SSE (Secure Service Edge). Autrement dit, il s'agit d'un WAN offrant une connectivité parfaitement intégrée dans n'importe quel environnement (mobile, Internet public, réseau privé, etc.) et bénéficiant d'une stack de sécurité complète. Les entreprises peuvent ainsi se protéger plus efficacement et simplifier la gestion de leurs politiques grâce à un framework unique faisant converger les capacités réseau et les fonctions de sécurité. Conjugué à une approche Zero Trust, le SASE renforce par ailleurs la gestion des accès, pour que seuls les utilisateurs et les appareils autorisés puissent se connecter au réseau. Enfin, il facilite le déploiement d'environnements cloud modernes et distribués dépassant les limites des modèles traditionnels de sécurité réseau, moins efficaces pour la configuration et la gestion des équipements.

> De plus en plus d'entreprises adoptent donc un modèle SASE pour tenter d'alléger la pression qui pèse sur leurs équipes de sécurité réseau.

Le SASE incarne donc une approche holistique permettant aux entreprises de fluidifier leurs opérations, de mieux se protéger des cybermenaces et de fournir un accès sécurisé aux équipes hybrides, où qu'elles se trouvent. Toutefois, la transition se fait rarement sans heurts. Qu'il s'agisse de gérer une intégration entre de multiples technologies ou de créer de nouveaux processus métier, l'adoption du SASE peut en effet se révéler complexe et présenter de nombreux défis.

# Les challenges de la migration SASE

## 1 Le poids des technologies et des environnements existants

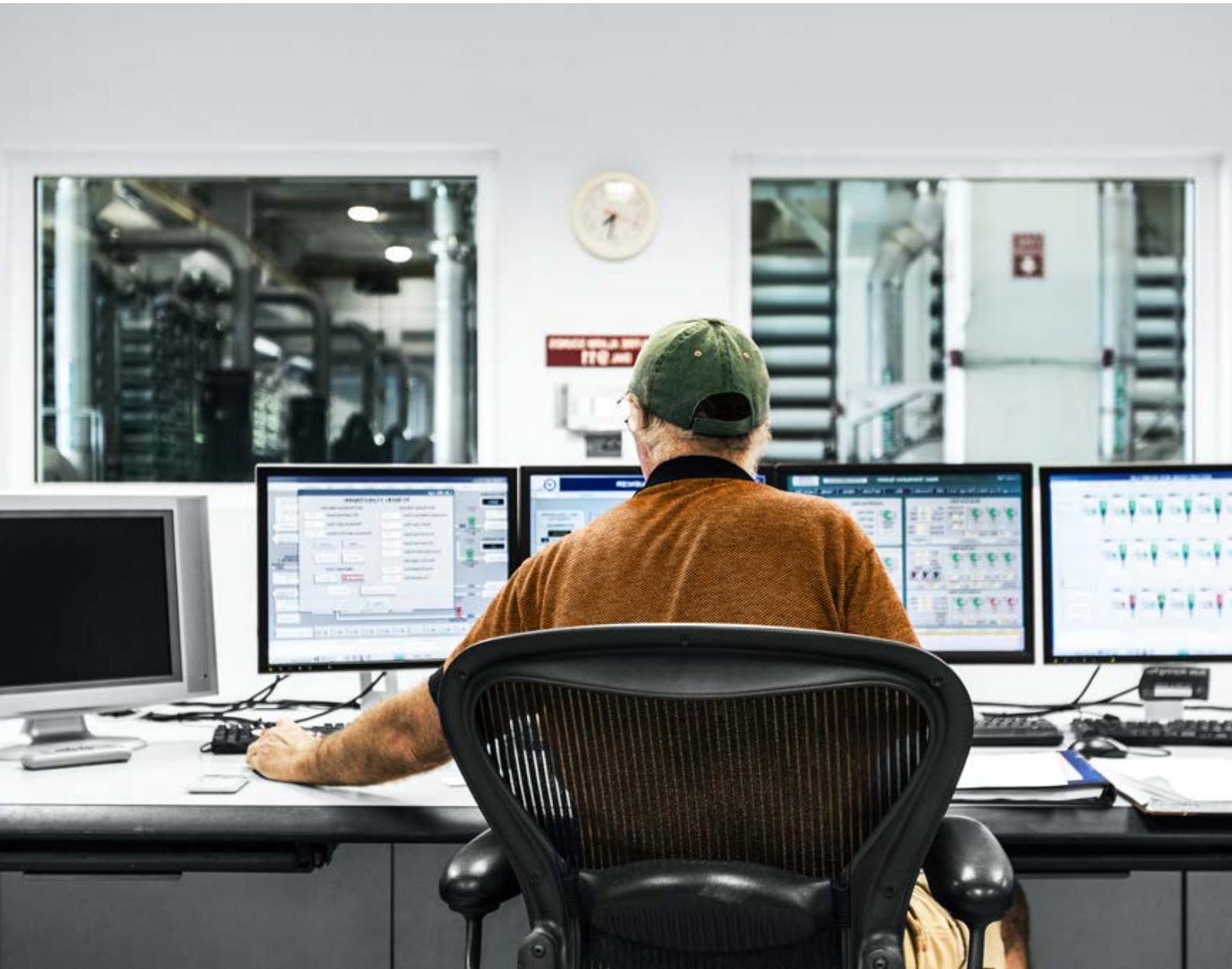
Pour un grand nombre de nos clients, la décision de s'engager dans une transition SASE est rythmée par deux facteurs clés : les contrats fournisseurs en cours et le cycle de vie des technologies utilisées. Nos méthodes de travail actuelles dépendent fortement de la technologie. Lorsqu'une entreprise envisage de remplacer son infrastructure IT vieillissante, elle sait que cette décision aura un impact majeur sur les processus métier et l'expérience client. Lors d'une migration SASE ou d'une mise à niveau d'envergure, la planification est dès lors essentielle pour assurer la continuité des opérations.

D'après Jeff Paterson, Solution Architect de Verizon au service des grandes entreprises internationales, « il ne s'agit pas simplement de remplacer l'architecture existante par un nouvel environnement SD WAN ou SASE flambant neuf. C'est aussi une question d'intégration. Il est donc primordial de choisir une technologie SD WAN et des composants SSE capables de s'intégrer à ces environnements hybrides déjà en place, mais aussi de s'incorporer en natif aux environnements CSP et cloud existants. Cette approche est essentielle pour réussir sa transition vers une solution SASE complète. »

## 2 Le choix du fournisseur : source de désaccord entre les équipes

De nombreuses entreprises éprouvent également des difficultés à fédérer des acteurs qui n'ont guère l'habitude de collaborer. Jusqu'à présent les équipes réseau et sécurité s'appuyaient en effet sur des fournisseurs « best-of-breed », spécialisés dans leur domaine de prédilection. Peu d'entre eux pouvaient revendiquer des compétences dans les deux disciplines. Mais bien que tous s'accordent sur l'importance de passer à une architecture SASE, il est parfois difficile de les mettre d'accord sur le ou les fournisseurs offrant la solution la plus adaptée. Cette question exige donc souvent des analyses et des discussions approfondies qui peuvent ralentir le processus.

> Il ne s'agit pas simplement de remplacer l'architecture existante par un nouvel environnement SD WAN ou SASE flambant neuf. C'est aussi une question d'intégration.
>
> **Jeff Paterson**
> Solution Architect, Verizon Business



## 3 L'intégration de multiples technologies

Les entreprises doivent parfois intégrer les technologies de différents fournisseurs. Un challenge de taille, dans la mesure où ces outils n'ont pas été conçus pour fonctionner en synergie, comme le ferait une solution unifiée. Cette difficulté concerne aussi bien le provisionnement et l'intégration d'un système de sécurité cloud au sein d'une solution SD WAN que la configuration de politiques SaaS. Et si un tableau de bord unifié est essentiel, il est parfois très compliqué d'y rassembler des informations provenant de différents fournisseurs.

Les entreprises doivent par ailleurs jongler entre les exigences fondamentalement différentes de leurs équipes réseau et sécurité. Par exemple, les équipes SecOps ont souvent besoin d'un accès total à la configuration des politiques de sécurité pour répondre en temps réel aux événements et aux menaces. En revanche, les équipes réseau peuvent se contenter d'un accès limité à la configuration des politiques SD WAN. Cette approche leur permet de mener à bien leur mission en toute autonomie, sans risquer d'introduire, par erreur, des modifications pouvant avoir des répercussions catastrophiques.

Face à ces obstacles, comment les entreprises doivent-elles réagir pour implémenter une architecture SASE en phase avec leurs objectifs métier ?

## La voie de la réussite

La planification est une étape essentielle pour réussir son intégration SASE. Il est par ailleurs primordial d'identifier les enjeux et les acteurs responsables à chaque stade du déploiement. Pour atteindre vos objectifs et vous assurer que toutes vos équipes sont au diapason, vous devez donc élaborer une feuille de route indiquant clairement la marche à suivre. Comme le souligne Jeff Paterson : « Vous devez définir des objectifs précis, avec l'aide de votre partenaire si besoin. Enfin, il est primordial que vous documentiez ces lignes directrices pour les faire valider par vos parties prenantes. »

> Vous devez définir des objectifs précis, avec l'aide de votre partenaire si besoin. Enfin, il est primordial que vous documentiez ces lignes directrices pour les faire valider par vos parties prenantes.
>
> **Jeff Paterson**
> Solution Architect, Verizon Business

## Impliquer les bonnes personnes, au bon moment

Une intégration SASE est un processus complexe impliquant un grand nombre de personnes et de composants. Dans ce contexte, il est essentiel de s'assurer que toutes les parties prenantes concernées disposent des informations nécessaires et s'investissent pleinement dans le projet. Fyllon Papadopoulos, Associate Fellow et responsable technique SASE de l'équipe Design Authority Tier 2 pour Verizon Business, est formel. Le manque de concertation entraîne « des problèmes d'alignement entre les équipes réseau et sécurité et crée une approche fragmentée pour la sélection des fournisseurs. Résultat, le développement des architectures et des concepts se fait en silo, pour les composants SSE et SD WAN. »

Si elle est reléguée au second plan, sans planification efficace, l'intégration des différents composants du SASE peut se heurter à de nombreux obstacles. « En fonction du choix du fournisseur, ajoute Fyllon Papadopoulos, le provisionnement des tunnels SSE sur les terminaux SD-WAN peut ne pas prendre en charge l'automatisation, et nécessiter ainsi une charge de travail significative pour la configuration.

Ou alors le manque de contrôles de sécurité ou l'absence d'API entre le SD WAN et les composants SSE peut empêcher les tunnels de basculer automatiquement et exiger une intervention manuelle. En outre, les inspections de sécurité à déployer pour certaines applications peuvent requérir des politiques SD WAN particulièrement complexes à configurer. »

Pour éviter ces écueils, il est important que les équipes réseau et sécurité travaillent en étroite collaboration dès les premières étapes du projet. Le but :

- S'accorder sur le choix du fournisseur et l'interopérabilité
- Vérifier que l'architecture et le design sont en phase avec les objectifs
- Réaliser des économies grâce à l'intégration et à la consolidation
- S'assurer que les technologies déployées répondent à des cas d'usage spécifiques

## Élaborer un plan sur mesure

Votre stratégie d'implémentation doit se baser sur les besoins spécifiques de votre entreprise ainsi que sur votre budget et votre écosystème actuel. Ces éléments doivent en effet être pris en compte dès le départ si vous ne voulez pas vous retrouver avec une solution inadaptée et trop chère par rapport à vos objectifs. Jeff Paterson pose clairement la question : « Que voulez-vous faire ? Vous concentrer sur les applications critiques qui permettent à votre entreprise de fonctionner ? Ou étendre le processus à toutes vos applications, sachant qu'il peut y en avoir des centaines, voire des milliers, avec les délais, les efforts et le budget que cela implique ? » Élaborer un plan cohérent dès le départ vous permettra de gagner en efficacité et d'optimiser l'implémentation.

> Que voulez-vous faire ? Vous concentrer sur les applications critiques qui permettent à votre entreprise de fonctionner ? Ou étendre le processus à toutes vos applications ?
>
> **Jeff Paterson**
> Solution Architect, Verizon Business

## Avancer pas à pas

Il n'existe pas de formule universelle pour réussir sa transition. Les organisations doivent donc définir leur stratégie d'implémentation en fonction de leurs besoins. Il est toutefois généralement déconseillé aux grandes entreprises de mener de front la migration du réseau et des systèmes de sécurité. Une telle opération se révèle en effet risquée pour la continuité d'activité et mobilise de nombreuses ressources. Comme l'explique Mike Hannan, Security Solutions Architect chez Verizon : « Lorsque nos clients sont implantés sur de nombreux marchés et disposent déjà d'une multitude d'applications, nous avons tendance à adopter une approche progressive. Nous nous focalisons d'abord sur les applications critiques, pour lesquelles nous réalisons des PoC, puis nous passons aux projets pilotes, d'abord petits puis de plus en plus grands, avant de procéder à des déploiements complets. »

> Lorsque nos clients sont implantés sur de nombreux marchés et disposent déjà d'une multitude d'applications, nous avons tendance à adopter une approche progressive.

**Mike Hannan**
Security Solutions Architect, Verizon Business

## Fixer des délais réalistes

Le délai d'implémentation dépend lui aussi des spécificités de l'infrastructure et de la stratégie adoptée. « Migrer à la fois le réseau et les systèmes de sécurité n'est pas une mince affaire », ajoute Mike Hannan. « Vous aurez sans doute besoin de faire appel à un partenaire aguerri, mais aussi de mobiliser de nombreuses ressources internes. » Il est donc important de faire preuve de réalisme au moment de déterminer l'ampleur, la durée et les objectifs du projet. « Une transition progressive se révèle beaucoup plus accessible », poursuit Mike Hannan. « Par exemple, les entreprises peuvent se concentrer sur les accès à distance avant de se pencher sur les communications sur site pour acquérir la visibilité nécessaire à un modèle Zero Trust. »

> Migrer à la fois le réseau et les systèmes de sécurité n'est pas une mince affaire.
>
> **Mike Hannan**
> Security Solutions Architect, Verizon Business

## Miser sur le bon partenaire

Une intégration SASE peut se révéler d'une grande complexité. Pour mener à bien votre projet, il vous faudra peut-être faire appel à un partenaire expérimenté. Dans ce cas, Jeff Paterson recommande « de choisir et de collaborer avec un fournisseur versé dans la conception, l'implémentation et l'exploitation de réseaux complexes et sécurisés, quelle que soit la zone géographique concernée ».

En effet, un partenaire rompu à la transformation des infrastructures réseau et de sécurité des grandes entreprises sera le mieux placé pour guider et accompagner votre transition IT. Il pourra par ailleurs vous aider à définir vos objectifs, puis à déployer et à gérer un environnement SASE en parfaite adéquation avec vos besoins. « Il est essentiel de collaborer avec un fournisseur ayant déjà fait ses preuves dans le domaine des réseaux connectés sécurisés », conclut Jeff Paterson. « Vous aurez ainsi la garantie que votre architecture SASE s'intégrera parfaitement à votre environnement existant et que l'implémentation se déroulera sans encombre. Vous pourrez aussi vous appuyer sur son expertise pour vous assurer que les équipes opérationnelles disposent des connaissances nécessaires pour gérer votre nouvelle infrastructure ».

> Il est essentiel de collaborer avec un fournisseur ayant déjà fait ses preuves dans le domaine des réseaux connectés sécurisés.
>
> **Jeff Paterson**
> Security Solutions Architect, Verizon Business

# Contactez-nous

Avec plus de 20 ans d'expérience dans la conception réseau, la transformation des écosystèmes IT et la gestion de la sécurité réseau, Verizon vous accompagne à chaque étape de votre transition SASE. Armés de nombreuses certifications sectorielles, nos experts excellent dans l'art d'identifier les technologies les plus à même de répondre aux besoins spécifiques de chaque entreprise. Et grâce à nos investissements continus dans nos centres NOC et SOC, vous pouvez compter sur des solutions réseau sécurisées et automatisées, entièrement managées ou cogérées, parfaitement adaptées à l'ère du tout numérique.

Découvrez comment les solutions de Verizon vous aident à planifier et à gérer votre intégration SASE : verizon.com/business/fr-fr. Cliquez ici pour vous inscrire à notre newsletter et en savoir plus sur nos solutions SASE et de sécurité.

## Ressources

### SASE Management

Simplifiez la sécurité dans toute votre entreprise. Notre solution SASE Management combine sécurité réseau et cloud pour connecter l'humain, les données et les équipements dans tous vos environnements (périphérie, bureaux et cloud).

**Plus d'infos >**

### Partenaires

Nous collaborons avec les plus grands acteurs du marché pour fournir des solutions performantes et garantes d'une rentabilisation accélérée pour votre entreprise.

**Plus d'infos >**

### Digital Enablement Platform

Intégrez vos API à Verizon pour rationaliser votre gestion des stocks, des incidents et des changements sur notre Digital Enablement Platform.

**Visionner la vidéo >**

verizon business

© 2024 Verizon. Tous droits réservés. Verizon, le logo Verizon et tous les autres noms, logos et slogans identifiant les produits et services de Verizon sont des marques commerciales et des marques de service, déposées ou non, de Verizon Trademark Services LLC ou de ses filiales aux États-Unis et/ou dans d'autres pays. Les autres marques commerciales et marques de service citées sont la propriété de leurs détenteurs respectifs.