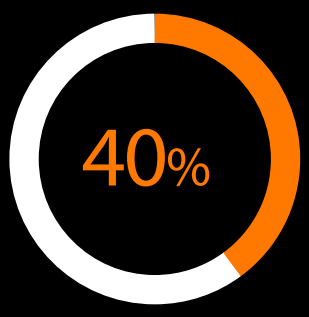
SASE : Quelle stratégie à adopter ?



Gartner prévoit que 40 % des entreprises auront une stratégie SASE d'ici 2024, mais le chemin est long de la stratégie à sa concrétisation.Les entreprises ont donc intérêt à se préparer dès aujourd'hui aux changements architecturaux et culturels profonds qu'implique ce modèle.

Nombreuses sont les organisations qui n'ont guère le choix car la pandémie leur a forcé la main. Certains concepts du SASE ont déjà été adopté, comme le zéro trust en réponse à la nécessité de travailler à distance.

Cette feuille de route a vocation de vous guider dans votre adoption SASE :

1 Réaliser un « business case »

Commencez par faire valoir le bien-fondé du SASE auprès des principaux décideurs. Cela implique à la fois une stratégie à long terme et des propositions plus simples et immédiates dans le cadre d'un déploiement progressif.

2 Créer des synergies entre équipes sécurité et réseau

Les équipes de sécurité et de réseau doivent absolument communiquer entre elles pour concevoir et déployer un modèle SASE. Créez, le plus tôt possible, des synergies entre ces équipes afin de fluidifier les travaux d'intégration à venir.

3 Evaluer l'impact opérationnel et organisationnel sur vos réseaux et votre sécurité

Lorsqu'elles élaborent une architecture SASE à long terme, les équipes de conception doivent tenir compte de l'impact opérationnel sur leurs systèmes.

4 Commencer par le SD-WAN

L'approche SASE a besoin d'une plateforme réseau « logicielle » pour le déploiement de services Cloud en périphérie. Il demande donc de s'appuyer sur une architecture SD-WAN, dont une transition des communications MPLS vers des communications Internet. Il est essentiel de maitriser cette étape en gardant à l'esprit les services logiciels de sécurité réseau, au nombre desquels une solution d'accès distant embarquée très tôt dans le SD-WAN afin de garantir un niveau de sécurité uniforme pour les télétravailleurs.

5 Migrer les services de cybersécurité vers le Cloud

Une fois la solution SD-WAN en place, il est temps de planifier la migration des services de sécurité sur site vers des Points de Présence (POP) sur le réseau logiciel, dans le Cloud. Cette étape implique une transition vers un fournisseur de services de sécurité dans le Cloud.

6 Déplacer votre modèle de sécurité vers un concept d'accès réseau zero-trust

Les organisations doivent envisager leur migration vers des services de sécurité dans le Cloud en gardant à l'esprit la notion de zero-trust lorsqu'il s'agit d'accès réseau. Ce principe implique de se préparer à identifier les accès à toutes les applications. Construire les composantes — gestion des identités et accès, gestion des cycles de vie — qui supporteront une migration vers des accès basés sur l'identité. À ce point, il convient aussi d'envisager des technologies complémentaires — authentification multifacteur et contrôle d'accès au réseau selon les équipements — pour protéger les outils mobiles qui accèdent à des applications métier.

7 Développer une structure d'automatisation

Une fois votre modèle logiciel de sécurité réseau en place, vous serez bien placés pour rendre votre infrastructure sécurité encore plus efficace en recourant à l'automatisation. Investir dans la création et l'amélioration de logiciels de contrôle de sécurité et réseau qui serviront de socle à des opérations sécurité robustes et évolutives.

8 Adopter une approche fondée sur le renseignement

Après avoir défini le modèle, il est crucial de l'étayer avec le niveau souhaité de renseignements et d'opérations de cybersécurité. Les attaquants ne restent pas immobiles. Votre tissu de sécurité SASE ne doit pas l'être non plus.

Notre approche SASE basée sur le renseignement

S'adapte à votre entreprise face au paysage des menaces

- Surveillance de l'infrastructure pour détecter les incidents et remédier aux cyberattaques.
- Construire et concevoir une expérience fiable et cohérente
- Renforcer la sécurité du réseau entre les utilisateurs, les applications et les données, quel que soit le lieu.

Orange Cyberdefense propose une approche SASE basée sur notre réseau de renseignements. Il s'agit d'un mécanisme de renseignement de cybersécurité de bout en bout qui combine notre R&D interne et nos données opérationnelles avec des dizaines de bases de données de menaces constamment mises à jour et des informations provenant des forces de l'ordre. Nous pouvons importer ce renseignement dans votre stratégie de sécurité basée sur le SASE afin d'offrir un niveau de sécurité basée sur les services, personnalisé en fonction de vos besoins, qui adaptera vos défenses aux menaces émergentes.

Découvrez comment l'approche SASE d'Orange Cyberdefense peut contribuer à la transformation de votre entreprise

https://orangecyberdefense.com/global/solutions/sase-secure-access-service-edge/