Orange
Cyberdefense

SASE : renforcer la sécurité des utilisateurs et de leurs ressources

Simplifier et protéger l'architecture réseau de votre organisation

Simplifier et protéger l'architecture réseau de votre organisation

Les organisations opèrent des changements inédits : elles basculent leurs services vers le Cloud et leurs employés travaillent davantage à distance. Dans ce nouveau modèle, Internet devient le nouveau réseau de l'entreprise. L'architecture de sécurité traditionnelle, orientée réseau, ne permet plus d'assurer une protection performante, permanente et uniforme sur tous les appareils des utilisateurs. L'heure est donc venue de réflechir à une nouvelle architecture de sécurité répondant aux besoins de protection de l'organisation.

Sommaire

Auteur : Jose Araujo, Group CTO, Orange Cyberdefense Pays-Bas

Avec la participation de Grégory Scola-Grimaldi, Cloud Security Leader, Orange Cyberdefense, et de Thomas Sourdon, Strategic Marketing and Innovation Director, Connectivity Business Unit, Orange Business.

Introduction

L'environnement métier moderne et la généralisation du télétravail nécessitent de pouvoir accéder en tout sécurité aux données et applications, à tout moment depuis n'importe quel appareil, où qu'elles soient hébergées. Le modèle de sécurité réseau traditionnel ne permet pas d'adresser ces nouveaux besoins de manière optimale.
En effet, les architectures de sécurité actuelles ont été conçues pour des équipements et des utilisateurs ne s'éloignant que rarement du périmètre du réseau de l'entreprise.

A présent, les utilisateurs, les équipements et les applications communiquent en dehors du réseau de l'entreprise. Le modèle de sécurité traditionnel s'avère donc moins pertinent puisqu'il ne permet pas d'assurer une parfaite sécurité des outils mobiles et du Cloud computing qui constituent aujourd'hui une partie majeure des activités des utilisateurs. Les organisations doivent réfléchir à une nouvelle stratégie de sécurité qui remplace leur modèle de sécurité actuel.

En août 2019, Gartner a proposé un nouveau modèle connu sous l'acronyme SASE (Secure Access Service Edge). Ce modèle repense l'architecture réseau et sa sécurité, aidant les organisations à s'adapter aux nouvelles exigences en matière de sécurité des utilisateurs et de leurs ressources, pour garantir le maintien d'un haut niveau de sécurité.

Le modèle SASE se présente comme un défi et une initiative ambitieuse. Le marché doit encore parvenir à appréhender les idées qu'il sous-tend pour soutenir ce modèle. Quant aux éditeurs, il est nécessaire qu'ils proposent des solutions suffisamment amples et poussées pour supporter ce modèle.

En attendant, nous pouvons commencer à échanger sur ce concept, à suivre les évolutions du marché SASE et à assister nos clients sur l'adoption d'une stratégie à long terme fondée sur la connaissance de la menace.

Ce livre blanc décrit le modèle SASE, liste ses avantages et aborde les défis actuels. Il vous aiguillera si vous vous apprêtez à adopter ce modèle pour sécuriser vos utilisateurs et leurs activités numériques.

Qu'est-ce que le SASE ?

Le modèle SASE est une nouvelle approche de la sécurité du réseau de l'organisation. Il crée un lien entre le réseau et sa protection, offrant à l'ensemble des utilisateurs — où qu'ils se trouvent — des accès sécurisés. Il ne s'agit pas simplement d'une solution que les entreprises peuvent installer et oublier. C'est une discipline qui nécessite une surveillance, une détection et une réponse continue, alimentée par un renseignement de la menace en constante évolution.

Ce modèle permet une meilleure protection des accès aux données échangées sur l'Internet et stockées dans le Cloud. Il met en place un ensemble de mesures de prévention des menaces par l'intermédiaire de services de sécurité, implantés en périphérie du réseau étendu, au plus près des utilisateurs. Il s'appuie grandement sur l'identité des utilisateurs pour autoriser les accès aux données et applications, plutôt que de faire confiance aux appareils et réseaux déjà identifiés.

Cette nouvelle approche redéfinit le périmètre traditionnel de sécurité, en le substituant par des services Cloud qui intègrent des systèmes de cybersécurité. Cela permet aux organisations de disposer de services de sécurité réseau via des logiciels qui permettent la création d'une plateforme unique capable d'appliquer des politiques de sécurités unifiées lors de chaque session de travail, pour plus de granularité dans les contrôles d'accès des utilisateurs.

Cet écosystème unifié de sécurité s'étend sur un réseau global, permettant aux utilisateurs d'accéder facilement à leurs ressources, où qu'ils soient, et de façon sécurisée. Il est également extensible, ce qui permet aux entreprises d'offrir davantage de services de sécurité à leurs utilisateurs, à mesure que les besoins métiers changent.

SASE : un challenge de sécurité pour les organisations

Le modèle SASE représente un changement radical dans la façon dont nous percevons la sécurité, ainsi qu'un investissement important en temps et en efforts. Pourquoi les entreprises devraient-elles alors l'envisager ?

Dans un monde où les pratiques et les infrastructures de travail sont confrontées à des changements profonds, les organisations doivent trouver d'autres moyens de garder le contrôle de leurs données. Aujourd'hui, des équipements non fiables se connectent à des ressources informatiques depuis des réseaux non contrôlés.

Les organisations ont besoin de ce modèle pour surmonter la complexité générée par ces changements dans l'organisation. SASE permet à l'organisation de bénéficier d'une infrastructure réseau intégrée, programmable et unifiée qui alie performance et sécurité des accès, en s'appuyant sur la flexibilité du Cloud.

Les services de sécurité doivent protéger les applications et données peu importe leur emplacement sur le Cloud. IDC estime que le total des dépenses mondiales en produits et services Cloud affichera un taux de croissance annuel composé (TCAC) de 15,7 % d'ici à 2024. La nouvelle approche SASE en matière de sécurité réseau progressera à mesure que les applications seront "Cloud-native".

> "IDC estime que le total des dépenses mondiales en produits et services Cloud affichera un taux de croissance annuel composé (TCAC) de 15,7 % d'ici à 2024.[1]

Les services qui découlent du modèle SASE deviennent aussi un prérequis pour l'entreprise face à l'évolution de nos modes de travail. La pandémie a accéléré la tendance grandissante du recours au télétravail. Selon la Commission européenne, près de 40 % des travailleurs dans l'Union européenne sont passés au télétravail à temps plein durant la pandémie de COVID-19. Une progression spectaculaire : avant la crise, seuls 15 % des employés européens avaient déjà télétravaillé.

En l'espace de quelques mois seulement, les organisations ont constaté des lacunes dans la sécurisation des utilisateurs qui

> "Selon la Commission européenne, près de 40 % des travailleurs dans l'Union européenne sont passés au télétravail à temps plein durant la pandémie de COVID-19.[2]

étaient en télétravail : les entreprises peinaient à répondre aux besoins de leurs nouvelles forces de travail à distance. En avril 2020 — au début de la pandémie — le National Cyber Security Centre britannique, l'US Cybersecurity et l'Infrastructure Security Agency (CISA) avaient émis un communiqué commun avertissant de plusieurs attaques liées à l'épidémie de COVID-19, ciblant les infrastructures d'accès distant et les comptes d'employés qui opéraient à distance.[3]

Dans un monde post-pandémie, la priorité est de prendre l'utilisateur comme élément central de la sécurité. Les télétravailleurs nécessitent des accès plus rapides, plus simples et plus sécurisés à leurs applications, même lorsqu'ils n'utilisent pas des appareils de confiance. Le mode SASE se présente comme la clé garantissant un accès sécurisé pour les utilisateurs.

La croissance de l'Internet des Objets (IoT) crée aussi un besoin qui justifie ce modèle. Selon IDC, d'ici 2025, on dénombrera 55 milliards d'objets connectés dans le monde, dont 75 % se connecteront à une plate-forme IoT. Ils généreront un volume important de données que les entreprises devront gérer et sécuriser. Toujours selon IDC, ce volume issu de l'IoT passera à 73 zettaoctets en 2025, contre 18 zettaoctets en 2019.

Cette croissance nécessite d'augmenter les capacités d'accès aux infrastructures Cloud pour un nombre d'appareils grandissant. Cela consistue un challenge pour les organisations. La combinaison de l'augmentation du nombre de endpoints et de la limitation des capacités de ces mêmes endpoints, fait de la mise en œuvre des mesures de sécurité au niveau des endpoints, un défi. Déplacer la sécurité en périphérie du Cloud aide à adresser ces problématiques infrastructurelles de volume et de complexité.

Sécuriser le réseau dans le Cloud pour protéger l'utilisateur et ses ressources

Les avantages

Le modèle SASE assurera un vaste ensemble de services de sécurité réseau homogènes et intégrés, qui soutiendra la transformation numérique de l'organisation, à l'ère de l'edge computing et du travail à distance. Son adoption permettra de bénéficier des avantages suivants :

Fléxibilité
Le modèle SASE permet aux organisations d'orienter le trafic vers le Cloud, en tout lieu, plutôt que de le router par les datacenters, pour délivrer des services évolutifs en capacités de traitement et en niveau de sécurisation.

Performances améliorées
Le modèle SASE améliore et accélère les accès aux ressources sur Internet via une infrastructure réseau globale et optimisée pour une latence moindre, des capacités élevées et une disponibilité accrue.

Économies budgétaires
Placer la sécurité réseau dans le Cloud contribue à limiter les dépenses infrastructurelles sur site. Les entreprises qui adoptent un modèle SASE peuvent prévoir leurs charges opérationnelles, puisque leur modèle de sécurité repose sur des services.

Zero Trust
Le principe de confiance zéro (Zero Trust) siège au cœur du modèle opérationnel SASE.
Il garantit un accès sécurisé fondé sur l'identité, le rôle et la posture de sécurité au sein d'environnements Cloud et datacenters publiques, plutôt que des accès au niveau réseau.

Complexité moindre
Les organisations peuvent réorienter les tâches de leurs équipes sécurité. Elles ne gèrent plus des appareils individuels, mais délivrent des services de sécurité basés sur des politiques spécifiques en un point unique. Elles peuvent ainsi plus aisément configurer de bout en bout les structures de sécurité réseau.

Prévention des menaces
En plaçant la sécurité en périphérie du réseau, entre l'utilisateur et le Cloud, le modèle SASE permet aux entreprises de mieux détecter et prévenir les attaques Cloud, notamment, le phishing, les malwares, les ransomwares et les malveillances internes.

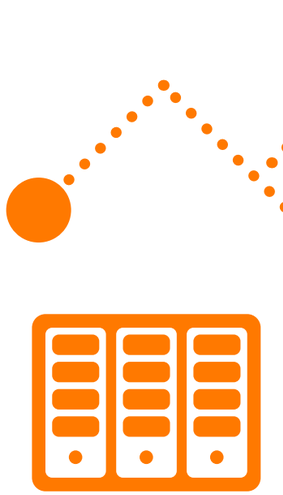
Automatisation accrue
L'infrastructure reposant sur des logiciels constitue un fondement de la proposition SASE. Elle crée une plate-forme technologique convergente, supportant la mise en vigueur de politiques programmées et unifiées. À l'instar des développeurs qui s'appuient sur DevOps, les administrateurs peuvent avoir recours à un modèle de sécurité opérationnel automatisé de bout en bout.

Protection des données
En axant la protection sur l'identité, l'approche SASE offre une protection au niveau des données, en accordant aux personnes l'accès aux ressources de données clés sur la base du moindre privilège dans le cadre d'un processus strict de vérification de l'identité. Les données sont ainsi protégées partout, de l'intérieur de l'organisation au Cloud public, sur des réseaux non fiables, et au-delà.

Une architecture de sécurité d'avant-garde

Pendant des années, les réseaux ont connecté les utilisateurs à des applications hebergées dans des datacenters. Ces réseaux disposaient de nombreux contrôles de sécurité périmétriques pour protéger les applications et les données d'éventuelles menaces externes. Les entreprises ajoutaient parfois des mécaniques de segmentation pour limiter l'effet de potentielles intrusions dans un périmètre donné. Des outils de sécurité avancés pouvaient être installés dans certains périmètres de réseau, ajoutant une couche de protection supplémentaire.

Au commencement, le réseau qui connectait les utilisateurs aux datacenters reposait sur des connections lentes, onéreuses et dédiées. Puis, plusieurs changements dans les organisations se sont produits simultanément : les applications ont migré vers le Cloud, les réseaux edge ont gagné du terrain à mesure que les technologies IoT évoluaient et le monde a opté pour des connexions Internet moins coûteuses et plus rapides. Plus récemment, le travail à distance est devenu la nouvelle norme. Les utilisateurs se connectent davantage hors du périmètre réseau traditionnel, à mesure que les modes de travail ont évolués.



1 Le problème avec l'architecture d'aujourd'hui

Le modèle périmétrique de sécurité réseau n'est plus apte à supporter ce nouveau contexte organisationnel. Il induit en effet de la complexité et des coûts supplémentaires.
Il nécéssité que toutes les connexions passent par des datadenters, même pour des applications hébergées dans le Cloud. Les datacenters deviennent donc limitants et coûteux.

Les outils de sécurité qui sont présents dans les datacenters sont peu flexibles, tributaires de leur localisation, dépendants du trafic qui transite par un réseau spécifique et peu ajustables selon les besoins et activités de l'organisation. Ils s'appuient rarement sur une couche de contrôle logicielle et sont donc difficiles à configurer et à intégrer. Dans ce contexte, il n'est donc pas évident d'appliquer et de maintenir des politiques de sécurité optimales et de maintenir une posturesde sécurité conforme aux bonnes pratiques.

Ce modèle peut fonctionner pour des employés sur site, il nous faut le repenser dans un environnement impacté par la pandémie qui place la plupart des travailleurs hors de portée des contrôles de sécurité traditionnels. Il nous faut reconsidérer nos capacités et méthodes de réponse à incident et réévaluer les responsabilités en matière de sécurité dans ce nouvel environnement de travail.

2 Comment le modèle SASE nous fait avancer

Dans une entreprise numérique moderne centrée sur le Cloud, les utilisateurs et les équipements sont partout. Il en va de même pour les ressources auxquelles ils doivent accéder. Des services sont donc aussi requis pour sécuriser les accès en tout lieu et ils doivent s'intégrer dans un réseau global prêt à servir les utilisateurs où qu'ils soient.

Dans ce réseau étendu, les services de sécurité installés dans des environnements flexibles fonctionnant dans le Cloud au sein de Points de Présence (PoP) situés en périphérie. Ces services comprennent : des pare-feux, des passerelles Web sécurées (SWG), des Cloud Access Security Brokers (CASB), des accès réseau Zero Trust (ZTNA), des DNS sécurisés.

Le modèle SASE s'appuie sur ces services au travers de logiciels de sécurité pour protéger le réseau de bout en bout. Les données sont ainsi sécurisées tout au long de leur parcours, de l'utilisateur à l'application, quel que soit le lieu.

Dans ce modèle, le trafic est routé dynamiquement selon des exigences propres à chacune des sessions. Il permet d'accéder directement aux applications Cloud sans avoir à passer par le datacenter, ce qui réduit les taux de latence et la charge sur les ressources d'entreprise, tout en renforçant la sécurité.

Ce modèle de sécurité en périmétrie place les services de cybersécurité plus près des actifs qu'ils protègent. Ces actifs peuvent être des locaux d'agences, mais aussi des utilisateurs individuels ou des objets connectés. Ce modèle de sécurité réseau prend en charge l'ensemble de ces cas de figure.

L'identité est essentielle au processus d'authentification dans un modèle d'accès au réseau Zero Trust. Plutôt que de s'appuyer sur des outils de confiance pour ce mécanisme, ces services de cybersécurité se basent sur l'identité de l'individu qui se connecte.

Cette approche protège les utilisateurs opérant sur des réseaux qui ne sont pas uniquement ceux de l'entreprise et qui ne sont pas vérifiés : depuis leur domicile ou des réseaux publics, par exemple. Typiquement, les utilisateurs accédant à une plateforme SASE depuis chez eux recourent à un logiciel de gestion des terminaux distants installé sur leurs postes pour les protéger contre d'éventuelles attaques, voire, pour isoler les actifs d'entreprise des actifs personnels. Il est toutefois possible de supporter des outils non gérés en les routant vers des environnements sandbox, directement depuis le Point de Présence.

> “ L'identité est essentielle au processus d'authentification dans un modèle d'accès réseau Zero Trust. Plutôt que de s'appuyer sur des outils de confiance pour ce mécanisme, ces services de cybersécurité se basent sur l'identité de ce qui se connecte.

Néanmoins, le télétravail implique des changements culturels plus vastes et requiert des couches de sécurité additionnelles. Les réseaux domestiques abritent des outils non sûrs (ordinateurs personnels, télés connectées, etc.). Les architectures de sécurité doivent aussi les prendre en compte.

Il faut alors que les organisations réfléchissent sur ce qui constitue le réseau d'entreprise, dans un monde de travail à distance. Les foyers des employés sont-ils une extension du réseau d'entreprise ? Les employeurs doivent-ils traiter les menaces dans ces environnements domestiques comme ils traitent celles susceptibles d'affecter les réseaux d'entreprise ? Faut-il inclure ces environnements dans leurs programmes de gestion des vulnérabilités ? Ces questions architecturales ont une grande importance.

3 Simplifier le réseau

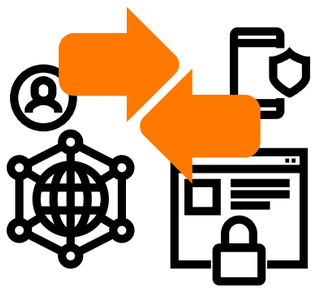
Plus que de la sécurité, le modèle SASE promet aussi de la simplicité. Les réseaux actuels sont souvent encombrés par un mélange de produits de sécurité conçus par différents éditeurs. Ces portefeuilles grandissent de façon organique ou par le biais d'acquisitions, donnant lieu à des ensembles de solutions incompatibles et complexes, dont la gestion est difficile et chronophage. Ils affectent les performances réseau et entravent la sécurité.

Le modèle SASE consolide ces environnements cybersécurité fragmentés sous l'égide d'une plate-forme plus simple et unifiée impliquant un moindre nombre d'éditeurs. Ce principe garantit une sécurité optimale, en tout point du réseau, favorise l'interopérabilité et permet d'identifier les menaces avant qu'elles ne s'immiscent dans le réseau. Il réduit aussi l'impact des outils de sécurité sur la performance et sur les coûts.

4 Au-delà du SD-WAN

Nous avons pris le temps de dire ce qu'est le SASE, mais il faut aussi dire ce qu'il n'est pas. Le modèle SASE ne se résume pas au SD-WAN.

SD-WAN reste un concept assez nouveau : sa mise en œuvre par les éditeurs varie grandement. Il n'est donc pas évident de fournir une composante cybersécurité fiable et uniforme. Nombre d'entre eux fournissent des services de sécurité via des équipements présents dans les locaux des clients et qui peuvent être couteux à mettre en oeuvre et à gérer quotidiennement.



Il ne s'agit pas non plus d'une simple sécurité basée sur le Cloud. Les services Cloud de cybersécurité ne s'intégrant pas parfaitement à des fonctionnalités réseau logicielles passent à côté de la protection Zero Trust SASE, de ses performances et des avantages d'une politique de sécurité uniforme.

Avec le SASE, la combinaison entre réseau et sécurité donne lieu à une approche de la cybersécurité plus simple, moins onéreuse et plus flexible que lorsqu'on considère SD-WAN et la sécurité séparément. Placer les services de cybersécurité sur le réseau logiciel, en tant que services natifs du Cloud, sur des Points de Présence en périphérie, les rend plus faciles à mettre en œuvre et à gérer.

SASE est également plus que la combinaison de ces technologies. Si SASE donne la priorité à l'automatisation comme moyen d'étendre l'accès sécurisé au réseau, il nécéssite d'être abordé sur les services qui sont, eux aussi, automatisés. Les entreprises doivent alimenter leur réseau sensible à la sécurité avec des données de qualité qui mettent en évidence les menaces émergentes des acteurs malveillants. Elles doivent également surveiller en permanence les opérations du réseau pour repérer les signes de compromission et réagir en conséquence.

> “ Avec le SASE, la combinaison entre réseau et sécurité donne lieu à une approche de la cybersécurité plus simple, moins onéreuse et plus flexible que lorsqu'on considère SD-WAN et la sécurité séparément.

L'importance de l'utilisateur

Le modèle SASE unit le réseau et la sécurité, en assurant les deux sous la forme d'un service Cloud, mais sa préoccupation principale réside dans la sécurité du réseau.

Dans un environnement SASE, l'identité appuie les services de sécurité réseau. Il s'agit de la clé permettant d'automatiser la mise en œuvre des politiques de sécurité.

Le modèle SASE permet de contextualiser les prises de décision pour appliquer des politiques de gouvernance de sécurité et définir des droits d'accès. La première donnée contribuant à cette contextualisation est l'identité de l'utilisateur, de l'appareil ou du service qui accède à la ressource. D'autres paramètres, dont le lieu et l'heure de connexion, le niveau de confiance et les informations requises agissent aussi sur le contexte.

Comme ces paramètres peuvent tout changer d'une session à l'autre, dans un environnement SASE, les politiques de cybersécurité s'adaptent lors de chaque session.

> “ Dans un environnement SASE, l'identité appuie les services de sécurité réseau. Il s'agit de la clé permettant d'automatiser la mise en œuvre des politiques de sécurité.

Les principes directeurs

Nous avons décrit l'environnement SASE idéal, mais il faut être réaliste : parvenir à ce but demande des efforts importants. Les chemins vers une solution SASE sont également variés, et les détails de la mise en œuvre dépendront du contexte et des objectifs de l'entreprise. Gartner souligne de nombreux risques dans son rapport et beaucoup ont pour origine une même préoccupation : le manque de compétences des éditeurs.

Nous vous conseillons d'échanger autour de votre projet d'architecture SASE sur le long terme, avec des prestataires de services de sécurité (Managed Service Providers – MSP). Pensez au-delà de vos choix technologiques, en prenant aussi en compte les politiques de sécurité et profils qui peuvent être supportés par les technologies SASE. L'inspection du trafic et la mise en application de la loi - l'un des principes fondamentaux d'une solution d'accès réseau Zero Trust - sont aussi des sujets à traiter en priorité si l'on envisage une architecture SASE.

Mettre en place une stratégie de sécurité qui repose sur un modèle SASE implique un effort de longue haleine : elle redéfinit la façon dont les entreprises appréhendent la sécurité et touche chacune des composantes de leur infrastructure. Entre inertie organisationnelle, investissement conséquent et dette technique, ce projet est à amorcer sur le long terme.

Restez agile

En gardant cela à l'esprit, l'adoption d'un modèle SASE impliquera une série d'étapes incrémentales. Examinez les exigences fondamentales de ce modèle lors du renouvellement de projets existants ou quand vous en implémentez de nouveaux, surtout s'ils ont trait à des services de sécurité (SWG, CASB et VPN).

Cherchez des occasions de consolidation de la sécurité du réseau lors des renouvellements, remplacements et nouveaux développements. Il est temps de combiner des services existants, de simplifier et de dédupliquer les fonctionnalités. Étudiez les décisions d'achat de services de sécurité d'un point de vue stratégique, comprenez comment ils s'intégreront dans votre architecture SASE, plutôt que de vous concentrer de manière isolée sur les caractéristiques de chaque produit.

Tout achat ou redéveloppement est une occasion de migrer des services traditionnels vers une architecture logicielle, gérable depuis une unique console. Veillez à la destruction des silos de sécurité et à l'intégration de produits visant à supporter des politiques unifiées par une seule opération d'inspection.

Ces décisions architecturales façonneront la capacité d'adaptation de l'infrastructure de sécurité. Elles amélioreront leur adaptabilité face à des menaces et des pressions changeantes.

Optez pour l'approche “mini-plateforme”

Le modèle SASE met l'accent sur la consolidation, mais nous estimons qu'il est irréaliste de s'appuyer sur un seul éditeur pour sécuriser l'ensemble des utilisateurs, activités et ressources. Même si les entreprises seront en mesure de travailler avec moins d'éditeurs cybersécurité, elles ne pourront pas se procurer une solution englobant toutes les bases requises fournie par un unique éditeur.

A titre d'exemple, un requis pour les solutions SASE est l'inspection du trafic chiffré à l'échelle. Ce point est particulièrement important dans les environnements qui appliquent plusieurs protections de cybersécurité au trafic. Tous les éditeurs ne supportent pas cette inspection du trafic, chiffré par un traitement unique et multi-services.

Les clients attendent aussi des éditeurs qu'ils soient conscients du contexte des données. Au -delà de l'inspection du trafic chiffré, il convient donc de vérifier comment les données sont utilisées en environnement Cloud. Cette attente sous-entend d'inspecter les environnements des fournisseurs de services Cloud et les interfaces de programmation d'applications (API). Tous les éditeurs ne sont pas à même d'accomplir cette tâche.

La capacité des éditeurs à bien s'approprier le Cloud est aussi remise en question par Gartner. Du fait de leur ancrage dans les outils matériels, le groupe se demande si ces éditeurs n'éprouveront pas des difficultés à passer à la fourniture de services Cloud-native, cruciale en environnement SASE.

Au lieu de vous fier à un seul éditeur, optez pour une approche “mini-plateforme” et limitez le nombre d'éditeurs pour chacune. Trouvez des solutions qui s'appuient sur trois à cinq éditeurs et remplacez-les par des solutions délivrées par un seul fournisseur. Ce principe crée un équilibre entre excellence et efficacité opérationnelle. Les clients devraient faire pression pour négocier des contrats courts avec des licences flexibles auprès des éditeurs pour, au besoin, disposer d'autres choix en cette période d'évolution et de changement.

Bien que la plupart de ces décisions d'achat ne se concrétiseront pas avant un certains temps, vous pouvez commencer à mettre les éditeurs au défi en insistant sur ces exigences naissantes et sur vos critères d'achat. Discutez de votre feuille de route technologique avec des fournisseurs de services réseau et sécurité pour identifier des solutions SD-WAN, SWG, CASB et ZTNA à court et long terme.
La stratégie d'intégration doit être un élément clé de la discusssion car les fournisseurs développeront souvent leurs offres SASE par le biais d'acquisitions.

> “ Les clients devraient faire pression pour négocier des contrats courts avec des licences flexibles auprès des éditeurs pour disposer d'autres choix en cette période d'évolution et de changement.

Pilotez la sécurité à tous les niveaux

Plus que des choix techniques, les initiatives SASE sont aussi culturelles. Leur succès dépend de coopérations entre plusieurs équipes dans l'organisation, dont certaines peuvent être peu enclines ou ambivalentes face au changement.

Les entreprises envisageant sérieusement une transition SASE doivent être prêtes à piloter la sécurité au plus haut de leur hiérarchie et à s'assurer de l'adhésion de la haute direction. Désignez des cadres supérieurs qui seront aptes au pilotage de ce changement et à surmonter des résistances au niveau des équipes. La transition demandera du temps, de la persévérance et de la patience pour l'ensemble des parties prenantes.

Impliquez dès le départ le RSSI

Le modèle SASE intègre la sécurité dans l'infrastructure réseau, pour en faire un élément fondamental de chaque flux de travail de l'entreprise. Maintenant, plus que jamais, l'équipe sécurité doit être mise à contribution.

Le RSSI doit être impliqué dans toutes les discussions en lien avec l'acquisition ou la transformation de solutions réseau ou de sécurité réseau, en interne, avec les éditeurs et les architectes principaux. Cette équipe doit l'aider à évaluer les offres et les feuilles de route de chaque éditeur.

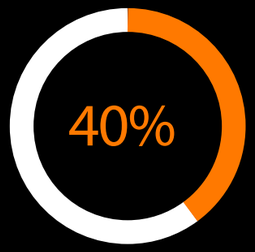
L'avantage d'adopter une approche SASE fondée sur la connaissance de la menace

Définir une approche efficace pour conduire votre Stratégie SASE à long terme est un défi. Voici nos recommandations :

- Identifier : Construire et concevoir une expérience fiable et cohérente en identifiant les priorités, en préparant la transistion et en proposant un cadre SASE évolutif et personnalisé.
- Protéger : Renforcer la sécurité du réseau entre les utilisateurs, les applications et les données quelque soit la localisation, avec nos services managés, en concevant, en mettant en oeuvre et en gérant votre architecture SASE.
- Détecter et répondre : Surveiller l'infrastructure pour détecter les incidents et remédier aux cyberattaques en améliorant continuellement votre posture de sécurité.

Toutes ces actions nécessitent une compréhension approfondie de la situation, des risques et des menaces auxquels vous êtes confronté.

SASE : quelle stratégie à adopter ?



Gartner prévoit que 40 % des organisations 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.

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 un 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 du 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 Évaluez 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 Commencez 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, avec 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. Une solution d'accès distant doit être embarquée très tôt dans le SD-WAN afin de garantir un niveau de sécurité uniforme pour les télétravailleurs.

5 Migrez les services de cybersécurité vers le Cloud

Une fois la solution SD-WAN mise 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 Déplacez votre approche et votre modèle de sécurité vers un concept d'accès réseau Zero Trust

Les clients doivent envisager leur migration vers des services de sécurité Cloud en gardant à l'esprit la notion de "zéro confiance" lorsqu'il s'agit d'accès au réseau. Ce principe implique de se préparer à identifier les accès à toutes les applications. Construisez 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

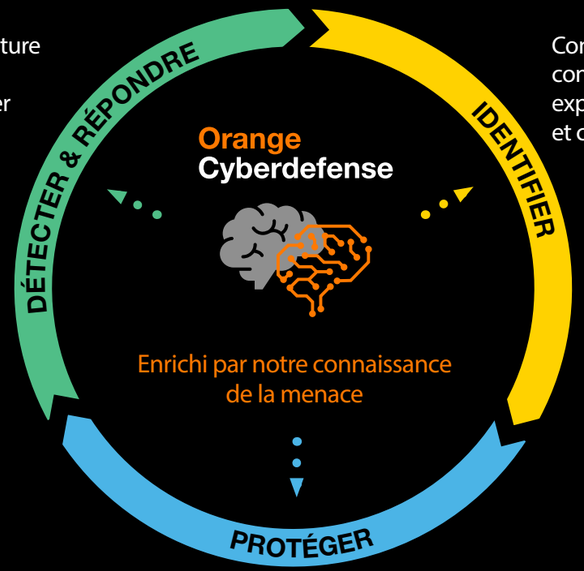
Une fois votre modèle logiciel de sécurité réseau en place, vous serez bien placés pour rendre votre infrastructure sécurité encore plus efficace en recourant à l'automatisation. Investissez dans la création et l'amélioration de logiciels de contrôle de sécurité et réseau qui serviront de socle à des opérations de 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 fondée sur le renseignement
S'adapte à votre entreprise face au paysage des menaces

Surveiller l'infrastructure pour détecter les incidents et remédier aux cyberattaques.



Contruire 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 fondé sur des services personnalisés en fonction de vos besoins, qui adaptera vos défenses aux menaces émergentes.

A propos d'Orange Cyberdefense

Orange Cyberdefense est l'entité opérationnelle, experte en cybersécurité du groupe Orange. Leader Européen en matière de services de sécurité, nous nous efforçons de construire une société numérique plus sûre.

Spécialiste sécurité, axé sur la recherche sur les menaces cyber et le renseignement, nous offrons un accès sans égal à un ensemble d'informations ayant trait aux menaces actuelles et émergentes.

Orange Cyberdefense s'appuie sur plus de 25 ans d'expérience dans le domaine de la sécurité de l'information, compte plus de 250 chercheurs et analystes, 17 SOCs, 11 CyberSOCs et 4 CERTs répartis dans le monde entier. Nos services et nos propositions d'assistance sont disponibles dans 160 pays.

Nous sommes fiers de proposer une protection globale, tout en garantissant une expertise locale et en soutenant nos clients tout au long du cycle de vie des menaces.

Sources:
1. IDC - https://www.idc.com/getdoc.jsp?containerId=prUS46934120 European Commission – https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf
2. IDC Webinar - Envisioning a Resilient Cloud Based Digital Infrastructure webinar April 2020
3. US Cybersecurity and Infrastructure Security Agencies - https://us-cert.cisa.gov/ncas/alerts/aa20-099a
4. IDC - https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IDC%20estimates%20data%20generated%20from,significant%20portion%20of%20this%20data

Orange
Cyberdefense

orange™