Disponibilité et options sur le marché émergent du SASE

Par Paula Musich
Rapport d'étude ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)
Février 2021

En partenariat avec :

paloalto® NETWORKS

EMA™

ÉTUDES, ANALYSES ET CONSEIL
EN INFORMATIQUE ET GESTION DE DONNÉES

Disponibilité et options d'achat sur le marché émergent du SASE

Sommaire

Disponibilité et options d'achat sur le marché émergent du SASE

Introduction

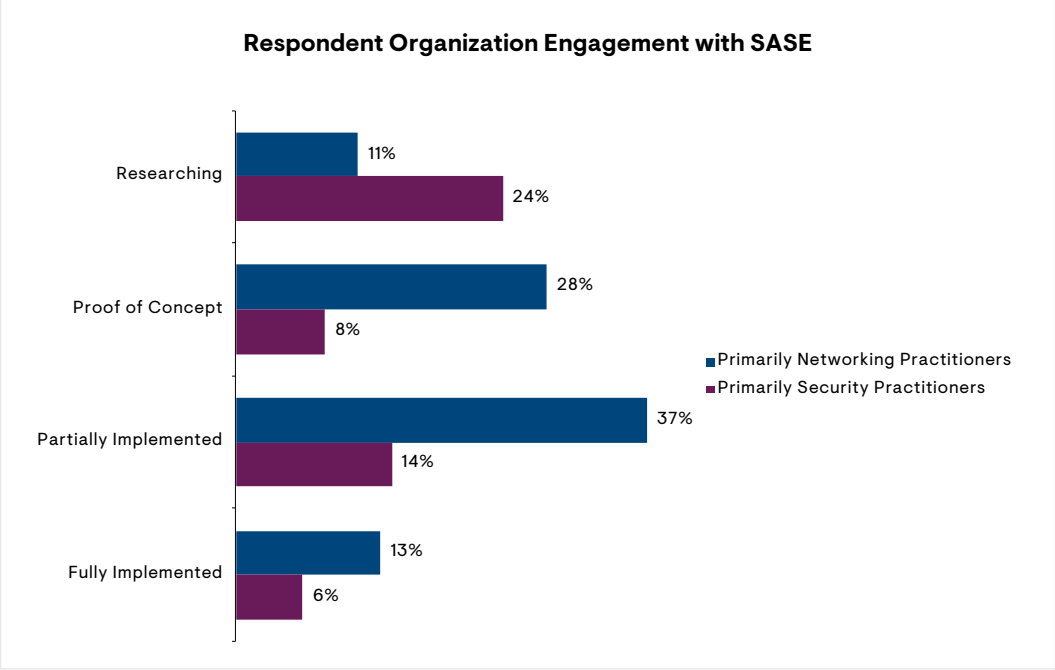
L'opportunité présentée par les analystes de Gartner sous le nom de « Secure Access Service Edge », ou SASE, n'est pas tant un marché en soi qu'une description prospective du point d'intersection du réseau et de la sécurité, deux marchés aujourd'hui séparés mais appelés à converger pour mieux répondre aux besoins de transformation numérique des entreprises. Basées sur des infrastructures réseau et de sécurité distinctes, les anciennes architectures ne répondent plus aux exigences de la plupart des entreprises. Ces architectures ont été conçues pour acheminer le trafic des sites distants et des clients VPN mobiles vers un data center central où il fait l'objet d'un suivi visant à détecter les problèmes de performance, les activités malveillantes et les malwares. Ensuite, le trafic est envoyé vers sa destination finale, souvent dans le même data center. Mais à l'heure où les entreprises adoptent toutes sortes de services cloud, les applications autrefois centralisées ne se concentrent plus toutes au sein de ces data centers. Par ailleurs, la pandémie mondiale de Covid-19 et le passage rapide au télétravail ont accéléré les initiatives de transformation numérique, au point de dépasser largement les prévisions les plus optimistes.

Pour les équipes de sécurité, il devient de plus en plus difficile de gérer une multitude de produits spécialisés, un nombre croissant d'agents de terminaux, et une pléthore de relations/contrats fournisseurs. La sécurité du périmètre, où tout ce qui se trouve la zone démilitarisée est considéré comme fiable une fois authentifié, c'est de l'histoire ancienne. Maintenir ces vieux paradigmes, tout en s'efforçant de trouver le meilleur moyen de sécuriser les applications, workloads, données SaaS, IaaS, PaaS et data centers, est trop complexe et trop coûteux – sauf pour les équipes de sécurité les plus matures et les mieux dotées financièrement. Dans le même temps, l'application d'anciennes architectures de sécurité à des nouveaux schémas de trafic réseau créent des goulets d'étranglement qui entravent l'expérience des utilisateurs. Ces points de saturation incitent également ces derniers à contourner les contrôles de sécurité existants, ce qui génère de nouveaux risques pour leurs entreprises.

Avec le SASE, ce n'est plus sur le data center mais sur les identités que se fondent les politiques de sécurité. Une fois les niveaux d'accès ou de privilèges déterminés, les politiques sont appliquées en fonction de l'identité de l'utilisateur, de l'appareil et de l'application. À l'aide de ces informations, et de données contextuelles supplémentaires, un éventail de services réseau (SD-WAN, optimisation du WAN, routage/sélection des chemins, QoS, etc.) et de sécurité (FWaaS, IDS/IPS, analyses anti-malware, DNS récursif, SWG, CASB, ZTNA, etc.) est appliqué à chaque session. Bien que Gartner insiste sur le fait que tout ceci devrait être fourni en mode cloud, beaucoup des aspirants au marché naissant du SASE proposent de multiples approches. C'est le cas des modèles hybrides permettant de distribuer une partie des workloads entre des équipements sur site et des logiciels clients déployés sur des sites distants. Parmi ces entreprises figurent Cato Networks, Cisco, Fortinet et Versa Networks. D'autres, comme VMware, proposent à la fois un déploiement 100 % cloud et un déploiement via des passerelles sur site. Les fournisseurs qualifient ces architectures de *thin branch* (sécurité en mode cloud)et de *heavy branch* (sécurité exécutée en local). Les tenants de l'approche heavy branch sont essentiellement les fournisseurs de pare-feu nouvelle génération (NGFW) matériels, comme Fortinet, pour protéger leurs technologies existantes tout en transitant vers des services de sécurité davantage axés sur le cloud.

SASE : parcours de l'acheteur

Bien que Gartner n'ait publié son document sur le SASE qu'au second semestre 2019, il est étonnant de voir à quel point les professionnels de l'informatique sont déjà au fait du SASE et de ses principes de base. Selon Enterprise Management Associates,[1] au moins 75 à 78 % des personnes interrogées dans ses deux études sont familières du terme. L'étude axée sur les professionnels réseau et celle axée sur les experts de la sécurité présentent toutefois des disparités intéressantes concernant le rapport de leurs entreprises respectives aux technologies SASE. Ainsi, parmi les professionnels réseau familiers du SASE, 37 % affirment que leur entreprise l'avait déjà partiellement mis en œuvre, contre seulement 14 % pour les experts de la sécurité. Parallèlement, 28 % des spécialistes réseau déclarent que leur entreprise est en phase d'évaluation ou de preuve de concept (POC) du SASE. À l'inverse, seulement 8 % des professionnels de la sécurité indiquent que leur entreprise procède actuellement à une POC. Malgré le faible niveau de maturité de ce marché émergent et des solutions disponibles, 13 % des spécialistes réseau (6 % pour leurs homologues de la sécurité) déclarent que leur entreprise a terminé son déploiement d'une solution SASE. Par ailleurs, environ 10 % des experts réseau sont partagés entre l'évaluation du SASE et la planification du déploiement de la solution d'un fournisseur donné. Seulement 2 % déclarent n'avoir aucune initiative SASE en cours. En d'autres termes, dans la plupart des entreprises, l'adoption du SASE est menée par les équipes réseau qui cherchent à déployer des technologies émergentes plutôt que par les équipes de sécurité. Toutefois, il convient de noter que les fournisseurs SD-WAN sont en avance sur les fournisseurs de sécurité pour ce qui est d'orienter leurs messages marketing sur le SASE. Cela a probablement eu un impact sur les réponses des professionnels réseau ayant participé à ces études. Dans le même temps, de nombreux professionnels IT aiment à se considérer comme des pionniers de l'adoption de nouvelles technologies prometteuses. Il y a sans aucun doute une certaine concurrence entre les différents groupes revendiquant leur leadership dans l'adoption du SASE.

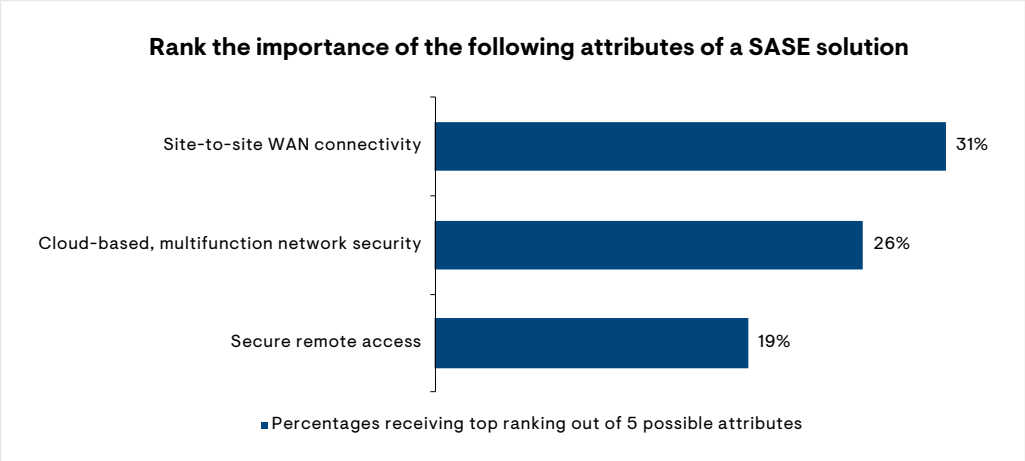


[1] Dans le cadre de deux études distinctes menées fin 2020 et ciblant principalement les professionnels réseau et de la sécurité.

Mais quelle que soit l'équipe informatique qui mène la cadence, même sans tenir compte de la nécessité de gérer des collaborateurs distants, on remarque que les entreprises poursuivent trois objectifs : 1) améliorer l'expérience des utilisateurs, 2) faciliter les processus de gestion, et 3) réduire la complexité en diminuant le nombre d'infrastructures réseau et de sécurité à déployer et maintenir. Les équipes de sécurité, qui utilisent généralement plus d'outils pour protéger les ressources numériques de leur entreprise, souhaitent notamment réduire le nombre de relations (et de contrats) fournisseurs à gérer. Ceci dit, malgré un intérêt plutôt marqué pour le SASE, la cacophonie croissante des messages marketing autour de ce concept entraîne également une certaine confusion sur ce qu'est exactement une solution SASE.

Parmi les professionnels réseau interrogés, dont les entreprises sont plus ou moins avancées sur la voie de l'adoption du SASE, au moins la moitié déclare que la pandémie de Covid-19 a accéléré leur transition vers le SASE. En revanche, un tiers d'entre eux pense que la pandémie n'a pas eu d'influence sur l'intérêt de leur entreprise pour le SASE. Autrement dit, même avant le basculement soudain vers le télétravail, il existait déjà un besoin latent d'améliorer la gestion de collaborateurs de plus en plus mobiles et dispersés, dans un contexte d'adoption accélérée du cloud et de convergence du réseau et de la sécurité. Ceci étant dit, 82 % des personnes interrogées pensent que le SASE peut assurer la continuité des activités en cas de choc majeur comme la pandémie que nous venons de vivre. Parmi eux, 82 % disent que le SASE peut garantir cette continuité grâce aux connexions à distance sécurisées, 78 % par le biais de services de sécurité cloud, et 68 % par l'accès à des services et applications cloud.

L'étude portant sur la transformation du WAN, dont les principaux participants étaient des professionnels réseau, a également cherché à évaluer les principaux critères de sélection d'une solution SASE chez les acheteurs potentiels. Parmi les cinq attributs classés par ordre d'importance, la connectivité SD-WAN site à site arrive en tête avec 31 %, suivi de la sécurité réseau multifonction en mode cloud avec 26 %. Parmi les personnes interrogées, 19 % classent les accès distants sécurisés (par ex., VPN pour les télétravailleurs et les utilisateurs mobiles) comme l'attribut le plus important, tandis que 30 % le classent en deuxième position. Les accès directs/les connexions onRamp au cloud et la visibilité opérationnelle intégrée ont été jugés moins importants pour ces participants. Compte tenu de cette répartition, il n'est pas surprenant de voir que le plus grand pourcentage de participants en phase d'adoption du SASE préfère combiner trois solutions – SD-WAN, sécurité réseau/cloud, et sécurisation des accès distants – chacune adaptée aux exigences du SASE. Ils sont en effet 26 % à avoir choisi cette option, tandis que 24 % ont préféré opter uniquement pour une solution SD-WAN adaptée aux besoins du SASE. Enfin, 23 % déclarent préférer opter pour une solution de sécurité réseau/cloud adaptée au SASE.



Comme dans tout processus d'adoption d'une nouvelle technologie, la plupart des entreprises commenceront probablement leur déploiement SASE par de petits projets et des cas d'usage spécifiques : remplacement du MPLS, remplacement des pare-feu de périphérie ou de l'infrastructure VPN par une sécurité en mode cloud, etc. Parmi les primo-adoptants les plus probables figurent les acteurs de la tech cloud-native et les petites entreprises moins contraintes par l'existant que les grandes structures. Pour ces dernières, l'adoption prend généralement plus longtemps en raison d'une certaine inertie et du temps qu'il faut pour convaincre toutes les parties prenantes.

Panorama de la concurrence

La publication du rapport Gartner fin 2019, qui a ensuite bénéficié d'un climat porteur avec l'adoption en masse du télétravail début 2020, a incité les fournisseurs de tous bords à se positionner sur le marché du SASE. Selon EMA, au moins 16 fournisseurs commercialisent activement des services SASE, et ce nombre devrait augmenter rapidement au vu de l'intérêt grandissant pour ce type de services. Les fournisseurs SD-WAN ne sont pas les seuls à s'être précipités sur ce marché émergent. Les fournisseurs réseau et de sécurité, tant traditionnels que cloud-native, et les fournisseurs de réseaux de livraison de contenu leur ont emboîté le pas. Ils rejoignent les pure-players SASE existants, comme Cato Networks et Open Systems.

On peut classer les approches adoptées par ces concurrents en deux catégories : les SASE monofournisseur et les SASE multifournisseur. Ceux qui proposent un ensemble complet de fonctions SASE, à la fois pour le réseau et la sécurité, répondent aux problèmes de complexité des entreprises devant gérer des relations et des contrats avec une multitude de fournisseurs. Un SASE monofournisseur offre aux entreprises un point de résolution central en cas de problème et une interface de gestion unique pour réduire la complexité opérationnelle. À l'autre extrémité du spectre, le SASE multifournisseur permet au client de sélectionner des technologies « best-of-breed », c'est-à-dire celles les mieux à même de répondre à des problèmes spécifiques. Ces technologies peuvent ensuite être intégrées à des chaînes de service qui permettent de préserver les relations existantes avec des fournisseurs réseau et/ou de sécurité IT de confiance.

Il est cependant plus instructif de comprendre comment chaque concurrent en est arrivé à sa solution SASE, car cela peut révéler les lacunes dans la gamme de fonctions intégrées et mettre en lumière les faiblesses de leur approche. Les paragraphes suivants classent les différentes approches adoptées à ce jour par la plupart des fournisseurs identifiés comme acteurs du SASE.

Catégorisation des fournisseurs SASE

Fournisseurs de solutions SASE autonomes	Fournisseurs rachetés par de grands acteurs du réseau/de la sécurité	Fournisseurs de sécurité en partenariat avec des fournisseurs SD-WAN	Fournisseurs de solutions CDN intégrant des fonctions SD-WAN
Cato Networks	Cisco/Viptela	Forcepoint	Akamai
Open Systems	Fortinet/OPAQ	McAfee	Cloudflare
Versa Networks	Aruba (HPE) Silver Peak	Netskope	
	Palo Alto Networks/ CloudGenix	Symantec	
	VMware/VeloCloud	Zscaler	
		Check Point	

Parmi les protagonistes du marché du SASE, EMA a choisi de se focaliser sur neuf fournisseurs qui semblent être les plus avancés dans l'élaboration d'un ensemble intégré de services réseau et de sécurité indispensables à la transformation numérique des entreprises. Ces fournisseurs sont les suivants :

- Cato Networks
- Cisco Systems
- Cloudflare
- Fortinet
- Aruba (HPE) Silver Peak
- Palo Alto Networks
- Versa Networks
- VMware
- Zscaler

Cisco, Fortinet et Palo Alto Networks, trois des plus grands concurrents entrés sur le marché émergent du SASE par le biais d'une acquisition, ont planté leurs drapeaux dans ce sol fertile à l'automne 2020 en lançant leurs offres et leurs solutions d'intégration initiales. Au lancement de sa solution, Cisco, qui avait acquis Meraki en 2012 et Viptela en 2017, a affirmé travailler depuis plusieurs années à la convergence du réseau et de la sécurité, notamment avec les technologies acquises via OpenDNS en 2015.

Fonctionnalités de sécurité

Pour EMA, le même ensemble de services qui protège les collaborateurs directement connectés au réseau de l'entreprise doit être appliqué aux utilisateurs mobiles, aux utilisateurs des sites distants et aux services cloud auxquels ils souhaitent accéder. SD-WAN, SWG, CASB, ZTNA, FWaaS, identification des malwares et des données sensibles (y compris les données chiffrées), cohérence des opérations en débit de ligne dans le cloud et en périphérie du réseau… une offre SASE digne de ce nom doit inclure un certain nombre de fonctionnalités de base. Ce prérequis fait que très peu (voire aucun) des fournisseurs dans cette étude peut prétendre à ce statut. Par exemple, même dans la poignée de partenaires de sécurité qui répondent aux besoins de sécurité, Silver Peak n'a toujours pas la capacité d'identifier les données sensibles et de détecter les malwares, même s'il convient de préciser que cela figure sur la feuille de route de l'entreprise. Fortinet, lui, propose le CASB et le ZTNA sous forme d'offres distinctes dans le cadre de sa solution Fortinet Security Fabric. De son côté, Cloudflare n'offre pas d'accès par API au SaaS mais prévoit d'intégrer prochainement plusieurs fonctionnalités : SD-WAN, identification des données sensibles, FWaaS et sandboxing du réseau. VMware ne devrait pas offrir de fonctionnalités SWG, CASB et FWaaS avant le deuxième trimestre. Quant aux intentions de Cisco en matière d'opérations en débit de ligne à la périphérie et depuis le cloud, elles restent floues. Enfin, Zscaler possède l'ensemble le plus complet de fonctions réseau et de sécurité intégrées dans son offre SASE, bien qu'il les propose en partenariat avec un fournisseur SD-WAN et WAAP. Cela témoigne du peu de maturité du marché et du long chemin que tous les participants doivent encore parcourir avant de concrétiser les avantages de la vision SASE.

Au-delà de ces fonctionnalités de base, certains prospects pourront être séduits par les offres auxiliaires de certaines solutions SASE : protection des applications web et des API, isolement du navigateur à distance, DNS récursif, sandboxing du réseau, accès par API au SaaS pour la contextualisation des données, prise en charge des appareils gérés et non gérés, etc. Parmi les neuf

fournisseurs sélectionnés par EMA, seuls Cloudflare, Versa Networks et Zscaler proposent des fonctions WAAP, tandis que Fortinet ne propose que le WAF. Palo Alto Networks, Fortinet et Cato ne prennent pas en charge le RBI, tandis que Cisco et VMware prévoient de l'ajouter prochainement. En termes de RBI, Silver Peak propose son offre en partenariat avec un autre fournisseur, tandis que Versa Networks vient de lancer cette fonctionnalité. Le DNS récursif est disponible chez Cisco, Palo Alto Networks et Versa, tandis que le sandboxing du réseau figure dans les offres de Cisco, Palo Alto Networks, Fortinet, Versa, Zscaler et Silver Peak, via un partenaire.

Enfin, certaines entreprises trouveront sans doute certaines options utiles : protection des bornes Wi-Fi, masquage du réseau, gestion des VPN d'ancienne génération, protection de l'Edge Computing, UEBA, etc. Cato Networks et Aruba (HPE) Silver Peak ne disposent pas de ces fonctionnalités, tandis que Cisco, Fortinet, Palo Alto Networks et Versa Networks les proposent directement ou par l'intermédiaire de partenaires. Zscaler ne prend pas en charge les VPN d'ancienne génération et n'offre pas de protection de l'Edge Computing ni de fonctionnalités UEBA. Enfin, VMware a inscrit la protection de l'Edge Computing à sa feuille de route.

Architectures SASE

La manière dont les fournisseurs ont conçu leurs solutions SASE peut avoir un impact considérable non seulement sur les performances, mais aussi sur le coût d'exploitation, le coût de déploiement du service et l'emplacement des points de présence (PoP). Par exemple, le service SASE Prisma Access de Palo Alto Networks fonctionne sur AWS et GCP, et l'entreprise dédie un seul nœud de traitement de sécurité à chaque client. Ce service est donc certes plus coûteux à exploiter, mais il assure une bonne séparation entre chaque client et évite les pertes de performances liées aux infrastructures partagées. L'entreprise affirme que son architecture est « cloud-agnostique », bien qu'elle soit actuellement limitée aux points de présence AWS et GCP, ce qui représente aujourd'hui plus de 100 sites.

Par contraste, Fortinet n'a pas l'intention d'exécuter toutes les fonctions de sécurité de son offre SASE dans le cloud. Étant donné la force de son offre NGFW haute performance basée sur ASIC, le fournisseur doit tirer profit de son avantage concurrentiel. Fortinet entend promouvoir l'idée de renforcer la périphérie WAN au moyen de ses équipements sur site pour certaines opérations de sécurité. De son côté, Cato Networks met un point d'honneur à exploiter une seule et unique stack logicielle sur des sites de colocation sélectionnés, où il estime avoir un avantage en termes de coût et de flexibilité. Le fournisseur développe sa propre dorsale sur les marchés tertiaires afin d'étendre sa présence géographique au-delà de ses 65 points de présence. Cloudflare s'appuie également sur sa propre dorsale, développée comme réseau de livraison de contenu au fil du temps. Aujourd'hui, elle comprend 200 data centers dans le monde, où l'entreprise assure la sécurité et le filtrage des données via une architecture single-pass. Chaque data center exécute le moteur de politiques unique de Cloudflare. Les connexions à l'environnement Edge de Cloudflare comprennent des tunnels GRE, des interconnexions de réseau, et les clients mobiles de Cloudflare. Autre fournisseur SASE 100 % cloud, Zscaler exploite sa vaste infrastructure développée au fil des ans pour délivrer des services de passerelles web sécurisées (SWG) dans le cloud. Sa dorsale est composée de 150 points de présence répartis dans le monde entier.

Cisco, pour sa part, vante les relations de peering directes de ses plus de 30 data centers régionaux avec des milliers d'opérateurs réseau, avec à la clé des accès haute performance et à faible latence aux applications. Si son objectif est de simplifier ses solutions Meraki avec une série de fonctions de sécurité intégrées de manière transparente, ses antécédents en matière d'intégration ne sont pas des plus glorieux. Toutefois, Cisco continue de faire des progrès dans l'intégration de sa solution SD-WAN Viptela et son service cloud Umbrella de sécurité multifonction, avec une intégration plus poussée prévue en mars.

L'architecture d'Aruba (HPE) Silver Peak s'articule autour d'une appliance « thin edge » sur site combinant un SD-WAN, un pare-feu à état basé sur les zones avec segmentation avancée, une interopérabilité des routages, une optimisation du WAN, une visibilité sur le réseau et les applications, des analyses et une intégration automatisée avec des services de sécurité fournis par des partenaires cloud. Elle propose sept modèles d'appliances matérielles et une appliance virtuelle tournant sur des hyperviseurs standard. Son offre SASE s'appuie sur un écosystème de partenaires d'intégration pour la plupart de ses fonctionnalités de sécurité. Aruba (HPE) Silver Peak ne dispose pas de ses propres PoP, mais s'appuie sur ses partenaires de services de sécurité cloud pour cette connectivité, notamment Check Point, Netskope, Palo Alto Networks Prisma et Zscaler. Versa utilise un seul système d'exploitation et une seule stack logicielle pour donner à ses clients la possibilité d'exécuter ses services en mode cloud et/ou via des passerelles sur site. Son service cloud compte 90 points de présence dans le monde et l'entreprise continue de s'étendre géographiquement. VMware adopte une approche similaire, en donnant à ses clients la possibilité de s'abonner à des services SASE en mode cloud et d'exécuter ces services sur site. L'entreprise compte actuellement 33 PoP et prévoit de porter ce nombre à 50 dans les 12 à 18 prochains mois. Elle collabore également avec d'autres fournisseurs de services pour augmenter le nombre de ses PoP.

Comparatif des options d'achat

Le modèle le plus courant chez les neuf fournisseurs de cette étude combine tarification à la bande passante et tarification par utilisateur pour les offres SASE alliant réseau et sécurité. C'est le modèle utilisé par Cisco, Palo Alto Networks, Cato Networks, VMware et, dans une certaine mesure, Cloudflare et Versa Networks. Le modèle de tarification de Versa est basé sur plusieurs couches de services (tiering) que les clients choisissent d'activer, ainsi que sur les exigences de débit pour chaque site desservi. Fortinet, qui n'a pas encore complètement fixé ses prix, a choisi de baser sa tarification SASE sur un modèle par utilisateur/par an. Aruba (HPE) Silver Peak utilise un modèle similaire à celui de VMware, basé le nombre d'appareils, la bande passante et les options de support. Cependant, les clients peuvent également acheter une licence logicielle d'instance virtuelle basée sur le niveau de bande passante dont ils ont besoin. Bien qu'il varie selon les fonctionnalités, le modèle de tarification SASE de Zscaler est défini par utilisateur et par an. Par exemple, les VPN sont configurés sous forme de comptes.

Le modèle de tarification de Cato Networks fait appel à la fois à la bande passante (vers le cloud Cato) et à la tarification par utilisateur. En fonction de leurs besoins, les clients peuvent opter pour une tarification par utilisateur, par bande passante ou les deux. Les clients peuvent réaffecter les capacités entre les sites d'une même région sans frais. Ils peuvent également choisir d'augmenter la couverture pendant la période du contrat et payer la différence. Le basculement vers un contrat de niveau inférieur n'est pas permis, mais les clients peuvent réaffecter les capacités à d'autres régions. Les remises accordées aux clients sont traitées au cas par cas. Les prix varient d'une région à l'autre en fonction du coût du service dans chaque région.

Cisco octroie des licences pour son offre SASE DNA Premier en fonction des niveaux de bande passante. Le client a droit à un nombre spécifique de licences utilisateur selon son niveau de bande passante. En entrée de gamme, un petit site avec une bande passante de 5 Mbit/s donne droit à 10 licences Umbrella SIG Essentials. Pour un QG d'entreprise, une bande passante de 10 Gbit/s donne droit à 500 licences Umbrella SIG Essentials. Les clients peuvent également acheter séparément des licences utilisateur supplémentaires. Cisco a constaté que la plupart des clients qui migrent vers Office 365 déploient simultanément le SD-WAN, l'intention étant d'intégrer Umbrella SIG Essentials dans ce mix. L'entreprise propose également plusieurs options d'accord de licence d'entreprise (ELA) pour DNA Premier, et un nombre croissant de composants disponibles via des accords de licence de fournisseur de services (SPLA). Des contrats de 1, 3 et 5 ans sont disponibles. L'abonnement à la licence logicielle Cisco DNA Premier (DNA-P) est vendu sous forme de référence (SKU) unique. Cisco compte intégrer prochainement une autre SKU combinant gestion du réseau, de la sécurité et des accès – plus précisément SD-WAN, accès à distance, VPN, SWG, FWaaS, CASB et ZTNA. D'autres offres groupées (bundles) en cours d'étude porteront sur les options de sécurité hybride pour les clients qui transitent de pare-feu et SWG sur site vers une sécurité en mode cloud. Les clients peuvent dépasser le nombre d'utilisateurs pendant la période contractuelle, avec une régularisation effectuée en fin d'année ou de contrat.

Cloudflare utilise un système de licence flexible qui permet aux clients d'opter pour un paiement mensuel ou annuel par utilisateur. Ils ont également la possibilité de choisir un paiement à l'usage (« pay as you go ») ou de souscrire des accords de licence d'entreprise (ELA). Dans le cas d'un paiement à l'usage, les clients peuvent ajuster leur abonnement à la hausse ou à la baisse selon leurs besoins et le nombre de postes requis sur une base mensuelle. Ceux qui optent pour les contrats ELA peuvent se rapprocher de leur chargé de compte pour ajuster les contrats au moment du renouvellement. La tarification est homogène d'une région à l'autre. La tarification de Cloudflare s'effectue par utilisateur et par mois pour la plupart des composants (Zero Trust Network Access, Secure Web Gateway, FWaaS, isolement du navigateur à distance, etc.), mais les services réseau sont facturés en fonction du nombre de connexions et de la bande passante.

Bien que Fortinet n'ait que récemment finalisé ses tarifs pour FortiSASE, ceux-ci sont basés sur un modèle d'abonnement annuel, avec des niveaux allant de 25 à plus de 10 000 utilisateurs. Les packs et bundles de Fortinet en sont encore à un stade préliminaire, mais l'entreprise envisage des niveaux de 25, 500, 2 000 et 10 000 utilisateurs. Appelée Secure Internet Access, le premier bundle SASE de Fortinet est ciblé sur la sécurisation des accès Internet dans un contexte de télétravail. Le second bundle s'étendra aux entreprises avec des politiques pour les cas d'usage « light branch » et « heavy branch ». Enfin, un troisième se concentrera sur le contrôle et la microsegmentation. Et c'est là que le ZTNA entrera en jeu. Fortinet compte proposer à la fois des contrats ELA et SPLA, mais les modalités n'ont pas encore été finalisés. Leurs tarifs seront homogènes dans toutes les régions, principalement parce que le fournisseur cible et travaille avec de grandes multinationales.

Le modèle de tarification d'Aruba (HPE) Silver Peak comprend l'achat initial d'une appliance, ainsi qu'un contrat d'assistance annuel pour la maintenance et une licence d'abonnement annuel basée sur des niveaux de bande passante. Les clients peuvent s'engager sur des contrats de 1, 3, 5 et 7 ans. Les services de sécurité cloud sont achetés directement auprès des partenaires de sécurité de Silver Peak. Les tranches de bande passante sont les suivantes : 50 Mbit/s, 100 Mbit/s, 200 Mbit/s, 500 Mbit/s, 1 Gbit/s et 2 Gbit/s. Les clients peuvent passer à tout moment à un niveau de bande passante supérieur, mais ne peuvent rétrograder qu'au moment du renouvellement.

Les modèles de tarification de Prisma Access Palo Alto Networks sont basés sur la bande passante totale utilisée sur tous les sites. Les pools de bande passante sont divisés suivant les quantités dont chaque site a besoin, avec un pool minimum de 200 Mbit/s. La licence Prisma Access for Users est basée sur le nombre total d'utilisateurs, avec un minimum fixé à 200 utilisateurs. Cette dernière offre une prise en charge étendue des terminaux (MacOs, IoS, Windows, Android, Google Chrome OS, Linux, etc.). Tous les modèles reposent sur un abonnement annuel. Prisma Access n'est pas disponible sous forme de contrat de licence d'entreprise (ELA) ou de tarification à l'usage. Les clients peuvent passer à un niveau supérieur à tout moment, mais ils ne peuvent descendre à un niveau inférieur qu'après l'expiration du contrat en cours. Palo Alto Networks ne loue pas d'équipements sur site. L'achat des appliances CloudGenix SD-WAN peut s'effectuer selon un modèle classique (CapEx) avec abonnement, ou selon un modèle de coûts opérationnels (OpEx).

Le modèle de tarification de Versa est basé sur le tiering, sur les services que les clients choisissent d'activer et sur les exigences de débit pour chaque site desservi. Les services liés à des utilisateurs individuels sont facturés en fonction du nombre d'utilisateurs, tandis que les services basés sur la bande passante et/ou les performances sont facturés en fonction des exigences de débit et de performance (comme Secure SD-WAN). Par exemple, le tarif pour un client qui ne sélectionne que Versa Secure Access n'est basé que sur le nombre d'utilisateurs. Lorsqu'un client choisit plusieurs services (FWaaS, SWG, SA, etc.), Versa regroupe plusieurs services SASE en une seule offre pouvant inclure jusqu'à 5 000 utilisateurs mobiles, jusqu'à 250 Mbit/s de débit par site distant, des performances élevées pour les services cloud simultanés, etc. Les offres sont vendues sous forme d'abonnement et les clients peuvent choisir des contrats de 1, 2 ou 3 ans. Versa propose également des programmes d'achat avec contrats de licence d'entreprise et contrats de licence de fournisseurs de services. Les clients peuvent passer à un contrat de niveau supérieur ou inférieur en fonction de leurs besoins de bande passante et du nombre de postes.

Les offres SASE de VMware sont réparties entre les licences basées sur la bande passante et les licences basées sur l'utilisateur. Le fournisseur propose trois types d'abonnements pour sa solution SD-WAN : Standard, Enterprise et Premium. Chacun permet au client de bénéficier des fonctionnalités d'orchestration et d'optimisation dynamique des chemins multiples, d'une prise en charge des passerelles partenaires et d'un tunnel direct d'un site distant jusqu'aux services de sécurité cloud. Les éditions Enterprise et Premium ajoutent l'orchestration pour les pare-feu de périphérie, des fonctions réseau avancées et des niveaux distincts de bande passante inférieure. L'édition Premium ajoute des passerelles hébergées dans des PoP. La fonctionnalité ZTNA de VMware s'appuie sur une tarification par utilisateur et est traitée comme un module supplémentaire de l'offre Workspace One. Les clients qui souhaitent souscrire des abonnements en volume et acheter du matériel séparément peuvent opter pour un ELA. VMware propose également des SPLA pour les fournisseurs de services. Les clients qui souscrivent un contrat ELA ont la possibilité d'évoluer vers des éditions logicielles supérieures en cours de contrat.

Zscaler décline son offre SASE en trois éditions pour Zscaler Internet Access. L'édition Professional combine plusieurs fonctionnalités : authentification du transfert de trafic, génération de rapports et mises à jour, filtrage d'URL, contrôle du type de fichiers, FWaaS, analyses anti-malware, protection contre les menaces basée sur la réputation, et visibilité sur les applications cloud. L'édition Business y ajoute les prestations suivantes : inspection SSL, gestion des flux de journaux, contrôle des accès au web, contrôle de la bande passante, contrôle des applications mobiles, protection contre les menaces avancées, contrôle des applications cloud, DLP et CASB. L'édition Transformation va plus loin avec un FWaaS avancé, un système IPS, une sandbox cloud et un CASB plus avancé. Le modèle de tarification le plus courant repose sur un abonnement annuel par utilisateur.

Comparatif des modèles de support

Pour ce qui est du support de base des neuf fournisseurs, l'offre de Palo Alto Networks est quelque peu limitée car son support n'inclut que l'accès au portail en ligne. Le support téléphonique nécessite de souscrire une formule d'assistance Premium, qui représente 20 % du prix catalogue. En revanche, Versa et Fortinet sont les seuls à proposer directement une assistance sur site (Premium), tout comme certains partenaires de Cisco. Par ailleurs, on observe une grande disparité dans les délais d'autorisation de retour de marchandise (RMA), Fortinet et Palo Alto Networks proposant des délais de quatre heures sur ses contrats d'assistance Premium. Le RMA le plus long qui nous ait été communiqué était de 10 jours pour Palo Alto. Enfin, les accords de niveau de service (SLA) varient également entre les neuf fournisseurs. Aruba (HPE) Silver Peak ne s'engage sur aucun accord SLA avec ses clients. Quant à Cato Networks, Cisco, et Fortinet, ils proposent tous des SLA spécifiant une disponibilité de 99,999 % pour leurs services cloud.

Comparatif des offres de support SASE

	Basic	Premium	Assistance sur site	Délai de réponse	RMA	SLA
Cato Networks	24h/7j/365j	Ingénieur support dédié	Non	1 à 2 heures	Jour suivant	99,999
Cisco	24h/7j (téléphone + web)	Responsable support dédié	Via un partenaire			99,999 (pour les services Umbrella)
Cloudflare	24h/7j	Support VIP	via un partenaire			100 % de disponibilité
Fortinet	24h/7j	Ingénieur support avancé	Oui		4 heures – jour suivant par colis express	99,999
Aruba (HPE) Silver Peak	24h/7j/365j	Aide au déploiement	Non	30 min à 24 heures		Aucun
Palo Alto Networks	24h/7j (web)	24h/7j (téléphone + conseils)			4 heures à 10 jours	99,999
Versa	24h/7j (web + téléphone)	24h/7j	Oui	1 à 4 heures		99,999
VMware	24h/7j	Analyses des causes racines	Facultatif	30 min à *12 heures	De 4 heures au JOS**	Aucun
Zscaler	24h/7j	Ingénieur niveau 2	Non	15 min à 48 heures		99,999

* Heures de bureau

** Jours ouvrable suivant

Les clients Cato Networks bénéficient d'un support mondial disponible 24 heures sur 24, 7 jours sur 7 et 365 jours par an, et de l'assistance d'un ingénieur dédié (option Premium). Cato utilise pour cela une petite équipe de sept membres, néanmoins appelée à s'étoffer. L'entreprise ne fournit pas d'assistance sur site, mais propose une assistance à distance au déploiement initial. Elle garantit des RMA pour le jour suivant, bien qu'elle recommande à ses clients de conserver des pièces de rechange pour leurs appliances SD-WAN sur site. Son SLA spécifie une disponibilité de 99,999 % pour son service cloud.

Cisco a ajouté une nouvelle série de services de planification stratégique SASE à son portefeuille de services de sécurité, ainsi que des services de déploiement et de support déjà offerts sur ses autres produits réseau et de sécurité. Les forfaits d'assistance comprennent un support téléphonique et en ligne 24h/7j, ainsi que des conseils de configuration, et un support Premium avec une assistance technique prioritaire et un gestionnaire de service dédié. Le SLA des principaux services Umbrella spécifie une disponibilité de 99,999 %. Des détails supplémentaires sont disponibles sur https://umbrella/cisco.com/support.

Cloudflare propose à ses clients un forfait d'entreprise comprenant une assistance 24h/7j, une assistance de niveau 1, un Customer Success Manager et un expert technique pour faciliter la prise en main. Son support Premium fournit une assistance haut de gamme. Cloudflare ne fournit pas d'assistance directe sur site, mais celle-ci est disponible auprès de certains fournisseurs de services managés (MSP). L'entreprise garantit une disponibilité de 100 % pour son service cloud.

L'assistance FortiCare de Fortinet intervient dans le cadre de FortiSASE. Ses réseaux de distribution et de partenaires mondiaux permettent aux clients de bénéficier de services et d'une assistance via Fortinet directement, ou via des fournisseurs de services et des partenaires agréés. Les SLA de FortiSASE spécifient une disponibilité de 99,999 %. Pour plus de détails sur FortiCare, rendez-vous sur https://www.fortinet.com/support/support-services/forticare-support.

Aruba (HPE) Silver Peak fournit une assistance 24h/7j/365j avec un accès direct à des ingénieurs support. Un service d'abonnement distinct, Silver Peak Assist, offre aux clients un support technique dédié pour les activités de déploiement. Les équipes de support d'Aruba (HPE) Silver Peak collaborent avec des partenaires de services de sécurité pour garantir la réussite des déploiements. L'entreprise travaille également avec des partenaires de déploiement agréés et certifiés qui aident les clients à concevoir, déployer et gérer leurs implémentations SD-WAN. Les remplacements de composants sont classés par ordre de priorité (quatre niveaux) par les ingénieurs du support technique lorsqu'un nouveau cas est soumis. Les problèmes critiques font l'objet d'une première intervention dans les 30 minutes, les problèmes majeurs dans l'heure, et les problèmes normaux dans les quatre heures. Les demandes d'informations sont, quant à elles, traitées sous 24 heures.

Palo Alto Prisma Access propose deux niveaux de support :

- Le niveau Standard (inclus) offre un accès 24h/7j au portail d'assistance, à la base de connaissances et à toute la documentation en ligne de Palo Alto Networks, ainsi qu'à des vidéos de formation gratuites et à la LiveCommunity.
- Le niveau Premium (20 % du prix catalogue) ajoute au support Standard une assistance téléphonique 24h/7j, un délai de réponse Premium, des conseils et un accompagnement continus, un engagement pour la réussite du client, et des conseils sur la configuration optimale et les bonnes pratiques.

Les contrats Standard et Premium couvrent l'un comme l'autre des pièces certifiées et l'accès à des techniciens qualifiés. Pour les clients ayant besoin d'options avancées en termes de RMA, Palo Alto Networks propose 130 dépôts de pièces détachées situés en des points stratégiques dans le monde entier. Options de remplacement :

- Retour et réparation – Les clients renvoient un appareil défectueux et reçoivent un appareil de remplacement dans les 10 jours ouvrables. Cette prestation fait partie du contrat de support Standard.
- RMA pour livraison le jour ouvrable suivant – Les équipes mettent tout en œuvre pour que le produit de remplacement d'un matériel défectueux soit livré le jour ouvrable suivant. Cette prestation fait partie du contrat de support Premium.
- RMA Premium de 4 heures – Option facultative engageant les équipes à faire un effort commercialement raisonnable pour livrer un matériel de remplacement dans les quatre heures suivant l'émission d'une RMA. Elle est destinée aux clients de data centers dont les temps de réponse sont critiques. Cette option n'est cependant pas disponible dans toutes les zones géographiques.

Versa propose des abonnements Basic et Premium. Le support Basic comprend une assistance web et téléphonique 24h/7j, ainsi qu'une fenêtre de réponse initiale de quatre heures et des mises à jour et correctifs logiciels. Le support Premium est disponible 24h/24 et 7j/7, et comprend une fenêtre de réponse initiale d'une heure. Une assistance sur site est disponible en option directement auprès de Versa. L'entreprise offre une garantie de deux ans sur ses appliances matérielles, mais les clients peuvent souscrire des options de support étendu, tel que le retour en usine 24h/7j pour accélérer le processus de retour et prolonger la couverture au-delà de la garantie de deux ans. Le matériel défectueux est réparé ou remplacé dans un délai de quatre semaines. Les clients peuvent également souscrire une option permettant un remplacement le jour ouvrable suivant afin de contourner le processus de retour en usine et d'obtenir un remplacement sur site par un technicien de service, qui s'occupe également de l'enlèvement de l'unité défectueuse pour réparation. D'autres options de support comprennent le remplacement anticipé le même jour ouvrable. Ces services sont fournis par le biais d'un réseau RMA mondial couvrant les États-Unis/Canada, l'Union européenne et d'autres pays d'Europe, l'APAC/Japon, l'Australie, le Moyen-Orient et l'Afrique. Le SLA de Versa pour son service cloud garantit une disponibilité de 99,999 %.

VMware propose trois formules de support pour son offre SD-WAN : Basic, Production et Premier. Le support Basic offre un accès mondial 24h/7j pour les problèmes critiques. Également au menu : demandes de support illimitées, temps de réponse d'une heure pour les problèmes critiques (gravité 1), de quatre heures pour les problèmes majeurs (gravité 2) et de huit heures pour les problèmes mineurs (gravité 3), accès en ligne à la documentation et à la base de connaissances. Le support Production y ajoute des temps de réponse de 30 minutes pour les problèmes critiques (gravité 1). Le support Premier ajoute un accès mondial 24h/7j pour les problèmes majeurs (gravité 2), une analyse des causes racines, des délais de réponse de deux heures pour les problèmes majeurs (gravité 2), et des délais de réponse de quatre heures pour les problèmes mineurs (gravité 3).

Zscaler propose trois formules de support : une formule Standard fournie avec son service, une formule Premium en option, et une formule Premium Plus également en option. Ces trois formules offrent un accès 24h/7j au support (assistance par téléphone, portail web, interface utilisateur d'administration, formations en ligne, guides d'utilisation, articles, etc.). Le support Standard donne accès à des ingénieurs support de niveau 1 et à une fenêtre d'escalade pour les problèmes de gravité 1, aux heures de bureau locales. Le support Premium donne accès à des ingénieurs support de niveau 2 et à une fenêtre d'escalade pour les problèmes de gravité 1, 24 h/7j. Le support Premium Plus donne accès à un chargé de compte technique (TAM) dédié et à des échanges supplémentaires avec celui-ci sur une base hebdomadaire, mensuelle ou trimestrielle. Les fenêtres de réponse aux tickets soumis sur le portail de support de Zscaler varient selon les trois formules, et les délais dépendent du niveau de gravité du problème : P1 (plus urgent) à P4 (faible priorité). Les SLA pour les problèmes P1 vont de deux heures pour le support Standard à 30 minutes pour le support Premium et 15 minutes pour le support Premium Plus.

Angles d'approche du marché du SASE

Cato Networks vend ses produits par l'intermédiaire d'un réseau de partenaires, notamment des agents télécoms ou des agents principaux aux États-Unis. Dans le reste du monde, l'entreprise passe par des MSP, des distributeurs et des VAR. Les MSP fournissent leur service sur l'infrastructure cloud de Cato. L'entreprise est en train d'en recruter aux États-Unis. Les remises accordées aux partenaires sont de 20 % pour les agents télécoms, 30 % pour les VAR et 40 % pour les distributeurs. Des remises de 15 % sont offertes dans certains cas.

Cisco vend son offre SASE directement aux grandes entreprises, mais aussi par l'intermédiaire de partenaires (distributeurs, VAR, fournisseurs de services, etc.). L'entreprise cible une grande variété de marchés verticaux, bien qu'elle ne s'attende pas à une demande aussi forte dans les secteurs de la santé et des services financiers en raison de problèmes de conformité. Parmi les marchés verticaux ciblés figurent les collectivités locales/territoriales et l'enseignement, auxquels elle propose des formules destinées à des cas d'usage spécifiques (tarifs basés sur le nombre d'étudiants, par exemple).

Cloudflare vend son offre SASE à la fois directement aux entreprises et par l'intermédiaire de partenaires de distribution. Ses fournisseurs de services partenaires s'appuient sur l'infrastructure de Cloudflare pour fournir leurs services SASE, disponibles dans 100 pays à travers le monde. Ses cibles sont généralement des centres d'achat IT et de sécurité IT, bien que dans certains cas, les équipes réseau influencent les décisions d'achat.

Fortinet se targue d'être une entreprise de vente indirecte à 100 %, et compte vendre ses offres SASE naissantes par l'intermédiaire de ses fournisseurs de services habituels, de MSSP, de distributeurs et de VAR. L'entreprise ne cible pas de marché vertical spécifique, mais considère la demande comme très diversifiée. Toutefois, Fortinet constate que l'intérêt le plus fort vient des secteurs de la tech, de l'industrie et des pouvoirs publics. Concernant les clients actifs ou les POC, Fortinet propose quelques POC à de grandes multinationales de niveau 1 basées en Amérique du Nord. L'entreprise prévoit de poursuivre activement les opportunités SASE chez ses clients en Amérique du Nord dans un premier temps, puis d'étendre ses activités commerciales et POC à d'autres parties du monde au cours du second semestre de l'année prochaine.

Aruba (HPE) Silver Peak est commercialisé par l'intermédiaire de distributeurs, de VAR, d'intégrateurs systèmes, de fournisseurs de services et de partenaires d'alliances technologiques de sécurité. Les VAR bénéficient d'une remise de 33 %, qui reste la norme dans le monde entier. À ce jour, grâce à ces partenaires, Silver Peak a réalisé plus de 2 000 déploiements en production de sa plateforme SD-WAN Unity EdgeConnect. Sur le marché des fournisseurs de services, les clients peuvent opter pour des appliances matérielles Aruba (HPE) Silver Peak sur site ou déployer la plateforme sous forme de fonction réseau virtuel (VNF) sur son matériel CPE standard. La VNF EdgeConnect peut également être déployée avec la VNF de sécurité d'un partenaire sur différentes appliances matérielles. Le fournisseur de services gère le déploiement du client à l'aide d'une version multi-tenant d'Aruba Orchestrator. Le plus grand déploiement de l'entreprise, qui gère des milliers de sites pour une grande enseigne du Fortune 50, a été réalisé par un fournisseur de services. Aruba (HPE) Silver Peak cible des opportunités sur les marchés de l'enseignement et des collectivités locales/territoriales avec des partenaires dotés d'une expertise spécifique dans ces domaines. Grâce aux tests FIPS 140-2 validés au premier trimestre 2020, Silver Peak cible également les opportunités au sein des administrations centrales.

Palo Alto Networks vend ses produits Prisma Access et SD-WAN par l'intermédiaire de fournisseurs de services, de distributeurs et de VAR. Pour les déploiements via des fournisseurs de services, Palo Alto Networks héberge Prisma Access pour les partenaires de distribution. L'entreprise n'a pas voulu divulguer les remises qu'elle offre à ces partenaires, ni le nombre de ses clients Prisma Access ou les POC dans lesquelles elle est activement engagée.

Versa commercialise son service SASE par l'intermédiaire de son réseau mondial de partenaires (VAR, intégrateurs systèmes, fournisseurs de services managés, opérateurs télécoms, revendeurs, agents principaux, etc.). Sur demande, Versa peut également vendre directement aux clients finaux. Les fournisseurs de services revendent et/ou vendent l'offre SASE de Versa en marque blanche. Ils peuvent l'héberger dans leur propre cloud et utiliser leurs propres réseaux et PoP. En outre, ils peuvent gérer les équipements sur site d'un client, et la version cloud sous forme de service managé. Parmi les partenaires fournisseurs de services figurent Comcast, Deutsche Telekom, Lumen, Verizon et NTT Communications. Avant, Intelisys et Telarus comptent parmi les principaux agents télécoms. Finance, grande distribution, santé, high-tech, industrie, énergie, secteur public (collectivités et enseignement compris)… Versa cible un large éventail de marchés verticaux.

VMware vend son offre SASE directement ainsi que par l'intermédiaire de partenaires de distribution (VAR, MSP, opérateurs télécom, etc.). Concernant le canal des fournisseurs de services, les déploiements peuvent être effectués sur site, hébergés par VMware ou par les fournisseurs eux-mêmes. VMware ne cible pas de marchés verticaux particuliers pour son offre SASE.

Zscaler vend ses services SASE directement aux entreprises via sa force de vente régionale, ainsi que par l'intermédiaire de partenaires de distribution. Les partenaires fournisseurs de services revendent le produit, souvent sous leur propre marque, mais ces services restent hébergés par Zscaler. Bien que Zscaler ne cible pas de marchés verticaux spécifiques, l'entreprise est très présente dans la tech, la santé, les services financiers, l'industrie et les collectivités locales et territoriales.

Aperçu des fournisseurs SASE

Cato Networks

La start-up Cato Networks a été fondée en 2016 avec un capital-risque de 332 millions de dollars. Sa solution Cato Cloud est la première plateforme SASE au monde. Son offre SASE de base se présente sous la forme d'un service cloud où convergent SD-WAN, NGFW et services SWG et sa propre dorsale fournie sur une gamme de réseaux d'opérateurs. Parmi ses options Premium supplémentaires figurent un système IPS, une prévention des menaces avancées, une connectivité mondiale et des analyses anti-malware. Cette dernière option est une fonctionnalité OEM intégrée, gérée et mise à niveau par Cato Networks pour une totale transparence aux yeux des utilisateurs. DLP, NAC, RBI… d'autres options Premium sont prévues à l'avenir.

Cato Networks
Fonctions SASE

Indispensables	Accessoires	Et quelques extras…
● SD-WAN	○ WAAP	○ Protection des bornes Wi-Fi
● SWG	Planifié ● RBI	○ Masquage du réseau
● CASB	○ DNS récursif	● VPN d'ancienne génération
● ZTNA	Partenaire ● Sandboxing du réseau	○ Protection de l'Edge Computing
● FWaaS	○ Accès par API au SaaS	○ UEBA
● Données personnelles sensibles / Malwares	● Prise en charge des appareils gérés et non gérés	
● Débit de ligne (périphérie)		
● Débit de ligne (cloud)		

Cato Cloud repose sur une stack logicielle cloud-native intégrant des fonctionnalités SD-WAN et de sécurité. Le logiciel est aujourd'hui déployé dans 60 points de présence dans le monde et propose une console de gestion centralisée. Cato déploie entre trois et quatre nouveaux points de présence par trimestre. Géographiquement parlant, au-delà des marchés primaires sur lesquels Cato a déployé ses PoP, l'entreprise s'est implantée sur divers marchés tertiaires, notamment à Casablanca (Maroc) et à Santiago (Chili). Elle peut traiter des flux de trafic de plusieurs gigabits à vitesse de ligne, avec un déchiffrement complet pour une inspection jusqu'à 2 Gbit/s. Tout le trafic client est inspecté dans un proxy cloud pour les contrôles d'accès et la prévention des menaces. Les points de présence sont symétriques (avec redondance totale) et sont interconnectés avec deux ou trois opérateurs Tier 1. Les PoP assurent un traitement du trafic Internet et accélèrent le trafic WAN, avec possibilité de bénéficier de fonctionnalités supplémentaires : optimisation du cloud, accélération TCP, optimisation globale du routage, sélection dynamique des opérateurs, calcul du meilleur chemin paquet par paquet. Côté sécurité, la plateforme utilise une architecture single-pass, avec trois moteurs distincts inspectant le trafic à la recherche de malwares. Elle est conçue à l'origine comme une architecture multi-tenant. Le logiciel fonctionne sur des serveurs physiques que Cato Networks déploie dans des installations de colocation. Bien que la plupart des fonctions à forte intensité de traitement soient exécutées dans le cloud, Cato Networks utilise une architecture « thin-edge » qui

nécessite l'installation d'appliances SD-WAN sur les sites distants. L'entreprise fournit également un accès client et sans client pour les appareils mobiles (postes de travail, ordinateurs portables, smartphones, etc.). Les accès sans client s'effectuent via des applications web internes publiées sur un portail configurable par l'utilisateur.

Cato Networks vend ses produits à des entreprises comptant entre 5 et 2 000 sites et dont les effectifs se situent entre 500 et 45 000 salariés. La plus grande entreprise couverte par son service emploie 40 000 collaborateurs, dont 20 000 y accèdent à distance. À ce jour, Cato Networks compte plus de 750 clients dans le monde. Parmi les cas d'usage types, on peut citer le remplacement de MPLS, le remplacement de pare-feu périphériques sur site par une sécurité réseau en mode cloud, et le remplacement du VPN par une sécurité cloud. Cato Networks se différencie essentiellement par sa stack logicielle unique et intégrée, avec gestion centralisée et expérience utilisateur transparente. Palo Alto Networks (Prisma), Cisco (Meraki et Umbrella), VMware, Fortinet et Zscaler (ZIA et ZPA) sont ses principaux concurrents, auxquels s'ajoutent des télécoms comme British Telecom et CenturyLink.

Cisco Systems

Cisco affirme s'être engagé sur la voie de la convergence des services réseau et de sécurité bien avant que Gartner n'invente le terme « Secure Access Service Edge ». Son objectif : permettre aux utilisateurs de se connecter, en toute sécurité et de n'importe où, à leurs applications professionnelles. Cisco se positionne comme le seul fournisseur à proposer à la fois des fonctionnalités SD-WAN et de sécurité conçues en interne. En réalité, son offre SASE rassemble des éléments de propriété intellectuelle acquis par le biais de multiples rachats : Meraki et Viptela pour le SD-WAN, et OpenDNS (rebaptisé Umbrella), Scansafe (SWG cloud), CloudLock (CASB), etc., pour la sécurité. Seuls sa Threat Intelligence Talos et son framework SecureX de gestion et d'orchestration SecureX ont été développés en interne.

Aujourd'hui, Cisco propose trois offres combinées de service SD-WAN, de routage et de sécurité, sous les noms de Cisco DNA Essentials, Cisco DNA Advantage et Cisco DNA Premier. DNA Essentials combine tout un ensemble de fonctionnalités : overlay WAN, gestion centralisée vManage, topologies multiples, politiques d'application, NGFW, Snort IDS/IPS avec signatures de la Threat Intelligence Talos, surveillance du DNS et connecteurs Umbrella, optimisation des chemins de base, protocoles de routage OSPF et BGP, etc. DNS Advantage ajoute à ces éléments les fonctionnalités suivantes : segmentation illimitée, vAnalytics, connexion onRamp au cloud pour l'IaaS, filtrage d'URL, protection contre les malwares avancés, et Umbrella Application Discovery. L'offre haut de gamme, DNA Premier, représente ce que Cisco commercialise comme sa solution SASE. Elle se superpose à Umbrella SIG Essentials, qui apporte sécurité de la couche DNS, SWG, CASB, FWaaS, Threat Intelligence interactive, SecureX (XDR), protection anti-malware Secure Endpoint, sandboxing Secure Malware Analytics et clients utilisateurs distants AnyConnect.

Cisco Systems
Fonctions SASE

Indispensables	Accessoires	Et quelques extras...
◉ SD-WAN	○ WAAP	◉ Protection des bornes Wi-Fi
◉ SWG	Planifié ◉ RBI	◉ Masquage du réseau
◉ CASB	◉ DNS récursif	◉ VPN d'ancienne génération
◉ ZTNA	◉ Sandboxing du réseau	○ Protection de l'Edge Computing
◉ FWaaS	◉ Accès par API au SaaS	◉ UEBA
◉ Données personnelles sensibles / Malwares	◉ Prise en charge des appareils gérés et non-gérés	
? Débit de ligne (périphérie)		
? Débit de ligne (cloud)		

Disponibilité et options d'achat sur le marché émergent du SASE

L'architecture SASE de Cisco a été conçue comme un service cloud-native basé sur des containers et des microservices. L'objectif est d'étendre la simplicité d'opération des produits Meraki à une offre de services réseau et de sécurité convergents, reposant sur les passerelles cloud Cisco de périphérie réseau réparties à travers le monde. Ces passerelles permettent un peering direct avec un large éventail de fournisseurs IaaS et SaaS. À ce jour, Cisco a déployé plus de 30 data centers régionaux avec un accès direct à plus de 1 000 FAI, CDN et fournisseurs SaaS. L'entreprise prévoit d'ajouter 10 autres data centers régionaux au cours de l'année prochaine. Le moteur de politiques de Cisco Umbrella est intégré aux fonctions SD-WAN et SecureX pour permettre des actions automatisées sur ses propres produits réseau et de sécurité, ainsi que sur ceux d'autres fournisseurs. Pour s'intégrer aux pare-feu sur site existants, Cisco a apporté des améliorations à Defense Orchestrator afin de connecter les politiques des pare-feu sur site au service cloud.

Cisco a abaissé la barrière à l'adoption de sa nouvelle offre SASE en proposant une seule SKU pour simplifier son processus d'achat, et en facilitant le déploiement par des tunnels automatisés du SD-WAN à Umbrella. Son offre SASE se différencie également par l'exhaustivité de ses contrôles ; l'efficacité de sa sécurité ; sa vaste couverture de réseaux, terminaux et clouds ; ainsi que par sa longue expérience dans le développement et la gestion d'un réseau haute performance et haute capacité, y compris le réseau mondial Umbrella. L'efficacité des produits/fonctions de sécurité Cisco est due en grande partie à la Threat Intelligence de Talos. L'entreprise se targue ainsi de disposer de la plus grande équipe de Threat Intelligence du secteur privé. Cisco affirme également être le plus grand fournisseur SD-WAN au monde grâce à ses deux offres SD-WAN pour grandes entreprises.

Cloudflare One

La nouvelle offre SASE Cloudflare for Teams s'appuie sur le vaste réseau mondial de l'entreprise, qui s'étend sur 200 villes et 100 pays dans le monde et possède une capacité globale de 42 Tbit/s. Appelée Cloudflare One, la plateforme sur laquelle repose cette offre SASE s'appuie sur l'infrastructure réseau étendue de l'entreprise et sur son portefeuille d'applications web, ses services d'accès Zero Trust et ses solutions de protection du réseau. Au menu : interconnexion des réseaux, transit IP, agent d'itinérance, routage intelligent, accélération du trafic, passerelle web sécurisée, accès Zero Tust, protection anti-DDoS et filtrage du trafic entrant. L'objectif de Cloudflare for Teams est de fournir un accès sécurisé, rapide et transparent à Internet et n'importe quelle application depuis n'importe quel appareil et n'importe quel emplacement.

La version initiale de Cloudflare One offre les fonctionnalités suivantes : SWG, ZTNA, isolement du navigateur, DNS récursif avec prise en charge des appareils gérés et non gérés, protection des bornes Wi-Fi, cas d'usage CASB et protection de l'Edge Computing. Cloudflare One fonctionne également sur le réseau Edge de Cloudflare avec des opérations en débit de ligne et une protection de l'Edge Computing. Ajoutons à cela un proxy s'intégrant à au moins huit fournisseurs de gestion des identités, un tableau de bord centralisé, une intégration simple avec les principaux SIEM, Terraform pour la gestion, et une intégration des appareils avec Azure AD et Tanium. Parmi ses autres partenaires, on peut citer CrowdStrike, Carbon Black et SentinelOne. À court terme, la feuille de route du SASE Cloudflare One prévoit d'inclure une offre SD-WAN, un FWaaS amélioré, une DLP, une analyse réseau améliorée et un système IDS. Cloudflare ne propose pas encore de SKU ou d'offre combinée pour sa solution SASE, mais l'entreprise affirme que son modèle de déploiement en mode cloud et piloté par un tableau de bord permet aux clients d'activer facilement plusieurs services SASE à la fois. Tous les services SASE sont intégrés, ce qui libère le client de cette charge.

Cloudflare
Fonctions SASE

Indispensables	Accessoires	Et quelques extras…
Planifié ● SD-WAN	◉ WAAP	◉ Protection des bornes Wi-Fi
◉ SWG	◉ RBI	◉ Masquage du réseau
◉ CASB	◉ DNS récursif	○ VPN d'ancienne génération
◉ ZTNA	Planifié ● Sandboxing du réseau	◉ Protection de l'Edge Computing
Planifié ● FWaaS	○ Accès par API au SaaS	Planifié ● UEBA
Planifié ● Données personnelles sensibles / Malwares	◉ Prise en charge des appareils gérés et non-gérés	
◉ Débit de ligne (périphérie)		
◉ Débit de ligne (cloud)		

Cloudflare One s'appuie sur le réseau mondial de l'entreprise, qui se connecte aux utilisateurs via des tunnels GRE, des interconnexions réseau ou un client mobile qui crée un tunnel complet dans le data center Cloudflare le plus proche de l'utilisateur. À ce niveau, Cloudflare assure la sécurité et le filtrage des données dans une architecture single-pass. Réseau mondial haute performance de l'entreprise, disponibilité de toutes les fonctions dans chacun de ses 200 data centers, architecture single-pass pour le filtrage et la sécurité, et facilité de déploiement et d'utilisation… son offre SASE se différencie sur plusieurs points. Cloudflare considère Cisco, Netskope, Palo Alto Networks et Zscaler comme ses concurrents SASE les plus directs.

Disponibilité et options d'achat sur le marché émergent du SASE

Fortinet

Fortinet n'a que récemment livré la première version de son offre SASE en mode cloud, issue du rachat d'OPAQ Networks en juillet 2020. L'intégration initiale de la technologie Fortinet-OPAQ a permis de créer un plan unique de sécurité et de gestion des politiques pour les utilisateurs distants. Publiée fin 2020, la version initiale de la solution combine le SD-WAN à un ensemble de fonctionnalités : SWG, DNS récursif, IPS, DLP, sandboxing, FWaaS, identification des malwares et des données sensibles, et opérations en débit de ligne (périphérie et cloud). Fortinet met tout en œuvre pour que sa version initiale, axée sur la sécurisation des accès à Internet, offre une expérience utilisateur adaptée et une intégration transparente entre les technologies de gestion Fortinet et OPAQ. Cette version sera suivie dans la foulée par une seconde phase d'intégration qui inclura un CASB d'ici le deuxième trimestre 2021. Un troisième cycle d'intégration verra l'ajout de la fonctionnalité ZTNA à l'infrastructure FortiGate existante, prévu pour la fin du deuxième trimestre 2021. Parmi les autres fonctionnalités en cours de développement figurent l'isolement des navigateurs à distance, la protection des API et des fonctions UEBA. Pour ce qui est des options présentant un intérêt certain, on citera le sandboxing du réseau, la prise en charge des appareils gérés et non gérés, la protection des bornes Wi-Fi, le masquage du réseau, la protection de l'Edge Computing et la résolution des problèmes de sécurité liés aux anciens VPN.

Fortinet
Fonctions SASE

Indispensables	Accessoires	Et quelques extras...
SD-WAN	WAAP (WAF uniquement)	Protection des bornes Wi-Fi
SWG	RBI	Masquage du réseau
CASB (Planifié)	DNS récursif	VPN d'ancienne génération
ZTNA (Planifié)	Sandboxing du réseau	Protection de l'Edge Computing
FWaaS	Accès par API au SaaS	UEBA (Module supplémentaire)
Données personnelles sensibles / Malwares	Prise en charge des appareils gérés et non-gérés	
Débit de ligne (périphérie)		
Débit de ligne (cloud)		

Disponibilité et options d'achat sur le marché émergent du SASE

L'architecture FortiSASE acquise au moment du rachat d'OPAQ Networks a été spécialement conçue pour fonctionner dans le cloud, en tant que service multi-tenant intégré au réseau Secure Overlay de Fortinet. Fortinet progresse dans la mise en place d'un moteur de politiques unique pour les services réseau et de sécurité. L'entreprise gère actuellement un certain nombre de fonctionnalités : SD-WAN intégré avec FWaaS, IPS, DNS, DLP, SWG et ZTNA. Certaines fonctions de sécurité s'étendent à la périphérie « thin edge » et aux utilisateurs du réseau. D'autres seront également prises en charge par le moteur de politiques unique dans une nouvelle version de FortiSASE, dont le lancement est prévu au deuxième trimestre 2021. On ne sait pas exactement combien de points de présence Fortinet possède, mais il est probable qu'une trentaine seront disponibles en 2021, principalement en Amérique du Nord. Fortinet s'appuie également sur des relations de peering avec ses partenaires pour fournir une connectivité via ses dorsales privées. À court terme, l'entreprise prévoit de mettre en place une trentaine de partenariats. Elle espère notamment que ces accords de peering avec ses partenaires permettront de combler ses lacunes. Fortinet maintient que le durcissement de la périphérie WAN et son extension à la périphérie du cloud est une meilleure option architecturale, et qu'une architecture exclusivement Edge Cloud ne pourra pas s'imposer sur le long terme.

Fortinet considère que son offre SASE est en concurrence directe avec Umbrella de Cisco, Netskope, Cato Networks, Zscaler et Prisma Access de Palo Alto Networks. Pour se différencier, Fortinet entend fournir un certain niveau d'évolutivité en dehors de la périphérie WAN, sans pour autant trop s'engager en termes de performances et de latence. Fortinet considère Zscaler comme un leader dans ce domaine, qui toutefois n'offre pas un ensemble complet de services de sécurité.

Aruba (HPE) Silver Peak

La pièce maîtresse de l'offre SASE d'Aruba (HPE) est le portefeuille de produits SD-WAN Aruba EdgeConnect acquis en septembre 2020. Parmi ses fonctions phares : SD-WAN, routage, optimisation WAN, pare-feu à états basé sur les zones, segmentation avancée, et visibilité et contrôle sur les applications. D'autres fonctions de sécurité sont fournies par des partenaires, dont Check Point, Forcepoint, McAfee, Netskope, Palo Alto Networks, Symantec et Zscaler. Silver Peak a notamment mis en place une orchestration automatisée avancée avec Check Point, Zscaler et Netskope. Les intégrations incluent la possibilité d'établir des tunnels VPN IPsec primaires et secondaires vers les services ou la stack de sécurité cloud de chaque partenaire situés dans le PoP le plus proche de chaque site distant raccordé au SD-WAN. Les entreprises peuvent également définir des politiques de sécurité uniques par simple glisser-déposer dans l'interface Unity Orchestrator. Silver Peak ne propose pas de packs ou bundles spécifiques.

Aruba (HPE) Silver Peak
Fonctions SASE

Indispensables	Accessoires	Et quelques extras...
● SD-WAN	○ WAAP	○ Protection des bornes Wi-Fi
Partenaire ● SWG	Partenaire ● RBI	○ Masquage du réseau
Partenaire ● CASB	○ DNS récursif	○ VPN d'ancienne génération
Partenaire ● ZTNA	Partenaire ● Sandboxing du réseau	○ Protection de l'Edge Computing
● FWaaS	○ Accès par API au SaaS	○ UEBA
Partenaire ● Données personnelles sensibles / Malwares	Partenaire ● Prise en charge des appareils gérés et non-gérés	
Partenaire ● Débit de ligne (périphérie)		
○ Débit de ligne (cloud)		

Le pare-feu à états basé sur des zones d'Aruba (HPE) Silver Peak s'exécute sur une appliance physique ou virtuelle sur le site distant, comme partie intégrante d'Aruba EdgeConnect. En tant qu'appliance virtuelle, Aruba EdgeConnect peut être déployée dans les instances de cloud public AWS, Azure, Google ou Oracle d'un client. Si ce dernier souhaite créer une chaîne de services pour ses pare-feu ou d'autres services de sécurité de partenaires, EdgeConnect automatise cette opération par l'intermédiaire de son moteur de politiques Aruba Orchestration. Les responsables réseau peuvent configurer des politiques de sécurité uniques pour des applications ou des classes d'applications et, dans la même interface, automatiser la création de tunnels IPsec primaires et secondaires de chaque site distant vers le PoP de sécurité cloud le plus proche. Aruba (HPE) Silver Peak propose également une optimisation WAN en option, dont la licence est accordée par incréments de bande passante. À court terme, l'entreprise envisage d'étendre l'intégration des fonctions de sécurité – y compris IDS/IPS et le moteur de politiques de contrôle d'accès au réseau ClearPass d'Aruba, sans agent et basé sur des rôles – qui fournira une solution de contrôle des accès au réseau.

Les clients déploient Aruba Orchestrator sur site, dans leur(s) cloud(s) ou sous forme de service d'Aruba (HPE) Silver Peak. Il permet aux responsables réseau d'établir des superpositions virtuelles pour des classes d'applications et de définir, configurer et appliquer des politiques QoS uniques et de sécurité sur toute leur structure distribuée. L'entreprise prévoit d'étendre ses capacités d'automatisation autour de l'application de politiques dynamiques et de développer l'intégration automatisée avec d'autres partenaires technologiques.

En dehors de ses partenariats avec les principaux fournisseurs de sécurité, Aruba (HPE) Silver Peak a également mis en place des intégrations de sécurité automatisées avec Microsoft sur Office 365, Azure et Azure Virtual WAN, ainsi qu'avec AWS via son gestionnaire de réseau Transit Gateway.

Aruba (HPE) Silver Peak est un leader reconnu sur le segment des infrastructures de périphérie WAN. En tant que fournisseur de SD-WAN, il se différencie par sa capacité à prioriser les applications métiers critiques, à offrir des performances applicatives fiables grâce à l'IA pour s'adapter en permanence aux conditions changeantes du WAN, et à proposer une plateforme unifiée. La plateforme est unique en ce sens qu'elle permet aux clients de sélectionner les meilleures technologies de sécurité pouvant être intégrées à son offre SD-WAN et gérées via son moteur de politiques Aruba Orchestrator. Elle aide ainsi les clients à éviter tout enfermement propriétaire. Aruba (HPE) Silver Peak considère ses principaux concurrents comme étant VMware/VeloCloud, Cisco (principalement Viptela) et Aruba (HPE) et Meraki. L'entreprise s'attend à se retrouver de plus en plus face à Fortinet et Palo Alto Networks, via son acquisition de CloudGenix.

Palo Alto Networks

Palo Alto Networks a fait son entrée sur le marché du SASE début 2019 avec Prisma, sa suite de sécurité en mode cloud, comprenant Prisma Access SD-WAN pour fournir un accès sécurisé aux sites distants. Pour renforcer ses capacités SD-WAN, l'entreprise a acquis CloudGenix en avril 2020. Palo Alto Networks continue de bâtir sur ce socle en développant plusieurs axes : 1) intégrer le SD-WAN CloudGenix à sa suite Prisma, 2) appliquer le machine learning à la gestion de la bande passante, 3) étendre l'automatisation pour accélérer la résolution des problèmes, et 4) ajouter de nouvelles appliances en entrée de gamme pour les petits sites et en haut de gamme pour les plus grands sites, les campus et les data centers. Aujourd'hui, Palo Alto Networks propose quatre offres SASE :

- Prisma Access Business – filtrage d'URL et sécurité DNS
- Prisma Access Business Premium – filtrage d'URL, sécurité DNS, prévention des menaces et sandbox Wildfire
- Prisma Access Enterprise – filtrage d'URL, sécurité DNS, prévention des menaces, Wildfire et accès aux applications privées via des connexions de service (deux avec SKU locale, cinq avec SKU mondiale). Les modules optionnels de cette offre comprennent des connexions de services supplémentaires, la DLP et les interconnexions (accès utilisateur-à-site et site-à-site).
- Prisma Access ZTNA – filtrage d'URL, prévention des menaces et accès privé aux applications via des connexions de service (deux avec SKU locale, cinq avec SKU mondiale). Les modules complémentaires optionnels comprennent des connexions de services supplémentaires et la DLP.

Palo Alto Networks
Fonctions SASE

Indispensables	Accessoires	Et quelques extras...
◉ SD-WAN	○ WAAP	◉ Protection des bornes Wi-Fi
◉ SWG	○ RBI	◉ Masquage du réseau
◉ CASB	◉ DNS récursif	◉ VPN d'ancienne génération
◉ ZTNA	◉ Sandboxing du réseau	◉ Protection de l'Edge Computing
◉ FWaaS	◉ Accès par API au SaaS	◉ UEBA
◉ Données personnelles sensibles / Malwares	◉ Prise en charge des appareils gérés et non-gérés	
◉ Débit de ligne (périphérie)		
◉ Débit de ligne (cloud)		

Disponibilité et options d'achat sur le marché émergent du SASE

La solution Prisma Access de Palo Alto Networks a été conçue comme un service « cloud-agnostique », bien qu'elle s'appuie actuellement sur AWS, Google Cloud et le sous-ensemble de points de présence dotés de capacités de calcul, et non de simples fonctionnalités de passerelle. Palo Alto Networks revendique plus de 100 PoP dans 76 pays et prévoit d'en ajouter 5 à 10 dans les 12-24 prochains mois. La fonction d'orchestration de Prisma Access est multi-tenant et s'appuie sur des technologies cloud-native (containers, systèmes sans serveur, microservices, etc.). Chaque client bénéficie de SPN (Software-Based Security Processing Nodes) dédiés, déployés au sein de l'infrastructure cloud et basés sur les pare-feu nouvelle génération de l'entreprise. Si un tel déploiement garantit la séparation du trafic et des performances honorables, il augmente également le coût d'exploitation de Prisma Access. Le moteur de politiques single-pass de Palo Alto Networks effectue plusieurs inspections en une seule passe (single-pass), ce qui le rend très efficace dans l'application de politiques basées sur des informations contextuelles portant sur les utilisateurs, les applications et les contenus. Malgré l'intégration initiale du SD-WAN CloudGenix, celui-ci est toujours vendu séparément des offres SASE.

L'offre SASE de Palo Alto Networks se différencie par la profondeur et l'efficacité de ses fonctions de sécurité, basées sur son NGFW leader du marché, et par sa capacité à consolider au moins 10 outils spécialisés. L'entreprise revendique les meilleures capacités de sécurité et désormais de SD-WAN, soutenues par un moteur de politiques et un modèle de données communs servant à renforcer la sécurité et le réseau. Pour les clients NGFW existants, Palo Alto Networks propose une gestion consolidée des produits NGFW et Prisma Access afin de simplifier les opérations. L'entreprise estime également que le réseau de data centers de Google Cloud, relié par un réseau fibre dédié, combiné à sa sécurité inline à faible latence, permet d'améliorer la sécurité et la productivité, le tout garanti par des engagements SLA pour une latence inférieure à 10 ms. Prisma Access est en concurrence directe avec Zscaler, et lorsqu'il remporte des contrats face à son rival, c'est le plus souvent en raison de sa sécurité plus robuste, de son évolutivité dynamique et de sa facilité de gestion pour les clients NGFW existants.

Versa Networks

Versa est l'un, si ce n'est le dernier fournisseur SD-WAN pure-play encore indépendant après la récente vague d'acquisitions en 2020. Versa Networks est une société privée de 500 salariés au capital-risque de 196 millions de dollars. Huit ans après sa création, l'entreprise est devenue rentable en 2020 grâce à ses plus de 1 000 entreprises clientes et leurs centaines de milliers de sites.

Versa propose pas moins de six offres différentes, dont les fonctionnalités de base tournent autour de quatre axes : gestion du réseau, routage, SD-WAN, architecture multi-tenant. Côté fonctionnalités SD-WAN, on retrouve la qualité de service (QoS), la remédiation basée sur des politiques pour améliorer les performances d'applications spécifiques, la segmentation et les NGFW. Le service SASE de Versa combine routage, SD-WAN, sélection dynamique des chemins, routage du trafic et QoS, visibilité et priorisation d'applications spécifiques, ainsi qu'un NGFW intégré, un système IPS nouvelle génération et le filtrage d'URL. Les SWG et d'autres services de sécurité avancés sont également proposés séparément. Pour les environnements de télétravail, Versa décline son offre en deux formats : un équipement domestique et l'offre Versa Secure Access déployée dans le cloud et reposant sur un client IOS, Windows ou Linux. Son offre SASE Premium comprend presque toutes les fonctions de sécurité indispensables, y compris (plus récemment) le CASB et l'isolement du navigateur. Les bundles de Versa sont conçus pour répondre aux exigences des entreprises de quasiment toutes les tailles, des sites de tous les types et des quantités d'utilisateurs distants les plus variées.

L'architecture de Versa permet de fournir des services SASE intégrés sur site, dans le cloud, ou les deux. Elle utilise pour cela le même système d'exploitation, Versa Operating System (VOS), au sein d'une seule et unique stack logicielle. VOS peut être déployé sous forme de service hébergé par Versa, mais aussi sous forme de service cloud privé hébergé, exploité et géré par le client via sa propre passerelle Versa Cloud Gateway. Il peut également être déployé dans un modèle hybride lorsque le client exige de hautes performances sur une de ses implantations, comme un très grand site distant. Dans ce cas, 80 % des fonctions sont généralement exécutées localement et 20 % dans le cloud. Le service cloud de Versa est fourni via ses Versa Cloud Gateways situées dans 90 points de présence dans le monde. Dix nouveaux PoP sont prévus dans les 12-24 prochains mois. Les PoP sont situés dans des installations en colocation, des data centers publics et privés, et des environnements de cloud public (AWS, Azure et Google Cloud).

Les fonctionnalités SASE de Versa s'appuient sur l'architecture single-pass de traitement parallèle de VOS qui intègre dans une seule image logicielle des fonctions complètes (SD-WAN, sécurité, routage avancé, multi-tenancy, analyse, etc.). VOS est conçu pour réduire la latence, améliorer les performances et réduire le nombre de vulnérabilités liées à l'utilisation de plusieurs stacks logicielles, chaînes de services ou appliances. Versa Director fournit une interface de gestion commune qui simplifie la création, l'automatisation et la mise à disposition de services SASE. Il peut être déployé sur site ou dans le cloud. La plateforme d'orchestration Versa Concerto a été ajoutée à Versa Director à la mi-2020 pour automatiser les déploiements VOS à grande échelle. Elle automatise la création de topologies de sécurité réseau communes, les fonctions d'auto-réparation pour les utilisateurs, les appareils et les sites distants, et la redirection vers des fournisseurs SASE tiers.

Disponibilité et options d'achat sur le marché émergent du SASE

Versa Networks
Fonctions SASE

Indispensables	Accessoires	Et quelques extras...
SD-WAN	WAAP	Protection des bornes Wi-Fi
SWG	RBI	Masquage du réseau
CASB	DNS récursif	VPN d'ancienne génération
ZTNA	Sandboxing du réseau	Protection de l'Edge Computing
FWaaS	Accès par API au SaaS	UEBA
Données personnelles sensibles / Malwares	Prise en charge des appareils gérés et non-gérés	
Débit de ligne (périphérie)		
Débit de ligne (cloud)		

Versa considère son offre SASE unique à trois niveaux. Premièrement, elle offre le même ensemble de politiques de sécurité, de gestion du réseau et d'analyse, quel que soit l'endroit où elles sont déployées (dans le cloud, sur site, ou une combinaison des deux), selon les exigences des différents sites des clients. Ses concurrents ne proposent parfois qu'un sous-ensemble de services SASE dans le cloud ou ne proposent pas de services SASE sur site. Deuxièmement, Versa estime que son VOS offre une série d'avantages uniques grâce à son architecture single-pass de traitement parallèle. Parmi ses avantages : réduction de la latence, amélioration des performances, réduction du risque, et ensemble complet de services SASE fournis à partir d'une seule image logicielle. Ce dernier atout élimine la nécessité d'effectuer un chaînage de services, une mise en cascade ou de créer des interconnexions virtuelles entre différents services SASE. Troisièmement, Versa considère être le seul fournisseur SASE à donner à ses clients et à ses partenaires fournisseurs de services la possibilité de créer leur propre service SASE privé, sur site ou dans un cloud privé, ce qui donne davantage de contrôle sur le service qu'avec l'offre des autres fournisseurs SASE. Ses concurrents directs sont Cisco/Viptela.

VMware

Pour promouvoir sa nouvelle offre SASE, VMware met en avant sa solution SD-WAN leader du marché, rachetée à VeloCloud fin 2017 pour 449 millions de dollars. L'entreprise met également à disposition un composant ZTNA via sa fonctionnalité VMware Secure Access, qui est actuellement un module complémentaire de sa solution Workspace One. Les composants SD-WAN et ZTNA bénéficient tous deux d'importantes bases installées, avec plus de 12 000 clients SD-WAN. L'offre SD-WAN permet l'identification des données sensibles et des malwares, le fonctionnement en débit de ligne à la périphérie et depuis le cloud, le masquage du réseau et la prise en charge des VPN d'ancienne génération.

Par ailleurs, l'entreprise travaille actuellement à la mise en place d'une série de fonctionnalités de sécurité supplémentaires intégrées (SWG et CASB) qui devraient être disponibles prochainement. Parmi les autres fonctions de sécurité sur la feuille de route du SASE VMware : FWaaS, isolement du navigateur à distance, sandboxing du réseau (via son acquisition de Lastline), accès par API au SaaS pour la contextualisation des données, et protection de l'Edge Computing. La stratégie de VMware consiste à offrir ces fonctionnalités directement aux clients et à s'associer à des fournisseurs de sécurité de premier plan. Aujourd'hui, VMware affiche l'intégration la plus étroite avec Zscaler, mais collabore aussi avec Check Point, Cisco, Fortinet, Menlo Security et Palo Alto Networks.

VMware
Fonctions SASE

Indispensables	Accessoires	Et quelques extras...
○ SD-WAN	○ WAAP	○ Protection des bornes Wi-Fi
Planifié ○ SWG	Planifié ○ RBI	○ Masquage du réseau
Planifié ○ CASB	○ DNS récursif	○ VPN d'ancienne génération
○ ZTNA	Planifié ○ Sandboxing du réseau	○ Protection de l'Edge Computing
Planifié ○ FWaaS	Planifié ○ Accès par API au SaaS	Planifié ○ UEBA
X-SD-WAN aujourd'hui ; SWG planifiée ○ Données personnelles sensibles / Malwares	○ Prise en charge des appareils gérés et non-gérés	
○ Débit de ligne (périphérie)		
○ Débit de ligne (cloud)		

VMware vante le fait que son offre SASE, basée sur l'infrastructure VeloCloud, est 100 % cloud tout en proposant une option de déploiement sur site. Idem pour ses fonctionnalités SD-WAN et ZTNA existantes. L'infrastructure cloud de VMware s'appuie sur des sites en colocation dotés de capacités réseau et de calcul autogérées. Elle compte actuellement 33 PoP et prévoit de porter ce nombre à 50 au cours des 12 à 24 prochains mois. Les sites sont interconnectés via des FAI Tier 1, sans oublier des relations directes de peering avec tous les principaux fournisseurs cloud. VMware collabore également avec ses partenaires fournisseurs de services pour étendre sa présence mondiale, le but affiché étant de disposer d'un total combiné de 100 PoP au fur et à mesure que ces partenaires modernisent leurs installations.

Les offres SASE de VMware sont en concurrence directe avec celles de Cisco (Meraki et Viptela), Fortinet, Aruba (HPE) Silver Peak et Palo Alto Networks. Pour VMware, son offre SASE se différencie sur plusieurs points : déploiement dans le cloud, leadership dans le domaine du multi-cloud, large base installée à la fois pour l'infrastructure Edge WAN et la gestion unifiée des terminaux, expérience utilisateur de qualité, facilité de gestion et sécurité.

Zscaler

Zscaler est probablement le fournisseur de services de sécurité cloud-native le mieux établi, grâce à ses services de passerelle web sécurisée (SWG) fournis depuis longtemps dans le cloud. L'entreprise dispose de 150 PoP dans le monde et d'une architecture single-pass pour déchiffrer le trafic, détecter des malwares et données sensibles, et appliquer les contrôles appropriés en fonction des identités et du contexte. Son architecture multi-tenant utilise un proxy pour fournir des performances en débit de ligne à la fois en périphérie et dans le cloud.

L'offre SASE de Zscaler remplit toutes les conditions requises pour un service SASE digne de ce nom, bien que sa fonctionnalité SD-WAN soit fournie par des partenaires, notamment Aruba (HPE) Silver Peak et VMware. Parce que l'entreprise élargit depuis longtemps sa gamme de services cloud de sécurité au-delà des SWG, elle gère déjà des services de sécurité supplémentaires en plus de ses services de base : protection des applications web et des API, isolement du navigateur à distance, DNS récursif, sandboxing du réseau, accès par API aux applications SaaS pour la contextualisation des données, prise en charge des appareils gérés et non gérés, protection des bornes Wi-Fi et masquage du réseau. Les fonctions pour sites distant s'appuient également sur des offres partenaires, notamment Cisco, Aruba (HPE) Silver Peak et VMware. En outre, Zscaler propose une intégration avec Okta et Ping pour la gestion des identités, et avec CrowdStrike pour l'état des appareils. La solution SASE de Zscaler est fournie dans le cadre de ses offres Zscaler Internet Access et Zscaler Private Access, disponibles en éditions Basic et Standard.

Zscaler
Fonctions SASE

Indispensables	Accessoires	Et quelques extras...
◉ SD-WAN	◉ WAAP	◉ Protection des bornes Wi-Fi
◉ SWG	◉ RBI	◉ Masquage du réseau
◉ CASB	◉ DNS récursif	○ VPN d'ancienne génération
◉ ZTNA	◉ Sandboxing du réseau	○ Protection de l'Edge Computing
◉ FWaaS	◉ Accès par API au SaaS	○ UEBA
◉ Données personnelles sensibles / Malwares	◉ Prise en charge des appareils gérés et non-gérés	
◉ Débit de ligne (périphérie)		
◉ Débit de ligne (cloud)		

Dans un véritable esprit de coopération, plusieurs des participants à cette étude collaborent avec Zscaler pour certaines fonctionnalités SASE. Zscaler considère Netskope et Palo Alto Networks comme ses principaux concurrents SASE, et met en avant les principaux facteurs de différenciation suivants : sécurité cloud fournie depuis 150 data centers, proxy inline haute performance, architecture « thin-branch », inspection complète du trafic chiffré et architecture multi-tenant cloud-native.

Conclusion

Il ressort clairement de cette étude que les capacités SASE, les modèles de tarification, les offres et les efforts d'intégration de ces fournisseurs en sont encore aux stades initiaux de leur développement. On peut donc s'attendre à des évolutions à mesure qu'ils acquièrent de l'expérience opérationnelle. Ce qui sera essentiel pour les primo-adoptants du SASE et, en définitive, pour les fournisseurs de solutions, c'est le niveau d'intégration et de simplicité opérationnelle des fonctions réseau et de sécurité, ainsi que la facilité (ou la difficulté) des relations avec les fournisseurs. Plus le client devra composer avec un grand nombre de contrats et de tarifs différents, plus la courbe d'adoption sera longue. Pour les fournisseurs SASE travaillant avec des partenaires d'intégration, il sera également essentiel d'éviter les renvois de responsabilité lorsque des problèmes surviendront, ce qui ne manquera pas de se produire. Un chaînage de services lourd et compliqué à gérer pour les clients sera la recette idéale de l'échec.

Au-delà de ces questions opérationnelles, les cycles de vente dépendront du centre d'achat, des détenteurs de budgets, et de la manière dont différentes équipes s'associeront pour mettre en œuvre les projets de convergence. Ce marché prendra probablement plus de temps à se développer et se stabiliser que les marchés technologiques habituels. Dans les grandes entreprises en particulier, la combinaison du réseau et de la sécurité en un seul marché soulève des enjeux organisationnels et culturels majeurs, qui prendront plus de temps à se tasser que de simples changements architecturaux. Les entreprises devront revoir leur structure, leur approche de l'adoption et la provenance des lignes budgétaires. Il leur faudra surmonter un certain degré de méfiance entre différentes équipes informatiques, qui devront mettre de côté leurs différences pour faire du SASE un succès. Les équipes de direction devront, quant à elles, veiller à la cohérence des objectifs de façon à fédérer les énergies et à doper la productivité.

Les acheteurs n'en sont encore qu'au début de leur parcours et la plupart des entreprises tentent encore de tracer un cap clair vers la destination finale qu'est la convergence transparente du réseau et de la sécurité dans un monde dominé par la mobilité et le cloud.

À propos d'Enterprise Management Associates, Inc.

Fondé en 1996, Enterprise Management Associates (EMA) est un cabinet d'étude leader spécialisé dans l'analyse d'un large éventail de technologies dans les domaines des systèmes d'information et de la gestion des données. Les analystes EMA s'appuient sur leur vaste expérience, leurs observations pointues des bonnes pratiques sectorielles et une excellente connaissance des solutions actuelles et futures pour aider leurs clients à atteindre leurs objectifs. Rendez-vous sur www.enterprisemanagement.com pour en savoir plus sur les services EMA de recherche, d'analyse et de conseil pour les entreprises, les professionnels IT et les fournisseurs de services IT. Suivez également EMA sur Twitter et LinkedIn.

Siège social :
1995 North 57th Court, Suite 120
Boulder, CO 80301
Téléphone : +1 303 543 9500
www.enterprisemanagement.com

4068.021221-fr