L'INFORMATICIEN

PAYS :France
PAGE(S) :32-34
SURFACE :245 %
PERIODICITE :Mensuel

DIFFUSION :(15000)
JOURNALISTE :B. G

► 1 juin 2021 - N°197

SECURE ACCESS SERVICE EDGE

Le SASE : un concept pour le long terme

Dans son numéro 190, *L'Informaticien* présentait le concept du SASE, pour Secure Access Service Edge, prôné par le cabinet Gartner dans un document de 2019. Il nous est revenu que sa mise en œuvre se révèle complexe. Nous faisons un point sur la réalité du SASE en France aujourd'hui et les principaux freins rencontrés.

Le SASE affole le secteur de la cybersécurité ! Pour rappel, le modèle SASE développé par le cabinet Gartner vise à combiner le contrôle à la fois sur le réseau et la cybersécurité en développant une nouvelle architecture et un point de contrôle unique dans le Cloud. S'appuyant sur une plateforme, le SASE regroupe à la fois le SD-WAN, le Zero Trust Network Access, un Firewall as a service, un CASB (Cloud Access Service Broker) et un DLP (Data Leak, ou Loss Prevention selon les éditeurs). Le modèle SASE regroupe ainsi un ensemble de techniques qui permettent d'identifier, de contrôler et de protéger l'information grâce à des analyses de contenu approfondies, que l'information soit stockée, en mouvement ou traitée et d'empêcher sa sortie à l'extérieur d'un périmètre de confiance. Ce ne sont pas les seules fonctions préconisées dans le modèle du Gartner mais ce sont les plus importantes et les plus couramment proposées actuellement par les éditeurs de la sécurité.

Le modèle est compris

« Nous avons une demande croissante des services SASE (RFx), dopée par le besoin de déployer SD-WAN, nous indique Hector Avalos », responsable de la zone EMEA chez Versa Networks. *« Nous avons fait le constat suivant : beaucoup d'autres solutions SASE mêlent défaut d'harmonisation, complexité de conception et d'intégration, et sont en outre inadaptées aux organisations dotées d'effectifs IT modestes, révélant alors le besoin criant d'une solution SASE prête à l'emploi pour les PME et le mid-market. »* Arnaud Gaugé, Sales Engineer Manager Réseau et Sécurité chez VMware, témoigne, lui, d'un projet dans une grande banque française. Frédéric Saulet, Regional Sales Manager pour la France chez Netskope, renchérit et pointe plusieurs appels d'offres autour de ce concept chez Axa, Pernod-Ricard, Airbus ou Eiffage. Selon lui, si le modèle se conçoit étape par étape *« en théorie, on n'est pas* SASE ready *en un claquement de doigt et cela prend des mois voire des années pour l'être »*. Patrick Sena, responsable avant-vente de Sailpoint constate, lui, les hésitations des entreprises sur le modèle. *« Si les entreprises sont assez convaincues de l'approche et s'y intéressent, peu d'entre elles se projettent dans quelque chose de concret, pas plus d'un quart des entreprises que j'ai rencontrées. »* Frédéric Saulet constate que le client est *« un peu perdu. Tout le monde met sa sauce marketing car tout le monde veut l'être. On essaie tous de l'adapter à notre contexte »*. Arnaud Gaugé renchérit : *« Il y a un peu de SASE Washing. »* Finalement, *« cela frise avant de bouillir »* !

Des freins de différents ordres

Si l'optimisme est de mise sur le long terme quant à la mise en œuvre du modèle SASE, les différentes personnes interrogées lors de cette

« Si le modèle se conçoit étape par étape en théorie, on n'est pas "SASE ready" en un claquement de doigt et cela prend des mois voire des années pour l'être »

Frédéric Saulet – Netskope

L'INFORMATICIEN

PAYS :France
PAGE(S) :32-34
SURFACE :245 %
PERIODICITE :Mensuel

DIFFUSION :(15000)
JOURNALISTE :B. G

► 1 juin 2021 - N°197

Le SASE en **chiffres**

Selon le cabinet Gartner, 30 % des entreprises auront adopté en 2024 des fonctions de SASE provenant d'un seul fournisseur. Ils n'étaient que 5 % l'année dernière. D'ici à 2025, 60 % des entreprises auront une stratégie et une feuille de route explicite pour le SASE. Elles étaient 10 % l'année dernière.

enquête relèvent des freins différents qui retardent ou obèrent la mise en œuvre dans les entreprises. Le premier est d'ordre organisationnel. Arnaud Gaugé relève ce point : *« Réseau et sécurité sont souvent des équipes distinctes, qui se parlent plus ou moins, avec des managements différents et qui n'ont pas les mêmes intérêts. Nous avons déjà vécu cela au début de NSX et du réseau virtualisé. Il faut casser les silos et il n'est pas si simple de mettre tout le monde autour de la table. »* Frédéric Saulet ajoute : *« Nous sommes obligés de parler aux deux voire de faire l'introduction entre les deux pour mettre en place une direction commune et une même feuille de route. »* Laurent Maréchal met le doigt sur les silos encore existant. *« Le modèle SASE comprend plus d'une dizaine de nécessités fonctionnelles qui demandent de défractionner ou de rompre les silos existants dans les infrastructures en place. Il convient de relever les freins business et opérationnels et ne pas se tromper sur la conception du modèle pour concrétiser la démarche. Là est la difficulté : comprendre le concept et les objectifs. »*

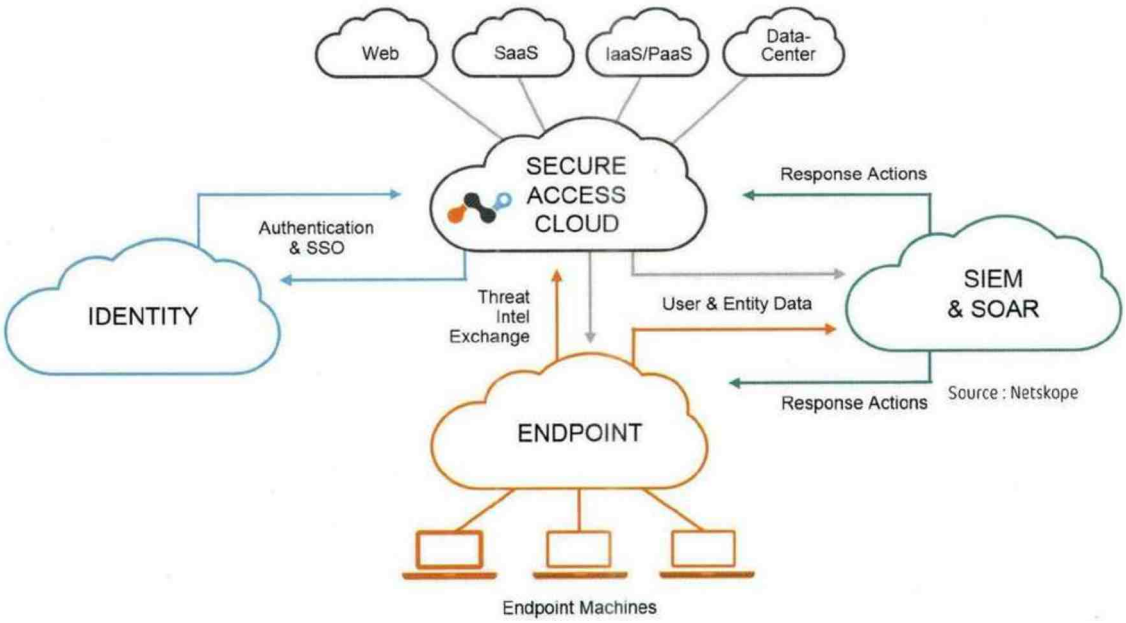
Des maturités différentes des entreprises

Arnaud Gaugé voit dans la maturité des entreprises sur le Cloud un élément déterminant dans l'acceptation du modèle SASE. *« Quelles que soient les raisons, les entreprises qui n'ont pas encore accepté l'idée du Cloud et qui ne sont pas dans cette démarche n'ont pas d'appétence pour le SASE et il est difficile de leur en parler. Pour les autres, elles sont prêtes. J'ai par exemple vu une entreprise qui avait un projet SD-WAN le transformer en projet de SASE avec tout ce qui l'accompagne : étude faisabilité, maturité des offres, retours d'expérience d'autres clients… »* Il ajoute : *« Cette entreprise appréciait la flexibilité du modèle qui lui permettait d'ajouter des services de manière flexible lui permettant de s'adapter rapidement. »* Frédéric Saulet relève aussi que le SASE ne répond pas à toutes les situations ni à tous les enjeux en citant le cas des applications dans les centres de données s'il n'y a pas d'interconnectivité. Il ajoute : *« Cela nécessite d'avoir aussi d'autres outils pour le suivi des autres activités. »*

Le poids du legacy

L'existant est souvent un frein, ou il ralentit les projets de mise en œuvre.

La future **architecture** de sécurité

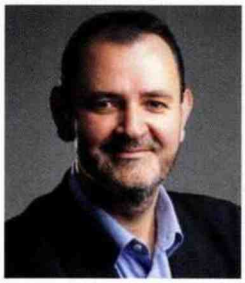


L'INFORMATICIEN

PAYS :France
PAGE(S) :32-34
SURFACE :245 %
PERIODICITE :Mensuel

DIFFUSION :(15000)
JOURNALISTE :B. G

► 1 juin 2021 - N°197



> *« Quelles que soient les raisons, les entreprises qui n'ont pas encore accepté l'idée du Cloud et qui ne sont pas dans cette démarche n'ont pas d'appétence pour le SASE »*
>
> Arnaud Gaugé – VMware

Arnaud Cassagne, le fondateur d'ACK Knowledge, spécialisée dans la modernisation des infrastructures IT, avec un focus sur la cybersécurité et le Cloud, indique que *« les entreprises sont engluées dans les infrastructures complexes qu'elles ont monté, et ont du mal à faire place nette, pour réfléchir aux nouvelles approches. Le fait de sans cesse réfléchir à la façon de reprendre toutes les fonctionnalités, toutes les exceptions que l'on a dû couvrir fait qu'on ne peut pas basculer vers quelque chose de nouveau »*. Il ajoute : *« Il y a aussi une incapacité de se débarrasser de solutions qui ont été mises en place – souvent dans la douleur –, qui ont fait le job pendant longtemps, mais qui ne sont plus adaptées. »* Il constate aussi la frilosité à innover et à *« s'adapter aux nouveaux modes fonctionnement »*. Arnaud Gaugé est du même avis : *« La maturité est souvent inégale dans les domaines de la sécurité et sur les solutions mises en place. Cela peut ralentir les projets avec des briques justes renouvelées ou inexistantes. »*

Le manque de compétence

Arnaud Cassagne relève sévèrement la pénurie d'expertise sur ce domaine : *« Le manque de compétences techniques et le nuage de fumée marketing viennent brouiller les pistes. Trop de termes et des définitions pas claires des acteurs qui essaient d'aller marcher sur les plates-bandes de solutions qui n'ont rien à voir. Il devient difficile d'y voir clair ! SASE, SD-WAN, Zero Trust, NGSWG… Tous les six mois on a un nouveau concept, qui vient s'appuyer sur un autre »*. Arnaud Gaugé note lui aussi ce point comme un élément qui peut ralentir les projets. Il constate par ailleurs que la vision sur le côté technique et sécurité fait parfois oublier le côté réseau dans la solution : *« Il ne faut pas oublier de simples choses comme la détection d'un problème réseau rapidement et d'y remédier. Ces points ont aussi leur valeur dans le modèle SASE. »*

Des offres encore incomplètes

Pour Mortada Ayad, Technical Regional Manager et Sales Engineering Manager - Emerging Markets chez Thycotic, *« Il n'y a pas de fournisseur capable de fournir l'ensemble dans le Cloud. À mon avis, ce modèle fait miroiter des choses qui ne sont pas encore réalisables. »* On assiste d'ailleurs à une vague de consolidation capitalistique dans le secteur avec des rachats pour compléter les plates-formes afin de proposer le modèle de manière complète. ✖

B. G.

Gartner fournit une **feuille de route** pour le SASE

Dans un document de mars dernier, le cabinet Gartner revient sur le modèle SASE et son adoption. Ce document détaille une feuille de route et les priorités pour le déploiement du SASE indiquant que le modèle peut être déployé de manière totale ou partielle. À court terme, soit dans les 18 mois, le document préconise de déployer des solutions Zero Trust pour remplacer les solutions VPN en place. Il recommande aussi de réaliser l'inventaire des équipements et des contrats à mettre en œuvre sur un plan pluriannuel pour supprimer les équipements sur site et les remplacer par des services SASE dans le Cloud. Il propose aussi de profiter des renouvellements de contrats pour consolider les vendeurs et réduire la complexité.

Le Gartner recommande d'engager activement la transformation dans les sites distants des entreprises et d'accélérer l'abandon de MPLS pour intégrer des services de sécurité de périphérie dans le Cloud dans le périmètre du projet prévu. À plus long terme, le cabinet conseille de consolider, autour d'un ou deux fournisseurs de plates-formes SASE. La mise en place de Zero Trust devra être totale sans tenir compte de la localisation ou de la taille de l'unité. Le choix de la solution SASE doit permettre de contrôler où se situe la console, comment le trafic est routé vers elle, ce qui est remonté et comment ces informations sont stockées. Dernière recommandation du Cabinet – et non la moindre : il prône de créer une équipe non seulement dédiée, mais comprenant et des experts sécurité, et des experts réseau ; avec une responsabilité qui sera partagée concernant l'ensemble de la sécurisation des accès.