SD-WAN : vers une sécurité 100% Cloud ?

En 2020, IBM publiait le rapport Cyber Resilient Organization montrant qu'une entreprise comptait une moyenne de 45 solutions de sécurité dans son système d'information.

L'enquête menée par Ponemon Institute à l'échelle mondiale auprès de 3 400 personnes montre que gérer une telle diversité de solutions aussi complexes implique à la fois beaucoup de ressources, mais aussi beaucoup d'inefficience. Les entreprises qui ont plus de 50 solutions estiment elles-mêmes leurs capacités à détecter les menaces inférieures de 8% aux autres entreprises, de même que leur capacité à répondre à une attaque, inférieure de 7%…

L'explosion du télétravail a notamment poussé l'intérêt des entreprises pour les solutions de SWG, (Secure Web Gateway). Plutôt que de gérer en interne l'infrastructure VPN, celle-ci est opérée dans le Cloud par un acteur spécialisé.

« Nos clients nous connaissent souvent pour le volet Internet Access, mais notre offre SWG , nous la proposons depuis maintenant 12 ans ! » explique Didier Schreiber, directeur Marketing pour la zone EMEA chez Zscaler. « Nous avons démarré avec l'Internet Access, le ZTNA pour accès aux applications privées, puis le CASB, le DLP, le CSPM (Cloud Security Posture Management) pour la protection des workloads ou encore du Threat Protection contre les menaces. »

Six fournisseurs sur le marché SD-WAN

Le fournisseur colle au modèle SASE du Gartner, avec150 points de présence, mais se refuse d'entrer sur le volet purement réseau du modèle, le SD-WAN : « Nous ne sommes pas un acteur du SD-WAN, mais nous travaillons avec des partenaires opérateurs de réseaux SD-WAN. »

Selon Dell'Oro Group, le marché mondial du SD-WAN a bondi de +39% entre le premier semestre 2020 et 2021 et se concentre désormais sur 6 vendeurs qui captent 70% du gâteau. Cisco devance Fortinet, VMware / VeloCloud, Versa et HPE Aruba. Ce marché est ultra compétitif et les fournisseurs enrichissent très régulièrement leurs offres de nouveaux services de sécurité à leur stack.

« A la base, l'objectif du SD-WAN est d'utiliser la connectivité Internet pour interconnecter les sites de l'entreprise pour faire baisser le coût des télécoms » souligne Hector Avalos, Vice-Président en charge des ventes sur les zones Europe, Moyen-Orient, Afrique & Russie de Versa Networks.

« Internet n'étant pas sécurisé, nous avons embarqué dans notre offre tout le stack de sécurité jusqu'au niveau 7, avec le Next Gen Firewall, le filtrage d'URL, le filtrage de contenu, l'antivirus, soit l'ensemble des briques nécessaires à la sécurisation des communications avec l'extérieur. » poursuit-il.

Versa Networks compte de nombreux grands opérateurs parmi ses clients, dont Verizon, Orange et Colt dont les offres SD-WAN s'appuient sur ses technologies.

Intégration Cybersécurité /SD-WAN

De nombreux fournisseurs de cybersécurité sont positionnés sur le marché SD-WAN, mais certains sont allés plus loin et ont intégré le réseau à leurs offres. C'est le cas du californien Aryaka qui n'est pas un « simple » fournisseur de boîtiers SD-WAN, mais aussi un opérateur WAN.

Alexandra Dunas, Directrice Commercial Europe du Sud d'Aryaka explique les atouts de cette approche. « Nous disposons à la fois de la technologie SD-WAN breveté, mais aussi de notre réseau WAN de niveau 2. Cette intégration nous permet d'offrir une gestion du trafic en bout en bout et éviter les multiples interconnexions d'un réseau à un autre. »

En France, cette approche a notamment séduit en France le Groupe Armor, Alstom, ou encore Shiseido où Aryaka est venu remplacer le réseau européen opéré par Verizon. De même, la couverture réseau de la Chine a séduit le groupe L'Oréal sur la plaque asiatique.

Pour ses briques sécurité, Aryaka s'appuie sur divers partenariats, mais l'américain vient de réaliser l'acquisition d'éditeur allemand SecuCloud qui nous apporte un portefeuille de solutions qui va lui permettre de proposer à ses clients une offre SASE 100% Aryaka.

Cato Networks mise aussi sur cette intégration entre réseau mondial et sécurité dans le Cloud.
L' éditeur israélien délivre un service d'interconnexion et des fonctions de sécurité 100% Cloud comme un Nextgen-Firewall, l'IPS, l'antimalware SentinelOne, des services de CASB et de Secure Web Gateway à l'image de ce que proposent Zscaler ou Netskope. Très prochainement, son offre va être compléter de briques DLP et Remote Browser Isolation (RBI).

Sylvain Chareyre, Manager of Sales Engineering EMEA , souligne la spécificité de l'approche Cato Networks : « Par opposition aux acteurs qui font du « Service Chaining » ou qui achètent des solutions auprès de multiples acteurs pour constituer une offre SASE, nous avons une seule offre totalement intégrée, convergée et présente dans le monde entier. La convergence c'est aussi une gestion sur seule console sans la dépendance avec de multiples produits. »

L'approche 100% Cloud a permis à Cato Neworks de signer So.bio, filiale de Carrefour, pour déployer sa solution sur 200 magasins en un mois et demi seulement. Dans l'hexagone, Cato Networks a séduit Haulotte, Fidal et a décroché le contrat Grand Frais pour interconnecter 400 sites.