CATO NETWORKS

Qu'est-ce que le SASE et comment va t-il révolutionner votre réseau ?

Les moyens historiques d'interconnexion des ressources d'une entreprise n'offrent pas l'agilité et la flexibilité demandées par les nouveaux usages IT.

De multiples couches de sécurité

Sécurité Cloud
+
Sécurité réseau
+
VPN/SDP

Une solution de sécurité fragmentée dont vous devez prendre en charge la gestion complexe.

Un réseau peu flexible

- Pas d'optimisation ou d'accélération Cloud
- Réseau MPLS dépendant d'infrastructures physiques
- Déploiement de nouvelles branches long et couteux
- Sécurité non intégrée
- Réseau global rigide et statique

Les infrastructures multi-sites se retrouvent alors avec des couches de sécurité éparses et une multitude de solutions à opérer.

CATO NETWORKS

La solution SASE par CATO Networks vient alors révolutionner l'infrastructure réseau et sa sécurité en les réunissant dans une solution convergée et Cloud native.

Le SASE vise donc à converger les infrastructures réseaux avec une sécurisation intégrée globale et optimale.

Le SASE c'est :

S pour Security

- Un Next Gen Firewall adapté aux applications (NGFW)
- Un Secure Web Gateway avec filtrage des URL (SWG)
- Un système Anti-Malware de nouvelle génération (NGAM)
- Un contrôle au sein des applications Cloud (CASB)
- Un Intrusion Prevention System géré en tant que service (IPS)
- Un service complet de détection et de réponse aux menaces (MDR)
- Une protection contre la fuite de données confidentielles (DLP)

A pour Access

Un backbone mondial privé de plus de 75 PoPs (Point of Presence) connectés via de multiples opérateurs réseaux pour permettre une optimisation des routes pour le trafic WAN et Cloud.

S pour Service

La proximité des PoPs du global backbone CATO aux fournisseurs Cloud (AWS, Azure...) et l'accélération intégrée de CATO :

- Maximise jusqu'à 20 fois le débit de bout en bout.
- Améliore les performances des applications pour les opérations gourmandes en bande passante.

E pour Edge

C'est pour toutes les ressources (devices, applications SaaS, Workload On Premise ou dans des clouds privés/publics).

- Avec les clients CATO (SDP/ZTNA), les ressources se connectent automatiquement et en toute sécurité au PoP (Point of Presence) le plus proche.
- Tout au long de la session, le trafic est entièrement inspecté par la sécurité CATO pour empêcher la propagation de logiciels malveillants à partir des terminaux compromis.

CATO NETWORKS | SASETY

Pour plus d'informations, rendez-vous sur www.sasety.com/cato-networks