Sécurité IT : Cisco révise sa gamme

Après le lancement mondial de SecureX en juin 2020, Cisco adapte son portefeuille de solutions logicielles de sécurité pour mieux répondre à l'évolution du marché.

Qu'en est-il dans la pratique ?

Cisco a mis en exergue les points suivants lors d'un récent Partner Summit Digital :

– Détection et réponse à incidents (XDR) :

La plateforme cloud SecureX, console de gestion centralisée pour les produits de sécurité du groupe américain et de fournisseurs tiers, fournit dorénavant des capacités étendues de détection et réponse (XDR ou eXtended Detection and Response) aux incidents. Et ce pour sécuriser endpoints, serveurs, charges de travail cloud et réseaux.

– Zero Trust en matière de sécurité réseau :

Duo, outil Cisco d'authentification multifacteur et de gestion d'accès aux applications d'entreprise, détecte désormais automatiquement les connexions suspectes en s'appuyant sur l'apprentissage machine (machine learning). L'alerte aux équipes de sécurité passe par une intégration (API) avec différentes plateformes, dont SecureX.

– Sécurité du réseau à la périphérie (SASE) :

L'architecture Cisco SASE (Secure Access Service Edge) connecte l'environnement réseau et informatique des clients à une sécurité cloud multifonction. L'intégration avec des outils comme Cisco SD-WAN, Secure VPN et, plus largement, SecureX est proposée.

Sécuriser le travail à distance

Parallèlement à ces initiatives, l'équipementier réseau dit avoir « réduit de moitié » le nombre de noms de produits présents dans son portefeuille de sécurité.

Cisco ambitionne ainsi d'aligner l'offre à sa stratégie SecureX et d'en simplifier l'intégration auprès de partenaires et de clients finaux. En outre, protéger et bénéficier de la bascule massive vers le travail distance sont des enjeux clés.

« Les nouvelles méthodes de travail obligent les organisations à faire évoluer leur approche de la cybersécurité », a déclaré Gee Rittenhouse, vice-président et directeur général de Cisco Security Business Group. Les utilisateurs « doivent pouvoir se connecter en toute sécurité, en tout lieu, à tout moment et sur n'importe quel appareil », a-t-il ajouté.