VMware annonce un pare-feu “service defined”

A l’occasion de la conférence RSA, VMware a présenté une nouvelle solution de sécurité. Il s’agit d’un pare-feu “service defined” qui se concentre sur le “bon comportement” d’une application au lieu de faire la chasse aux menaces.

Utilisant VMware NSX (visibilité réseau et applicatif) et AppDefense (surveille les workload par rapport à leur état prévu), le pare-feu modélise le comportement des applications et automatise la protection avec ce qu’il appelle la » sécurité intrinsèque « .

Le système s’appuie sur la plateforme de virtualisation de VMware pour valider le bon comportement des applications sans utiliser d’agents installés.

Disponible sur les plateformes de Cloud hybride

Selon Tom Gillis, vice-président et directeur général de la division réseaux et sécurité de VMware, il s’agit d’un “véritable pare-feu”. Il ajoute que “ce n’est pas un blocage de ports. Nous avons une inspection de la couche 7 de la connexion réseau. Nous avons l’inspection avancée de l’hôte lui-même. Et c’est couplé à la génération automatique des règles de pare-feu basées sur cette connaissance et la compréhension du comportement de l’application.”

Le pare-feu fonctionne avec des environnements d’applications en bare metal, machine virtuelle et conteneur.

Il sera ultérieurement compatible avec les plateformes de cloud hybride tels que VMware Cloud sur AWS (Amazon Web Services) et AWS Outposts.