SÃ©curitÃ© des rÃ©seaux cloud : 5 pratiques efficaces pour les organisations
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 17/5/2023 14:00:00

Les rÃ©seaux cloud gÃ©nÃ¨rent de la complexitÃ© et Ã©tendent Â« naturellement Â» la surface d'attaque d'une organisation, ce qui la rend plus vulnÃ©rable aux cyberattaques.

La complexitÃ© croissante va de pair avec la sophistication des cybercriminels dont les attaques et les violations de donnÃ©es sont plus frÃ©quentes, plus importantes et plus persistantes.

Assurer la protection de son organisation, de ses Ã©quipes, de ses donnÃ©es et de l'ensemble des actifs informatiques est devenue une tÃ¢che techniquement difficile mais tout Ã fait essentielle.

La bonne nouvelle est qu'il existe aujourd'hui des solutions Ã©prouvÃ©es qui, si elles sont dÃ©ployÃ©es de maniÃ¨re rigoureuse et appropriÃ©e, peuvent protÃ©ger les entreprises contre les menaces qui pÃ¨sent sur la sÃ©curitÃ© des rÃ©seaux dÃ©matÃ©rialisÃ©s.

Focus sur les 5 pratiques socle de sÃ©curitÃ© des rÃ©seaux cloud

Comprendre le modÃ¨le de responsabilitÃ© partagÃ©e - toute organisation qui migre sur le cloud doit apprÃ©hender le modÃ¨le de responsabilitÃ© partagÃ©e du ou des fournisseurs de plateforme avec lesquels elle s'associe.

Cela signifie qu'il faut dÃ©terminer exactement quelles sont les responsabilitÃ©s du fournisseur de la plateforme cloud, quelles sont celles de lâ□□entreprise et quelles sont Â« les zones grises Â» qui existent entre ces deux ensembles de responsabilitÃ©s.

S'assurer de tout voir - "on ne peut pas protÃ©ger ce que l'on ne voit pas". Cette expression est dâ□□autant plus vraie lorsqu'il s'agit de rÃ©seau cloud. Disposer d'une visibilitÃ© complÃ¨te sur les donnÃ©es au repos, en mouvement, les applications, les utilisateurs et les charges de travail est le fondement non nÃ©gociable de tout modÃ¨le de sÃ©curitÃ© de rÃ©seau dans le cloud.

CrÃ©er une posture de sÃ©curitÃ© uniforme - la crÃ©ation d'une posture de sÃ©curitÃ© uniforme, câ□□est-Ã -dire gÃ©rÃ©e par des outils communs, appliquÃ©e par des politiques communes et visibles via une console unique, reprÃ©sente une des pratiques exemplaires les plus importantes mais Ã©galement une des plus difficiles Ã mettre en Å□uvre.

La difficultÃ© rÃ©side dans les disparitÃ©s des besoins, des normes et des outils utilisÃ©s par les entreprises dâ□□un cÃ´tÃ© et les fournisseurs de services cloud de lâ□□autre.

Simplifier et rÃ©duire la palette d'outils de sÃ©curitÃ© - les fournisseurs de cloud proposent souvent des outils diffÃ©rents et rares sont ceux conÃ§us pour interopÃ©rer. Par consÃ©quent, les entreprises doivent utiliser plusieurs outils de sÃ©curitÃ© qui peuvent se chevaucher.

Cette situation est non seulement inefficace, mais elle peut aussi crÃ©er des angles morts et des vulnÃ©rabilitÃ©s dans l'ensemble du rÃ©seau. Pour sÃ©curiser et gÃ©rer le rÃ©seau cloud, la meilleure pratique consiste Ã utiliser le moins d'outils possible et Ã rechercher des outils qui fonctionnent sur plusieurs plates-formes cloud.

Combiner l'intelligence artificielle et l'intelligence humaine - bien que l'IA soit particuliÃ¨rement

adaptÃ©e Ã de nombreuses tÃ¢ches telles que l'ingestion et la recherche de modÃ¨les de menaces dans des quantitÃ©s massives de donnÃ©es, elle ne saurait remplacer l'intelligence et l'intuition humaine, les entreprises ont intÃ©rÃªt Ã associer l'homme et l'IA pour automatiser et optimiser le plus grand nombre de processus de sÃ©curitÃ©.