FICHE SOLUTION

Les 5 défis de sécurité des datacenters hyperscale et hybrides et les solutions proposées par Fortinet

Les entreprises tirent avantage de l'évolution des datacenters, mais sont confrontées à un certain nombre de défis en matière de sécurité lorsqu'elles migrent vers des architectures de datacenter hybrides et hyperscale. Heureusement, les solutions réseau orientées sécurité de Fortinet répondent à ces défis, via une sécurité et des performances adaptées aux besoins sans équivalent des architectures hybrides et hyperscale.

Voici les défis clés rencontrés, ainsi que les solutions qu'offre Fortinet et des liens vers les guides solution détaillés.

1. DÉFI : une visibilité restreinte

À mesure que les entreprises migrent des datacenters traditionnels vers une architecture hybride, l'infrastructure réseau et informatique s'étend, que ce soit sur site, dans les espaces mutualisés d'hébergement ou dans les clouds multiples. Cette tendance pèse sur la visibilité globale sur les segments de réseau. Dans le même temps, le trafic chiffré progresse et crée des zones d'ombre qui obèrent la visibilité sur le réseau. Une solution inadaptée ne fournira pas la visibilité adéquate sur tous les éléments de sécurité déployés dans différents environnements, ni de contrôle de bout en bout sur les utilisateurs, les applications et les appareils présents sur le réseau.

Les pare-feux réseau FortiGate de Fortinet éliminent ces zones d'ombre en détectant les applications non autorisées et les menaces furtives. FortiGate est une solution unifiée qui consolide toutes les fonctions de sécurité essentielles, du filtrage Web à la protection contre les menaces.

Pour en savoir plus : Fiche solution

2. DÉFI : une surface d'attaque en expansion

Nombre d'entreprises ne disposent pas des fonctions de sécurité interne qui permettraient de dissocier les ressources les unes des autres afin de maîtriser les menaces et empêcher leur propagation sur le périmètre interne d'un réseau. Pourtant, une segmentation du réseau empêche cette propagation tout en aidant les entreprises à mieux protéger les applications et à assurer leur conformité grâce au déploiement de plusieurs couches de sécurité.

Les solutions Fortinet protègent tout type de segmentation, y compris la segmentation au niveau du réseau, des ports et des applications. Cet objectif est tenu lorsque le trafic est orienté vers ou transite par un FortiGate. Cette sécurité se concrétise à l'aide de fonctions d'inspection évolutives, flexibles et performantes.

Pour en savoir plus : Présentation de la solution

3. DÉFI : protéger les vulnérabilités

Les systèmes de prévention des intrusions (IPS) doivent pouvoir sécuriser les datacenters hybrides et hyperscale. Les entreprises ont besoin d'un IPS intégré qui les aide à protéger leurs systèmes hérités, difficiles à patcher mais néanmoins essentiels à leur activité, contre les vulnérabilités connues et zero-day.

Les firewalls réseau Fortinet avec IPS permettent aux clients de préserver le design de leur réseau. Ces outils sont intégrés dans la Security Fabric de Fortinet, bénéficient d'une veille sur les menaces optimisée par intelligence artificielle et machine learning et proposée par les FortiGuard Labs, et offrent des services FortiSandbox sur site ou dans le cloud afin de prévenir les menaces inconnues. Ces pare-feux visent également l'excellence en matière de ratio performances/prix, tel que validé par des tiers comme NSS Labs.

Pour en savoir plus : Fiche solution

4. DÉFI : des performances hyperscale

L'avènement de l'hyperscale a donné lieu à des ensembles de données volumineux qui doivent être acheminés à très grande vitesse et bénéficier d'une sécurité performante. Comment gérer de très nombreuses connexions, sans sacrifier l'expérience de l'utilisateur ? La tâche s'annonce complexe. Si les équipes de réseau et de sécurité ne peuvent offrir le niveau d'expérience utilisateur qu'exigent les collaborateurs et les clients modernes, les conséquences peuvent s'avérer lourdes en termes de productivité et de réputation.

Les data centers hyperscale nécessitent une sécurité à grande échelle. Les pare-feux réseau Fortinet bénéficient des tout derniers processeurs de sécurité du constructeur, pour offrir une expérience utilisateur et applicative de tout premier rang et un score SCR (Security Compute Rating) de **12 x** sur le critère des connexions par seconde. Les pare-feux réseau Fortinet assurent un transfert de données **10 x** plus rapide et un chiffrement IPsec **11 x** plus performant. La fonction Virtual Extensible LAN (VXLAN) bénéficie d'une accélération matérielle et répond aux besoins de l'IT hybride, pour un provisioning ultra-rapide des services.

Pour en savoir plus : Fiche solution

5. DÉFI : une administration complexe

Alors que les datacenters s'étendent, leur gestion gagne en complexité, surtout lorsque plusieurs outils de gestion sont utilisés pour administrer des technologies et hubs de connectivité différents.

Fortinet Fabric Management Center (FMC) propose les plateformes FortiManager et FortiAnalyzer pour constituer un centre d'exploitation réseau qui gère efficacement l'architecture de sécurité intégrée, et ce, à partir d'une interface unique. FMC propose de multiples fonctionnalités pertinentes : gestion centralisée, reporting, traitement analytique et automatisation. Les équipes tirent également parti de FMC pour intégrer facilement des outils tiers tels que Ansible (automatisation), Terraform (automatisation), ServiceNow (ITSM), Splunk (SIEM), Tufin (NSPM), et de nombreux autres, au sein d'environnements hétérogènes à grande échelle.

Pour en savoir plus : Fiche solution

décembre 7, 2020 11:58 AM

760844-0-1-FR