Sécurité dynamique pour tous les scénarios de Cloud Computing

Les environnements Cloud mixtes, privé, public ainsi que les services SaaS apportent de nouvelles exigences en matière de sécurité. Un «Security Fabric», qui regroupe tous les aspects de la sécurité sous un même toit, est plus approprié que les solutions individuelles conventionnelles.

Le Security Fabric de Fortinet offre une sécurité complète pour les environnements dynamiques Multi-Cloud. Source: iLexx/iStock.com

L'informatique dans le Cloud est depuis longtemps la norme. Les études de marché d'IDC prévoient que les solutions de Cloud public et privé représenteront environ 50 % des dépenses mondiales en infrastructures informatiques en 2019. 85 % des personnes interrogées ont déclaré vouloir adopter une stratégie Multi-Cloud: Utiliser les services Cloud pour l'infrastructure (IaaS), les plates-formes de développement (PaaS), les applications logicielles (SaaS) et les ressources Cloud dans leurs propres datacenters.

Les solutions de sécurité traditionnelles atteignent leurs limites dans un environnement aussi segmenté et dynamique. La visibilité globale fait défaut, les différentes solutions communiquent mal entre elles, les réponses liées aux incidents de sécurité sont difficiles à corréler et le coût total de la sécurité est énorme.

Un environnement de sécurité pour le Cloud doit d'abord prendre en charge toutes les formes de Cloud (privé, public, hybride) et ensuite être capable de comprendre la nature élastique et très versatile du Cloud. Trois aspects jouent ici un rôle important:

- Évolutivité: La solution de sécurité doit être conçue à partir de zéro pour les charges de travail dynamiques dans le Cloud. Les solutions statiques et non automatisées empêchent de profiter pleinement des avantages du Cloud.
- Cohérence: Les cybercriminels exploitent toutes les vulnérabilités – par exemple des stratégies déployées de manière incohérente. Le Cloud augmente de façon exponentielle de telles possibilités. Les stratégies de sécurité et leur application automatisée doivent être appliquées de manière cohérente sur l'ensemble des ressources statiques et dynamiquement intégrées.
- Segmentation: Pour répondre aux exigences réglementaires et minimiser les risques, les systèmes, les charges de travail et même certains composants du réseau doivent être segmentables en fonction de leur profil de risque. Cela permet de surveiller le flux de données entre les segments et d'éviter la perte de données.

Security Fabric au lieu de solutions isolées

Le Security Fabric de Fortinet répond à ces exigences. Les solutions de sécurité Fortinet couvrent les vecteurs d'attaque les plus divers - dans tous les environnements (de l'IoT au Cloud) - et permettent la détection et la défense complète des cyber-menaces. Les pare-feu FortiGate peuvent être intégrés via des connecteurs avec tous les fournisseurs de Cloud public et les environnements de Cloud privé, de sorte que les informations sur les objets «dynamiques», les modèles de sécurité ou les renseignements sur les menaces ne sont capturés qu'une seule fois et ensuite partagés dans l'ensemble de l'environnement. Les plates-formes telles que AWS, Azure, Oracle et Google, ainsi que les solutions SDN telles que VMware NSX, Cisco ACI, Open Stack et Nuage Networks sont supportées. Les produits sont également disponibles pour tous les hyperviseurs courants. Fortinet maintient et partage l'information dans le cadre de son programme Fabric Ready avec divers partenaires technologiques et qu'industriels. Fortinet soutient également des organismes gouvernementaux tels qu'Interpol ou le Groupe de travail de l'OTAN sur la cybercriminalité.

Les produits Security Fabric offrent une interface de programmation (API) complète, particulièrement utile pour l'automatisation. L'API permet par exemple d'effectuer une quarantaine automatique basée sur les événements du journal. Une gestion et des rapports centralisés assurent une visibilité en temps réel sur l'ensemble de l'environnement Multi-Cloud. Toutes les solutions peuvent être gérées via une interface web moderne et uniforme - contrairement à d'autres fournisseurs, aucun client lourd supplémentaire n'a besoin d'être installé sur les postes de travail des administrateurs.

Le dynamisme d'un environnement Cloud est renforcé par le fait que les solutions Fortinet sont disponibles sous forme d'appliances virtuelles. Les pare-feu peuvent par exemple être ajoutés dynamiquement au fur et à mesure que la charge de travail augmente, et les environnements de développement peuvent être réduits après le démarrage de la production.

Fortinet Cloud Security: les points forts

- Une sécurité complète pour les environnements Multi-Cloud dynamiques.
- Intégration avec tous les principaux fournisseurs de Cloud public, les plates-formes SDN et les hyperviseurs.
- Intégration sécurisée des services SaaS tels que Office 365 et Salesforce ou des solutions de stockage dans le Cloud via le service Cloud Access Security Broker (CASB).
- API complètes pour une automatisation étendue.
- Solutions disponibles sous forme d'appliances virtuelles dynamiquement évolutives.
- De solides partenariats technologiques et industriels via le programme Fabric Ready.

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch | www.boll.ch