PRÉSENTATION DE LA SOLUTION

Une sécurité cloud dynamique pour les environnements AWS

Résumé

Amazon Web Services (AWS) est le plus grand fournisseur de services de cloud computing du monde. Pionnier de l'IaaS (Infrastructure-as-a-Service), AWS améliore rapidement sa plateforme PaaS (Platform-as-a-Service), permettant aux utilisateurs d'accélérer le développement logiciel et de simplifier les opérations. Même si AWS propose des fonctionnalités de sécurité, les entreprises clientes qui utilisent à la fois des environnements locaux et cloud doivent pouvoir mettre en œuvre des politiques de sécurité cohérentes sur l'ensemble de leurs sites. Fortinet Security Fabric s'intègre nativement à AWS afin d'offrir une visibilité et un contrôle complets des applications, une gestion centralisée ainsi que l'automatisation des dispositifs de sécurité dans les environnements hybrides.

74 % des entreprises transfèrent des applications entre le cloud et leurs locaux, ce qui crée un besoin crucial de sécurité cohérente entre les différents sites.[1]

L'uniformisation des dispositifs de sécurité dans les data centers et le cloud

Comme les fournisseurs de services cloud offrent un nombre croissant de services de sécurité, on suppose souvent que les plateformes cloud comme AWS sont sûres et que tout ce qui est exécuté dans ces environnements est automatiquement sécurisé. Mais la sécurité du cloud est assurée par un modèle de responsabilité partagée. Ainsi, AWS est uniquement responsable de la protection de l'infrastructure cloud qui gère les services proposés : la sécurité du cloud. Dès lors, les clients sont responsables de tous les services, applications et données qu'ils utilisent : la sécurité dans le cloud.

En effet, la grande majorité des défaillances de sécurité dans le cloud finit par être imputable au client. Ces problèmes sont généralement causés par un manque de compréhension du modèle de responsabilité partagée et de la façon dont les détails de ce modèle varient d'un cloud à l'autre.

Des défenses intégrées couvrant tout le spectre des attaques

Les différentes solutions qui composent Fortinet Security Fabric pour AWS ont été conçues pour accroître la confiance des utilisateurs finaux dans les environnements cloud AWS. Toutes ces solutions reposent sur des formats de machine virtuelle (VM), des formats de conteneur et des offres SaaS (Software-as-a-Service) Fortinet. Elles sont également disponibles via des options d'achat flexibles :

- **Le modèle BYOL.** Les licences acquises auprès d'un partenaire revendeur Fortinet pour différents produits sont transférables d'une plateforme à l'autre. Par exemple, une licence VM pour FortiGate-VM sur VMware fonctionne aussi sur la plateforme FortiGate pour AWS grâce à l'utilisation du modèle BYOL.
- **Le modèle PAYG.** Il est possible de consommer un grand nombre de solutions Fortinet à l'usage (Pay-As-You-Go ou PAYG) directement depuis AWS Marketplace.

Les produits Fortinet suivants sont inclus dans Fortinet Security Fabric pour AWS :

- **FortiGate.** Les pare-feux NGFW de Fortinet proposent l'un des ensembles de fonctionnalités de protection contre les menaces les plus performants du secteur pour lutter contre les cyberattaques connues et inconnues les plus avancées. FortiGate-VM s'adapte en fonction des exigences du client et se décline en plusieurs tailles pour s'adapter à une variété de cas d'usage pris en charge. FortiGate est disponible via les modèles de licence PAYG et BYOL.
- **FortiWeb.** Les solutions WAF (Web Application Firewall) de Fortinet protègent les applications Web hébergées contre les attaques qui ciblent les failles connues et inconnues. À l'aide de méthodes de détection multicouches et corrélées, FortiWeb défend les applications contre les vulnérabilités connues et les menaces de type « zero-day ». FortiWeb est disponible via les modèles de licence PAYG et BYOL VM ou SaaS et conteneur BYOL ECS.
- **FortiMail.** Les passerelles de messagerie sécurisées (SEG) de Fortinet font appel aux veilles sur les menaces les plus récentes mises au point par FortiGuard Labs. Ces passerelles offrent une protection de haut niveau constante contre les menaces courantes et avancées tout en intégrant de puissantes fonctionnalités permettant d'éviter la perte de données. FortiMail est disponible via les modèles de licence BYOL VM.
- **FortiSandbox.** Les solutions Sandbox de Fortinet offrent une puissante combinaison de détection avancée, de réduction des risques automatisée, d'informations exploitables et de flexibilité de déploiement pour arrêter les attaques ciblées et la perte de données qui en découle. FortiSandbox est disponible via les modèles de licence BYOL et PAYG VM.

- **FortiManager.** Fortinet propose une interface de gestion unique et des contrôles de politiques appliqués à toute l'entreprise pour offrir un aperçu des menaces et du trafic à l'échelle du réseau. Cette solution comprend des fonctionnalités de lutte contre les attaques avancées, ainsi qu'une évolutivité permettant de gérer jusqu'à 10 000 appareils Fortinet. FortiManager est disponible via le modèle de licence BYOL VM.
- **FortiAnalyzer.** Cette solution collecte, analyse et corrèle les données des produits Fortinet afin de garantir une visibilité accrue et de solides informations sur les alertes de sécurité. Associée à un abonnement au service Indicator of Compromise (IOC) de FortiGuard, cette solution propose également une liste hiérarchisée des hôtes compromis pour permettre une intervention rapide. FortiAnalyzer est disponible via les modèles de licence BYOL et PAYG VM.
- **FortiCWP.** Le service de protection des charges de travail dans le cloud de Fortinet comprend des fonctionnalités CSPM (Cloud Security Posture Management) assurant la visibilité, la conformité, la sécurité des données et la protection contre les menaces. FortiCWP fournit des rapports de conformité et d'évaluation des configurations relatifs à des déploiements cloud AWS mondiaux. Il complète les fonctionnalités en ligne des appliances FortiGate-VM, avec une protection au niveau de l'API pour le cloud public. FortiCWP est disponible via le modèle de licence BYOL.
- **Les Fabric Connectors.** Ces connecteurs permettent l'intégration ouverte de Fortinet Security Fabric de façon à automatiser l'insertion des fonctions de pare-feu et de sécurité réseau dans le cloud AWS incluant plusieurs composants existants au sein de l'écosystème d'un client, ainsi que l'intégration aux services de renseignement de sécurité d'AWS.

Fortinet Security Fabric renforce la sécurité d'AWS

Fortinet Security Fabric protège les charges de travail des entreprises dans les data centers locaux comme dans les environnements cloud, offrant une sécurité multicouche cohérente pour les applications locales et cloud. Plus précisément, Security Fabric offre une protection multicouche approfondie et des avantages opérationnels en matière de sécurisation des applications contre les menaces connues et inconnues à l'intérieur comme à l'extérieur d'AWS, et sur le plan de la gestion des infrastructures de sécurité mondiales à partir d'AWS. Cette solution présente les fonctionnalités clés suivantes :

Le contrôle et la gestion via une interface unique. La Security Fabric permet de gérer de façon centralisée les fonctionnalités de sécurité cloud et sur site à partir d'AWS, ce qui contribue à éviter les erreurs humaines tout en réduisant la charge de travail des services informatiques limités en ressources. La Security Fabric offre une gestion cohérente de la sécurité basée sur un modèle opérationnel cohérent.

Une visibilité et un contrôle directement dans le cloud. Les entreprises gagnent en visibilité sur leurs déploiements d'applications AWS. Elles n'ont plus besoin de planifier des configurations de déploiement spécifiques, mais peuvent désormais appliquer des politiques davantage orientées sur l'intention. Grâce à l'utilisation de groupes d'adresses dynamiques, à l'attribution de noms logiques aux ressources cloud et aux flux d'informations sur les menaces AWS Guard Duty, il est possible de mettre en œuvre des politiques de sécurité en fonction de la montée en puissance des ressources Security Fabric dans toute l'infrastructure cloud.

Une protection étendue sur l'ensemble de la surface d'attaque. Fortinet offre la gamme de produits de sécurité réseau pour AWS la plus vaste du secteur, permettant aux entreprises d'exécuter n'importe quelle application n'importe où, que ce soit sur site ou dans le cloud. La sécurité de Fortinet offre des performances identiques et reste la mieux adaptée pour répondre aux exigences et aux contraintes opérationnelles des environnements AWS.

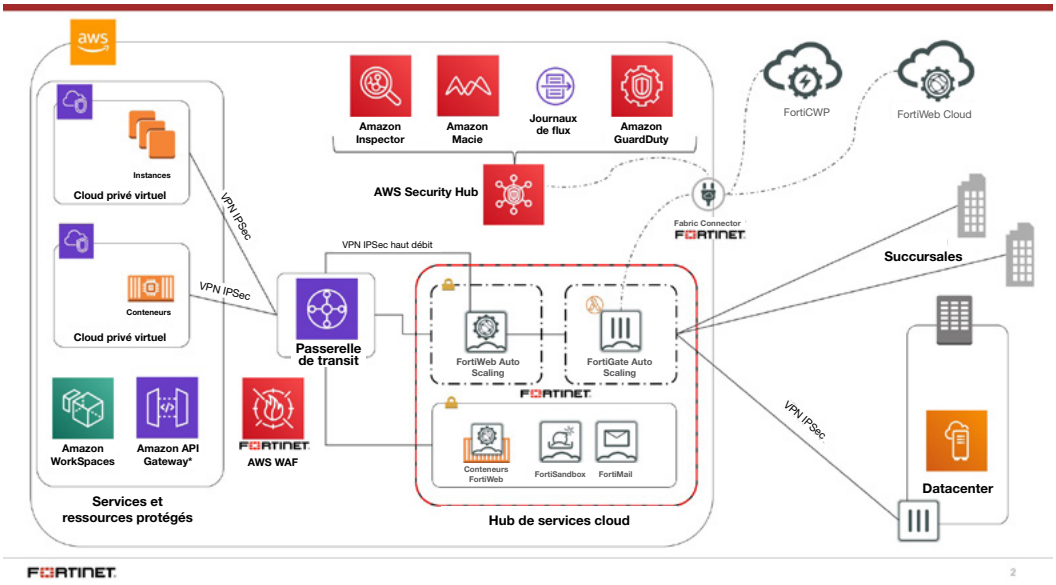

Schéma 1. La solution de sécurité cloud dynamique de Fortinet pour les environnements AWS

Une protection contre les attaques de type « zero-day ». Les solutions Security Fabric intégrées utilisent les veilles sur les menaces les plus récentes à l'échelle mondiale (des chercheurs de FortiGuard Labs) et partagent les informations en temps réel avec toute l'entreprise. Elles bénéficient ainsi d'une protection hautement évolutive, entièrement intégrée à AWS, pour contrer les attaques de type « zero-day ». De plus, l'entreprise réduit ainsi considérablement son exposition aux menaces persistantes avancées et se sent plus en confiance pour déployer des applications à n'importe quelle échelle dans le cloud.

La mise en conformité. Les solutions Fortinet offrent une protection incomparable destinée à garantir la mise en conformité des entreprises avec les normes du secteur en vigueur telles que la norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS) et la loi américaine sur l'assurance maladie (Health Insurance Portability and Accountability Act ou HIPAA), ainsi que la législation récente sur la confidentialité des données, notamment le règlement général sur la protection des données (le RGPD) de l'Union européenne.

La sécurisation d'une variété d'environnements cloud publics AWS

La solution de sécurité cloud dynamique de Fortinet étend Fortinet Security Fabric à AWS, offrant une sécurité d'entreprise cohérente et inégalée aux environnements cloud AWS. Fortinet Security Fabric prend en charge les environnements cloud publics suivants :

1. **La sécurité réseau.** En exploitant l'ampleur et la flexibilité de l'infrastructure AWS, les entreprises peuvent mettre en place des solutions de sécurité réseau aisées et efficaces. Un hub de services de sécurité cloud de Fortinet tire parti de la construction d'un cloud privé virtuel (VPC) AWS pour mettre en œuvre des fonctionnalités de sécurité multicouches évolutives dans un seul cloud privé virtuel par région. En même temps, il permet au reste des départements métiers de l'entreprise de fonctionner de façon autonome en utilisant leurs propres clouds privés virtuels. Ces derniers n'ont qu'à connecter leurs clouds privés virtuels au cloud privé virtuel du hub de services cloud en utilisant une passerelle de transit (ou une autre forme d'échange de trafic entre clouds privés virtuels).

   Un pare-feu de nouvelle génération (NGFW) FortiGate-VM est au cœur d'une solution de hub de services de sécurité cloud. Les performances réseau uniques, l'intégration au cloud et l'évolutivité de FortiGate-VM permettent aux équipes de sécurité de maintenir une protection et une visibilité cohérentes, tout en assurant la productivité dans l'ensemble des entreprises. La solution de hub de services de sécurité cloud de Fortinet répond à des besoins spécifiques, dont :

   - **Le SD-WAN.** En connectant plusieurs succursales au hub, les entreprises bénéficient des avantages de la fonctionnalité FortiGate Secure SD-WAN avec une qualité d'expérience (QoE), une visibilité et une sécurité accrues du réseau des succursales pour les applications exécutées dans AWS.
   - **Le cloud hybride.** Lorsqu'une connectivité à haut débit est nécessaire, le hub peut fournir une connectivité sécurisée entre les sites, ce qui en fait une solution cloud hybride idéale en raison des modèles d'utilisation opposés des utilisateurs et des sauvegardes ou des machines.
   - **Une segmentation entre clouds privés virtuels.** La nature centralisée du hub permet de définir des politiques de sécurité pour le trafic entre différents départements métier et les applications.
   - **Un accès à distance.** Le hub est également idéal pour mettre fin à toute connexion d'accès à distance aux applications et à l'infrastructure de l'entreprise, chaque fois qu'une connectivité VPN est nécessaire.

2. **La sécurité du Web et des applications.** Un pourcentage croissant d'applications métier modernes est déployé sur des infrastructures de cloud public en général, et AWS en particulier. Parallèlement à cela, les applications Web sont responsables d'un grand nombre de failles de sécurité. Plus de la moitié (52%) de toutes les failles impliquent le piratage d'applications Web, qui est de loin le vecteur le plus courant de failles basées sur le piratage.[2]

   La solution de sécurité cloud dynamique de Fortinet pour les environnements AWS, protège les applications essentielles contre les menaces connues et inconnues, y compris les menaces de type « zero-day », les botnets et les attaques API. Fortinet atténue les risques liés à la vulnérabilité des serveurs et assure la conformité aux lois, règlementations et normes les plus récentes. Les solutions de sécurité Web de Fortinet comprennent de multiples options pour les environnements AWS :

   - **FortiWeb WAF-as-a-Service.** Une mise en œuvre SaaS de la solution FortiWeb WAF, qui protège les charges de travail dans une même région AWS contre les attaques sophistiquées.
   - **FortiWeb ECS.** Inclus dans le service ECS (Elastic Container Service) disponible sur AWS Marketplace, FortiWeb répond aux besoins des clients en matière de fonctionnalités WAF mises en conteneur pour protéger les applications individuelles.
   - **FortiWeb VM.** Également disponible sur AWS Marketplace en tant qu'AMI (Amazon Machine Image), FortiWeb permet d'assurer la protection personnalisée de plusieurs applications.
   - **Les règles WAF Fortinet pour AWS WAF.** Une mise en œuvre simple de la sécurité Web utilisant une protection basée sur la correspondance d'expressions régulières statiques.

3. **La protection des charges dans le cloud (CWP).** Une mauvaise configuration contribue directement aux risques au sein des infrastructures cloud. L'année dernière, plus de la moitié des failles ont été causées par des erreurs humaines ou des problèmes système (au lieu d'attaques malveillantes ou criminelles).[3] Plus les incidents liés à la sécurité sont attribués à des erreurs de configuration, plus il est nécessaire de s'attaquer à ce type de menaces.

Le service Fortinet FortiCWP interagit avec la plateforme pour aider à maintenir l'hygiène de la plateforme ainsi que pour surveiller les activités dans AWS. FortiCWP s'intègre parfaitement aux différents services AWS, tels que Security Hub, GuardDuty, Inspector et VPC Flow Logs. Ses fonctionnalités spécifiques sont les suivantes :

- **L'évaluation de la configuration** de l'environnement AWS du client et la comparaison systématique avec les meilleures pratiques
- **La surveillance de l'activité des comptes cloud** afin d'atténuer les risques d'accès non autorisé ou non supervisé
- **La surveillance du trafic dans le cloud** pour tout trafic sur tout réseau cloud associé au compte AWS
- **L'analyse de la sécurité des données dans le cloud** via les compartiments AWS S3 pour les données sensibles et malveillantes

Une protection multicouche limitant les risques

Fortinet Security Fabric offre aux utilisateurs AWS des fonctionnalités de prévention des menaces et de sécurité multicouche complètes et entièrement programmables. Grâce à la sécurité cloud de Fortinet pour AWS, les entreprises disposent d'une solution de sécurité cohérente basée sur un modèle de responsabilité partagée, sur site et dans le cloud.

Dans le même temps, Fortinet permet de simplifier les opérations, la gestion des politiques et la visibilité afin d'améliorer la gestion du cycle de sécurité, avec des fonctionnalités entièrement automatisées. Avec Fortinet Security Fabric, les RSSI et autres responsables sécurité peuvent s'assurer que l'architecture de sécurité de leur entreprise couvre la totalité de la surface d'attaque.

[1] Daniel Hein, « 74% of Companies Move Apps To the Cloud, Then Back On-Premise », Solutions Review, 16 août 2019.

[2] « 2019 Data Breach Investigations Report », Verizon, avril 2019.

[3] « 2018 Cost of a Data Breach Study », Ponemon Institute et IBM Security, juillet 2018.

13 mai, 2020 3:21 PM

549977-0-1-FR

sb-Dynamic-Cloud-Security-AWS-A4_FR