FICHE SOLUTION

FortiCloud : la sécurité de vos applications et infrastructures cloud

Synthèse

Une sécurité adéquate des infrastructures et des applications cloud nécessite une solution spécialement conçue pour le cloud et pouvant être fournie, en tant que service, à partir du cloud. La suite FortiCloud protège vos applications, vos instances, vos données et vos e-mails sans investissement initial, ni matériel à déployer. FortiCloud s'impose auprès des entreprises qui requièrent l'agilité et la flexibilité du cloud computing, mais sans sacrifier la sécurité.

Parce que le cloud computing utilise une multitude de nouveaux systèmes de gestion, d'orchestration et d'analyse et parce que les applications et les utilisateurs n'évoluent pas sur un réseau sécurisé, le cloud computing contribue à élargir la surface d'attaque.

Les défis de sécurité des applications cloud-natives

De nombreuses entreprises migrent leurs ressources informatiques vers le cloud pour alléger leurs investissements, gagner en agilité et tirer parti de services sophistiqués, tels que les moteurs d'intelligence artificielle (IA) et les outils avancés de traitement analytique. Des entreprises de toutes tailles constatent que le cloud leur apporte des applications sophistiquées sans devoir mettre sur pied leurs propres data centers et en assurer la maintenance.

Le cloud computing peut être sécurisé au même titre que les infrastructures sur site, mais ce cloud introduit un certain nombre de nouveaux défis en matière de sécurité : extension de la surface d'attaque, nécessité de sécuriser de multiples applications résidant dans plusieurs clouds et/ou data centers, ou encore une pénurie générale de professionnels qualifiés en sécurité du cloud.

La surface d'attaque regroupe l'ensemble des vecteurs d'attaque potentiellement utilisés par un assaillant pour pénétrer dans un système informatique, le modifier ou le perturber. Parce que le cloud computing utilise de nouveaux systèmes de gestion, d'orchestration et d'analyse, et puisque les applications et leurs utilisateurs n'évoluent pas au sein d'un réseau sécurisé, le cloud computing contribue à étendre la surface d'attaque. De plus, les applications cloud natives, pilotées par une interface API, peuvent être gérées par programmation, créant ainsi un autre vecteur d'attaque. Parallèlement, la prévalence des méthodologies DevOps dans le développement d'applications cloud signifie que les équipes de développement ayant des privilèges élevés sortent de nouvelles applications ou mises à jour, souvent sans qu'elles ne soient validées par une équipe de professionnels de la sécurité.

Pour faire face aux nouvelles vulnérabilités introduites par l'adoption du cloud, de nombreuses entreprises ont déployé un parc hétérogène de produits de sécurité. Plus de 75 outils de sécurité différents sont utilisés, en moyenne, dans une entreprise, et nombre d'entre eux sont ciblés : chaque outil ne répond qu'à un seul risque de sécurité ou exigence de conformité. Au-delà des investissements récurrents liés à l'achat de nouveaux produits ciblés, ces derniers ne communiquent généralement pas entre eux, ce qui alourdit les charges de gestion et donne lieu à de nouvelles failles de sécurité permettant aux menaces de percer la ligne de défense en place. Les entreprises doivent adopter une approche cohérente pour gérer l'infrastructure et les applications cloud, une approche qui allège la charge de travail des équipes de sécurité, assure un retour sur investissement satisfaisant et permet aux entreprises de pérenniser leur conformité, leur sécurité et leur résilience.

Sécuriser les applications cloud-natives avec Fortinet

Les solutions de sécurité traditionnelles sont conçues pour établir un périmètre sécurisé autour de votre réseau. Mais à l'ère du cloud, cette approche est caduque : le « périmètre » est partout. La sécurisation des applications cloud-natives nécessite ainsi des solutions à la fois conçues pour le cloud et pouvant être fournies à partir du cloud. La sécurité cloud vise plusieurs objectifs, parmi lesquels :

- Protection des applications
- Protection des instances et du stockage
- Protection des e-mails
- Sécurisation des applications SaaS (Microsoft 365, Salesforce…)
- Configuration et gestion de la conformité
- Sandboxing
- Protection avancée contre les menaces grâce à des informations temps-réel sur les menaces adossées au machine learning et à l'intelligence artificielle
- Gestion et traitement analytique centralisés

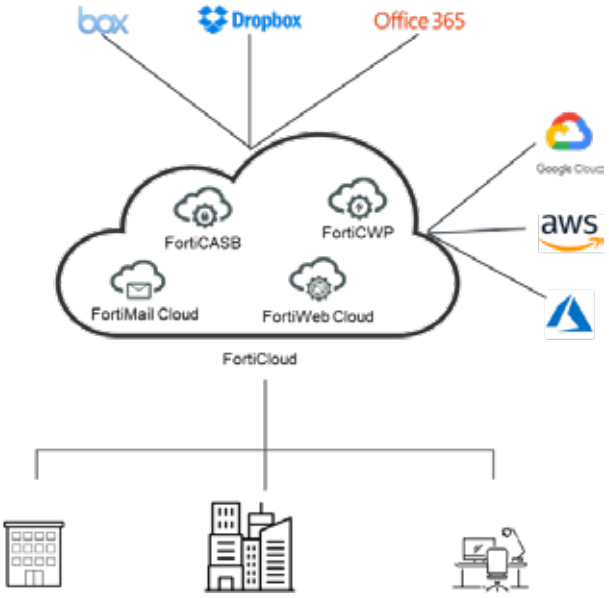

Schéma 1 : sécuriser les applications cloud-native avec Fortinet.

Contrairement aux approches concurrentes, FortiCloud apporte toutes les facettes d'une sécurité efficace et évolutive des applications cloud-natives. FortiCloud propose les outils qui assurent une sécurité sous forme de sécurité en tant que service (Security-as-a-service) comme FortiWeb Cloud et FortiCASB, des plateformes qui gèrent d'autres outils de sécurité comme FortiGate Cloud et FortiManager, ainsi que des outils de tracking des ressources, des licences et des autorisations de retour de matériel (RMA) comme FortiCare.

Solution complète, FortiCloud est un pilier de la Security Fabric, qui interconnecte les solutions de sécurité de Fortinet afin de détecter, analyser et répondre aux comportements malveillants, où qu'ils se produisent.

La sécurité cloud n'est certainement qu'une partie de la thématique plus vaste que constitue la cybersécurité, mais son importance ne doit pas être minimisée. Les composants clés de la suite FortiCloud pour la sécurité cloud incluent les éléments suivants.

FortiWeb Cloud

Conçu pour les applications Web qui exigent le niveau de protection le plus élevé, FortiWeb Cloud fournit une sécurité robuste, simple à déployer, facile à gérer et économique. Avec FortiWeb Cloud, les équipes DevOps et les architectes sécurité ont accès aux mêmes techniques de détection éprouvées des autres versions de FortiWeb, mais sans investissement initial lourd. Contrairement aux solutions qui se contentent de proposer des machines virtuelles pour chaque client et d'alourdir les charges de gestion d'équipes déjà sollicitées, FortiWeb Cloud propose une véritable solution Software-as-a-Service (SaaS) qui tire parti des principaux clouds publics pour offrir une sécurité des applications évolutive et à faible latence.

La Security Fabric de Fortinet couvre :

- La sécurité des terminaux clients
- La sécurité des accès filaires, sans fil et par VPN
- La sécurité réseau
- La sécurité des data centers (physiques et virtuels)
- La sécurité des applications (standards ou personnalisées)
- La sécurité cloud
- La sécurité des contenus (e-mails et Web)
- La sécurité des infrastructures (commutation et routage)

Au cœur de FortiWeb se trouve un moteur de détection basé sur l'IA, qui utilise le machine learning pour identifier tout comportement s'écartant de schémas normaux et prendre les mesures qui protègent les applications contre les menaces zero-day connues et inconnues. FortiWeb s'intègre avec FortiSandbox, qui utilise l'IA pour détecter des menaces nouvelles ou inconnues. Le framework MITRE ATT&CK, le top 10 OWASP et les informations en temps réel sur les menaces de FortiGuard Labs sont également pris en compte.

FortiWeb protège les applications Web et les API qu'elles utilisent. Cette application SaaS, fournie depuis le cloud, est tarifiée à l'utilisation et n'exige aucun déploiement de matériel.

FortiCWP

FortiCWP offre aux administrateurs de la sécurité et aux équipes DevOps la possibilité d'évaluer la posture de sécurité de leur configuration cloud, de détecter les menaces potentielles provenant d'erreurs de configuration des ressources cloud, d'analyser le trafic entre les ressources du cloud (dans et hors du cloud), et d'évaluer la configuration du cloud par rapport aux meilleures pratiques. Cette solution maîtrise les risques au sein des infrastructures multi-clouds, fournit des rapports de conformité réglementaire et intègre les mesures correctives dans le framework d'automatisation du cycle de vie des infrastructures multi-clouds.

FortiCASB

FortiCASB est un service cloud-native CASB (Cloud Access Security Broker) proposé sous forme d'abonnement et proposant des fonctionnnalités CSPM (cloud security posture management). Ces dernières fournissent visibilité, conformité et sécurité des données, ainsi qu'une protection contre les menaces pour les services cloud utilisés par une entreprise. FortiCASB fournit des informations stratégiques sur les utilisateurs, les comportements et les données stockées dans les principales applications SaaS, ainsi que des outils de reporting complets. FortiCASB s'intègre via API avec les principaux services SaaS et de cloud computing, notamment Microsoft Office 365, Microsoft OneDrive, Google Drive, Salesforce.com, Dropbox et Box. La solution offre également un reporting sur la conformité et la détection du Shadow IT.

FortiCASB s'intègre via API avec les principaux services SaaS et de cloud, notamment Microsoft Office 365, OneDrive, Google Drive, Salesforce.com, Dropbox et Box. La solution assure également un reporting de conformité et permet de détecter le Shadow IT.

FortiMail Cloud

FortiMail Cloud offre une sécurité complète des e-mails pour protéger vos collaborateurs et vos données contre les cyberattaques. Cette sécurité a été validée et reconnue par de nombreux tiers indépendants du secteur.[1] Proposé dans un format SaaS, FortiMail Cloud est facile à activer et ne nécessite qu'une gestion continue minimale pouvant, pour l'essentiel, être déléguée aux utilisateurs finaux. FortiMail offre un taux de détection du spam supérieur à 99,5 %, de multiples couches de détection des logiciels malveillants et un taux de faux-positifs extrêmement bas. Totalement géré par Fortinet, FortiMail Cloud vous permet de vous recentrer sur votre activité tout en déléguant à Fortinet la sécurité de vos e-mails.

FortiSandbox

FortiSandbox, optimisé par des techniques d'intelligence artificielle, fait partie de la solution Fortinet de protection contre les intrusions et s'intègre à la plateforme Security Fabric pour répondre aux menaces en évolution rapide (rançongiciels et crypto-malware) qui ciblent une surface d'attaque digitale en expansion. La solution fournit une veille temps-réel et décisionnelle sur les menaces, grâce à une détection et une réponse automatisées aux malware sophistiqués et zero-day. FortiSandbox renforce l'efficacité et les performances de la détection des menaces « zero-day » en tirant parti de deux modèles de Machine Learning : un algorithme de type forêts d'arbres décisionnels en instance de brevet et une optimisation par la méthode des moindres carrés appliquée à l'analyse statique et dynamique des objets suspects. La solution améliore aussi l'étude des menaces et les processus de gestion en adhérant à des normes basées sur le framework MITRE ATT&CK en matière de reporting sur les malware.

Étapes suivantes

FortiCloud est la solution idéale pour les entreprises qui ont besoin de l'agilité et de la flexibilité du cloud computing sans sacrifier la sécurité. En fournissant une sécurité en tant que service (« Security-as-a-service »), la gestion des autres outils de sécurité et le suivi des licences et autres ressources, FortiCloud se veut une solution de sécurité complète des applications cloud natives, notamment lorsqu'elle est proposée dans le cadre de la Security Fabric.

[1] « Email Security Services Protection », SE Labs, janvier-mars 2020.

FORTINET

www.fortinet.fr

décembre 7, 2020 11:27 AM

697050-0-1-FR