SÉCURISATION D'APPLICATIONS WEB DANS DES ENVIRONNEMENTS BASÉS SUR DES CONTENEURS

RÉSUMÉ

Lorsque les entreprises manquent de fonctionnalités de sécurité dynamiques capables de s'adapter à la nature en constante évolution des environnements DevOps, elles s'exposent aux risques émanant de logiciels malveillants avancés et autres formes d'attaque sophistiquées. Cette vulnérabilité s'applique aux outils de mise en conteneur qui permettent aux applications d'être packagées et déplacées d'un environnement de développement à un autre. Les firewalls pour applications Web traditionnels ne sont pas en mesure d'offrir une protection adéquate dans ces conditions. Cependant, la solution FortiWeb Web Application Firewall Container Edition est conçue pour protéger les applications Web et les données exposées à Internet contre les menaces provenant des environnements basés sur des conteneurs.

DEVOPS, DOCKER ET NOUVELLES PRÉOCCUPATIONS

- **25% des entreprises** ont adopté la plate-forme de mise en conteneur Docker pour DevOps.[1]
- **81% des RSSI** s'inquiètent des risques liés à DevOps qui favorisent l'infiltration de vulnérabilités avec l'accélération du rythme de développement.[2]

REPENSER LE DÉVELOPPEMENT ET LA MISE À DISPOSITION DES APPLICATIONS

Le développement traditionnel de logiciels combine une série de fonctions et de services (par ex., bases de données, serveurs Web et code d'application) en un package unique et intégré. Cependant, sur le marché numérique actuel, réactif et axé sur le consommateur, cette approche monolithique du développement ainsi que du déploiement peut sérieusement ralentir la capacité d'une entreprise à réagir aux demandes du secteur et du marché.

Face à ce défi, les architectes logiciels des business units utilisent de nouvelles architectures de microservices et des environnements basés sur des conteneurs afin d'accélérer le développement et le déploiement des applications. Contrairement aux approches traditionnelles hautement intégrées du développement d'architecture logicielle et réseau, ces méthodes plus agiles conçoivent chaque composant et chaque fonction de manière autonome, indépendamment des autres fonctionnalités. En général, elles tirent parti des normes de communication ouvertes ou des systèmes d'orchestration pour assurer l'interopérabilité entre les composants. Cette méthodologie itérative et progressive permet aux entreprises de développer, de livrer et de personnaliser plus rapidement leurs applications, logiciels et infrastructures. Cette possibilité leur permet de réagir plus promptement aux demandes en constante évolution des environnements numériques modernes.

DES PROCESSUS PLUS RAPIDES APPORTENT DE NOUVEAUX CHALLENGES DE SÉCURITÉ

La vitesse et l'agilité sont des facteurs importants, mais pas au détriment de la sécurité. Lors de l'élaboration d'une méthodologie des opérations de développement plus rapide et plus efficace (DevOps), il est facile de ne pas s'apercevoir qu'une porte arrière est restée ouverte ou qu'une faille de sécurité a été accidentellement créée en cours de route. Les vérifications du code et les tests d'acceptation par l'utilisateur (UAT, User Acceptance Testing) permettent d'identifier des problèmes évidents. Il est toutefois quasiment impossible de résoudre tous les types possibles de vulnérabilités via un code personnalisé.

Même en mettant en place un firewall pour application Web (WAF) traditionnel, les problèmes ne disparaissent pas. Les protocoles et les opérations DevOps changent constamment, rendant obsolète la configuration du pare-feu WAF, qui doit alors être effectuée manuellement. Ces processus manuels créent des surcharges supplémentaires au niveau de la sécurité et des risques d'erreurs. Quand bien même résoudre tous les problèmes et reconfigurer manuellement chaque paramètre de sécurité était possible, le temps consacré à ces tâches augmenterait les coûts et les processus seraient nettement ralentis.

UN CONDITIONNEMENT À DES FINS DE PORTABILITÉ ET D'ÉVOLUTIVITÉ

Les outils de mise en conteneur (tels que Docker) permettent de conditionner une application entière de façon à la déplacer en toute transparence d'un environnement à l'autre. Cela peut être fait depuis un ordinateur portable de développeur vers un environnement de test, d'un environnement intermédiaire à un environnement de production, voire d'une machine physique déployée dans un data center vers une machine virtuelle. Cette machine virtuelle étant située dans un cloud privé ou public. Les processus de déploiement, de gestion, de mise à jour et d'interopérabilité s'en trouvent considérablement simplifiés.

Dans le cadre de la mise en conteneur, tous les éléments de l'application (y compris les bases de données, les bibliothèques de codes et les applications de support) sont regroupés dans un lot de conteneurs distincts qui fonctionnent ensemble pour composer l'application. Le groupe résultant est communément appelé un pod ou une composition de services. Dans ce cas, tous les éléments de l'application sont opérationnels — à l'exception du système de sécurité de l'application.

L'exécution d'un environnement basé sur un conteneur pour applications Web comprend généralement un outil d'orchestration (tel que Kubernetes). La plate-forme d'orchestration augmente (le dimensionnement) ou réduit (le dimensionnement) automatiquement l'environnement d'application pour répondre à la demande (en hausse ou en baisse). L'ajout d'un WAF basé sur un conteneur à un environnement orchestré permet de dimensionner le système de sécurité parallèlement aux applications du fait de leur adaptation dynamique.

FORTIWEB WEB APPLICATION FIREWALL CONTAINER EDITION

Les WAFs FortiWeb fournissent une protection contre les menaces applicatives Web à couches multiples et renforcée par l'intelligence artificielle (IA) pour les moyennes et grandes entreprises, les fournisseurs de services applicatifs et les fournisseurs de Software-as-a-Service (SaaS). Ces pare-feux sont conçus pour protéger les applications Web et les données exposées à Internet contre les attaques et les failles. Grâce à des techniques de pointe, cette solution offre une protection bidirectionnelle contre les sources malveillantes, les attaques par déni de service distribué (DDoS) et les menaces sophistiquées de type injection de code SQL, script de site à site, dépassement de mémoire tampon, inclusion de fichiers et empoisonnement de cookies.

La solution FortiWeb Container Edition cible principalement les environnements basés sur des conteneurs qui prennent en charge Docker sur un grand nombre de plates-formes. Il s'agit notamment des registres privés/publics, de Docker Enterprise et du service ECS (Elastic Container Service) d'Amazon.

Contrairement aux solutions WAF traditionnelles n'existant qu'en dehors de l'application basée sur un conteneur, il est possible de déployer FortiWeb dans son propre conteneur et de l'inclure dans le package de l'application. Comme il n'a pas besoin d'être entièrement reconfiguré chaque fois que le conteneur est déplacé, le pare-feu WAF est rapidement opérationnel pour protéger l'application contre les exploitations de vulnérabilités tout en simplifiant simultanément la distribution.

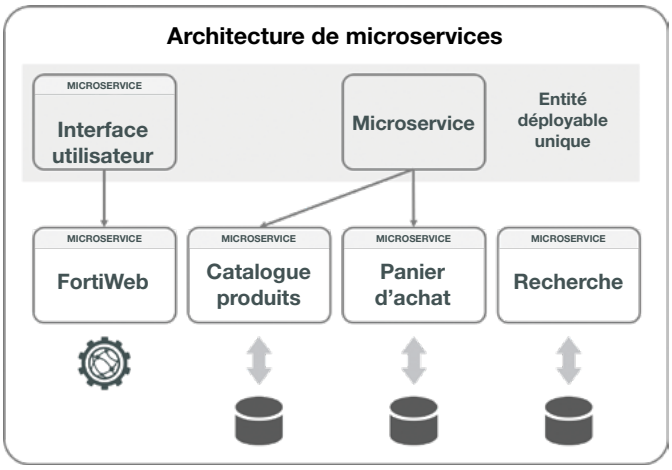

SCHÉMA 1 : ARCHITECTURE DE MICROSERVICES

À chaque étape du processus, l'accès aisé à FortiWeb permet aux développeurs d'applications de s'assurer que les mesures de sécurité sont appliquées tout au long des phases de développement, de test et de déploiement. Il est possible d'inclure dans un package une appliance conteneur virtuelle FortiWeb et l'application au cours des phases de préproduction de manière à tester les vulnérabilités pendant le développement du code. Cela permet également à FortiWeb de commencer à créer des profils d'application dans les environnements de test.

Au cours du déploiement, la version conteneur de FortiWeb peut être packagée avec l'application ou extraite et déployée en tant que conteneur autonome en production. Elle fournit instantanément une protection d'application plus précise sans qu'il soit nécessaire de réapprendre les éléments de l'application.

En addition à l'application incluant un pare-feu WAF mis en conteneur, FortiWeb Container Edition assure le dimensionnement et le provisioning automatiques par le biais du système d'orchestration de conteneurs. Lorsqu'il est nécessaire d'accroître le nombre d'appliances virtuelles FortiWeb pour répondre à la demande, le système d'orchestration peut lancer de nouvelles instances. À l'inverse, lorsque le trafic applicatif ralentit, les appliances virtuelles peuvent être interrompues afin d'économiser les ressources.

UNE SÉCURITÉ PRÊTE À L'EMPLOI POUR DEVOPS EN CONTENEUR

Les entreprises adoptent des stratégies de développement toujours plus agiles, la sécurité va donc demeurer un enjeu primordial. Lorsqu'une équipe de développement écrit, teste, met à jour ou déploie une application à l'aide d'une architecture de microservices mis en conteneur, l'environnement reste homogène pour toutes les facettes du cycle de vie de l'application. Cela facilite la collaboration entre les différentes équipes (développeurs, testeurs et administrateurs), car celles-ci travaillent toutes dans le même environnement mis en conteneur. Le pare-feu WAF basé sur le conteneur de FortiWeb offre des mesures de sécurité qui accompagnent l'application quel que soit son emplacement d'hébergement tout en dimensionnant la solution en fonction de la demande.

FortiWeb Container Edition est disponible auprès des partenaires revendeurs Fortinet. Les clients AWS ont également la possibilité de déployer cette édition en anticipant l'achat d'une licence.

[1] « 8 Surprising Facts About Real Docker Adoption », Datadog, juin 2018.

[2] « 2018 Security Implications of Digital Transformation Report », Fortinet, septembre 2018.

312399-0-1-FR mai 24, 2019 11:23 AM
SB-Web-applications-in-container-based-environments-FR-A4