FORTINET

Protection optimale des applications Web sur AWS

Les pare-feux d'application web offrent une sécurité simple à gérer et économique

Table des matières

FORTINET

Synthèse

Alors que les entreprises migrent leurs applications métiers de leurs environnements sur site vers le cloud, leur vulnérabilité face aux attaques ciblées connues et inconnues s'accentue. Chaque nouvelle application déployée dans le cloud est une nouvelle passerelle d'entrée potentielle qui contribue à étendre la surface d'attaque. D'autre part, le volume et la virulence des menaces continuent à progresser, ce qui met toujours plus de pression sur les entreprises et les incitent à déployer et gérer un panel disparate de solutions de sécurité.

Les entreprises qui hébergent leurs applications sur Amazon Web Services (AWS) pensent, souvent à tort, qu'elles n'ont pas à se soucier de la sécurité. En réalité, AWS assure la sécurité de l'infrastructure, tandis que le client reste responsable de la sécurité des applications et des données. D'autre part, une utilisation d'outils de sécurité sur site ne répond pas aux défis qu'impose l'univers actuel des menaces.

Au contraire, les entreprises ont besoin de solutions de sécurité conçues spécifiquement pour des applications Internet, à savoir des pare-feux d'application web (WAF). Un WAF, véritable barrière face aux attaques externes et internes, surveille et contrôle les accès aux applications web et recueille des informations à des fins de conformité et de traitement analytique. Les WAF sont proposés sous différents formats : appliance physique, appliance virtuelle ou plateforme cloud.

83%

des instances d’entreprise seront dans le cloud en 2020.[1]

Les défis de la sécurité du cloud

Une entreprise qui déploie ses applications dans le cloud, voit son profil de risque évoluer. Le cloud public est dépourvu de périmètre de sécurité et chaque nouvelle application est une cible potentielle qui élargit la surface d'attaque. Parallèlement, c'est le volume et la virulence des menaces qui continuent à progresser. Par exemple, les tentatives ont progressé de 5% sur le dernier trimestre de 2018, tandis que les cybercriminels font preuve d'intelligence et d'efficacité en définissant des attaques plus ciblées et sophistiquées.[2]

Nombre d'entreprises ont adopté le modèle DevOps pour rendre leurs opérations métiers plus rapides et agiles. Dans ce contexte, les équipes DevOps deviennent responsables de la sécurité des applications Internet et comptent sur le WAF. Cependant, ces équipes DevOps ne disposent pas du temps nécessaire et de l'expertise en sécurité pour assurer la configuration et la gestion d'un WAF, des tâches qui pèsent sur leur rôle plus stratégique qui est de concevoir de nouvelles fonctionnalités et applications. Bien sûr, il est envisageable de recruter un ingénieur en sécurité pour assurer ces tâches, mais la pénurie de compétences dans ce domaine ne facilite en rien cette tâche : les postes non pourvus en cybersécurité devraient s'élever à 1,8 million d'ici 2022, en progression de 20% par rapport à 2015.[3]

Alors qu'elles évaluent les solutions WAF disponibles, les entreprises doivent prendre en compte tous les facteurs présentés ci-dessus. Pour simplifier ce processus, la première étape pour les décisionnaires est de prendre en compte leurs besoins en matière de convivialité, de protection contre les menaces évoluées et de maîtrise des coûts (TCO).

Les applications web constituent le vecteur N° 1 des attaques aboutissant à un piratage de données.[4]

Prérequis 1 : déploiement et gestion simplifiés

La configuration des pare-feux constitue un des facteurs de succès majeurs de la sécurité des applications web. Pour éviter les erreurs de configuration et alléger le travail des développeurs, les équipes DevOps doivent évaluer les WAF selon des critères de simplicité de déploiement, de personnalisation des règles de sécurité et de précision.

Simplicité d'utilisation

Compte tenu de la pénurie de compétences en cybersécurité, les solutions de sécurité doivent pouvoir être déployées et opérées sans expertise importante. Pour tenir cet objectif, les entreprises sont invitées à retenir des WAF qui sont simples à déployer, à configurer et à gérer. Assistants d'installation, règles prédéfinies et tableaux de bord intuitif vont y contribuer.

Règles sur mesure

Une fois le WAF opérationnel, les professionnels DevOps et sécurité doivent pouvoir définir et affiner les règles de pare-feu pour ainsi alléger les tâches opérationnelles de gestion de la sécurité et s’adapter aux changements dans cet univers.

Précision

Les faux-positifs mobilisent les équipes et, lorsque trop nombreuses, peuvent masquer une menace réelle. Les solutions WAF capitalisent sur le Machine Learning pour améliorer leur capacité à identifier des menaces entrantes avec précision, avec un minimum d'impact sur les équipes.

En 2018, les erreurs de configuration ont contribué à 70% des piratages de données dans le cloud, soit un bond annuel de 424%.[5]

Prérequis 2 : protection évoluée contre les menaces

Les menaces continuent à progresser et à se diversifier. Ainsi, une enquête récente témoigne qu'au moins une nouvelle menace zero-day est détectée chaque semaine.[6] En évaluant la protection qu'offrent les solutions potentielles, les critères de sélection doivent porter sur le niveau d'efficacité, la protection des API et les mises à jour de sécurité.

Efficacité de la sécurité

Le Top 10 OWASP est un palmarès des menaces de sécurité les plus critiques pour les applications web. Les entreprises qui veulent protéger efficacement leurs applications web doivent retenir des solutions qui sauront neutraliser tous les risques de ce Top 10, ainsi que les exploits inconnus et zero-day (schéma 1).[7]

OWASP Top 10—2017
A1: 2017- Injection
A2: 2017- Authentification défaillante
A3: 2017- données sensibles exposées
A4: 2017- XML External Entities (XXE)
A5: 2017- Contrôle d'accès défaillant
A6: 2017- Erreur de configuration de la sécurité
A7: 2017-Cross-Site Scripting (XSS)
A8: 2017- Désérialisation non sécurisée
A9: 2017- Utilisation de composants avec vulnérabilité connue
A10: 2017- Logging et monitoring insuffisants

Schéma 1. Le TOP 10 OWASP des risques de sécurité pour les applications Web.

Protection des API

Les API non-protégées sont des vulnérabilités graves qui permettent aux assaillants d'exfiltrer des données et d'exécuter des attaques de déni de services (DDoS). Une sécurité applicative efficace implique des règles de sécurité distribuées pour protéger les API contre les acteurs malveillants.

Mises à jour de sécurité

Au-delà des fonctions de protection évoluées mentionnées ci-dessus, les solutions doivent bénéficier d'un abonnement à un service de veille sur les menaces pour une actualisation des signatures d'attaque, la réputation IP, l'antivirus et les sandbox.

48% des décisionnaires estiment que les attaques par DDoS progressent d'année en année.[8]

Prérequis 3 : maîtrise des coûts d'exploitation

Parmi les différents formats de déploiement, le WaaS (WAF-as-a-Service) constitue la solution la plus économique pour nombre d'entreprises. Avec ce modèle, le fournisseur de services cloud met à disposition les composants matériels et logiciels, ce qui élimine pratiquement tout investissement initial (CapEX), ainsi que les charges d'exploitation (OpEX) liées à la maintenance de la plateforme.

L'infrastructure mondiale d'AWS héberge 16 entités géographiques, cloisonnées physiquement les unes par rapport aux autres. Les entreprises peuvent capitaliser sur cette infrastructure mondiale en sélectionnant un WaaS situé dans la même région AWS que l'application protégée. Cette stratégie permet de réduire significativement la latence et les coûts de transfert : l'entreprise n'est redevable que du coût associé au trafic de données vers le WaaS, tandis que le fournisseur WaaS prend les coûts de trafic sortant à sa charge.

Le top 10 OWASP se base principalement sur plus de 40 entreprises spécialisées dans la sécurité applicative soumettant leurs données, ainsi que sur des enquêtes menées sur un panel de plus de 500 personnes. Les données portent sur des vulnérabilités recueillies à partir de centaines d'entreprises et plus de 100 000 applications et API sur le terrain. Les 10 éléments de ce classement sont hiérarchisés selon le critère de leur prévalence et les estimations en matière de vulnérabilité, de capacité à être détecté et d'impact.[9]

Options de déploiement WAF

AWS propose un WAF de base facturé à l'utilisation, mais cet outil seul peine à proposer la sécurité professionnelle exigée par nombre d'applications de sécurité. Les décisionnaires DevOps et sécurité devraient donc privilégier un WAF proposé sous différents formats de déploiement, qui offre une utilisation conviviale, une protection contre les menaces évoluées et une maîtrise du TCO.

Règles managées pour le WAF d'AWS

Proposés par des éditeurs tiers spécialisés dans la sécurité, des packages de règles managées permettent aux utilisateurs d'établir une sécurité plus robuste, en complément du WAF d'AWS. L'éditeur procède à des mises à jour automatiques, dès détection de nouvelles vulnérabilités et d'acteurs malveillants, ce qui assure une actualisation des règles de sécurité.

WAF-as-a-Virtual Machine

Le WAF proposé dans un format de machine virtuelle (VM) protège les applications hébergées sur des plateformes telles que VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM et Docker. Les VM WAF, qui disposent des mêmes fonctionnalités que les WAF matériels, se déploient au sein d'environnements d'hébergement temps-réel pour les applications.

WAF-as-a-Service

Le WaaS permet aux entreprises de déployer une protection évoluée contre les menaces dans un format que les équipes DevOps peuvent déployer de manière simple. Le fournisseur WaaS pilote l'infrastructure de sécurité, ce qui libère du temps pour les équipes Devops et leur permet de se focaliser sur des tâches à forte valeur ajoutée, innovantes et génératrices de revenus supplémentaires. Le WaaS intègre toutes les fonctionnalités du WAF au format matériel et virtuel et propose des options d'hébergement en local qui permettent de réduire les coûts de transfert et la latence.

Les entreprises qui utilisent des modèles SaaS tels que le WAF-as-a-Service dépensent 21% de moins en IT (en % du chiffre d'affaires) et 16% de moins en IT sur la base des utilisateurs, par rapport à celles qui ont opté pour un modèle applicatif sur site.[10]

Les entreprises qui utilisent des modèles SaaS tels que le WAF-as-a-Service dépensent 21% de moins en IT (en % du chiffre d'affaires) et 16% de moins en IT sur la base des utilisateurs, par rapport à celles qui ont opté pour un modèle applicatif sur site.[11]

Checklist d’évaluation des solutions WaaS

Voici une checklist à l'intention des responsables de DevOps pour évaluer et comparer les solutions de protection de leurs applications sur AWS :

Déploiement

- Déployé en tant que solution cloud-native sur AWS
- Propose des configurations prédéfinies
- Se déploie en quelques minutes à l'aide de règles

Administration simple

- Solution évolutive qui s'adapte à la versatilité des besoins en sécurité
- Permet un hébergement des applications à proximité locale pour alléger les coûts et simplifier la mise en conformité
- Offre une tarification flexible et à la demande

Efficacité

- Protège contre les vulnérabilités du Top 10 OWASP et les exploits zero-day
- Accès à des options de configuration avancée
- Propose des règles WAF personnalisées
- Offre une sécurité des API
- Intègre un abonnement à un service de recherche sur les menaces

FortiWeb Cloud WAF-as-a-Service protège les applications web hébergées dans le cloud face aux menaces évoluées : le Top 10 OWASP, les menaces zero-day et autres attaques sur la couche applicative. Pour plus d'informations, rendez-vous sur www.fortiweb-cloud.com.

[1] Louis Columbus, « 83% Of Enterprise Workloads Will Be In The Cloud By 2020, » Forbes, 7 janvier 2018.

[2] « Quarterly Threat Landscape Report: Q4 2018, » Fortinet, février 2019.

[3] « Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher, » (ISC)², 7 juin, 2017.

[4] « 2019 Data Breach Investigations Report: Summary of Findings, » Verizon, consulté le 2 juillet 2019.

[5] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, 6 avril 2018.

[6] « Quarterly Threat Landscape Report: Q4 2018, » Fortinet, février 2019.

[7] "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks," OWASP, consulté le 13 juillet 2019.

[8] « Q1, 2019 Cyber Threats & Trends Report, » Neustar, 17 avril 2019.

[9] "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks," OWASP, consulté le 13 juillet 2019.

[10] "Cloud Users Enjoy Significant Savings," Computer Economics, consulté le 13 juillet 2019.

[11] Idem.

www.fortinet.fr

431437-0-0-FR

mars 2, 2021 10:49 AM

eb-advanced-protection-web-applications_FR