CLOUDFLARE

Présentation de solution

Pare-feu WAF Cloudflare

Un pare-feu WAF pour la sécurité des applications modernes

Difficultés liées à la sécurité des applications

Les applications n'ont jamais été aussi essentielles à l'activité des entreprises, c'est pourquoi elles sont constamment la cible d'acteurs malveillants, ce qui vient s'ajouter aux préoccupations de l'organisation en matière de sécurité.

Les préoccupations vont du maintien de la protection contre les exploitations zero day émergentes, à la détection des tentatives d'évasion, en passant par la réduction du risque de bourrage d'identifiants qui conduit à des usurpations de comptes, la détection des pertes de données, et même la recherche d'importations malveillantes dans les applications.

Ces préoccupations sont associées au besoin de faire en sorte que les protections des applications s'inscrivent dans un niveau de sécurité unifié et plus vaste, protégeant également les API, bloquant les bots et réduisant les risques côté client. Et il est important que tout cela ne vienne pas ajouter de charges complexes aux équipes.

Pare-feu WAF Cloudflare

Le pare-feu d'applications web (WAF) de Cloudflare constitue la pierre angulaire de notre catalogue de solutions avancées de sécurité des applications. Il est compose de services permettant d'assurer la sécurité et la productivité de ces dernières. Seul le WAF de Cloudflare accorde une visibilité totale en matière de sécurité, propose des protections par couches contre les attaques identifiées par l'OWASP et les exploitations e émergentes, détecte les évasions et les nouvelles attaques avec l'apprentissage automatique, bloque les usurpations de comptes, détecte les pertes de données, et plus encore. Il est par ailleurs très facile à intégrer dans le flux de travail plus largement consacré à la sécurité de l'entreprise. Nos puissantes capacités en matière de sécurité des applications, telles que la sécurité des API et la gestion des bots, sont entièrement intégrées à notre WAF, faisant appel au solide moteur de règles performant, proposé à partir de plateformes cloud mondiales parmi les plus connectées au monde.

Visibilité et détection des attaques

Nous proposons des analyses de sécurité différenciées permettant de visualiser l'ensemble du trafic, qu'il soit atténué ou non. Elles renseignent les équipes de sécurité sur les attaques inconnues et les mesures protectrices qu'elles doivent créer. Elles affichent les scores d'attaque du WAF, les scores de bots et des analyses de contenu.

Protections rapides contre les attaques émergentes

Avec dix mille vulnérabilités par an, notre WAF ajoute rapidement de nouvelles règles gérées pour bloquer l'exploitation des vulnérabilités dès leur découverte (Zero Day). Nos règles gérées bloquent les exploitations, elles sont enrichies par l'apprentissage automatique issu des scores d'attaques du WAF, afin de détecter les évasions.

Dix principales menaces identifiées par l'OWASP

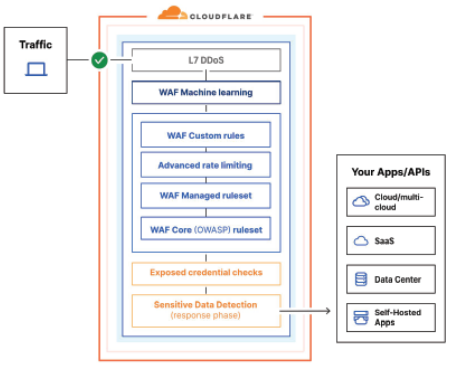
Les attaques exigent des défenses par couche, y compris pour les types d'attaques connus et figurant parmi les dix principales menaces identifiées par l'OWASP. Notre ensemble de règles principal de l'OWASP est constamment mis à jour et conçu pour fonctionner comme une entité unique qui calcule un score de menace avant d'exécuter une action en fonction de ce score. Cet ensemble de règles peut être configuré différemment selon le risque et les exigences en matière de sécurité.

Pourquoi choisir le pare-feu d'applications web de Cloudflare

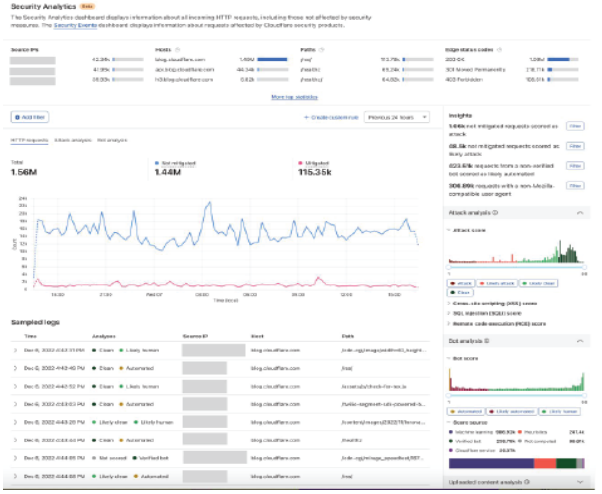
- **Cloudflare protège plus efficacement.** Nous garantissons une sécurité par le WAF plus efficace avec des protections par couche :
  - Données d'analyse de sécurité
  - Ensembles de règles gérées multiples
  - Règles personnalisées
  - Détections par l'apprentissage automatique
  - Détection des données sensibles
  - Vérifications des identifiants volés
  - Limitation avancée du taux
  - Recherche des importations malveillantes

- **Cloudflare répond rapidement.** Nous assurons une protection plus rapide contre les exploitations. Pour les vulnérabilités majeures telles que Log4j, nous avons mis en place de nombreuses règles gérées avec un jour d'avance sur les autres fournisseurs de WAF.

- **Cloudflare coordonne de manière globale la sécurité des applications.** Notre WAF est totalement intégré au reste de notre portefeuille consacré à la sécurité des applications, y compris la sécurité des API et la gestion des bots, le tout étant proposé ensemble depuis l'une des plateformes cloud mondiales les plus connectées.



Données d'analyse de sécurité du pare-feu WAF



Un WAF pour la sécurité de l'entreprise

Intégration aux plateformes SIEM, compatibilité avec les SOC

Grâce aux API de Cloudflare et aux intégrations aux journaux bruts, vous pouvez facilement intégrer votre plateforme SIEM ou approvisionner votre centre d'opérations de sécurité (SOC) avec les renseignements fournis par Cloudflare.

Rendre le DevSecOps plus simple

Avec notre intégration Terraform prête à l'emploi, l'incorporation de la sécurité des applications dans les approches DevOps devient une naturelle.

Étayé par Cloudforce One

La sécurité des applications par Cloudflare reçoit des informations sur les menaces de la part de Cloudforce One, notre équipe dédiée aux opérations sur les menaces, bloque les menaces via une détection reposant sur les informations émergentes et les tactiques, techniques et procédures (TTTP).

Prééminence de Cloudflare

Les organisations bénéficient d'une stratégie de sécurité des applications plus efficace lorsqu'elles utilisent le réseau mondial de Cloudflare comme périmètre de sécurité de l'entreprise. Le portefeuille de solutions de sécurité des applications de Cloudflare a reçu de nombreux éloges pour sa solidité et son étendue. Cloudflare a été désignée comme Leader dans le rapport Gartner® Magic Quadrant™ de 2022 consacré à la protection des API et des applications web (Web Application and API Protection, WAAP). Cloudflare a été reconnue leader dans le rapport The Forrester Wave™ consacré aux pare-feu WAF. Gartner a nommé le pare-feu WAF de Cloudflare « Customer's Choice » en 2022. Frost & Sullivan a décerné à Cloudflare le titre d'Innovation Leader en 2020 dans la catégorie « Global Holistic Web Protection », tandis qu'IDC et Forrester ont désigné l'entreprise leader des solutions de protection anti-DDoS pour l'année 2021.

Sécurité des applications web	
Protection multicouches assurée par plusieurs ensembles de règles de pare-feu WAF	Bloque les charges utiles malveillantes dans n'importe quel composant d'une requête grâce plusieurs ensembles de règles : 1. Règles gérées par Cloudflare 2. Ensemble de règles principal de l'OWASP 3. Ensembles de règles personnalisées pour arrêter toutes les attaques. Les nouvelles règles gérées sont testées sur d'immenses volumes de trafic, afin de garantir un minimum de faux positifs.
Règles mises à jour pour la protection contre les menaces zero-day	Les règles continuellement actualisées par l'équipe de sécurité de Cloudflare assurent une protection contre les nouvelles attaques et les vulnérabilités zero-day avant la mise à disposition de correctifs ou de mises à jour.
Détections par l'apprentissage automatique	Bloquez les tentatives de contournement grâce à des modèles d'apprentissage automatique complétant les ensembles de règles superposés. Il existe quatre scores d'attaques différents pour les règles : le score d'attaque du WAF global, le score d'attaque XSS, le score d'attaque SQLi, le score d'attaque RCE.
Ensembles de règles adaptées aux plateformes pour les CMS et les plateformes de commerce en ligne	Bénéficiez d'une protection immédiate sans frais supplémentaires pour les plateformes comme WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc.
Configuration de règles personnalisées	Faites votre choix parmi les options ALLOW, BLOCK, MANAGED CHALLENGE, JS CHALLENGE, SKIP, LOG, LEGACY CAPTCHA, CUSTOM RESPONSES lors du déploiement de règles ou d'ensembles de règles.
Limitation avancée du taux	Mettez un terme à l'utilisation abusive, aux attaques DDoS et aux tentatives de connexion par force brute visant les applications et les API en limitant le taux de requêtes d'adresses IP particulières ou en fonction d'un attribut d'en-tête (par ex. clé, cookie, jeton), d'un ASN ou d'un pays.
Flux d'informations sur les menaces	Bloquez les connexions provenant d'adresses IP issues de proxys SOCKS ouverts connus, de VPN, de botnets, de serveurs Command and Control, de sources de logiciels malveillants et de services d'anonymisation.
Détection des données sensibles	Bloquez les réponses contenant des données sensibles telles que, comme les informations d'identification personnelle, les informations financières, les numéros de carte de paiement ou les informations secrètes, comme les clés d'API.
Vérifications des identifiants compromis	Détectez les attaques par force brute utilisant des identifiants volés avant que les comptes d'utilisateurs finaux ne soient infiltrés.
Analyse des importations de contenu	La fonctionnalité d'analyse du contenu proposée par le pare-feu WAF examine les fichiers importés à la recherche de logiciels malveillants. L'atténuation est assurée via les règles personnalisées du pare-feu WAF.
SSL/TLS	Déchargez et configurez entièrement le trafic SSL pour votre application.
Moins de faux positifs	Les nouvelles règles sont testées sur d'immenses volumes de trafic, afin de garantir un minimum de faux positifs.
Prise en charge de gRPC et Websocket	Acheminez le trafic par proxy et sécurisez-le pour les points de terminaison gRPC et Websocket.
Pages de blocage personnalisables	Personnalisez les pages de blocage avec des détails correspondant aux visiteurs.
Intégration totale à l'ensemble de la suite de produits Cloudflare	Améliorez les performances des applications, géoroutez le trafic et tirez parti des possibilités de l'informatique périphérique.

Visibilité, rapports et programmabilité	
Données d'analyse de sécurité	Visualisation de toutes les attaques potentielles, selon le score établi par l'apprentissage automatique.
Journalisation en temps réel et accès aux fichiers journaux bruts	Gagnez en visibilité pour configurer plus précisément le pare-feu WAF. Réalisez une analyse en profondeur couvrant l'ensemble des requêtes transmises à celui-ci.
Journalisation du contenu	Journalisez et chiffrez les contenus malveillants à des fins d'analyse des incidents.
Intégrations aux plateformes SIEM	Transférez ou importez des journaux directement au sein de vos SIEM existants.
Intégration de Terraform	Intégrez la sécurité des applications aux flux de travail CI/CD.
Gestion	
Gestion depuis une console unique	Gestion rationalisée depuis une console unique, permettant de déployer et gérer la sécurité et les performances des applications à l'échelle mondiale.
Gestion au niveau du compte	Économisez du temps sur la gestion du pare-feu WAF grâce à une configuration WAF unique au niveau du compte, pour tous les domaines.
Disponibilité élevée (avec SLA)	Garantie de disponibilité de 100 % avec pénalités financières en cas de non-respect des SLA.
Aucun réglage, ni équipement physique ou logiciel requis	Le déploiement nécessite une simple modification du DNS.
Certification PCI	Cloudflare possède un certificat de fournisseur de services de niveau 1.
Un service autorisé par le FedRAMP	Notre suite Cloudflare for Government, qui inclut notamment des mesures de sécurité des applications, est autorisée par le programme FedRAMP.