Pare-feu Cloudflare WAF

Un pare-feu WAF pour la sécurité des applications modernes

Les problématiques de la sécurité des applications

Les applications n'ont jamais été aussi essentielles à l'activité des entreprises. Elles engendrent toutefois une surface d'attaque étendue et sont donc sans cesse prises pour cible par les acteurs malveillants.

Les préoccupations à leur égard vont du maintien de la protection contre les tentatives d'exploitation des vulnérabilités zero-day émergentes, à la détection des tentatives d'évasion, en passant par la réduction des risques de bourrage d'identifiants (Credential Stuffing) susceptibles de conduire à une usurpation de compte, la détection des pertes de données, voire la recherche d'importations de logiciels malveillants au sein des applications.

Ces inquiétudes s'associent au besoin de s'assurer que les mesures de protection des applications s'inscrivent au sein d'une stratégie de sécurité unifiée et plus vaste, qui permette également de protéger les API, de bloquer les bots et de réduire les risques côté client. Plus important encore : toutes ces opérations doivent pouvoir s'effectuer sans ajouter de complexité inutile aux équipes pour ce qui est de la gestion.

Pare-feu Cloudflare WAF

Le pare-feu applicatif web (WAF) de Cloudflare constitue la pierre angulaire de notre catalogue de produits avancés permettant d'assurer la sécurité et la productivité des applications. Le pare-feu Cloudflare WAF accorde une visibilité totale en matière de sécurité. Il propose également une protection par couches contre les attaques recensées par l'OWASP et l'exploitation des vulnérabilités émergentes, détecte les évasions et les nouvelles attaques grâce à l'apprentissage automatique (Machine Learning, ML), bloque les usurpations de comptes et détecte les pertes de données (parmi bien d'autres avantages encore) afin de protéger l'ensemble de vos applications, peu importe l'endroit où elles sont hébergées. Nos solides fonctionnalités de sécurité des applications (comme nos services de sécurité des API et de gestion des bots, par exemple) sont entièrement intégrées à notre pare-feu WAF. Elles font appel au même puissant moteur de règles que celui que nous proposons depuis l'un des premiers clouds de connectivité au monde.

Visibilité sur les attaques et processus d'intégration simplifié

Nous proposons des analyses de sécurité différenciées afin de visualiser l'ensemble du trafic, qu'il soit atténué ou non. Retour sur investissement concret, la visibilité immédiate sur le panorama des menaces permet aux équipes de mieux comprendre leur trafic hostile et les protections qu'elles doivent mettre en place dès l'intégration.

Mesures de protection rapides contre les attaques émergentes

Face aux dizaines de milliers de vulnérabilités identifiées chaque année, notre pare-feu WAF ajoute rapidement de nouvelles règles gérées afin de bloquer les tentatives d'exploitation des nouvelles failles (zero-day). Enrichies par nos WAF Attack Scores (scores d'attaque WAF) dérivés de l'apprentissage automatique, ces règles gérées permettent également de détecter les évasions.

Un ensemble d'informations sur les menaces soutenu par un vaste réseau mondial

L'efficacité en matière de sécurité commence par le fait de disposer des meilleures données. Or, en mettant 20 % d'Internet en proxy, notre vaste réseau mondial nous permet de bénéficier d'une vision inégalée sur le panorama des menaces. Ces données nourrissent des modèles d'apprentissage automatique que nous associons à des solutions plus traditionnelles de détection basée sur les signatures afin de détecter et d'atténuer les tentatives d'attaque avec une grande précision.

 +33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

Les problématiques de la sécurité des applications

Cloudflare vous protège plus efficacement.

Notre pare-feu WAF nous permet d'assurer une sécurité plus efficace grâce à ses mesures de protection superposées :

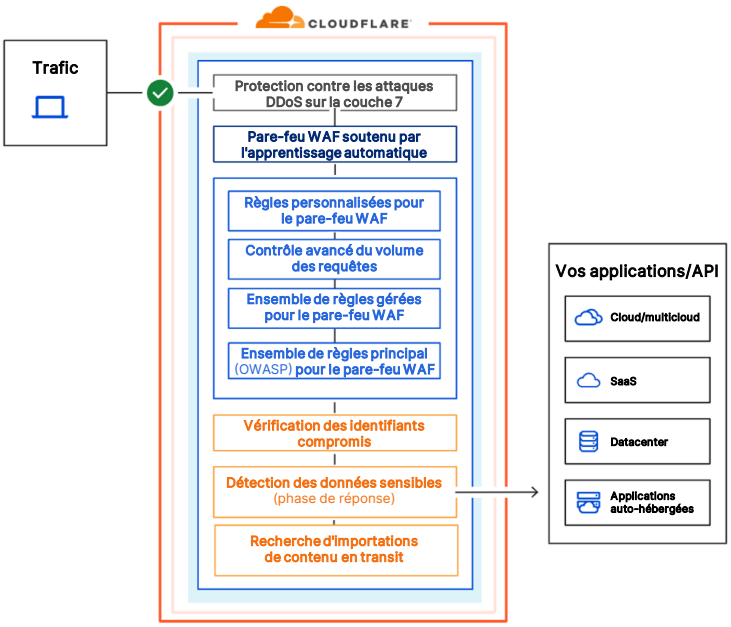
- outils d'analyse de la sécurité ;
- plusieurs ensembles de règles gérées ;
- règles personnalisées ;
- mesures de détection soutenues par ML ;
- détection des données sensibles ;
- mesures de contrôle des identifiants volés ;
- contrôle avancé du volume des requêtes ;
- recherche d'importations de logiciels malveillants.

Cloudflare réagit plus rapidement.

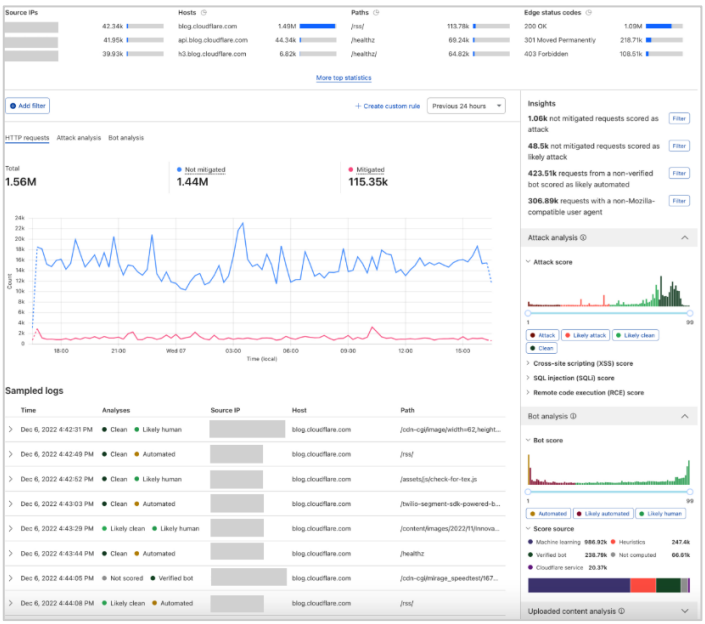
Nous vous protégeons à une vitesse inégalée contre les tentatives d'exploitation. En déployant plusieurs règles gérées avec un jour d'avance sur les autres fournisseurs de pare-feu WAF, nous avons ainsi permis à nos clients de lutter contre les failles majeures, comme les vulnérabilités HTTP/2 Rapid Reset, Log4j et bien d'autres.

Cloudflare intègre totalement la sécurité des applications.

Notre pare-feu WAF s'intègre totalement au reste de notre catalogue de produits de sécurité des applications (qui comprend notamment la solution API Gateway et notre service de gestion des bots) tous proposés en une seule passe depuis le cloud de connectivité Cloudflare.



Outils d'analyse de la sécurité du pare-feu WAF



Un pare-feu WAF pour la sécurité de l'entreprise

Intégration aux SIEM, compatibilité avec les SOC

Les API Cloudflare et l'intégration des journaux bruts vous permettent de vous incorporer facilement au SIEM de votre choix ou de soutenir votre centre d'opérations de sécurité (Security Operations Center, SOC) à l'aide des informations proposées par Cloudflare.

Faciliter les DevSecOps

Grâce à l'intégration Terraform immédiate, l'incorporation de la sécurité des applications aux approches DevOps devient une seconde nature.

Une solution soutenue par Cloudforce One

Les outils de sécurité des applications Cloudflare reçoivent des informations sur les menaces de la part de Cloudforce One, notre équipe de réponse aux menaces, afin de bloquer ces dernières à l'aide de nouvelles mesures de détection reposant sur les informations et les TTP (tactiques, techniques et procédures) émergentes.

Sécurité des applications web	
Protection multicouches assurée par plusieurs ensembles de règles pour le pare-feu WAF	Bloquez les contenus malveillants dans n'importe quel composant de requête grâce à plusieurs ensembles de règles : 1. règles gérées par Cloudflare ; 2. ensemble de règles principal de l'OWASP ; 3. règles personnalisées permettant d'arrêter n'importe quelle attaque. Les nouvelles règles gérées sont testées sur d'immenses volumes de trafic afin de garantir un minimum de faux positifs.
Mise à jour des règles pour vous protéger contre les menaces zero-day	Actualisées en continu par l'équipe de sécurité Cloudflare, ces règles assurent une protection contre les nouvelles attaques et l'exploitation de vulnérabilités zero-day avant la mise à disposition de correctifs ou de mises à jour.
Mesures de détection soutenues par ML	Bloquez les tentatives de contournement grâce à des modèles d'apprentissage automatique venant compléter les ensembles de règles superposés. Il existe quatre scores d'attaques différents pour les règles : le WAF Attack Score global, le score d'attaque XSS, le score d'attaque SQLi et le score d'attaque RCE.
Ensembles de règles spécifiques pour les principales plateformes de CMS et d'e-commerce	Bénéficiez d'une protection immédiate et sans frais supplémentaires pour diverses plateformes, comme WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc.
Configuration des règles personnalisées	Lors du déploiement de règles ou d'ensembles de règles, mettez en place un modèle de sécurité positive ou négative à l'aide des actions suivantes : BLOCK (blocage), MANAGED CHALLENGE (test géré), JS CHALLENGE (test JS), SKIP (ignorer), LOG (journaliser), LEGACY CAPTCHA (Captcha traditionnel), CUSTOM RESPONSES (réponse personnalisée).
Contrôle avancé du volume des requêtes	Mettez un terme à l'utilisation abusive, aux attaques DDoS et aux tentatives de connexion par force brute qui visent vos applications et vos API en contrôlant le volume de requêtes envoyées par des adresses IP particulières ou en fonction d'un attribut d'en-tête (par ex. clé, cookie, jeton), d'un ASN ou d'un pays.
Détection des données sensibles	Bloquez les réponses contenant des données sensibles, comme les informations d'identification personnelle (Personally Identifiable Information, PII), les informations financières, les numéros de carte de paiement ou les secrets (clés d'API, par exemple).
Vérification des identifiants compromis	Détectez les attaques par bourrage d'identifiants (Credential Stuffing) réalisées à l'aide d'identifiants volés avant que les utilisateurs finaux ne voient leur compte usurpé.
Analyse des importations de contenu	La fonctionnalité WAF Content Scanning proposée par le pare-feu WAF examine les fichiers importés à la recherche de logiciels malveillants. Vous pouvez associer ces signaux à d'autres paramètres de requête en définissant des règles personnalisées.
SSL/TLS	Déchargez totalement le trafic SSL et configurez-le 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 des protocoles gRPC et Websocket	Mettez le trafic des points de terminaison gRPC/Websocket en proxy et sécurisez-le.
Pages de blocage personnalisables	Personnalisez les pages qui s'affichent en cas de blocage et présentent les informations appropriées à communiquer à vos visiteurs.
Intégration totale à l'ensemble de la suite de produits Cloudflare	Améliorez les performances de vos applications, géoroutez votre trafic et tirez parti des possibilités de l'informatique de périphérie (Edge).

 +33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/ RÉV. : PMM-JAN-2025

Visibilité, reporting et programmabilité	
Outils d'analyse de la sécurité	Visualisez l'ensemble des attaques potentielles, telles que définies par nos modèles d'apprentissage automatique.
Journalisation en temps réel et accès aux fichiers journaux bruts	Gagnez en visibilité afin de 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 SIEM	Transférez ou importez des journaux directement vers votre SIEM existant.
Intégration de Terraform	Intégrez la sécurité des applications à vos flux de travail CI/CD.
Gestion	
Gestion depuis une console unique	Gérez vos ressources de manière rationalisée depuis une console unique permettant de déployer et de gérer les services d'amélioration de la sécurité et des performances de vos applications à l'échelle mondiale.
Gestion au niveau du compte	Économisez du temps sur la gestion du pare-feu WAF grâce à son processus de configuration unique, au niveau du compte, pour tous les domaines.
Disponibilité élevée (avec proposition de SLA)	Garantie de disponibilité de 100 % avec pénalités financières en cas de non-respect des SLA.
Aucun réglage, équipement physique ni logiciel requis	Le déploiement nécessite un simple changement de DNS.
Certification PCI	Cloudflare dispose d'un certificat de fournisseur de services de niveau 1.
Un service autorisé par le FedRAMP	Notre suite Cloudflare for Government, qui inclut notamment des services de sécurité des applications, est autorisée par le programme FedRAMP.

Êtes-vous prêts à en voir davantage ? Inscrivez-vous à notre série de démos consacrées à la sécurité des applications.

 +33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : PMM-JAN-2025