CLOUDFLARE

Pare-feu applicatif Web (WAF)

Protège votre site contre les injections SQL, les attaques de type cross-site scripting et plus encore

Le pare-feu applicatif Web (WAF) de Cloudflare protège votre site contre les injections SQL, le cross-site scripting (XSS) et les attaques zero-day, y compris les vulnérabilités et menaces identifiées par l'OWASP qui s'attaquent à la couche d'application. Parmi nos clients, nous comptons les 50 sites en tête du classement Alexa, des institutions financières, des entreprises de commerce en ligne et des grandes sociétés. Entièrement intégré à notre protection DDoS, notre WAF bloque chaque jour des millions d'attaques et se renforce à chaque menace grâce à l'auto-apprentissage.

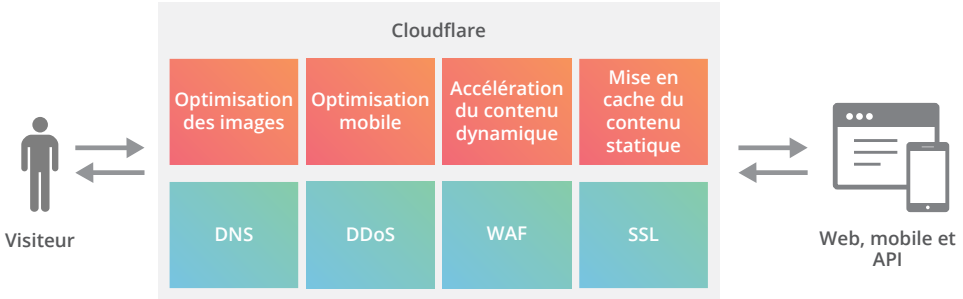
Un puissant générateur de règles à personnaliser en fonction de vos besoins

Notre pare-feu applicatif exécute immédiatement les ensembles de règles ModSecurity afin de vous protéger contre les failles d'applications les plus sévères identifiées par l'OWASP. Il prend également en charge vos ensembles de règles existants et les ensembles de règles personnalisés. Ils prennent effet en moins de 30 secondes.

Déploiement dans le cloud avec CDN et atténuation des attaques DDoS

En tant que service dans le cloud, le pare-feu applicatif de Cloudflare ne nécessite ni matériel ni logiciel, à l'installation comme pour son utilisation. Déployez le pare-feu applicatif en un clic et personnalisez-le selon vos besoins.

Son intégration au service global Cloudflare vous donne accès gratuitement à d'autres fonctionnalités. Vous pouvez protéger votre site Web contre les attaques DDoS tout en le rendant plus rapide avec notre CDN global.



Points clés :

- **Protection automatique** contre différentes menaces, avec des ensembles de règles par défaut efficaces et de nombreux réglages possibles visant à protéger la couche 7, entièrement intégrée à l'atténuation des attaques DDoS
- **Temps de traitement éclair de 0,3 ms**, avec mises à jour instantanées au niveau global
- **Conformité avec l'exigence 6.6 de la norme PCI DSS** : le pare-feu applicatif Web de Cloudflare vous permet d'être conforme à la norme PCI de manière rentable
- **Rapports en temps réel** : une journalisation efficace vous permet de savoir ce qui se passe à tout moment
- **Déploiement dans le cloud** sans matériel, logiciel ni réglages nécessaires

Fonctionnalités principales	Avantages
Sécurité	
Inspection des paquets en profondeur couvrant les applications/la couche 7	Garantit que vos applications Web standard et personnalisées sont toujours protégées contre les injections SQL, les attaques de type cross-site scripting et des milliers d'autres
SSL	Interrompez les connexions SSL sans overhead ni latence supplémentaire. Appliquez la stratégie de votre WAF au trafic SSL chiffré sans devoir télécharger de certificats ni investir dans des solutions matérielles coûteuses.
Pour les requêtes HTTP/S GET et POST	Couvre l'ensemble du trafic HTTP/S
Ensembles de règles personnalisables par URL	Vous permet d'inclure/d'exclure des URL ou sous-domaines spécifiques à la protection WAF afin de tester les domaines ou d'inclure/exclure des sous-domaines spécifiques
Intégration de la protection contre les attaques DDoS	Permet de protéger entièrement la pile contre les attaques DDoS (pas d'implémentation supplémentaire requise)
Intégration de la base de données de réputation IP	Renseignements en temps réel sur plus d'un milliard d'adresses IP uniques utilisés pour bloquer tout trafic malveillant (pas d'implémentation supplémentaire requise)
Patch virtuel	Corrige automatiquement les vulnérabilités avant que vous n'appliquiez des correctifs à votre serveur ou ne mettiez à jour votre code, ce qui vous laisse plus de temps pour appliquer des correctifs et tester des mises à jour.
Restriction par adresse IP ou par géolocalisation	Permet de mettre le trafic issu d'adresses IP ou de pays spécifiques sur liste noire ou blanche afin de bloquer les pirates informatiques
Peu de faux positifs	Un taux de faux positif de 1/50 millions garantissant que du trafic légitime vous atteint
Intégration complète des services CDN, permettant la transformation du contenu sortant	Latence réduite pour les visiteurs de vos sites (pas d'implémentation supplémentaire requise)
Ensembles de règles	
Apprentissage automatique combiné à une recherche axée sur la sécurité	Protège contre les vulnérabilités zero-day ou les nouvelles menaces avec des correctifs
Compatibilité avec la logique et le format ModSecurity	Vous permet d'importer facilement des ensembles de règles existants pour maintenir la protection existante
Ensembles de règles OWASP ModSecurity Core Rule Set	Protège contre les vulnérabilités OWASP, c'est-à-dire les failles sévères identifiées par l'Open Web Application Security Project (OWASP) (compris par défaut sans frais supplémentaires)
Ensembles de règles zero-day Cloudflare	Faites confiance au service de sécurité Cloudflare pour vous protéger contre les menaces identifiées parmi nos clients (compris par défaut sans frais supplémentaires)
Ensembles de règles adaptées aux plates-formes pour les CMS et les plates-formes de commerce en ligne	Bénéficiez d'une protection immédiate sans frais supplémentaires pour les plates-formes comme WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc.
Règles personnalisées	Couvrent des situations uniques à vos applications Web (compris par défaut sans frais supplémentaires pour les clients Business et Entreprise)
Paramètres WAF	
Blocage	Bloquer une attaque mettra fin aux actions avant qu'elles n'atteignent votre site Web.
Simulation	Pour tester les faux positifs, vous pouvez régler le pare-feu applicatif en mode Simulation. Il enregistrera alors la réponse à une attaque possible, sans blocage ni vérification.
Vérification	Une page de vérification demande aux visiteurs d'entrer un CAPTCHA pour pouvoir se rendre sur le site Web.
Paramètre de seuil/de sensibilité	Paramétrez les règles pour configurer leur déclenchement en fonction de la sensibilité.
Pages de blocage personnalisables	Personnalisez la page vers laquelle les visiteurs sont redirigés en cas de blocage. Par exemple : « Appelez ce numéro de téléphone si vous avez besoin d'assistance. » Disponible pour les clients Entreprise.
Création de rapports	
Journalisation en temps réel	Gagnez en visibilité pour régler le WAF avec précision
Accès aux fichiers journaux bruts	Les clients de l'offre Entreprise peuvent lancer des analyses en profondeur de l'ensemble des requêtes WAF
Administration	
Haute disponibilité : basé sur des SLA d'offre de service	Les clients Business et Entreprise jouissent d'un temps d'activité garanti de 100 %, avec remboursement au cas où cette garantie n'est pas respectée
Aucun matériel, logiciel ou réglage requis	Inscrivez-vous avec un simple changement dans le DNS
Certification PCI	Cloudflare a reçu un certificat de fournisseur de services de niveau 1