CLOUDFLARE

FICHE TECHNIQUE

Cloudflare API Shield

Déployer Cloudflare comme passerelle de sécurité pour vos API leur assure de soutenir votre activité comme jamais auparavant.

Les API sont au cœur de toutes les activités, et près de 58 % du trafic Internet mondial est lié à celles-ci. Les acteurs malveillants en sont conscients, et Gartner estime que les API deviendront bientôt le vecteur d'attaque le plus fréquent.

La solution Cloudflare API Shield préserve la sécurité et la productivité des API grâce à ses fonctions d'identification des API et à ses défenses en couches innovantes. API Shield fait partie du portefeuille de solutions de sécurité des applications de Cloudflare, qui permettent également d'arrêter les bots, de déjouer les attaques DDoS, de bloquer les attaques contre les applications et de surveiller les attaques contre la chaîne logistique.

Nos produits de sécurité des applications s'intègrent étroitement à notre suite d'amélioration des performances, mise en œuvre depuis la plateforme cloud mondiale la plus connectée du marché.

Innovation en matière de sécurité des API

La solution API Shield identifie toutes les API utilisées et assure leur sécurité grâce à une protection en couches. API Shield inclut nos exceptionnelles solutions de protection contre les attaques DDoS sur la couche réseau et la couche application, offrant une protection supplémentaire.

Identification des API

L'identification automatique des API permet d'éliminer les API fantômes en assurant l'identification et la surveillance des points de terminaison d'API, permettant une meilleure gestion des API.

Validation des schémas d'API

Sécurisez vos API avec un modèle de sécurité positive reposant sur un schéma d'API. Une fois votre schéma OpenAPI v3 en place, les requêtes seront automatiquement validées en fonction de celui-ci, et toute opération non conforme au schéma sera bloquée.

Une authentification plus robuste

Vérifiez l'identité en fonction des certificats grâce au protocole Mutual TLS (mTLS). Géré par Cloudflare, ce modèle fondé sur une liste d'autorisation est important pour les appareils mobiles et IdO, permettant de bloquer les requêtes sans certificat en cours de validité. Cloudflare contrôle également l'utilisation d'identifiants dérobés.

Mettre fin aux utilisations abusives et aux pertes de données

La fonctionnalité avancée de détection des anomalies bloque le trafic abusif et volumétrique lié aux API en fonction de l'analyse du volume particulier d'une API. Le réseau Cloudflare propose également une fonction de prévention des pertes de données, permettant de détecter et de bloquer l'exfiltration d'informations sensibles dans les réponses d'API.

Principaux risques pour la sécurité des API

En raison des défis que présentent les API en matière de sécurité, OWASP a publié le classement « Top Ten » des plus importants risques ciblant les API. Cloudflare vous aidera à faire face à l'ensemble des risques affectant les API recensés par OWASP. Vous trouverez ci-dessous une liste décrivant certaines des principales préoccupations.

Broken Object Level Authorization

Une attaque par violation de l'autorisation au niveau de l'objet désigne la manipulation d'identifiants d'objets au sein d'une requête afin d'obtenir un accès non autorisé à des données sensibles. Dans une attaque BOLA, les acteurs malveillants accèdent à des objets (données) auxquels ils ne devraient pas avoir accès, en modifiant simplement les identifiants.

Broken User Authentication

L'authentification constitue un élément essentiel, qui est toutefois souvent incorrectement mis en œuvre. Les acteurs malveillants exploitent les failles (ou l'absence d'authentification) afin de se connecter de manière illicite ou d'usurper l'identité d'un autre utilisateur. La sécurité des API est compromise si les systèmes ne parviennent pas à authentifier correctement les clients ou les utilisateurs.

Lack of Resources & Rate Limiting

En l'absence de mesures adéquates de protection contre l'utilisation abusive ou de limites de débit permettant de restreindre la taille ou le nombre de ressources demandées, les API restent vulnérables aux attaques par force brute ou par déni de service, et les performances des serveurs d'API en souffrent.

Improper Assets Management

Une gestion erronée des ressources survient en l'absence de fonctionnalité d'identification des API capable d'assurer la surveillance des API de production actuellement utilisées et des API abandonnées, entraînant la présence d'API fantômes ou indésirables. Ce problème peut également résulter d'une mauvaise journalisation de l'activité des API.

Une sécurité des applications de renommée mondiale

La protection la plus précise

Trouvez toujours le point d'équilibre entre votre sécurité et votre activité grâce à des mesures de protection précises contre les menaces, les bots et les attaques ciblant les API. Les solutions Cloudflare ont été testées et optimisées pour les plus grandes entreprises.

Une vaste capacité intégrée

Pas de bases de code d'acquisition assemblées à la hâte, mais une sécurité intégrée et pilotable depuis une console unique, qui affûte continuellement sa capacité à bloquer les menaces. Toutes nos solutions d'amélioration des performances, telles que le réseau CDN, le DNS et l'accélération du trafic, sont intégrées.

Des stratégies de sécurité complètes

Nous proposons des fonctionnalités complètes et rentables, adaptées aux entreprises. Nous ne grèverons jamais vos finances en vous proposant des offres de base limitées, nécessitant des ajouts coûteux ou des intégrations tierces disponibles sur les marketplaces pour assurer une stratégie de sécurité solide.

Prééminence de Cloudflare

Les entreprises bénéficient d'une stratégie de sécurité des applications plus efficace en utilisant le réseau mondial de Cloudflare comme leur périmètre de sécurité. Le portefeuille de solutions de sécurité des applications de Cloudflare a reçu de nombreuses récompenses pour sa fiabilité et son étendue. Gartner a désigné le pare-feu WAF de Cloudflare « Customer's Choice » en 2021. Frost & Sullivan a décerné à Cloudflare le titre de « Innovation Leader » dans la catégorie « Global Holistic Web Protection », tandis qu'IDC et Forrester ont désigné l'entreprise leader dans la catégorie des solutions de protection contre les attaques DDoS.