Cloudflare API Shield

Gérez et sécurisez les API qui soutiennent votre activité

Les problématiques modernes liées aux API

Dans le collimateur des acteurs malveillants

Le monde moderne tourne autour des API. 58 % du trafic HTTP dynamique circulant sur le réseau Cloudflare présente un lien avec ces dernières.

En permettant aux entreprises de proposer leurs produits plus rapidement et d'améliorer l'expérience client, les API présentent des opportunités opérationnelles particulièrement porteuses. Les responsables de la sécurité et de l'IT d'aujourd'hui doivent trouver un équilibre entre la sécurisation de leurs API et celle de leurs applications web, sans ralentir l'innovation.

Les équipes chargées de l'IT et de la sécurité doivent sécuriser les données sensibles de leurs clients, tout en permettant le bon déroulement des activités sur l'ensemble des applications et des API web.

La confiance des clients est en jeu, après tout.

Cloudflare API Shield

Les clients peuvent identifier, sécuriser et simplifier la sécurité et la gestion de leurs API publiques en consolidant leurs mesures de protection WAAP (Web Application and API Protection, protection des API et des applications web) à la périphérie du réseau Cloudflare.

Le service API Shield fait partie du catalogue de sécurité des applications proposé par Cloudflare, dont les produits permettent également d'arrêter les bots, de déjouer les attaques DDoS, de bloquer les attaques sur les applications et de surveiller les attaques sur la chaîne d'approvisionnement (supply chain).

Risques liés aux API clandestines (Shadow API)

Les équipes de développement lancent souvent de nouvelles API sans en informer le service informatique. Ces API s'exécutent alors « dans l'ombre », sans gestion ni sécurité.

Inquiétudes liées à l'authentification, à la perte de données et à l'utilisation abusive

Une fois identifiées, les API doivent être protégées contre les attaques et l'utilisation abusive à l'aide de solutions d'authentification, de validation de schémas, de protection contre l'utilisation abusive des API et de détection de l'exfiltration de données.

Surveillance des performances des API

Les API sont le moteur de l'activité. Une fois ces dernières surveillées et sécurisées, les entreprises doivent donc garder un œil sur leurs performances, notamment en analysant le volume de requêtes par point de terminaison, le taux d'erreur et la latence.

CLOUDFLARE

PRÉSENTATION DE SOLUTION

Cloudflare API Shield

Gérez et sécurisez les API qui soutiennent votre activité

Principales fonctionnalités	
Gestion des API	
Identification et apprentissage des schémas	Identifiez les points de terminaison d'API activement utilisés et leurs schémas associés grâce à des modèles pilotés par apprentissage automatique (Machine Learning) et basés sur l'heuristique.
Analyses des séquences et des performances	Identifiez les séquences les plus importantes en matière de comportement des appels d'API et analysez les performances de vos points de terminaison d'API (p. ex. les requêtes, la latence, le taux d'erreurs, le volume des réponses, etc.).
Portail développeurs et gestion	Gérez la documentation interactive de vos API et hébergez-la sur votre domaine grâce à Cloudflare Pages.
Sécurité des API	
Validation de l'authentification	Authentifiez et validez le trafic de vos API à l'aide de certificats mTLS, de JSON Web Tokens (JWT), de clés d'API et de jetons OAuth 2.0 afin de bloquer les requêtes de clients illégitimes.
Validation de schémas	Utilisez les schémas d'API pour accepter les requêtes valides aux API et bloquer les requêtes mal formées et les anomalies HTTP. Cette approche vient compléter le modèle de sécurité négative du pare-feu Cloudflare WAF pour une sécurité plus complète.
Protection contre l'utilisation abusive du REST et du GraphQL	Arrêtez les abus volumétriques et séquentiels à l'aide de suggestions de contrôle du volume des requêtes en fonction de la session et du point de terminaison. Étendez vos protections contre les attaques par déni de service (DoS) aux points de terminaison GraphQL.
Détection des données sensibles	Détectez les données sensibles contenues dans les réponses d'API qui quittent votre serveur d'origine et recevez des alertes de chaque point de terminaison.
Plateforme intégrée	Les solutions de sécurité des applications Cloudflare sont gérées par l'intermédiaire d'une console unique et intégrée assurant toutes les tâches : triage, règles et analyses.

Avantages du produit

- Réduction des risques liés à la surface d'attaque et des cyber-risques
- Amélioration des performances des API
- Réduction de la charge opérationnelle (temps et coûts)
- Consolidation sur une plateforme unifiée d'outils d'amélioration des performance et de la sécurité pour l'ensemble de vos applications web et de vos API

RÉV. : PMM-JAN-2025

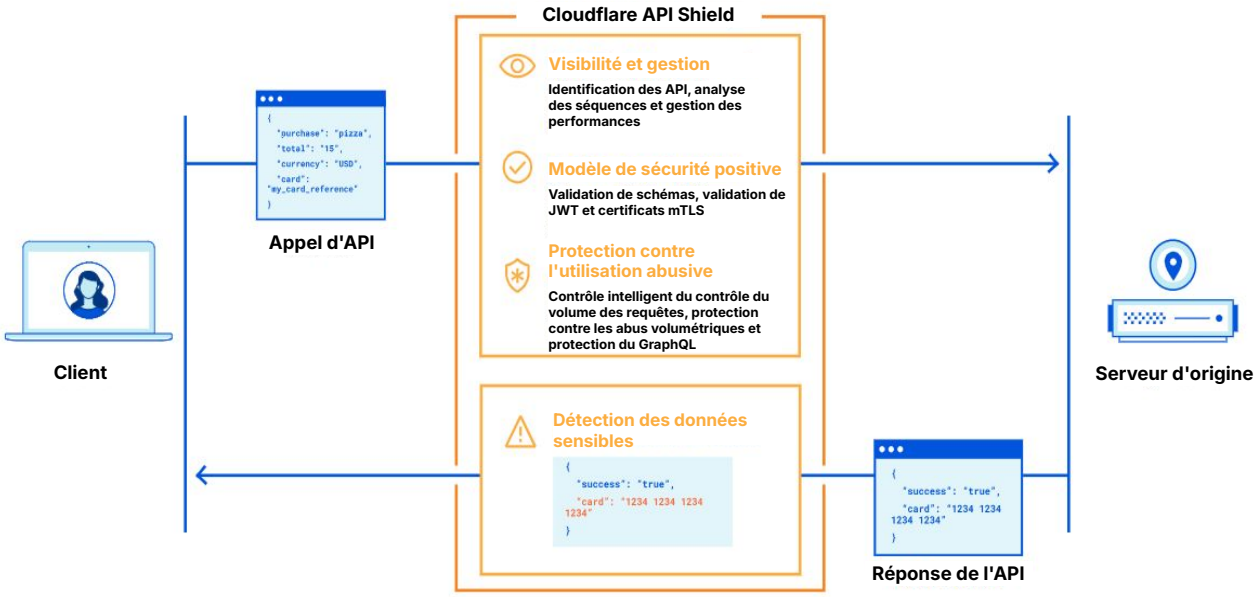

Figure 1 : l'architecture du service Cloudflare API Shield

Prééminence de Cloudflare

Le catalogue de solutions de sécurité des applications proposées par Cloudflare a reçu de nombreux éloges pour sa robustesse et son étendue. Cloudflare fait partie des Leaders dans le dernier rapport Forrester Wave™ consacré aux pare-feu applicatifs web (Web Application Firewalls). Gartner a été reconnue comme Leader dans la catégorie « Choix des clients » (Customers' Choice) en matière de solutions d'atténuation des attaques DDoS dans le rapport Gartner® Peer Insights™ « Voice of the Customer: DDoS Mitigation Solutions » (La voix des clients : solutions d'atténuation des attaques DDoS) 2023. Forrester a désigné Cloudflare comme Strong Performer (Fournisseur performant) dans le rapport The Forrester Wave™ consacré à la gestion des bots du troisième trimestre 2024. IDC a désigné Cloudflare comme Major Player (Acteur majeur) dans l'édition 2024 de l'IDC MarketScape consacré aux plateformes de protection des API et des applications web (WAAP, Web Application and API Protection) destinées aux entreprises.