CLOUDFLARE

L'état de la gestion et de la sécurité des API

Les interfaces de programmation d'applications (Application Programming Interfaces, API) entraînent de nouvelles expériences dans les applications, du suivi des données médicales à la personnalisation des jeux en ligne. Elles sont également source d'innombrables avantages opérationnels, comme l'analyse des clients, les intégrations SaaS et les fonctionnalités d'IA générative, parmi bien d'autres.

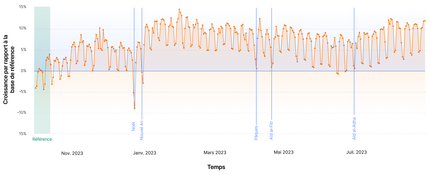
En parallèle, les API se montrent complexes à gérer et sont constamment sous attaque. Découvrez les tendances en matière de sécurité et de gestion du trafic lié aux API, qui constitue désormais **plus de la moitié (57 %) de l'ensemble du trafic Internet dynamique***.

30,7 %

Nous avons identifié près de 31 % de points de terminaison d'API REST supplémentaires via l'apprentissage automatique (Machine Learning) plutôt qu'à l'aide d'identifiants de session fournis par les clients.

Un monde orienté API

Dans l'ensemble, le trafic d'API total à l'échelle mondiale a augmenté régulièrement tout au long de l'année 2023.



Les dix secteurs principaux présentant la part la plus élevée de trafic lié aux API par rapport à leur trafic web total

1. Plateformes communautaires IdO
2. Trains, bus et taxis
3. Services juridiques
4. Multimédia, jeux et logiciels graphiques
5. Logistique, approvisionnement et transport
6. Électronique grand public
7. Logiciels financiers
8. Services de sécurité et d'investigation
9. Banque, assurances et services financiers
10. Appareils médicaux

API non protégées

Les entreprises qui ne disposent pas d'un inventaire complet de leurs API risquent de se retrouver avec des API « fantômes », qui constituent essentiellement des surfaces d'attaque dissimulées.

59,2 %

Le fait de proposer l'accès « en écriture » à la mauvaise personne peut conduire à des risques de sécurité.
De nombreuses entreprises (59,2 %) accordent un accès « en écriture » (la capacité d'effectuer des mises à jour) à au moins la moitié de leurs API.

Plus de 15 000

Plus de 15 000 comptes utilisateurs de Cloudflare présentaient des points de terminaison qui ont uniquement pu être identifiés à l'aide de méthodes reposant sur le Machine Learning.

Vulnérabilités courantes affectant les API

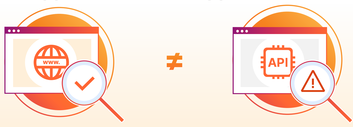
La demande de solutions de sécurité et de gestion des API sur le marché a explosé parallèlement à la hausse du trafic, des erreurs et des attaques concernant les API.

La première menace envers les API
Les anomalies HTTP (la menace la plus fréquente envers les API) sont des signaux courants de requêtes malveillantes adressées aux API.

La première erreur affectant le trafic lié aux API
Plus de la moitié (51,6 %) des erreurs de trafic provenant des origines des API se composaient de **codes d'erreur « 429 » : « Trop de requêtes ».**

Première méthode d'atténuation
Un tiers des mesures d'atténuation des menaces liées aux API comprenaient le blocage d'attaques par déni de service distribué (DDoS).

Les défis liés à la protection des API par rapport à celle des applications web



Une application web

- Est **visible** de l'utilisateur final.
- Est **accessible aux utilisateurs finaux** par l'intermédiaire d'un navigateur web.
- **Visualise les données** du back-end (en utilisant le HTML, le CSS et le JavaScript) à l'aide de diverses interactions utilisateur.
- Est généralement protégée à l'aide d'un modèle de **« sécurité négative »** qui bloque le trafic malveillant connu.

Une API

- Est **invisible** à l'utilisateur d'une application.
- Permet **aux systèmes et aux applications** d'échanger des données.
- **Transporte les données** en accédant aux serveurs et aux applications à l'aide d'un format défini (le plus couramment, RESTful JSON, gRPC, XML ou GraphQL).
- Est plus efficacement protégée par l'intermédiaire d'un modèle de **« sécurité positive »** n'autorisant que le trafic validé et authentifié.

Trois moyens de protéger les API

Migrer vers un modèle de « sécurité positive » plutôt qu'un modèle de « sécurité négative »

Dans un modèle de « sécurité positive », le système n'accepte que le trafic d'API « connu pour être fiable » (la fiabilité étant définie par des schémas d'API). Il s'agit d'une approche plus efficace que la sécurité négative, qui ne se concentre que sur la limitation du trafic d'API « connu pour être malveillant ».

Appliquer l'apprentissage automatique pour libérer des ressources et réduire les coûts

L'apprentissage automatique (Machine Learning) peut identifier l'ensemble du trafic lié aux API (y compris les variations d'attaques), faire la différence entre les pics de trafic légitimes et le trafic malveillant lié aux bots, mais aussi traiter les autres tâches de gestion des API gourmandes en ressources.

Unifier le développement, la visibilité, les performances et la sécurité des applications

La connectivité cloud, qui permet la connectivité point à point (any-to-any) entre les réseaux, les clouds, les applications et les utilisateurs, assure le tissu conjonctif entre les services de déploiement d'applications et de défense en profondeur des API.

CLOUDFLARE

Vous souhaitez en savoir plus ?

Consultez l'intégralité du rapport Cloudflare 2024 consacré à la gestion et à la sécurité des API

Consulter le rapport

* Les conclusions et les données présentées dans cette infographie se basent sur les schémas de trafic agrégé observés par le réseau mondial de Cloudflare (notamment les services de pare-feu d'applications web, de protection contre les attaques DDoS, de gestion des bots et de passerelle d'API proposés par Cloudflare) entre le 1er octobre 2022 et le 31 août 2023.