CLOUDFLARE

Lo stato della sicurezza e della gestione delle API

Le interfacce di programmazione delle applicazioni (API) promuovono nuove esperienze con le app, dal monitoraggio dei dati sanitari alla personalizzazione dei giochi online. Inoltre, alimentano innumerevoli vantaggi aziendali: analisi dei clienti, integrazioni SaaS, capacità di IA generativa e altro ancora.

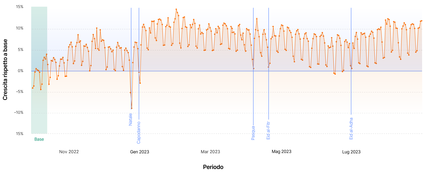
Allo stesso tempo, le API sono complesse da gestire e costantemente sotto attacco. Dai un'occhiata alle tendenze in materia di sicurezza e gestione del traffico API, che ora comprendono **più della metà (57%) di tutto il traffico dinamico di Internet*.**

30,7%

Quasi il 31% in più di endpoint REST API sono stati scoperti tramite il machine learning rispetto agli identificatori di sessione forniti dal cliente

Un mondo incentrato sulle API

Nel complesso, il traffico totale delle API in tutto il mondo è cresciuto costantemente nel corso del 2023.



I 10 principali settori con la quota più elevata di traffico API rispetto al traffico Web complessivo:

1. Piattaforma della community IoT
2. Ferrovia, autobus e taxi
3. Servizi legali
4. Multimedia, giochi e software grafico
5. Logistica, supply chain e trasporti
6. Elettronica di consumo
7. Software finanziario
8. Sicurezza e investigazioni
9. Servizi bancari, finanziari e assicurativi
10. Dispositivi medici

API non protette

Le organizzazioni che non dispongono di un inventario API completo rischiano di avere "API shadow", essenzialmente superfici di attacco nascoste:

59,2%

Fornire l'accesso in "scrittura" API alla persona sbagliata può portare a rischi per la sicurezza. Molte organizzazioni (59,2%) consentono l'accesso in "scrittura" (la possibilità di inviare aggiornamenti) ad almeno la metà delle proprie API.

Più di 15.000

Gli endpoint API di oltre 15.000 account che utilizzano Cloudflare sono stati scoperti solo tramite metodi di machine learning

Vulnerabilità API comuni

La domanda del mercato per la sicurezza e la gestione delle API è salita alle stelle parallelamente alla crescita del traffico, degli errori e degli attacchi API.

La minaccia numero 1 nei confronti delle API
Anomalie HTTP: la minaccia più frequente nei confronti delle API sono segnali comuni di richieste API dannose.

Il principale errore di traffico API
Più della metà (51,6%) degli errori di traffico provenienti dalle origini API comprendeva i **codici di errore '429': "Troppe richieste".**

Principale metodo di mitigazione
Un terzo delle mitigazioni API prevedeva il blocco degli attacchi DDoS (Distributed Denial of Service).

La sfida tra la protezione delle API e le app Web

e

Un'applicazione Web

- È **visibile** all'utente finale.
- È **accessibile dagli utenti finali** tramite browser Web.
- **Visualizza i dati** dal backend (tramite HTML, CSS e JavaScript) con interazioni utente variate.
- Di solito è protetto con un modello di "**sicurezza negativa**" che blocca il traffico dannoso.

Un'API

- È **invisibile** all'utente delle applicazioni
- Consente a **sistemi e applicazioni di** scambiare i dati
- **Trasferisce i dati** accedendo a server e applicazioni utilizzando un formato definito (più comunemente RESTful JSON, gRPC, XML, GraphQL).
- Viene protetto in maniera più efficace con un modello di "**sicurezza positiva**" che consente solo traffico confermato e autenticato.

Tre modi per difendere le API

Andare verso un modello di "sicurezza positiva" rispetto a un modello di "sicurezza negativa"

In un modello di sicurezza positivo, accetti solo il traffico API "definito come buono" (come definito dagli schemi API). Questo è più efficace della sicurezza negativa, che si concentra solo sulla limitazione del traffico API "definito come dannoso".

Applica il machine learning per liberare risorse e ridurre i costi

L'apprendimento automatico può scoprire tutto il traffico API (comprese le variazioni di attacco), distinguere tra picchi di traffico legittimo e traffico bot dannoso e gestire altre attività di gestione API ad uso intensivo di risorse.

Unifica lo sviluppo, la visibilità, le prestazioni e la sicurezza delle app

La connettività cloud, che consente la connettività any-to-any tra reti, cloud, app e utenti: fornisce un tessuto connettivo fondamentale tra lo sviluppo di app e i servizi approfonditi di difesa delle API.

CLOUDFLARE

Vuoi saperne di più?

Accedi al report completo sulla sicurezza e la gestione delle API 2024 di Cloudflare

Leggi il report

*I dati rilevati in questa infografica si basano su modelli di traffico aggregato osservati dalla rete globale di Cloudflare (inclusi il firewall per applicazioni Web di Cloudflare, la protezione da attacchi DDoS, la gestione del bot e i servizi gateway API) tra il 1° ottobre 2022 e il 31 agosto 2023.