CLOUDFLARE

The State of API Security and Management

Application programming interfaces (APIs) drive new app experiences — from tracking health data to personalizing online gaming. They also fuel countless business advantages: customer analytics, SaaS integrations, generative AI capabilities, and more.

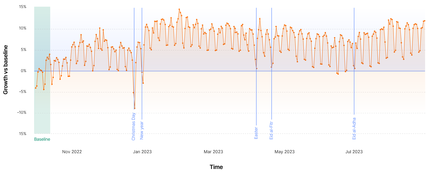
At the same time, APIs are complex to manage and constantly under attack. Take a look at security and management trends in API traffic — which now comprises **more than half (57%) of all dynamic Internet traffic*.**

30.7%

Nearly 31% more API REST endpoints were discovered through machine learning than through customer-provided session identifiers

An API-centric world

As a whole, total API traffic throughout the world grew steadily throughout 2023.



Top 10 industries with the highest share of API traffic out of their overall web traffic:

1. IoT Community Platforms
2. Rail, Bus & Taxi
3. Legal Services
4. Multimedia, Games & Graphic Software
5. Logistics, Supply Chain & Transportation
6. Consumer Electronics
7. Financial Software
8. Security and Investigations
9. Banking, Financial Services & Insurance
10. Medical Devices

Unprotected APIs

Organizations that lack a comprehensive API inventory risk having 'shadow APIs' — essentially hidden attack surfaces:

59.2%

Providing API 'write' access to the wrong person can lead to security risks. Many (59.2%) organizations permit 'write' access (the ability to push updates) to at least half of their APIs.

15,000+

More than 15,000 accounts using Cloudflare had API endpoints discovered through machine learning methods only

Common API vulnerabilities

Market demand for API security and management has skyrocketed in parallel to the growth of API traffic, errors, and attacks.

#1 threat toward APIs
HTTP anomalies — the most frequent threat toward APIs — are common signals of malicious API requests.

#1 API traffic error
More than half (51.6%) of traffic errors from API origins comprised **'429' error codes: "Too Many Requests."**

#1 mitigation method
One-third of API mitigations comprised blocking Distributed Denial of Service (DDoS) attacks

The challenge of protecting APIs vs. web apps

vs.

A web application

- Is **visible** to the end user
- Is **accessed by end users** through a web browser
- **Visualizes data** from the backend (using HTML, CSS, and JavaScript) with varied user interactions.
- Is typically protected through a **"negative security"** model that blocks known malicious traffic.

An API

- Is **invisible** to the app user
- Lets **systems and apps** exchange data
- **Transports data** by accessing servers and applications using a defined format (most commonly RESTful JSON, gRPC, XML, GraphQL).
- Is more effectively protected through a **"positive security"** model that only allows validated, authenticated traffic.

3 key ways to defend APIs

Move toward a "positive security" model vs. "negative security"

In a positive security model, you only accept "known good" API traffic (as defined by API schemas). This is more effective than negative security, which focuses only on restricting "known bad" API traffic.

Apply machine learning to free up resources and reduce costs

Machine learning can uncover all API traffic (including attack variations), differentiate between legitimate traffic spikes vs. malicious bot traffic, and manage other resource-intensive API management tasks.

Unify app development, visibility, performance, and security

A connectivity cloud — which enables any-to-any connectivity between networks, clouds, apps, and users — provides critical connective tissue between app development and API defense-in-depth services.

CLOUDFLARE

Want to learn more?

Access Cloudflare's full 2024 API Security and Management Report

Read Report

*The data findings throughout this infographic are based on aggregated traffic patterns observed by Cloudflare's global network (including Cloudflare's web application firewall, DDoS protection, bot management, and API gateway services) between Oct. 1, 2022 and Aug. 31, 2023.