CLOUDFLARE

DOCUMENT TYPE

Cloudflare API Gateway

Manage and secure the APIs that drive business

The API status quo

In attacker crosshairs

APIs make the world go around. 55% of global traffic on the Cloudflare network is API-related.

This means API endpoints must be tightly managed and secured. What's more, API are now firmly in the sights of attackers--Cloudflare currently blocks a greater percentage of API traffic than web traffic.

With APIs driving more business and representing an important attack vector, organizations must stay on top of many API challenges:

API Management

- Visibility into shadow APIs
- Managing endpoints
- Understanding API performance

API Security

- OWASP API top 10 attacks
- API abuse
- Data exfiltration

Cloudflare API Gateway

Cloudflare API Gateway keeps APIs secure and productive with API discovery, central API management and monitoring, and innovative, layered defenses. API Gateway is part of Cloudflare's application security portfolio that also stops bots, thwarts DDoS attacks, blocks application attacks and monitors for supply chain attacks.

API visibility and management

Many development teams push new APIs into production without notifying security or IT teams - leading to shadow APIs exposing the company to risk.

Security needs tools to help discover and register these APIs to then properly secure and management them.

OWASP API Top ten threats

Security must account for the OWASP list of API security risks. API security and management tools must offer protection against these attacks, including authentication and authorization issues, abuse (lack of resources), and improper assets management when lack of visibility and logging becomes an issue.

Stopping abuse and data loss

Attacks will often abuse and overwhelm APIs, necessitating new ways to throttle authenticated API sessions. Also, data must never be exfiltrated in the API response phase given APIs often share important, sensitive data.

API Gateway	
API Management	
API discovery	Discovery of API endpoints in use.
API management	Centrally register and manage endpoints discovered or added to the central API endpoint console.
API analytics	Understand API performance: total requests, latency, error rate, and response size, etc.
API Security	
mTLS authentication	One button mTLS authentication support to block requests from illegitimate clients.
Schema validation	Enforce positive security model based on uploaded API schema.
Abuse detection	Stop abuse with automated rate limiting based on observed traffic baselines in API discovery.
Sensitive data detection	Detect sensitive data leaving in API response phase.
Integrated Application Security	All application security (WAF, Bot Management, API security and management, Page Shield, mTLS,) is managed through an integrated console.

Why Cloudflare API Gateway

- Consolidated API management and API security in a single, unified console, eliminating the need for separate API Gateways and API security tools.
- Fully integrated into the Cloudflare Application Security portfolio that includes our WAF, Bot Management, Advanced Rate Limiting, Page Shield, and DDoS protection.
- API Gateway customers also utilize the Cloudflare Zero Trust portfolio, Workers serverless and storage, and our world-class performance portfolio.

Cloudflare Leadership

Organizations gain a more effective application security posture with the Cloudflare global network as their enterprise security perimeter. The Cloudflare application security portfolio has received numerous accolades for its strength and breadth. Gartner named Cloudflare a leader in the 2022 Gartner® Magic Quadrant™ for Web Application and API Protection (WAAP). Gartner also named the Cloudflare WAF a 2022 Customer's Choice. Frost & Sullivan recognized Cloudflare as an Innovation Leader in the 2020 Global Holistic Web Protection while IDC and Forrester named the company a 2021 DDoS leader.