Cloudflare API Shield

With Cloudflare as your API security gateway, APIs will drive business like never before.

APIs make the world go around - some 58% of global internet traffic is API-related. Attackers know this, prompting Gartner to estimate that APIs will soon become the most frequent attack vector.

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

Our application security products work closely with our performance suite, delivered by the world's most-connected global cloud platform.

API Security Innovation

API Shield discovers all APIs in use while delivering layered API security. Our world-class DDoS protections at the network and application layers accompany API Shield for additional protection.

API discovery

Automatic API discovery eliminates shadow APIs by ensuring all API endpoints are discovered and monitored for better API management.

Stronger authentication

Verify certificate-based identity with mutual TLS (mTLS). This allowlist model, managed by Cloudflare, is important for mobile and IoT devices, blocking requests without a valid certificate. Cloudflare also checks for stolen credentials being used.

API schema validation

Secure APIs with a positive security model, that enforces on an API schema. With an OpenAPI v3 schema in place, requests will automatically be validated against it. Any operations that do not conform to the schema are blocked.

Stopping abuse and data loss

Advanced anomaly detection stops abusive, volumetric API traffic based on an understanding of an API's particular volume. The Cloudflare network also delivers data loss prevention that detects and blocks exfiltration of sensitive information in API responses.

Key API security risks

Given the security challenges APIs present, OWASP released a top ten list of API security risks that must be accounted for. Cloudflare will help with all OWASP API risks - see a few top concerns outlined below.

Broken object level authorization

Broken object level authorization (BOLA) is manipulation of object IDs within a request to gain unauthorized access to sensitive data. With BOLA, attackers access objects (data) that they should not have access to, by merely changing the IDs.

Broken User Authentication

Authentication is critical but is often implemented improperly. Attackers exploit flaws (or lack of authentication) to log-in illicitly or assume another user's identity. API security is compromised if systems can't correctly authenticate clients/users.

Lack of Resources & Rate Limiting

Without proper abuse protections and rate limits that restrict the size or number of resources requested, APIs are susceptible to brute force and denial of service attacks, while API server performance suffers.

Improper Assets Management

Improper assets management occurs when there is no API discovery that tracks both current, production APIs and those that have been deprecated, leading to shadow or rogue APIs. This can also occur via poor API activity logging.

World-class application security

The most precise protection

Always thread the needle between security and business with precise protections against API threats, bots and attacks. Cloudflare has been tested and tuned for the largest businesses.

Vast integrated capability

No slapdash acquisition code bases thrown together. Rather, integrated security, from a single console, constantly sharpening its threat stopping ability. Performance like CDN, DNS, and traffic acceleration is all built-in.

Comprehensive security postures

We deliver full, enterprise-ready, cost-effective security capabilities. We'll never bleed you dry with limited base offerings requiring expensive add-ons or 3rd party marketplace integrations for a strong security posture.

Gartner peerinsights customers' choice 2021 ™

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 the Cloudflare WAF a 2021 Customer's Choice. Frost & Sullivan recognized Cloudflare as an Innovation Leader in Global Holistic Web Protection while IDC and Forrester named the company the DDoS leader.