CLOUDFLARE

SOLUTION BRIEF

The power of consolidated API protection

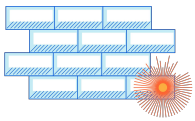
Modern application security requires an integrated API Gateway and Web Application Firewall (WAF)

APIs present a unique attack surface from web apps - from the very purpose of APIs in transferring data between systems to the variety of data formats.

With the fast growth in APIs, both behind modern web apps and as standalone external APIs, security teams are worried about API risks, sophisticated bots, client-side malware risks on top of web applications. The security risks with APIs include shadow APIs, authentication abuse, data loss, availability abuse, and vulnerability exploitation.

Modern CISOs require an API Gateway integrated with the rest of their application security solutions - WAF, Bot Management, API-centric Rate Limiting and Client-Side Protection.

Customers and Analyst Recognition



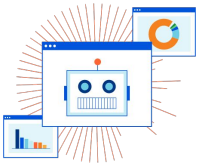
2023 GigaOM Radar for Application & API Security: LEADER

2022 Gartner Magic Quadrant for Web Application and API Protection: LEADER

2022 Forrester Wave for Web Application Firewall: LEADER

2022 Gartner Peer Insights 'Voice of the Customer': WAAP: Customer's Choice LEADER

2022 Gartner Critical Capabilities for Cloud Web Application Firewall: TOP 3 SHORT-LIST for 'Core Security' & 'Web-Scale' Business Applications



2022 Forrester Wave for Bot Management: STRONG PERFORMER

2020 QKS Bot Management Market: TECHNOLOGY LEADER

APIs and their unique attributes

	Web Apps	Modern APIs
Who interacts with app/API	Human to system	System to system
Data formats	Flexible (e.g.: JavaScript, HTML, CSS)	Structured & machine readable (e.g.: JSON)
Request and response structure	Flexible (usually contains no request body) and returns views	Defined by API schema (contains a request body) and returns only data
Typical Threats	DDoS, Malicious Bots, OWASP Top 10 Web App Risks (e.g.: SQL Injection, Cross-site scripting)	Abuse, Data Exfiltration, Malicious Bots, OWASP Top 10 API Risks (e.g.: Broken access controls in authorisation and authentication)

Key Challenges for CISOs with APIs

Shadow API risks

Companies must track and formally manage all their API endpoints that expose data. Development teams often publish new APIs without telling others in IT, so APIs are operating in the shadows without management or security.

Authentication, data loss and abuse concerns

Once APIs are discovered, they must be secured from attacks and abuse with authentication, schema validation, API abuse protections, and data exfiltration detections.

API performance monitoring

Given APIs drive business, once APIs are monitored and secured, companies must keep an eye on their performance: understand request volumes per endpoint, error rates, latency.

The power of consolidated API protection

WAFs protect organizations from new and known application attacks and exploits such as SQL injection attacks in web apps and APIs. API Gateways extend those protections to the unique risks in APIs such as API discovery and authentication management

	Traditional WAF	Cloudflare API Gateway
Customer use cases		
Health/performance analytics	Web app & bot traffic	Web app, bot and API traffic
Zero-day vulnerabilities	✓	✓
JavaScript supply chain attacks	✓	✓
Web app threats (e.g.: XSS, SQLi)	✓	✓
API threats (e.g.: Broken authorization)	✓	✓
Abuse protection (DDoS, Credential Stuffing, Inventory Hoarding)	✓	✓
Data exfiltration & compliance		✓
Positive security model		✓
API discovery and management		✓
Schema discovery and validation		✓
Authentication management		✓

LEGEND ✓ WAF ✓ WAF + API Gateway ✓ API Gateway

The Cloudflare application security portfolio

Cloudflare keeps applications and APIs secure and productive, thwarts DDoS attacks, keeps bots at bay, detects anomalies and malicious payloads, and encrypts data in motion, all while monitoring for browser supply chain attacks.