CLOUDFLARE

SOLUTION BRIEF

Security for application programming interfaces (APIs)

The power of consolidated API protection

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.

Application Programming Interfaces (APIs) and their unique attributes

	Web Apps	**Modern APIs**
Key user persona	Human to system. Built for humans	System to system. Built for apps
HTTP data formats	Flexible (e.g.: JavaScript, HTML, CSS)	Structured (e.g.: JSON, XML)
Request and response structure	• Accepts all requests (usually contains no request body) • Returns data for human consumption.	• Defined by API schema (contains a request body) • Returns only data for machine consumption
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)

Cloudflare provides a consolidated solution for API security

Modern security and development teams require API security that is an integral and consolidated part of their existing application security processes - across API discovery, data leakage, real-time OWASP Top 10 and abuse protection, and performance analytics.

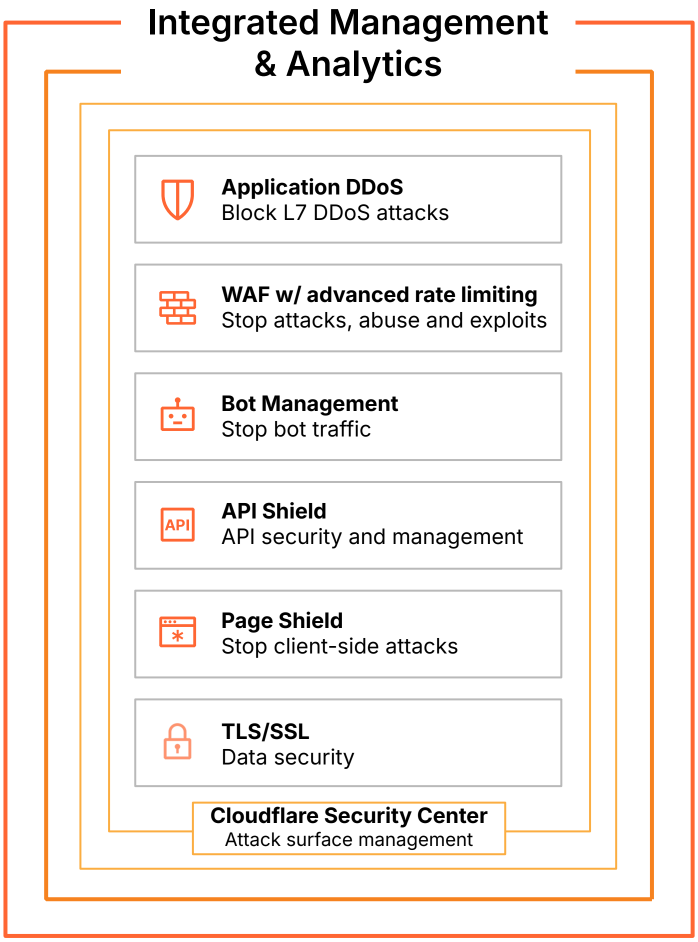
Web Application Firewalls (WAFs) protect organizations from new and known application attacks and exploits such as SQL injection attacks in web apps and APIs. API security tools extend those protections to the unique risks in APIs such as API discovery and authentication management

Consolidated API security requirements	Traditional WAF	Cloudflare API Shield
Health/performance analytics	**Web app & bot traffic**	**Web app, bot and API traffic**
Web app & zero-day threats (e.g.: 0-day vulnerabilities, XSS, SQLi)	✓	✓
JavaScript supply chain attacks	✓	✓
Data exfiltration & compliance	✓	✓
Abuse protection (DDoS, Credential Stuffing, Inventory Hoarding)	✓	✓
API threats (e.g.: BOLA, sequence analysis)		✓
Positive security model		✓
API discovery and management		✓
Schema discovery and validation		✓
Authentication management		✓

LEGEND ✓ **WAF** ✓ **WAF + API Shield** ✓ **API Shield**

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.



Integrated Management & Analytics

Application DDoS
Block L7 DDoS attacks

WAF w/ advanced rate limiting
Stop attacks, abuse and exploits

Bot Management
Stop bot traffic

API Shield
API security and management

Page Shield
Stop client-side attacks

TLS/SSL
Data security

Cloudflare Security Center
Attack surface management

Leadership recognised over 60x by top 3 analyst firms

Gartner
Recognized in **28 reports**

FORRESTER
Recognized in **22 reports**

IDC
Recognized in **11 reports**

LEADER in Forrester Wave for Web Application Firewalls (2022)
LEADER in Gartner® Peer Insights™ "Voice of the Customer": DDoS Mitigation Solutions (2023)
STRONG PERFORMER in Forrester Wave™: Bot Management Software (2024)