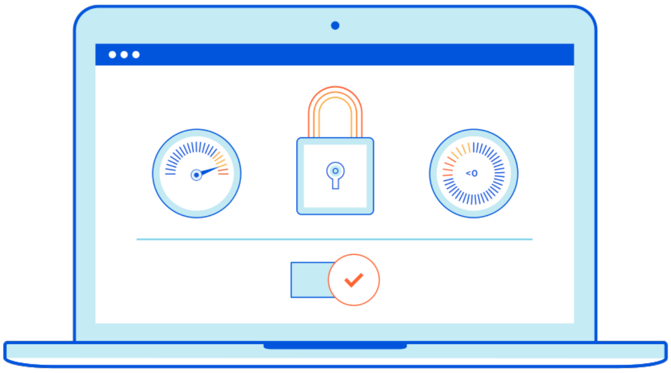
Cloudflare Advanced Rate Limiting

Protect your applications and APIs with powerful, granular rate limiting controls from Cloudflare.



Cloudflare Advanced Rate Limiting protects against denial-of-service attacks, brute-force login attempts, API traffic surges and other types of abuse targeting APIs and applications.

Advanced Rate Limiting is integrated with our Web Application Firewall (WAF) and is part of Cloudflare's application security portfolio. The portfolio also stops bots, protects APIs, and monitors for malicious payloads and browser supply chain attacks.

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

Enterprise customers get unmetered Advanced Rate Limiting.

Key rate limiting use cases

Advanced Rate Limiting protects against a variety of scenarios where applications or APIs are being abused. Integration with Cloudflare WAF makes it easy to configure rate limiting rules and add them to any custom rule.

Layer 7 DDoS mitigation

Contain high precision distributed denial-of-service attacks with granular configuration options.

API protection

Stop volumetric abuse of APIs by counting traffic on specific API attributes such as tokens, API keys, or cookies.

Brute force & credential stuffing protection

Safeguard accounts and APIs against brute force login and credential stuffing attempts without inadvertently locking out legitimate users.

Content scraping protection

Protect website content and assets from bot scraping and unauthorized reuse by setting custom rate limiting rules for specific URLs.

Rate limiting that adapts to your business

Build flexible rate limiting rules that incorporate business logic to curb malicious traffic without penalizing legitimate users. Confidently configure thresholds, define and tier request parameters, and customize responses.

Configurable request thresholds

Define and tier thresholds that protect websites and APIs from suspicious requests. Choose from a range of configuration options including specific URLs, request methods, status codes, and request limits.

Customizable response actions

Trigger custom responses when request thresholds are hit, such as mitigation actions (Challenge, CAPTCHA), response codes (Error 401 - Unauthorized), timeouts, and blocking.

Traffic insights

Gain valuable insights into specific URLs of websites, applications, or API endpoints. See how much malicious traffic is blocked by rule, how many requests make it to your origin, and more.

Transparent and cost-effective

Enterprise customers get unmetered advanced rate limiting. Avoid unpredictable costs associated with traffic spikes and enumeration attacks.

World class application security

The most precise protection

Always thread the needle between security and business with precise protections against API threats, bots, and application 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.