Web Application Firewall

Protect your website against SQL injections, cross-site scripting attacks and more

Cloudflare's Web Application Firewall (WAF) protects your web application from a wide range of attacks including SQL injection, cross-site scripting (XSS), common application vulnerabilities, zero-day attacks, malicious bots and much more. Our customers include the Alexa-ranked Top 50, financial institutions, ecommerce companies and major enterprises. Fully-integrated with our DDoS protection, our WAF blocks millions of attacks daily, automatically learning from each new threat.

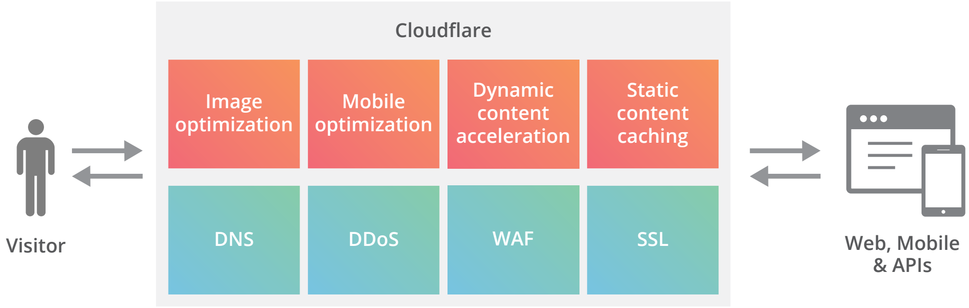
Cloudflare is listed in the top 3 "short-list" of Cloud WAF vendors for Public-Facing Web Applications and Web-Scale Critical Business Applications among 12 other Cloud WAF vendors in Gartner Critical Capabilities for Cloud Web Application Firewalls Services, 2019.

A robust rules engine customizable to your needs

Our WAF comes with a number of pre-built managed rule sets to protect you against the most critical web application security vulnerabilities. It also provides a powerful firewall rule engine editor with Wireshark-inspired syntax, allowing you to build your own customized rule sets. Once published, rules propagate globally and are effective in under 30 seconds.

Cloud deployment plus DDoS mitigation and performance

As a cloud-based service, Cloudflare's WAF requires no hardware or software to install and maintain. With an intuitive interface, the WAF is easy to onboard, use and manage, allowing you numerous customizations to meet your security needs. Cloudflare WAF integrates seamlessly with other products including Cloudflare DDoS protection, DNS, CDN, Bot Management and more.



Highlights:

- **Automatic protection** from diverse threats, with strong default rule sets and extensive customization providing Layer 7 protection that is fully integrated with DDoS mitigation
- **Lightning-fast 0.3 ms processing times,** with instant global updates
- **Real-time reporting** — robust logging and analytics lets you see what's happening instantaneously
- **Cloud deployment** with no hardware or software
- **Integrated** seamlessly with the larger Cloudflare feature set
- **Full API support** so you can integrate the WAF with your application, development pipeline or Terraform configuration

Key features	Benefit
Security	
Deep Packet Inspection, covering applications / Layer 7	Ensures your standard and custom web applications are always protected from SQL injection, cross-site scripting attacks and thousands more
SSL	Terminate SSL connections without any overhead or additional latency. Apply your WAF policy to SSL encrypted traffic without having to upload certificates or invest in costly hardware solutions
All request methods including Websockets	Covers all HTTP/S based traffic
URL-specific custom rule sets	Allows you to include/exclude specific URLs or subdomains for WAF protection to test domains or include/ exclude specific subdomains
DDoS mitigation integration	Allows full-stack protection against DDoS — no extra implementation required
IP reputation and bot mitigation integration	Real-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required
Virtual patching	Protects your web application against vulnerability before you patch your server or update your code, allowing you more time to patch and test updates
Restrict by IP or geolocation	Can blacklist/whitelist traffic from specific IP addresses, ASNs, or countries to protect against hackers from specific IPs or countries
Low false positive	Overall 1/50M false positive rate ensures legitimate traffic reaches you
Full integration with CDN service, offering outbound content transformation	Reduces web latency for your site visitors — no extra implementation required
Rule sets	
Automatic learning paired with security-driven research	Protects against zero-day vulnerabilities or new threats with patches automatically deployed by our security team
Fully customizable firewall rules	Allows you to easily build your own rules taking full advantage of the firewall capabilities
Core OWASP ModSecurity rule sets	Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP)
Zero-day Cloudflare rule sets	Rely on Cloudflare's security team to protect you against threats identified across our customer base
Platform-specific rule sets for major CMS and eCommerce platforms	Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, IIS and more
WAF settings	
Block	Blocking an attack will stop any action before it is sent to your website
Simulate	To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking.
Challenge/ JS challenge	A challenge page asks visitors to submit a CAPTCHA to continue to your website or a JavaScript problem to block and slow down bots
Threshold / sensitivity	For the OWASP rule set, rules to trigger more or less depending on sensitivity
Customizable block pages	Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers
Reporting	
Real-time logging	Gain visibility to help you fine-tune the WAF and import the logs into your SIEM with out-of-the-box integration with Splunk, Sumologic, Datadog and more
Powerful analytics	Filter and examine security event logs directly from the dashboard or leverage our GraphQL API
Access to raw log files	Enterprise customers can conduct in-depth analysis covering all WAF requests with out-of-the-box integrations with Amazon S3, GCP, Azure and more
Administration	
High availability — built on service offering SLAs	Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met
No hardware, software or tuning required	Sign up with a simple change in DNS
Compliance for PCI DSS requirement 6.6	Cloudflare's WAF enables you to cost-effectively fulfill PCI compliance