CLOUDFLARE

Web Application Firewall

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

CloudFlare's Web Application Firewall (WAF) protects your website from SQL injection, cross-site scripting (XSS) and zero-day attacks, including OWASP-identified vulnerabilities and threats targeting the application layer. 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.

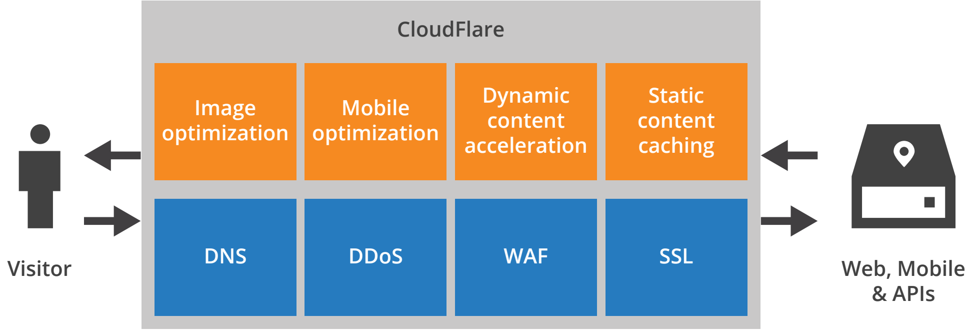
A robust rules engine to customize to your needs

Our WAF runs ModSecurity rule sets out of the box, protecting you against the most critical web application security flaws as identified by OWASP. It can also handle your existing rule sets and custom rules. Rules become effective in under 30 seconds.

Cloud deployment plus DDoS mitigation and CDN

As a cloud-based service, CloudFlare's WAF requires no hardware or software to install and maintain. Deploy the WAF with a single click, customizing it to meet your needs.

Its integration into the overall CloudFlare service means you get additional functionality for free. You can secure your website against DDoS attacks and use our global content delivery network to make it run faster.



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
- **Compliance for PCI DSS requirement 6.6** — CloudFlare's WAF enables you to cost-effectively fulfill PCI compliance
- **Real-time reporting** — robust logging lets you see what's happening instantaneously
- **Cloud deployment** with no hardware, software or tuning required

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.
For GET and POST HTTP/S requests	Covers range of HTTP/S 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 database integration	Real-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required
Virtual patching	Fixes a 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 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
Compatibility with ModSecurity logic and format	Allows you to easily import existing rule sets to maintain existing protection
Core OWASP ModSecurity rule sets	Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees
Zero-day CloudFlare rule sets	Rely on CloudFlare's security team to protect you against threats identified across our customer base — included as default with no extra fees
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, etc.
Custom rules	Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers
WAF settings	
Block	Blocking an attack will stop any action before it is posted 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	A challenge page asks visitors to submit a CAPTCHA to continue to your website.
Threshold / sensitivity setting	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
Access to raw log files	Enterprise customers can conduct in-depth analysis covering all WAF requests
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
PCI certification	CloudFlare's service has received Level 1 service provider certification