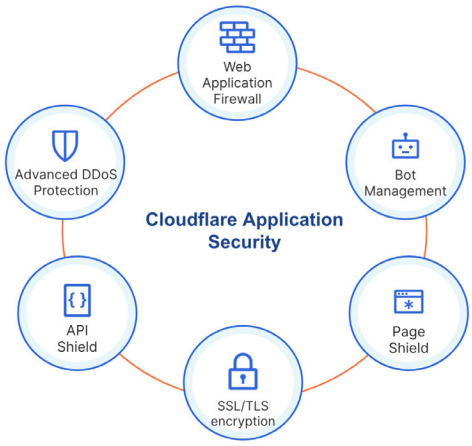
A WAF for Modern Application Security

Enterprises rely on applications and APIs for growth--and with world-class Cloudflare application security, expanding attack surfaces and novel attacks never get in the way.



The Cloudflare web application firewall (WAF) is the cornerstone of our advanced application security portfolio that keeps applications and APIs secure and productive, thwarts DDoS attacks, keeps bots at bay, detects anomalies and malicious payloads, all while monitoring for browser supply chain attacks.

Our powerful application security capabilities are integrated with the rest our leading application performance portfolio, all delivered from the world's most connected global cloud platform.

Cloudflare Web Application Firewall

Our WAF is delivered from our global edge network for enterprise-grade security, spanning over 250 cities in more than 100 countries for incredible performance and reliability, capable of unlimited, instant scaling.

Powerful Cloudflare protections

Cloudflare offers powerful rulesets that stop threats including newly discovered zero days, as well as bypasses and attack variations using machine learning. Additionally, with granular custom rules, you can configure the WAF to protect against any threat or implement business-specific security policies.

Fast deployment and easy management

Global WAF protection is in place in clicks. Nothing to deploy, no weeks-long training or professional services expenses. You have a single pane of glass to manage it all.

Better security from global intelligence

Our threat intelligence is constantly sharpened by insights gained from our global network processing 2 trillion daily requests, ensuring our WAF keeps organizations safer against emerging threats.

Global protection in seconds

Threats move fast - and our protections keep pace. New rules are active in seconds for instant protection unlike other WAFs that need 45 minutes or more to protect.

Application Security from the edge of the Internet

Organizations gain a more effective application security posture, whether apps are on-prem or in the cloud, with the Cloudflare global network as their enterprise security perimeter, that blocks 86 billion threats a day.

The fastest, most precise protection

Always thread the needle between security and business with precise protections, tested against vast amounts of traffic, that never block business. Our network ensures customers are protected up to 10x faster than competitors.

Vast integrated capability

No slapdash acquisition code bases thrown together. Rather, integrated security constantly sharpening its threat stopping ability. Performance like CDN, DNS, load balancing and traffic acceleration is all built in.

A Powerful Single Pane of Glass

Manage security easily and add new capabilities fast with our single console. No overly complex interfaces or rule syntax. Just powerful security from our single, intuitive console.

Comprehensive Security Postures

Our security capabilities always deliver full, enterprise-ready, cost-effective 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.

Enterprise Application Security

L7 security innovation

We include advanced protections against exposed credential usage and warnings on potentially infected 3rd party Javascript in your applications that may be performing supply chain based attacks.

SIEM-integrated, SOC-ready

With Cloudflare APIs and raw log integrations, it is easy to integrate with your SIEM or power your security operation center (SOC) with intelligence provided by Cloudflare.

DevSecOps made easier

Ready to shift security left? So are we. Our out-of-the-box Terraform integration makes incorporating application security into DevOps approaches second nature.

Cloudflare Recognition

We have received ongoing accolades for the effectiveness of our application security portfolio from practitioners and analysts alike.

- "Customers' Choice" for WAF in 2021 Gartner's Peer Insights report.
- Innovation Leader in the Frost & Sullivan Frost Radar™: Global Holistic Web Protection Market Report.
- Recognized as a 'Leader' in The Forrester Wave for

Key Features	Benefits
WEB APPLICATION SECURITY	
Layered protections from multiple WAF rulesets	Stops malicious payloads in any request component with multiple rulesets; • Cloudflare-managed rules • Third-party rulesets (OWASP Top Ten) • Custom rulesets to stop any attack
WAF ML: Machine learning based detections	Stop bypasses, attack variations, and anomalies by leveraging ML-generated attack scores in WAF custom rules.
Updated rules for zero-day protections	Rules continuously updated by Cloudflare security team for protection against novel attacks and zero-day vulnerabilities before patches or updates are available.
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 rule configuration	Choose from BLOCK, LOG, CHALLENGE, CAPTCHA CHALLENGE, RATE LIMIT and other options when deploying rules or rulesets.
Advanced rate limiting	Stop abuse, DDoS, and brute-force attempts targeting applications and APIs by rate limiting individual IPs or by header, ASN or country.
IP reputation database	Block connections from malicious IPs with real-time intelligence on over 1 billion unique IPs.
Data loss prevention	Block responses containing sensitive data such as personally identifiable information, financial Information, credit card numbers or secrets like API keys.
Exposed Credential Checks	Detect brute force attacks with stolen credentials before end user accounts are taken over.
SSL/TLS	Fully offload and configure SSL traffic for your application.
Fewer false positives	New rules tested on vast amounts of traffic to ensure the fewest false positives.
gRPC and Websocket support	Proxy and secure traffic for gRPC and Websocket endpoints.
Customizable block pages	Customize block pages with appropriate detail for visitors.

APPLICATION SECURITY CAPABILITIES	
Bot Mitigation	Protection against bots with sophisticated layered protections, visibility and challenge options
DDoS Mitigation	Allows full-stack protection against DDoS.
Client Side Security	Detect and block browser-based supply chain attacks.
API protections	Protect API traffic as defined by schemas or detected by Cloudflare's machine learning models.
REPORTING and PROGRAMMABILITY	
Real-time logging and raw log file access	Gain visibility to help you fine-tune the WAF; Conduct in-depth analysis covering all WAF requests.
Payload logging	Log and encrypt malicious payloads for incident analysis.
SIEM integrations	Push or pull logs directly into your existing SIEMs.
Terraform integration	Incorporate application security into CI/CD workflows.
MANAGEMENT	
Single console management	Streamlined management with a single console to deploy and manage global application security and performance.
High availability — built on service offering SLAs	100% uptime guarantee including financial penalties if SLAs are broken.
No hardware, software or tuning required	Deploy with a simple change in DNS.
PCI certification	Cloudflare possesses Level 1 service provider certification.