CLOUDFLARE

PRODUCT BRIEF

Cloudflare WAF

A WAF for modern application security

Application security challenges

Applications are as critical as ever to business, which is why they are relentlessly targeted by attackers, amounting to an expanded attack surface.

Concerns range from remaining protected against emerging zero-day exploits, to detecting evasion attempts, to reducing risk of credential stuffing that leads to account takeover, to detecting data loss, even scanning for malware uploads to applications.

These concerns are coupled with the need to ensure application protections are part of a broader, unified security posture, that also protects APIs, stops bots, and reduces client-side risks. All of this must happen while not burdening teams with undue management headaches.

Cloudflare WAF

The Cloudflare Web Application Firewall (WAF) is the cornerstone of our advanced application security portfolio that keeps applications secure and productive. Only the Cloudflare WAF provides full security visibility, delivers layered protections against OWASP attacks and emerging exploits, detects evasions and new attacks with machine learning, blocks account takeover, detects data loss, and more, protecting applications wherever they are hosted. Our powerful application security capabilities, such as API security and bot mitigation, are fully integrated with our WAF, calling on the same powerful rules engine, delivered from one of the world's first connectivity cloud.

Attack visibility and simple onboarding

We offer differentiated security analytics to visualize all traffic, mitigated or not. Immediate visibility into the threat landscape offers tangible return on investment, allowing teams to understand their attack traffic and the protections they should create right after onboarding.

Fast protections for emerging attacks

With tens of thousands of vulnerabilities per year, our WAF quickly adds new managed rules to block exploits of newly-discovered (0-day) vulnerabilities. Our managed rules block exploits complemented by machine learning-derived WAF attack scores, to detect evasions.

Threat intelligence powered a vast global network

Security efficacy starts with having the best data, and our vast global network proxies 20% of the Internet, giving us unparalleled insight into the threat landscape. This data powers machine learning models that we alongside traditional signature-based detections to find and mitigate attack attempts with high accuracy.

Application security challenges

Cloudflare protects more effectively.

We deliver more effective WAF security with layered protections:

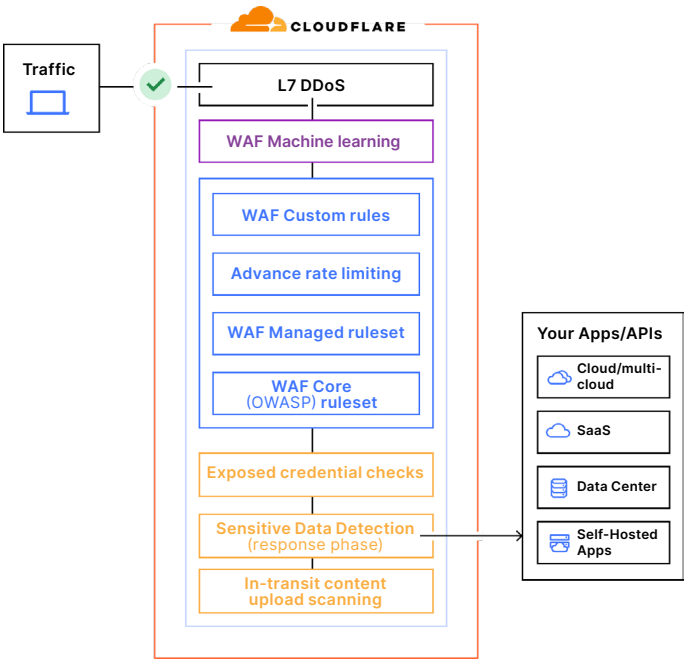
- Security analytics
- Multiple managed rulesets
- Custom rules
- Machine learning detections
- Sensitive data detection
- Stolen credential checks
- Advanced rate limiting
- Anti-malware upload scanning

Cloudflare responds faster.

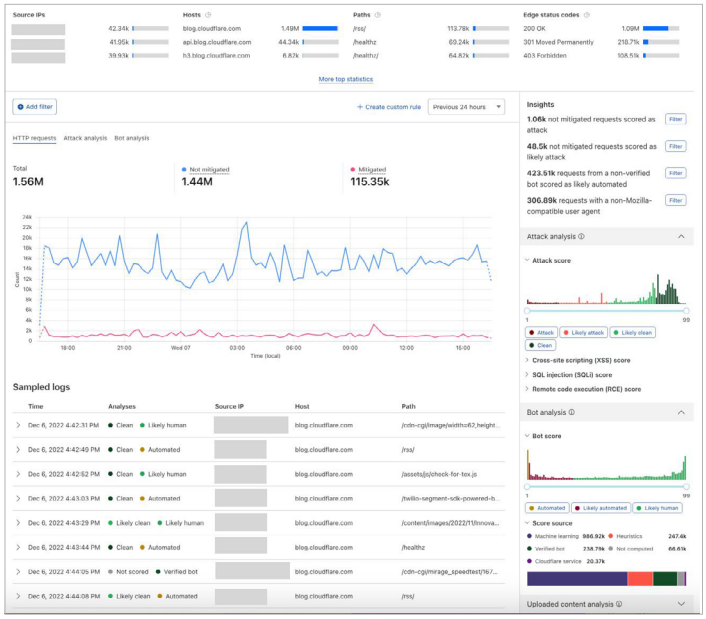
We protect faster against exploits. For major vulnerabilities like HTTP/2 Rapid Reset, Log4j, and many others, we had multiple managed rules in place a workday faster than other WAF vendors.

Cloudflare fully integrates application security.

Our WAF is fully integrated with the rest of our application security portfolio, including API Gateway and Bot management, all delivered in a single pass from Cloudflare's connectivity cloud.



WAF security analytics



A WAF for enterprise security

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

Our out-of-the-box Terraform integration makes incorporating application security into DevOps approaches second nature.

Backed by Cloudforce One

Cloudflare application security receives threat intelligence from Cloudforce One, our threat operations team, blocking threats via new detections based on emerging intelligence and TTPs.

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 Cloudflare a leader in the 2022 Gartner® Magic Quadrant™ for Web Application and API Protection (WAAP). Cloudflare was recognized as a Leader in The Forrester Wave™ for WAF. Gartner also named the Cloudflare WAF a 2022 Customer's Choice.

Gartner Peer Insights Customers' Choice 2022

Web Application Security	
Layered protections from multiple WAF rulesets	Stops malicious payloads in any request component with multiple rulesets: 1. Cloudflare-managed rules 2. OWASP Core Ruleset 3. Custom rules to stop any attack. New managed rules tested on vast amounts of traffic to ensure the fewest false positives.
Updated rules for zero-day protections	Rules continuously updated by Cloudflare security teams for protection against novel attacks and zero-day vulnerability exploits before patches or updates are available.
Machine learning detections	Stop bypass attempts with machine learning models to complement layered rulesets. Four different attack score are available for rules: overall WAF attack score, XSS attack score, SQLi attack score, RCE attack score.
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	Create a positive or negative security model by using the following actions: BLOCK, MANAGED CHALLENGE, JS CHALLENGE, SKIP, LOG, LEGACY CAPTCHA, CUSTOM RESPONSES 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 attribute (e.g. key, cookie, token), ASN or country.
Sensitive data detection	Detect responses containing sensitive data such as personally identifiable information, financial Information, credit card numbers or secrets like API keys.
Exposed credential checks	Detect credential stuffing attacks with stolen credentials before end user accounts are taken over.
Content upload scans	WAF content scanning will scan uploaded files for malwarend you can combine its signals with other parameters of the request by creating Custom Rules
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.
Full integration with the broader Cloudflare product suite	Improve application performance, geo route traffic and leverage edge computing.

Visibility, Reporting, and Programmability	
Security analytics	Visualization of all potential attacks, as scored by machine learning.
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 SIEM.
Terraform integration	Incorporate application security into CI/CD workflows.
Management	
Single console management	Detect responses containing sensitive data such as personally identifiable information, financial Information, credit card numbers or secrets like API keys.
Account-level management	Detect credential stuffing attacks with stolen credentials before end user accounts are taken over.
High availability — with SLAs	WAF content scanning will scan uploaded files for malwarend you can combine its signals with other parameters of the request by creating Custom Rules
No hardware, software or tuning required	Fully offload and configure SSL traffic for your application.
PCI certification	New rules tested on vast amounts of traffic to ensure the fewest false positives.
FedRAMP Authorized	Proxy and secure traffic for gRPC and Websocket endpoints.

REV:BDES-6052.2024AUG01