DDoS Protection with Cloudflare

Industry leading DDoS protection

Cloudflare has received the most number of 'High' ratings as compared to the other 6 DDoS vendors across 23 assessment criteria in Gartner's 2020 'Solution Comparison for DDoS Cloud Scrubbing Centers'

Cloudflare was named a "Leader" according to the 2019 'IDC MarketScape: Worldwide DDoS Prevention Solutions'

Cloudflare has been recognized as a "Leader" in the 2017 'Forrester Wave: DDoS Mitigation Solutions'

Distributed denial of service (DDoS) attacks are on the rise and have evolved into complex and overwhelming security challenges for organizations. Although DDoS attacks are not a recent phenomenon, the methods and resources available to conduct and mask such attacks have dramatically evolved. A milestone in the evolution of DDoS attacks is the formation of the Mirai botnet; this botnet consisted of over 300,000 hacked IoT devices used to generate the current largest known DDoS attack, with peak attack traffic exceeding 1 Tbps of throughput. According to Cloudflare's experience, anybody - large and small organizations - can be targeted. Even though many jurisdictions have laws under which DDOS attacks are illegal, there are DDOS-as-a-Service providers offering subscriptions, some starting as low as at $5 - $10/month. Lost revenue is only one of the many threats that these kinds of attacks can bring upon your website or business. DDoS impacts such as site inaccessibility brings about less quantifiable losses, such as brand degradation and worsening customer satisfaction.

A Scalable and Precise DDoS Solution

Cloudflare's global Anycast network has a network capacity of over 37 Tbps which is over 30x bigger than the largest DDoS attack ever recorded, allowing all internet assets on Cloudflare's network to withstand massive modern-day DDoS attacks. Cloudflare's DDoS protection for layers 3, 4, and 7 is delivered through every one of Cloudflare's 200+ data centers globally available at the network edge. Legacy DDoS protection solutions are based on scrubbing centers which act as 'choke-points', introducing latency and manual intervention in the face of sophisticated DDoS attacks. Cloudflare's unique and modern distributed architecture is built to the scale of modern-day threats, and can be used to mitigate DDoS attacks of all forms and sizes. Rate Limiting complements Cloudflare's DDoS protection by allowing for precise mitigation of the most sophisticated attacks against the application layer.

PROTECTION AGAINST LAYER 3/4/7 DDOS ATTACKS

Cloudflare's DDoS solution provides comprehensive DDoS protection against Layer 3, 4 and 7 DDoS attacks. A variety of DDoS attack techniques including DDoS amplification, SYN flood, ICMP flood and more which typically would overwhelm a unicast based network are quickly mitigated by Cloudflare's Anycast based network in under 10 ms. In addition to the massive network capacity Cloudflare's Anycast network is interconnected with over 600 Internet Exchanges, and peers with more than 8,800 networks globally, to simply absorb the attack traffic.

DDoS Protection Features

- Layers 3, 4, and 7 DDoS protection
- DNS attack protection
- Fine-grain threat blocking with Rate Limiting
- Predictive security with IP reputation database
- Unlimited and unmetered DDoS mitigation

"Thomson Reuters operates on-premise and cloud networks around the world. I'm excited about Cloudflare Magic Transit — the potential to unify our IP transit, DDoS mitigation, and traffic steering solutions into something we can manage with a single pane of glass will be game-changing. Cloudflare continues to impress me with its network's scale, in terms of geography, capacity, and product breadth."

- Jesse Haroldson,
Principal Software Architect,
Thomson Reuters

- Global Anycast network spanning Cloudflare data centers in over 200 cities globally
- 37+ Tbps throughput to absorb volumetric attacks
- Over 27 million Internet properties protected by Cloudflare

"The reason we use Cloudflare is because the security features are excellent, the CDN is high performing, and it's really convenient that these solutions are packaged together. It makes managing everything easy, and allows us to focus on our core business."

-Amanda Kleha GM, Zendesk Online Business Unit

PROTECTION AGAINST LAYER 7 APPLICATION VULNERABILITIES

Common types of Layer 7 attacks include SQL injection and Cross-Site Scripting (XSS), which might allow attackers to access and tamper with customer or any other kind of application data. Cloudflare addresses these threats via its Web Application Firewall (WAF). The WAF automatically blocks threats found in the OWASP top 10 rule set, Cloudflare's Managed Rules as well as custom rules that customers can create through Firewall Rules. Cloudflare has been able to protect their customers against known application vulnerabilities as well as zero-day vulnerabilities, including the Shellshock vulnerability and the Heartbleed Bug.

RATE LIMITING

Activate Cloudflare Rate Limiting for fine-grained traffic control that complements Cloudflare's DDoS protection and Web Application Firewall (WAF) services. Rate Limiting protects against denial-of-service attacks, brute-force password attempts, and other types of abusive behavior targeting the application layer. Configure request thresholds, define custom responses — such as mitigating actions (challenges or CAPTCHAS) or response codes — and gain analytical insights into endpoints of your website, application, or API.

Predictive Security

Cloudflare provides an automatic learning platform, where network traffic is analyzed in real time to identify anomalous or malicious requests. Over 1 billion unique IP addresses pass through Cloudflare's network every day, which enables us to continuously enhance our IP reputation database and deliver comprehensive DDoS protection. In addition, we harness the full power of Cloudflare's threat intelligence curated through machine learning models that continuously learn from the vast amount of traffic from over 27 million Internet properties protected by Cloudflare. Once a new attack is identified, Cloudflare automatically starts to block that attack type for both the particular website and the entire community.

Flat-Rate Bandwidth Pricing

Cloudflare provides unlimited and unmetered enterprise-grade DDoS protection at a flat monthly rate. Cloudflare believes that customers shouldn't be penalized for the spike in network traffic associated with a DDoS attack. Hence we never charge for the attack traffic. With Cloudflare DDoS protection, customers can rest assured that their website will stay online and they'll have a predictable monthly bill.

Sign up for Cloudflare

Sign up with Cloudflare and activate our advanced DDoS Protection, Rate Limiting, Web Application Firewall to protect your website, application, or APIs, while reducing latency and utilizing the latest web technologies. The set up is easy and usually takes less than 5 minutes to get up and running. Check out the plans, ranging from Free to Enterprise, at www.cloudflare.com.