CLOUDFLARE

Cloudflare Security Services

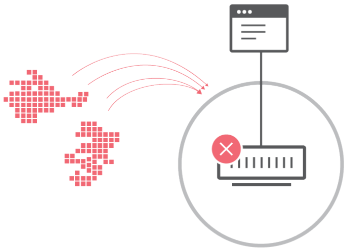
Cloudflare Security Services protect and secure Internet applications against denial-of-service attacks, customer data compromise, and abusive bots.

Mitigate DDoS Attacks

Protect Internet applications from malicious traffic targeting network and application layers, to maintain availability and performance, while containing operating costs.

SERVICES

- Anycast Network
- IP Reputation Database
- Heuristic-Based Mitigation
- Web Application Firewall (WAF)
- Rate Limiting
- DNS
- Spectrum
- Argo Tunnel



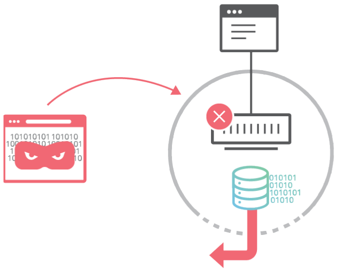
DDoS Attack
Attack traffic impacts availability or performance

Prevent Customer Data Breaches

Protect attackers from compromising sensitive customer data, such as user credentials, credit card information, and other personally identifiable information.

SERVICES

- Web Application Firewall (WAF)
- Rate Limiting
- DNS
- SSL / TLS 1.3
- Spectrum
- Access



Data Theft Attempt
Compromise of sensitive customer data

Block Malicious Bot Abuse

Block abusive bots from damaging Internet properties through content scraping, fraudulent checkout, and account takeover.

SERVICES

- IP Reputation Database
- Web Application Firewall (WAF)
- Rate Limiting

Bots
Prevent malicious bots from abusing site or application

Cloudflare Security Services

Global Anycast Network

With data centers in 180+ cities across 80 countries and 30 Tbps of capacity, Cloudflare's Anycast network absorbs distributed attack traffic by dispersing it geographically, while keeping Internet properties available and performant.

IP Reputation Database

Cloudflare's IP reputation database — with hundreds of millions of IPs — offers effective security intelligence by employing a data-driven security layer with real-time feedback, and a dynamic reputation scoring.

DNS

Cloudflare DNS is DDoS protection for domain resolution. It sits behind the same 30 Tbps network that protects over 16 million Internet properties from denial-of-service attacks. DNSSEC guarantees a web application's traffic is safely routed to the correct servers, so that visitors are not intercepted by an attacker.

Web Application Firewall (WAF)

Cloudflare's enterprise-grade web application firewall (WAF) detects and blocks common application layer vulnerabilities at the Cloudflare network edge, enforcing rulesets: OWASP Top 10, Cloudflare-built application, and custom created.

Rate Limiting

Rate Limiting protects critical resources by supplementing Cloudflare's DDoS protection with fine-grained control to block or qualify visitors with suspicious request rates.

SSL / TLS 1.3

Transport Security Layer (TLS) encryption enables HTTPS connections between visitors and origin server(s), preventing man-in-the-middle attacks, packet sniffing, the display of web browser trust warnings, and more.

Argo Tunnel

Cloudflare creates an encrypted tunnel between its nearest data center and an application's origin server without opening a public inbound port.

Cloudflare Spectrum

Spectrum protects TCP applications and ports from volumetric DDoS attacks and data theft by proxying non-web traffic through Cloudflare's Anycast network.

Heuristic-Based Mitigation

With Cloudflare's visibility into 16M Internet properties, our DDoS protection service develops heuristics based on attacks on one website to protect many others.

Access

A Zero Trust access control model which allows you to secure, authenticate, and monitor user access to any domain, application, or path on Cloudflare, without the need for a VPN.

CLOUDFLARE®

The Cloudflare Advantage

SCALE

Cloudflare's Anycast network of data centers in 180+ cities and 30 Tbps capacity can defend against volumetric attacks 10x bigger than the largest DDoS attack ever recorded. By observing over 745B request per day, Cloudflare proactively defends against threats by learning from attacks targeting more than 16 million Internet properties on its network.

EASE OF USE

Setting up Cloudflare takes as little as 5 minutes. Cloudflare's ease of use enables companies to expand Internet security policy responsibilities across more employees, reduce time to deploy new policies, and improve timely adjustments to the security posture of complex applications.

INTEGRATED SECURITY AND PERFORMANCE

Cloudflare removes the need to sacrifice performance for security. Instead of decreasing performance, Cloudflare's security features can increase application performance because of low-latency security services integrated with traffic acceleration.