Cloudflare Services

Protect and accelerate mission-critical Internet infrastructure. Cloudflare provides a robust suite of products, including DDoS mitigation, web application firewall, security against bot traffic, and access tools that allow the protection of your internal resources by identity authentication.

Products including under Standard Enterprise under the Athenian Project:

- **Distributed Denial of Service (DDoS) protection:** *Mitigates against distributed denial-of-service attacks without incurring latency or interfering with legitimate users. To protect against DDoS attacks, Cloudflare's network spans over 200 cities in more than 100 countries and is built to automatically monitor and mitigate large DDoS attacks for all plan types because it uses an Anycast network. In anycast, one IP address can apply to many servers. Anycast DNS means that any one of a number of DNS servers can respond to DNS queries, and typically the one that is geographically closest will provide the response. This reduces latency, improves uptime for the DNS resolving service, and provides protection against DNS flood DDoS attacks. Anycast networks provide DDoS protection because traffic can be spread across the whole network. The largest DDoS attack Cloudflare has detected and mitigated peaked at 942 Gbps.*
- ***End to End HTTPs encryption****: free SSL certificate to keep user data secure, verify ownership of the website, prevent attackers from creating a fake version of the site, and gain user trust. By encrypting any data that goes between a user and a web server, SSL ensures that anyone who intercepts the data can only see a scrambled mess of characters. SSL also stops certain kinds of cyberattacks: It authenticates web servers, which is important because attackers will often try to set up fake websites to trick users and steal data.*
- ***Web Application Firewall****: Cloudflare Web Application Firewall's intuitive dashboard enables users to build powerful rules through easy clicks. Every request to the WAF is inspected against the rule engine and the threat intelligence curated from protecting approximately 25 million websites. Suspicious requests can be blocked, challenged or logged as per the needs of the user while legitimate requests are routed to the destination, agnostic of whether it lives on-premise or in the cloud. Cloudflare's WAF enables protection against malicious attacks that aim to exploit vulnerabilities including SQLi, XSS and more, by simply turning on the OWASP Core Ruleset. To quickly protect against new and zero-day vulnerabilities, toggle to turn on Cloudflare's Managed Ruleset. As the vulnerability landscape changes quickly, Managed Rulesets are updated regularly by Cloudflare to provide fast and seamless protection against the latest attack vectors.*

- ***Rate Limiting:*** *Cloudflare Rate Limiting automatically identifies and mitigates excessive request rates for specific URLs or for an entire domain. Request rates are calculated locally for individual Cloudflare data centers. The most common uses for Rate Limiting are DDoS protection, Brute-force attack protection, and to limit access to forum searches, API calls, or resources that involve database-intensive operations at your origin.*
- ***Analytics****: Cloudflare's built-in analytics give you deeper insights into your traffic patterns, threats observed (and blocked), and much more right from the dashboard. High-level analytic dashboards provide overviews of your traffic and security posture including overviews of traffic including firewall events, DNS query traffic, the geographical distribution of your DNS queries over time. Analytics also gives you the ability to identify origin server issues and accelerate remediation efforts in the case of downtime.*
- ***Logs:*** *Access to detailed logs of HTTP requests for domain. Logs are typically used for debugging, identifying configuration adjustments, and creating analytics, especially when combined with other data sources, such as application server logs. Logs are helpful when investigating incidents such as website outages.*
- ***Multi-User Organization:*** *enables multiple managers for your Cloudflare accounts ensuring security with two-factor authentication and account access tools.*
- ***Support:*** *Enterprise-level "I Am Under Attack" support and 24/7/365 uptime DDoS support with emergency phone number.*