SOLUTION BRIEF

Secure Web Apps and APIs

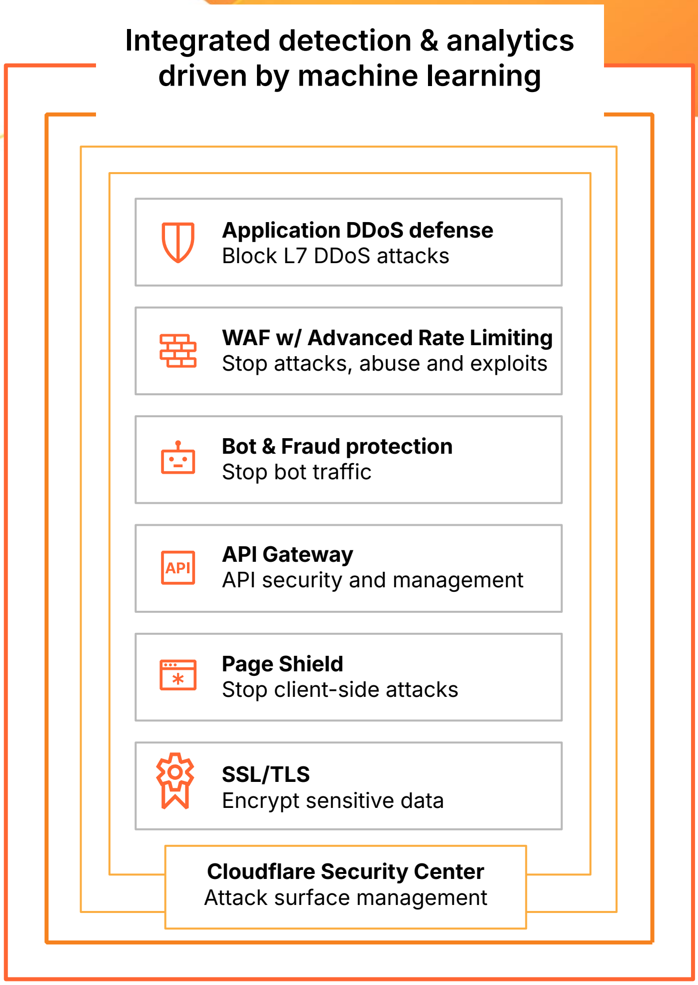
Improve visibility, control, and protection across your entire web footprint.

Defend expanding web application attack surfaces

Web app and API security is critical for organizations that rely on web apps as a source of revenue or to provide services. Websites that intake and store sensitive data, or provide critical infrastructure and services, are particularly susceptible to attacks.As web footprints (and attack surfaces) expand, organizations should be on the lookout for:

- Zero-day vulnerabilities
- Compromised third-party components
- Sensitive data exfiltration
- Account takeovers
- Volumetric attacks
- ...and other threats

Cloudflare Application Security protects applications and APIs from abuse, stops bad bots, thwarts DDoS attacks, and monitors for suspicious payloads and browser supply chain attacks.



Integrated detection & analytics driven by machine learning

Application DDoS defense
Block L7 DDoS attacks

WAF w/ Advanced Rate Limiting
Stop attacks, abuse and exploits

Bot & Fraud protection
Stop bot traffic

API Gateway
API security and management

Page Shield
Stop client-side attacks

SSL/TLS
Encrypt sensitive data

Cloudflare Security Center
Attack surface management

Figure 1: Centralize control and visibility with the Cloudflare Application Security portfolio

Protect web applications

Protect against zero-day attacks with ML-backed models that can detect vulnerabilities faster than public disclosure. Defend against record-breaking DDoS attacks, protect sensitive data, reduce client-side risks, and monitor your web application's software supply chain.

Defend against bots and fraud

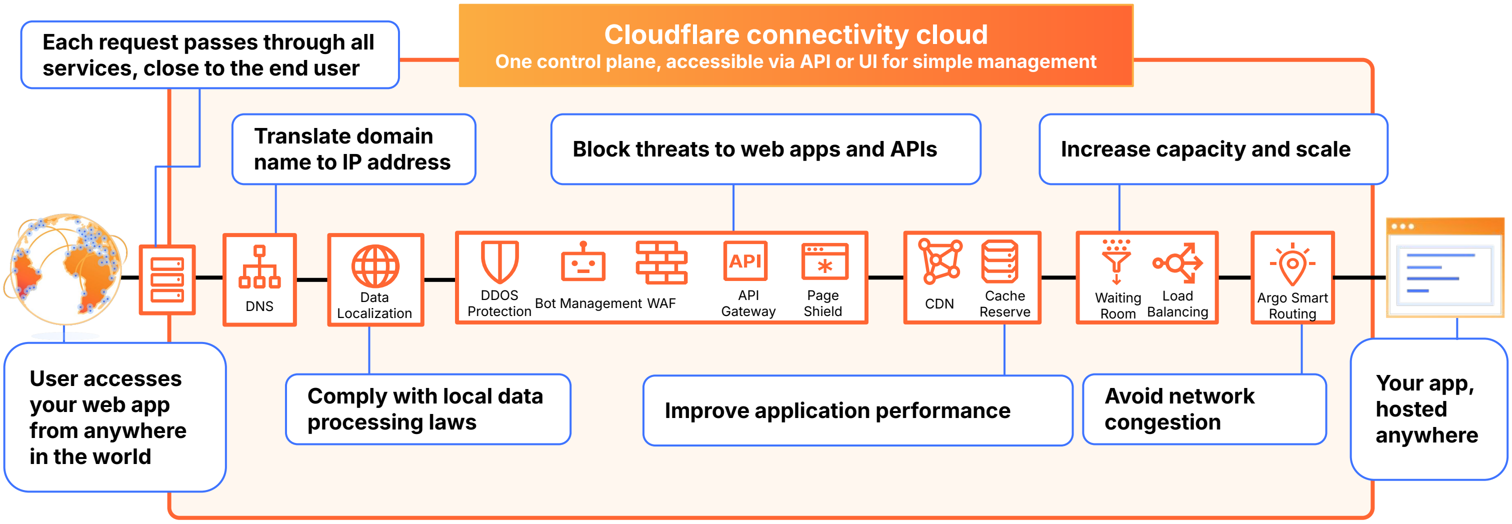
Protect your users from account takeovers and stop bad bots that affect end user experience. Stop malicious botnets, credential and card stuffing, content scraping, and inventory hoarding by combining ML models with client, network, and threat intelligence.

Secure and manage APIs

Discover all public-facing APIs with continuous ML-based API discovery, validate traffic with a positive security model, identify sensitive data used in APIs, and protect REST and GraphQL endpoints from DDoS, bot, and business logic abuse.

Application security and performance that work together seamlessly

Web app performance and reliability problems can be caused by numerous factors ranging from inefficient traffic routing to credential stuffing attacks, and more. Slow performing or unavailable web apps can result in brand damage, revenue loss, compliance violations, breaches, and more. Our application security products work closely with our performance suite, all delivered by Cloudflare's connectivity cloud in a single pass. All Cloudflare web application and API services are available at every data center, so you can spin up new capabilities to protect and accelerate your applications without tradeoffs between security and user load times.



Cloudflare connectivity cloud
One control plane, accessible via API or UI for simple management

Each request passes through all services, close to the end user

Translate domain name to IP address

Block threats to web apps and APIs

Increase capacity and scale

User accesses your web app from anywhere in the world

Comply with local data processing laws

Improve application performance

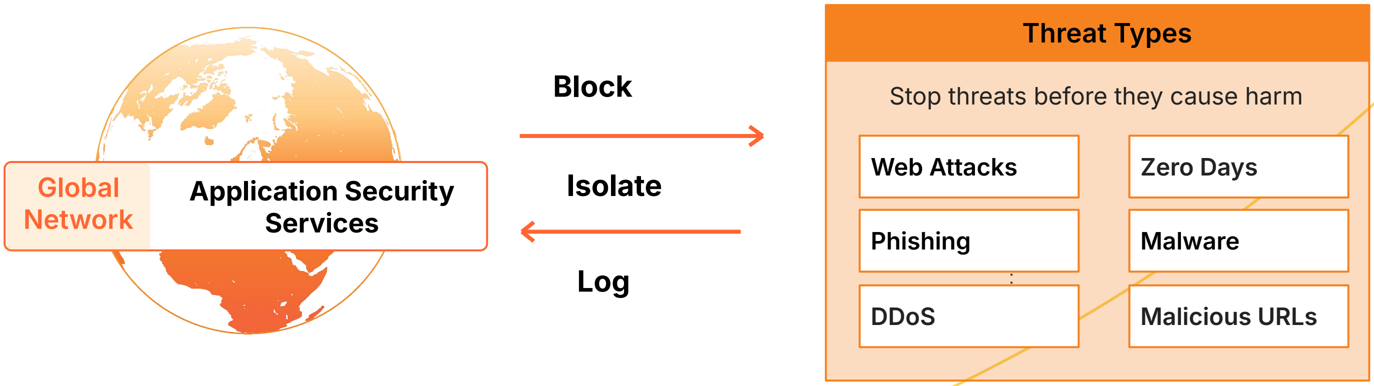
Avoid network congestion

Your app, hosted anywhere

Figure 2: Sample request path for combined usage of Cloudflare Application Security and Performance

Mass-scale threat intelligence ensures faster protections across all security products

About 20% of the web runs on Cloudflare, providing widespread visibility into web attacks, zero days, DDoS, and other attacks targeting our millions of customers. We combine that mass-scale threat visibility with ML models to identify attacks early in the attack chain and automatically deploy protections before they can cause harm. Telemetry from all Cloudflare products enhance protections at other layers — for example, phishing signals from Cloudflare Email Security are used to enhance WAF protections — ensuring customers have the most robust, up-to-date threat mitigations in the market.



Global Network

Application Security Services

Block

Isolate

Log

Threat Types

Stop threats before they cause harm

Web Attacks

Zero Days

Phishing

Malware

DDoS

Malicious URLs

Ready to see more? Register for our App Security Demo Series.