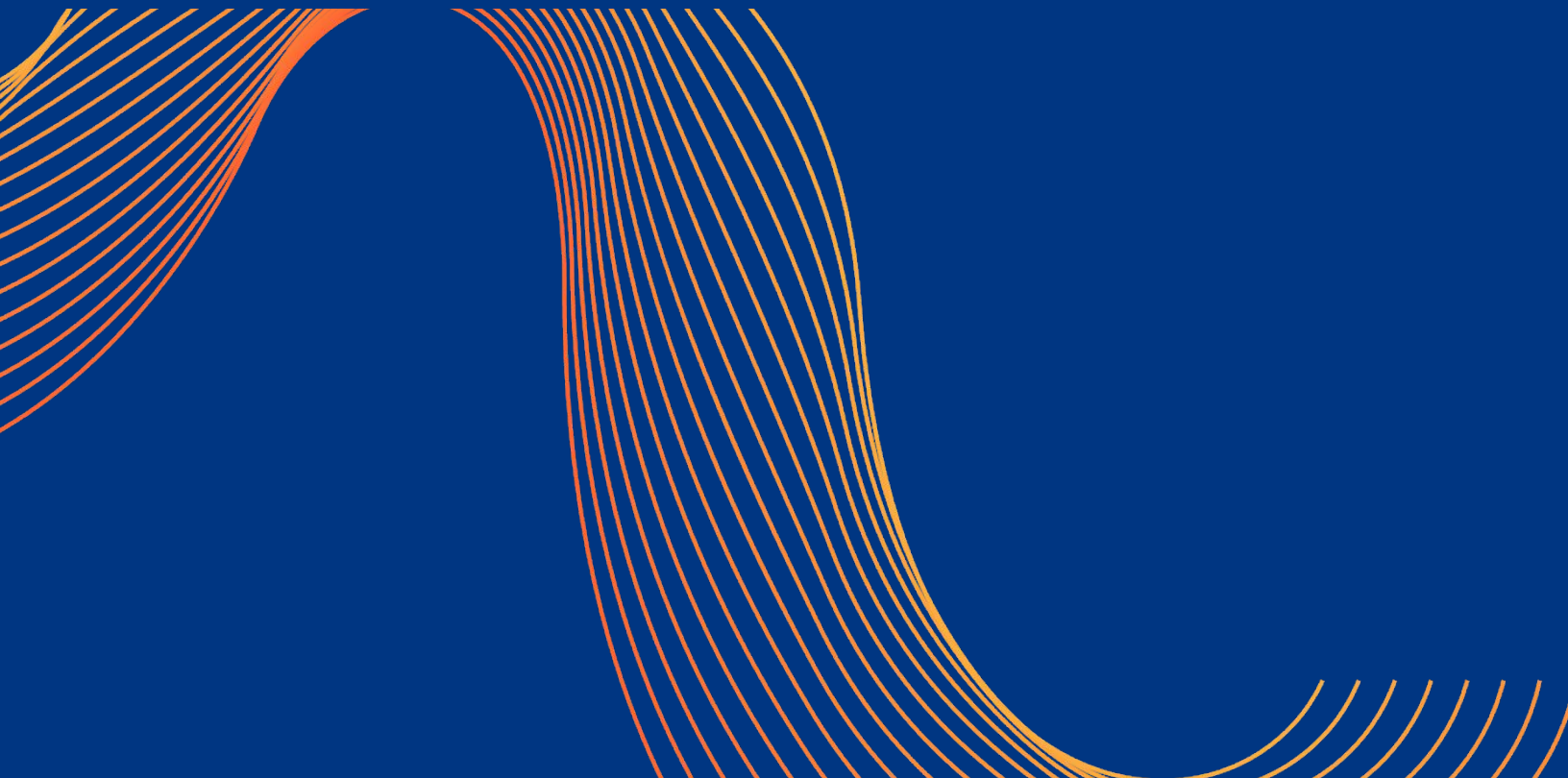# Cloudflare Product Cheat Sheet

This document contains the following:

- Product overview
  - Application Services
  - Zero Trust Services
  - Network Services

CLOUDFLARE®

Application Services

The **Cloudflare application services portfolio** keeps applications and APIs secure and productive, thwarts DDoS attacks, mitigates bots, detects anomalies and malicious payloads, and encrypts data in motion, all while making everything you connect to the Internet private, fast, and reliable.

These services run on every server in every data center over our global Anycast network, and all are easy to manage directly from the Cloudflare dashboard.

WAF

Our **Web Application Firewall (WAF)** blocks attacks heading towards applications - including L7 DDoS attacks - and offers better security with sophisticated, layered rulesets.

SSL/TLS

SSL / TLS enables encrypting as much web traffic as possible to prevent data theft and other tampering is a critical step toward building a safer, better Internet.

Managed Rules

The WAF **Managed Rulesets** are pre-configured rulesets that provide immediate protection against a range of threats, from zero-day vulnerabilities to top-10 attack techniques, use of stolen/exposed credentials, and extraction of sensitive data.

Custom Rules

Custom rules allow you to control incoming traffic by filtering requests. You can perform actions like *Block* or *JS Challenge* on incoming requests according to rules you define.

Security Center

Cloudflare **Security Center** brings together our suite of security products, our security expertise, and unique Internet intelligence as a unified security intelligence solution to help customers map their attack surface, review potential security risks and threats to their organizations, and mitigate these risks with a few clicks.

Dashboard Analytics

Dashboard Analytics are analytics in the Cloudflare dashboard, with the number of days referring to what is available in the Security Center.

API Management

API Management takes it beyond basic analytics (e.g. viewing the # of exposed APIs or % of API traffic) by including authentication through mutual TLS and a preview of discovery — for instance, identifying the number of endpoints found and showing top X.

Rate Limiting

Rate Limiting provides the ability to limit the rate of requests and gain valuable insights into specific URLs of websites, applications, or API endpoints.

Advanced DDoS

In addition to protecting against Layer 3 and 4 attacks, including TCP/UDP, Cloudflare **Advanced DDoS** automatically detects sudden changes in traffic and protects against layer 7 DDoS attacks, so they never reach the origin server.

Account Level Configuration

Account Level Configuration enables users to configure all application security products (e.g. WAF, Rate Limiting, API Shield) at the account level. This does not remove the granularity of zone-level configuration.

Bot Management

Bot Management stops malicious bots connecting to web sites, and uses machine learning on a curated subset of hundreds of billions of requests per day to create a reliable bot score for every request.

Argo Smart Routing

Argo Smart Routing improves Internet performance by intelligently routing end users through less congested and more reliable paths over the Internet using our network.

Load Balancing

Load Balancing improves application performance and availability by steering traffic away from unhealthy origin servers and dynamically distributing it to the most available and responsive server pools.

Zero Trust Security

Cloudflare Zero Trust is a security platform that raises visibility, eliminates complexity, and reduces risks as remote and office users connect to applications and the Internet. In a single-pass architecture, traffic is verified, filtered, inspected, and isolated from threats. There is no performance trade-off: users connect through data centers nearby in 270+ cities in over 100 countries.

Other providers offer multiple point products to protect from every threat vector, but leave customers to manage their attack surface. Cloudflare's platform stops more attacks by isolating applications and endpoints from the attack surface by shifting it to our edge, and applies threat defenses to shield that edge.

Zero Trust Network Access

Zero Trust Network Access augments or replaces corporate VPN clients by securing SaaS and internal applications. Access works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules limiting access to corporate applications, private IP spaces, and hostnames.

Secure Web Gateway

Secure Web Gateway is our threat and data protection solution. It keeps data safe from malware, ransomware, phishing, command and control, Shadow IT, and other Internet risks over all ports and protocols.

Cloud Email Security

Cloudflare Area 1's integrated **Cloud Email Security** solution crawls the Internet to stop phishing, Business Email Compromise (BEC), and email supply chain attacks at the earliest stage of the attack cycle, and enhances built-in security from cloud email providers.

Remote Browser Isolation

Web browsers are more complex and sophisticated than ever, but represent a large attack surface for businesses. **Browser Isolation** makes web browsing safer and faster, running in the cloud away from your network and endpoints, insulating devices from attacks.

CASB

A **Cloud Access Security Broker** gives customers comprehensive visibility and control over SaaS apps to easily prevent data leaks, block insider threats, and avoid compliance violations.

Data Loss Prevention

Cloudflare's **Data Loss Prevention** solution enables customers to detect and prevent data exfiltration or data destruction. Analyze network traffic and internal "endpoint" devices to identify leakage or loss of confidential information, and stay compliant with industry and data privacy regulations.

CLOUDFLARE®

Network Security

The **Cloudflare network security portfolio** exists to secure the networks of modern enterprises, helping to mitigate DDoS attacks, identify malicious traffic patterns, and monitor new and emerging threats. Our solutions offer unified, layered security and can be applied across all endpoints and users — no matter where they're located.

Our network solutions are delivered from our global network which operates at massive scale. Every network service - like every Cloudflare service - runs on every server in every data center over our global Anycast network. All are easy to manage from the Cloudflare dashboard, the one pane of glass for all our services.

Magic Firewall

Magic Firewall is a cloud-based firewall enabling administrators to set policies for all traffic entering and leaving the network.

Magic Transit

Cloudflare **Magic Transit** provides near-instant mitigation of network-layer threats (L3 DDoS attacks) from the Cloudflare global network, alongside next-generation firewall and traffic acceleration.

Magic WAN

Extends the benefits of our network to customers' private networks. **Magic WAN** enables IP level connectivity as well as a full suite of virtual network functions, including IP packet filtering and firewalling, load balancing, and traffic management tools.

Network Analytics

Network Analytics enables IT and network teams to inspect network traffic without performance tradeoffs, and apply advanced mitigation techniques via single-pass inspection.

Argo Smart Routing

Argo Smart Routing improves Internet performance by intelligently routing end users through less congested and more reliable paths over the Internet using our network.

WAN Optimization

WAN Optimization is an additional functionality existing on top of Magic WAN that improves performance of customer traffic (similar to Argo Smart Routing).
Forthcoming!