

Cloudflare Externa

G-Cloud 15



GCloud 15 Service Definition for Cloudflare Externa Bundle & Cloudflare Interna Bundle

Agenda

- 1 Overview of solution packages
- 2 External package details
- 3 Internal package details
- 4 Add-ons for solution packages
- 5 Customer Success Resources
- 6 Service Product Definitions

Connectivity cloud architecture & key differentiators

**One network,
one control
plane**

**Composable,
programmable
services**



**Global scale and
resilience**

**Simplified
management
interface**

One network, one control plane on a global scale



335+ cities

in 125+ countries, including mainland China



w/180+ cities

for AI inference powered by GPUs



~20%

of web properties sit behind Cloudflare



227 billion

cyber threats blocked every day



348 Tbps

of network capacity (and growing)



Overview of Solution Packages &

Connect, protect, and build **everywhere**

**Connect and protect
external-facing systems**



Cloudflare Network Services



Cloudflare Application Services

**Connect and protect
internal-facing systems**



Cloudflare Zero Trust Services

Build the next-generation of application



Cloudflare Developer Platform

One Platform  One Network

New use-case-oriented packages

New solution packages

Externa packages

Connect and protect external-facing systems

Essentials

- Manage web traffic and optimize routing to deliver even faster response times
- Foundational security controls addressing key application security risks



Advantage

- Deeper and more customizable protections against additional risks, including API abuse, bot control, data breaches, and advanced attacks



Premier

- Extend to the network layer
- Accelerate Internet traffic

Interna packages

Connect and protect internal-facing systems

Essentials

- Secure your workforce with Zero Trust controls to restrict access to data, apps, and services
- Minimize threat exposure with robust access management and data loss prevention
- Performant, reliable connectivity for your team, whenever they are



Advantage

- Eliminate sophisticated security risks with phishing protection and remote browser isolation
- Protect data by limiting allowed user actions
- Load balance across private infrastructure



Premier

- Customization for email security

Sold a la carte

Developer platform

Build on Cloudflare

Compute

- Create full-stack applications
- Deploy functions as a service

Media

- Deliver images and video quickly
- Build real-time audio and video apps

AI

- Run custom workloads on GPUs at the edge

Storage and databases

- Zero-egress object storage
- Globally distributed



Premium success, support and professional services, add-on products

Externa details

Externa

Connect and protect external-facing systems

→ **Connect and protect
external-facing systems**



Cloudflare Network Services



Cloudflare Application Services

**Connect and protect
internal-facing systems**



Cloudflare Zero Trust Services

Build the next-generation of application



Cloudflare Developer Platform

One Platform  One Network

Externa packages

Connect and protect external-facing systems (websites, applications, and networks)

- Base fee includes 1 TB and 50 M requests per month
- Additional traffic, requests, zones, and endpoints charged per unit
- No attack traffic tax — we only charge for clean traffic
- Every Externa package will include 50 seats of the Interna Essentials package

	Essentials	Advantage	Premier
Use cases	• Foundational security controls for applications • Optimal routing to deliver fastest response times	• Stop attacks on APIs • Discover attack surface • Malicious bot and fraud protection • Configurable traffic load balancing • Deeper and customizable protections for advanced attacks	• Centralize management and protection of infrastructure on cloud environments • Protect public-facing network infrastructure
	Includes the following WAAP/Edge Distribution Platform services: • Priority CDN • WAF • Advanced DDoS • IP-based rate limiting (Rate Limiting) • Foundation DNS • Advanced Certificates Manager • Managed Challenge (Turnstile) • Layer 7 Smart Routing (Argo) • Advanced Waiting Room	Includes everything in Essentials, plus: • Load Balancing • Payload Inspection • Content Scanning • API Security (API Shield) • Bot Management • Client-side Security (Page Shield) • Advanced Rate Limiting	Includes everything in Advantage, plus: • Layer 3 DDoS Protection (Magic Transit: Always On and Magic Transit Egress) • Firewall as a Service (Advanced Magic Firewall) • Layer 3 Smart Routing (Argo for Packets)
+ INCLUDED IN EVERY EXTERNA PACKAGE 50 seats of Interna Essentials			
+ OPTIONAL Global services, premium support, add-on products			

	Pro (up to 1 zone)	Business (up to 1 zone)	Essentials	Advantage	Premier
Use cases	- Deliver content to a global audience - Protect against DDoS and basic bot attacks - Implement basic firewall rules	Basic security controls for individual applications	- Foundational security controls for applications - Optimal routing to deliver fastest response times	- Stop attacks on APIs - Discover attack surface - Prevent bots and fraud - Traffic load balancing - Deeper and customizable protections for advanced attacks	- Centralize management and protection of infrastructure on cloud environments - Protect public-facing network infrastructure
Products	Includes: - Basic CDN - Layer 7 DDoS - WAF (≤20 custom rules) - Basic Bot Protection - Basic Managed Challenge - IP-based rate limiting (Rate Limiting, ≤2 rules) - Page Rules (≤20 rules)	Everything in Pro, plus: - DNS - WAF (≤100 custom rules) - IP-based rate limiting (Rate Limiting, ≤5 rules) - Image Optimization - Custom SSL (≤25 certs) - Page Rules (≤50 rules) - Basic Waiting Room	Everything in Business, plus: - Priority CDN - WAF (≤1000 custom rules) - Advanced DDoS (customizable) - IP-based rate limiting (Rate Limiting, ≤100 rules) - Foundation DNS - Advanced Certificates Manager - Managed Challenge (customizable) - Layer 7 Smart Routing (Argo) - Advanced Waiting Room (customizable)	Everything in Essentials, plus: - Load Balancing - Payload Inspection - Content Scanning - API Security (API Shield) - Bot Management (bot score, advanced detections) - Client-Side Security (Page Shield) - Advanced Rate Limiting (any header attribute)	Everything in Advantage, plus: - Layer 3 DDoS Protection (Magic Transit Egress and Magic Transit: Always On) - Firewall as a Service (Advanced Magic Firewall) - Layer 3 Smart Routing (Argo for Packets)
SLA	N/A	100% Uptime 1x Service Credits	100% Uptime 10x (Standard Support) or 25x (Premium Support) Service Credits		

Services	Capabilities and Impact	Essentials	Advantage	Premier
CDN	Edge content delivery: Ultra-fast static content caching and delivery via Cloudflare's global network, secured with SSL/TLS and protected by post-quantum cryptography.	✓	✓	✓
Web Application Firewall (WAF)	Blocks attacks on web applications and APIs: Protect apps and APIs from zero-day vulnerability exploits, common attack techniques, use of leaked credentials, and more with rulesets powered by machine learning and threat intelligence.	✓	✓	✓
Advanced DDoS	Cloud-native layer 7 distributed denial-of-service protection: Automatically detect and mitigate layer 7 DDoS attacks via our unmetered, unlimited, and autonomous DDoS protection systems.	✓	✓	✓
IP-based Rate Limiting	Traffic volume control based on IP address: Limit the number of HTTP requests to apps and APIs made over a set timeframe from each IP address. Reduces likelihood of web server overloading from volumetric attacks, such as credential stuffing, DDoS, and brute force attacks.	✓	✓	✓
Foundation DNS	Enterprise-grade managed DNS: Authoritative DNS service with advanced nameservers, zone-level DNS settings, unique DNSSEC keys, and enhanced analytics.	✓	✓	✓
Advanced Certificate Manager	SSL/TLS certificates for web apps: Secure web applications and user data with TLS certificates (supporting PQC key agreements) that are automatically issued and renewed, reducing certificate lifecycle management overhead.	✓	✓	✓
Managed Challenge (Turnstile)	Security verification of incoming traffic requests: Cloudflare dynamically chooses the appropriate type of verification of potentially malicious requests based on the characteristics of each request. This helps block illegitimate requests or users attempting to access apps.	✓	✓	✓
Layer 7 Smart Routing (Argo)	Dynamic content delivery optimization: Automatically detect network congestion in real time and route traffic across the most efficient path over the Internet for optimal content delivery and user experience.	✓	✓	✓
Advanced Waiting Room	Automatically manage legitimate traffic spikes: Route excess legitimate users to a custom-branded waiting room to preserve the customer experience and protect origin servers from being overwhelmed with legitimate requests.	✓	✓	✓

Services	Capabilities and Impact	Essentials	Advantage	Premier
Load Balancing	Global and private network load balancing: Ensure optimal performance, resilience, and high availability of services by proactively and intelligently steering traffic away from unhealthy endpoints based on geolocation, dynamic latency, proximity, and other policies.		✓	✓
Payload Inspection	Inspect body data and headers: Inspect payloads that matched WAF rules to aid in incident response or inspecting WAF rule behavior.		✓	✓
Content Scanning	Malware scan in web uploads: Identify and block malicious content objects being uploaded to apps.		✓	✓
API Security (API Shield)	Discover public APIs and protect APIs from attacks: Discover shadow APIs with machine learning models and protect them from business logic abuse and other attacks with a positive security model.		✓	✓
Bot Management	Detect and respond to bots: Identify and mitigate automated traffic to protect your web and mobile apps from bad bots based on bot scores. These scores are calculated based on machine learning models, heuristics, JavaScript detection, verified and AI bot categories, and mobile device verification signals.		✓	✓
Client-side Security (Page Shield)	Secure your visitors' browser environments: Keep your end users safe from compromised and malicious resources loaded on your websites, such as scripts and their connections, and cookies.		✓	✓
Advanced Rate Limiting	Traffic volume control based on any HTTP request characteristic: Limit the number of HTTP requests to apps and APIs made over a set timeframe based on any HTTP request characteristic — not just IP addresses — to block more sophisticated attackers. These limits adapt to changes in traffic patterns.		✓	✓

Services	Capabilities and Impact	Essentials	Advantage	Premier
Layer 3 DDoS Protection (Magic Transit: Always On and Magic Transit Egress)	DDoS protection for public-facing networks: Protect your app infrastructure using Cloudflare's network to globally detect, filter, and absorb DDoS attacks.			✓
	Improved security for egress traffic: Send return traffic over the same paths used for incoming traffic for improved security and operational efficiency.			✓
Firewall as a Service (Advanced Magic Firewall)	Cloud-native layer 3 and layer 4 firewall: Consistently enforce network security policies across your public-facing infrastructure, without backhauling traffic or creating choke points.			✓
Layer 3 Smart Routing (Argo for Packets)	Provides IP layer network optimizations: Dynamically route traffic through the fastest, most available path through Cloudflare's network.			✓

The value of Externa

Connect and protect external-facing systems

Predictable bills with no attack traffic tax

We only charge for clean traffic, not for the malicious requests we block. Cloudflare delivers predictable costs, even during a DDoS attack.



Only pay for clean traffic

Simple, value-driven price units

Say goodbye to origin fetch fees, duplicate charges per request, and charges per WAF rule. Our pricing scales directly with the value you receive.



Better together: On-ramp to SASE included

Every Externa package includes 50 Interneta Essentials seats, extending security to internal systems for 360-degree security across your organization.



Simplify, consolidate, and reduce TCO

Stop managing multiple vendors. Our integrated platform combines WAF, DDoS, API security, and more in one place, reducing vendor complexity and your total cost of ownership (TCO).



Interna details

Interna

Connect and protect internal systems

Connect and protect
external-facing systems



Cloudflare Network Services



Cloudflare Application Services

Connect and protect
internal-facing systems



Cloudflare Zero Trust Services

Build the next-generation of application



Cloudflare Developer Platform

One Platform  One Network

Internal packages

Connect and protect internal-facing systems (people, data, apps, and networks)

- Never double pay for seats and bandwidth through Cloudflare's device agent
- Charged per seat, with WAN traffic included*
- No licenses or fees to deploy or configure on-ramps
- Includes protection for data at rest and in transit, plus unlimited CASB API integrations

Use cases

Essentials	Advantage	Premier
• Adopt Zero Trust via VPN replacement • Protect distributed offices and workers from threats • Protect sensitive data and simplify compliance • Simplify enterprise networking	• Phishing and business email compromise (BEC) protection • Zero Trust browsing for risky sites • Data controls for contractors and unmanaged devices • Configurable load balancing for internal endpoints	• Customizable email security • Accelerated WAN
Includes the following SASE/SSE services: • Zero Trust Network Access (Access) • Secure Web Gateway (Gateway) • Cloud Access Security Broker (CASB) • Data Loss Prevention (DLP) • Digital Experience Monitoring (DEX) • Network-as-a-Service (Magic WAN) • Firewall-as-a-Service (Advanced Magic Firewall)	Includes everything in Essentials, plus: • Email Security — pre-, link-, post-delivery protection • Remote Browser Isolation (Browser Isolation) • Private Network Load Balancing • File Sandboxing	Includes everything in Advantage, plus: • Email Security — pre-, link-, post-delivery protection • Managed Detection and Response (MDR) for Email Security (PhishGuard) • Layer 3 Smart Routing (Argo for Magic WAN)



HIGHLY RECOMMENDED

Global services, premium support



OPTIONAL

Add-on products

*Includes 1, 2, or 3 Mbps of Magic WAN per seat purchased in Essentials, Advantage, and Premier, respectively. User (employee) traffic generated through Cloudflare's device client (i.e., WARP) does not count against this allotment.

INTERNA DETAILS: PACKAGING

	Pay-as-you-go	Essentials	Advantage	Premier
Use cases	Best for teams solving narrow SSE use cases that do not require enterprise support	- Adopt Zero Trust to reduce risk and complexity for employee and contractor access to self-hosted, SaaS, and web apps - Protect sensitive data in-transit and at-rest - Provide fast, reliable global WAN connectivity between data centers, offices, and cloud services with firewalling built in	- Eliminate sophisticated security risks with phishing protection and drastically reduce the attack surface with remote browser isolation - Load balance traffic between servers within a data center (origin steering) and between private applications	- Add protection against multi-channel phishing attacks and greater orchestration and integration across the security stack - Optimize and accelerate WAN traffic
Products	People - Zero Trust Network Access (Access) - Secure Web Gateway (Gateway) - Cloud Access Security Broker (CASB) — top-level findings, 2 API integrations - Data Loss Prevention (DLP) — limited predefined profiles	<i>Includes everything in PAYGO, plus:</i> People - CASB — full-featured; no limits - DLP — full-featured; no limits Network - Network-as-a-Service (Magic WAN*) - Layer 3 Firewall-as-a-Service with IDS (Advanced Magic Firewall*)	<i>Includes everything in Essentials, plus:</i> People - Browser Isolation — unlimited RBI usage - Email Security — pre-delivery protection - File Sandboxing Network/Application - Private Network Load Balancing*	<i>Includes everything in Advantage, plus:</i> People - Email Security — pre-, link, post-delivery protection - MDR for Email Security (PhishGuard) Network - WAN Traffic Acceleration and Smart Routing (Argo for Magic WAN * ***)
Built-in functionality	People - Gateway DNS locations (≤50 static IPs) - Digital Experience Monitoring (≤30 tests) Network - Network flow monitoring (Magic Network Monitoring) Platform - Log retention (≤30 days)	People - Gateway DNS locations (≤250 editable IPs) - Digital Experience Monitoring (≤30 days) - User risk score - Proxy endpoints (for PAC file support) Network/Application** - Mutual TLS authentication - Network Interconnect (CNI) Platform - Log retention (≤6 months) - Logpush (SIEM and cloud storage support)		
SLA	100% Uptime 1x Service Credits	100% Uptime 10x (Standard Support) or 25x (Premium Support) Service Credits		

(*) 100% of traffic from device agent (i.e., WARP) sources excluded from bandwidth, traffic, and/or request calculations (**) mTLS and CNI are available with any Enterprise contract (***) Requires direct connectivity using CNI

INTERNA DETAILS (1 of 2)

Services	Capabilities	Impact	Essentials	Advantage	Premier
ZTNA and SWG (Access and Gateway work together)	Granular context verification	Continuously verify identity, device posture, and other context to inform authorization decisions	✓	✓	✓
	Per-resource Zero Trust policy enforcement	Enforce default-deny rules for all resources: SaaS and self-hosted apps, internal IPs and hostnames, and infrastructure targets	✓	✓	✓
	Low-latency resource access	Eliminate VPN issues with cloud-native access controls that scale with your organization	✓	✓	✓
	DNS and network filtering and HTTP/S inspection	Enforce security, app, and content categories; AV and sandboxing; and traffic and tenant rules — <i>plus, DLP profiles explained below</i>	✓	✓	✓
	AI-backed threat intelligence	Block known and emerging threats using intelligence derived via AI models analyzing the vast amount of traffic on Cloudflare's network	✓	✓	✓
	File sandboxing	Quarantine previously unseen files downloaded by your users into a sandbox and scan them for malware		✓	✓
CASB and DLP	API integrations (<i>beyond inline protection explained above</i>)	Analyze SaaS and cloud apps for misconfigs, exposed files, shadow IT, and suspicious activity to protect data and ensure compliance	✓	✓	✓
	Discover and protect sensitive data across all services	Increase data visibility and prevent breaches, data exfiltration, and accidental exposure across web, email, and SaaS apps	✓	✓	✓
NaaS (Magic WAN) and FWaaS (Adv Magic Firewall)	Site-to-site branch connectivity	Easily facilitate site-to-site connectivity across network locations like branch offices, retail locations, or factory floors	✓	✓	✓
	Secure hybrid and multicloud connectivity	Centralized controls to route and secure traffic across varied public cloud environments and on-prem data centers	✓	✓	✓
	Cloud-native layer 3 network firewall	Consistently enforce network security policies across your entire WAN, without backhauling traffic or creating choke points	✓	✓	✓
	Intrusion detection	Expands the security coverage of your firewall to analyze and monitor network traffic against a broader threat signature database	✓	✓	✓
	Included WAN traffic	In addition to not charging for user bandwidth, each user license helps you build your WAN fabric	1 Mbps/seat	2 Mbps/seat	3 Mbps/seat

Services	Capabilities	Impact	Essentials	Advantage	Premier
Digital Experience Monitoring	Real-time intelligence and observability	Visualize user, application, and network performance data to proactively detect and mitigate connectivity issues	✓	✓	✓
Load Balancing	Private network load balancing	With private IP support, get near real-time failover across multiple servers, whether they are deployed in a private, public, or hybrid cloud		✓	✓
Remote Browser Isolation (Browser Isolation)	Secure, low-latency remote browsing	Eliminates the risk of zero-day browser vulnerabilities and prevents users from loading malicious web content on their device		✓	✓
	Controlled user actions	Restricts keyboard input, file download/upload, copy/paste, and print functions to prevent users from leaking credentials and sensitive information		✓	✓
Email Security	Inbox protection deployed inline (Advantage*)	Deploy inline (as MX) to protect against business email compromise (BEC), malware, and malicious email links.		✓	✓
	Enhanced deployment and integrations (Enterprise*)	Greater deployment flexibility, outbound DLP coverage, and link isolation capabilities — with enhanced reporting and orchestration through SIEM/SOAR integrations			✓
	Managed detection and response (PhishGuard*)	Accelerate phishing/threat investigation and response while reducing the time and effort dedicated to managing email security			✓
Layer 3 Smart Routing (Argo for Magic WAN)	AI-based smart traffic routing for best-path delivery	Optimizes your network performance and improves reliability using dynamic traffic intelligence from the Cloudflare network			✓

* Stand-alone product packages for email security

The value of Interna

A simpler, more powerful model for adopting SASE

Never pay for user bandwidth

Connect your remote, hybrid, and branch users with a single per-seat price. You'll never see bandwidth charges for devices with our user agent installed.



One price per user, not per location

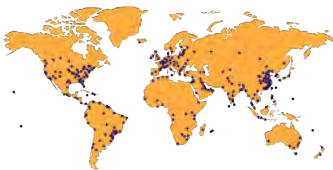
Every seat license builds your WAN fabric

Replace expensive WAN contracts. Every user license contributes to a shared bandwidth pool that connects your entire network of offices and data centers.



One global network, one simple price

Give every user a fast, low-latency connection. Access our entire global network* for one flat price, with no complex regional surcharges.



* Excludes mainland China PoPs

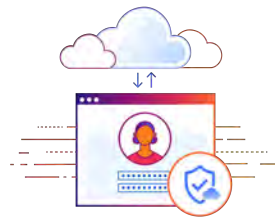
Simplified connectivity costs

Simplify your spending. Get unlimited software connectors and private interconnects to your clouds and data centers at no cost – we only charge for seats or bandwidth.



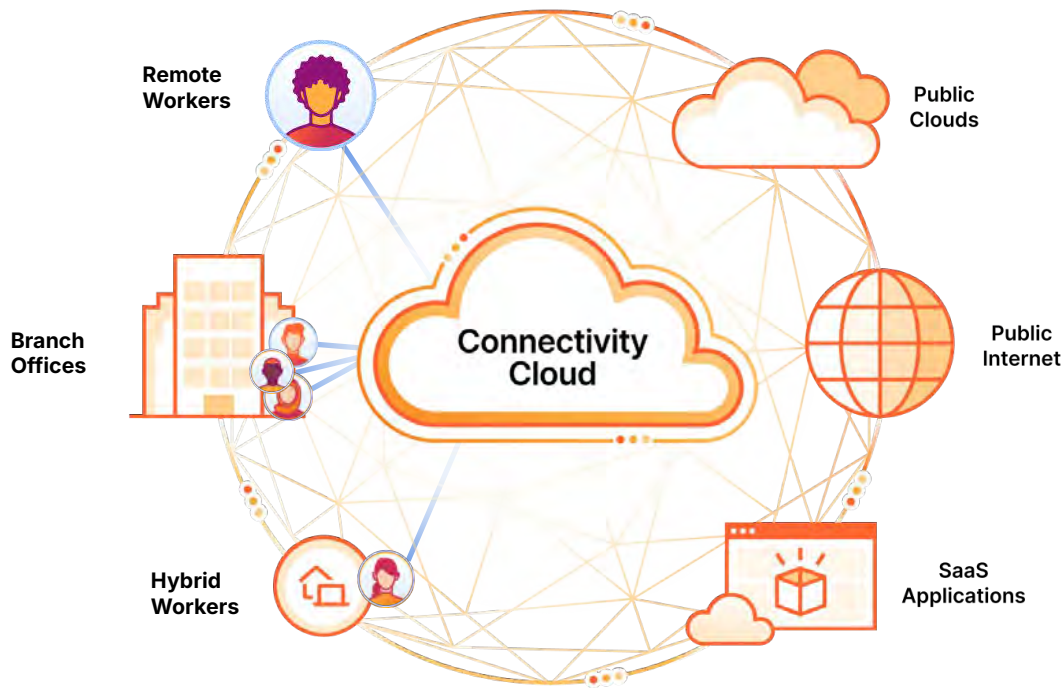
All-inclusive multimode CASB

Get unified data protection for all your SaaS applications. Includes unlimited API integrations and full coverage for data at rest and in transit.



Never pay for user bandwidth

User traffic is excluded from WAN calculation



— Connectivity included

Protect your users anywhere and take your WAN bandwidth bill for those users to \$0.

Cloudflare does not charge for bandwidth from devices with our user agent installed.

One price, every location. No double paying for seats and bandwidth.

Package add-ons

Customer success and support services

Success packages

Maximize value and Cloudflare experience

Standard

Included with every Enterprise subscription and provides the necessities, such as on-demand onboarding modules and priority support.

Premium

Available upgrades for organizations with complex technical environments, or that require high priority support SLAs.

[Learn more](#)

Professional services

Advise and assist with planning, configuration, and best practices to accelerate deployment

Quickstart

A solution SME works alongside your team to guide configuration with proven best practices, helping you deploy confidently.

Migration

Expert migration assistance when moving from legacy providers such as Akamai, Fastly, or Zscaler.

Expert

Project managers, consultants, and architects assist with custom, unique use cases, such as highly regulated organizations.

[Learn more](#)

Ongoing support services

Focused technical and security operations add-ons

Technical account management

Single point of contact to provide centralized technical support management.

SOC service

Cloudflare-managed SOC providing 24/7 monitoring, detection, and mitigation across your environment.

Incident response services

On-demand access to incident response experts, helping organizations contain attacks and accelerate recovery.

Learn more: [TAM](#) | [SOC](#) | [IR](#)

Product add-ons

These products are considered too niche to include in use-case packages out-of-the-box, and are available as add-ons to any bundle.

External solution package add-ons

App Performance

- ❑ Domains: Primary, Secondary, or >10K DNS-only
- ❑ IPs: BYO or Static
- ❑ Argo for Spectrum
- ❑ Cache Reserve

App Security

- ❑ Custom Domain Protection
- ❑ Static IPs for Magic Transit
- ❑ DNS Firewall
- ❑ Spectrum
- ❑ Custom SSL
- ❑ SSL for SaaS or Advanced SSL for SaaS

Internal solution package add-ons

SASE/SSE

- ❑ Dedicated Gateway Egress IPs (Static IPs)
- ❑ Dedicated Gateway DNS Resolver IPs (Static IPs or BYOIP)
- ❑ File Sandbox (for Gateway)
- ❑ Magic WAN Connector appliance (via partners, not via CPQ)

+ Platform offerings

- ❑ Cloudflare for Government
- ❑ Data Localization Suite
- ❑ Log Explorer
- ❑ China Network

Customer Success Resources

Ensuring your success



[Community](#)



[Docs](#)



[Resource Hub](#)



[Help Center](#)



[Discord](#)



[Blog](#)



[theNET](#)



[Cloudflare Radar](#)



[CloudflareTV](#)



[YouTube](#)

Service Product Definitions

Application Services Definitions



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.



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.



Advanced 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.



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.



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.



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.



CDN

A [CDN](#) helps address the challenges customers face around latency, performance, availability, redundancy, security, and costs. A CDN's core goal is to decrease latency and increase performance for websites and applications by caching content as close as possible to end users or those accessing the content.



DNS

[DNS](#) resolution involves converting a hostname into a computer-friendly IP address. An IP address is given to each device on the Internet. When a user wants to load a webpage, a translation must occur between what a user types into their web browser and the machine-friendly address necessary to locate the example.com webpage.

	Payload Inspection	Payload Inspection , is an available feature of the WAF, looks at request body data and headers to determine if they are malicious.
	Managed IP Lists	Managed IP Lists are WAF managed rulesets created and maintained by Cloudflare and are built based on threat intelligence feeds collected by analyzing patterns and trends observed across the Internet.
	Sensitive Data Detection	Sensitive Data Detection is a WAF managed ruleset that was created by Cloudflare to address common data loss threats. These rules monitor the download of specific sensitive data — for example, financial and personally identifiable information.
	API Shield	API Shield helps to identify and address API vulnerabilities and comes with a dedicated certificate authority (CA) to provide strong encryption for mobile applications and IoT device traffic.
	Images	Cloudflare Images provides an end-to-end solution to build and maintain your image infrastructure from one API.
	Stream	Cloudflare Stream offers end-to-end video encoding, accelerated global delivery and player for pre-recorded and live content all handled by Cloudflare.
	Waiting Room	Waiting Room limits the number of users to the origin while placing excess traffic into a Waiting Room to provide a great user experience. This protects customers infrastructure, reduces the number of errors served to users, and acts as an extension of the customer's brand; thereby maintaining a seamless experience.
	Account Level WAF	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.



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 330+ cities in over 10020

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 Access Security Broker (CASB)

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



Cloud Email Security

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. **Remote Browser Isolation** makes web browsing safer and faster, running in the cloud away from your network and endpoints, insulating devices from attacks.



Data Loss Prevention (DLP)

Data Loss Prevention (DLP) 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.



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 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.



Advanced 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.



Network Interconnect

[Cloudflare Network Interconnect](#) allows our customers to interconnect branch and HQ location directly with Cloudflare wherever they are, bringing Cloudflare's full suite of network functions to their physical network edge.



Smart Routing

[Smart Routing](#) improves Internet performance by intelligently routing end users through less congested and more reliable paths over the Internet using our network.



Intrusion Detection Systems

[Intrusion Detection Systems \(IDS\)](#) is an Advanced Magic Firewall feature you can use to actively monitor for a wide range of known threat signatures in your traffic.



Access

Access determines who can reach your application by applying the Access policies you configure.



Gateway

Gateway, our comprehensive Secure Web Gateway, allows you to set up policies to inspect DNS, Network, HTTP, and Egress traffic.



Advanced Browser Isolation

Browser Isolation complements the Secure Web Gateway and Zero Trust Network Access solutions by executing active webpage content in a secure isolated browser. Executing active content remotely from the endpoint protects users from zero-day attacks and malware.



Cloud Email Security

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.



CASB

Cloudflare's **Cloud Access Security Broker (CASB)** service gives comprehensive visibility and control over SaaS apps, so you can easily prevent data leaks and compliance violations. With Zero Trust security, block insider threats, Shadow IT, risky data sharing, and bad actors.



Data Loss Prevention

Cloudflare **Data Loss Prevention (DLP)** allows you to scan your web traffic and SaaS applications for the presence of sensitive data such as social security numbers, financial information, secret keys, and source code.

Thank you

Matt Johnson
Head of Public Sector

CDS, Yorkshire House, Greek Street, Leeds, LS1 5SH

Email: bidteam@cds.co.uk

Telephone: 07939 866831

Website: www.cds.co.uk