Connect and protect your internal-facing systems

Including people, data, apps, and networks

Modernize your security and network, together

Cloudflare Interna packages help you increase value and simplify procurement for broad SSE or SASE projects. Cloudflare's SASE solutions make it easy to secure and connect a distributed workforce — no matter where people, apps, or your infrastructure are. With a unified platform and device agent, you can quickly implement Zero Trust and modernization projects with less effort. And you'll never pay double for seats and bandwidth through Cloudflare's device agent.

Interna packages help organizations:

Modernize security
- Protect people, apps, and networks
- Safeguard data and stay compliant

Modernize networking
- Simplify your corporate network
- Secure offices and data centers

Consolidate tools and vendors
- Unified visibility across the attack surface — extended with Externa services
- Consistent policy enforcement without platform sprawl

Essentials	Advantage	Premier
• Adopt Zero Trust via VPN replacement • Protect distributed offices and workers • 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-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)

* Matches the stand-alone Cloudflare Email Security Advantage and Enterprise plans, respectively

Cloudflare | Interna Packages

Services	Capabilities	Impact	Essentials	Advantage	Premier
ZTNA & 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—*plus, DLP profiles explained below*	✓	✓	✓
	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 & DLP	API integrations *(beyond inline protection explained above)*	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) **& 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
Digital Experience Monitoring (DEX)	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		✓	✓

Products	Capabilities	Impact	Essentials	Advantage	Premier
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	Pre-delivery inbox protection (Inline) (Advantage*)	Deploy inline (as MX) to protect against business email compromise (BEC), malware, and malicious email links		✔	✔
	Pre- and post-delivery protection with link/attachment isolation (Inline, API) (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			✔

Transparent and inclusive pricing

- 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

* Stand-alone product packages for email security

** 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.

Why Cloudflare Interna packages?
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.

Each license expands your WAN

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 price

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

Simplified connectivity costs

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.

Premium DEM features

All advanced Digital Experience Monitoring (DEM) capabilities are part of your Interna Essentials package, not extra.

* Excludes mainland China PoPs

Get started on your path
to simple, secure access

Contact Sales

Not quite ready for a live conversation?

Keep learning more in our SASE reference architecture, or see how it works in an interactive tour of our Zero Trust platform.