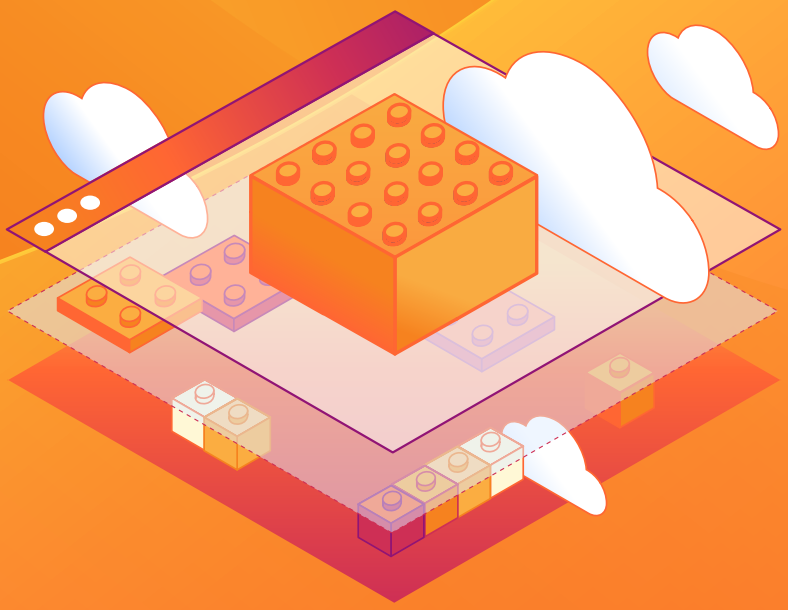
CLOUDFLARE

WHITEPAPER

Overview of Internet-Native SASE Architecture

Modernize how you secure user-to-application access



Content

Overview of Internet-Native SASE Architecture

Before Cloudflare

Most organizations rely on a 20+ year-old hub-and-spoke architecture. Internal users and apps are connected and secured differently than external users and apps. Access depends on the location, device, role, or identity provider (aka. IdP).

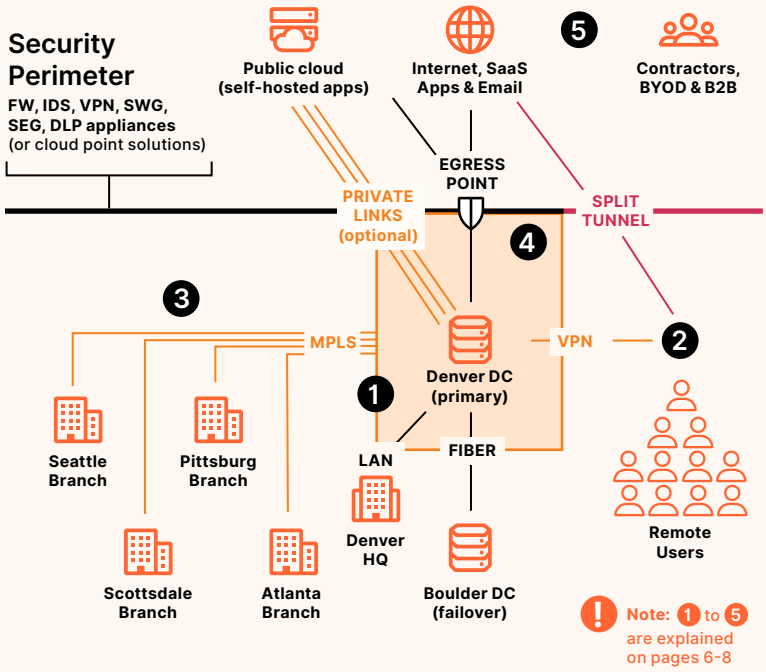
With Cloudflare

Your architecture is future-proofed with an Internet-native transformation embracing Zero Trust principles to consistently connect and secure all users and apps with a complete stack of cloud-native services that are easy to setup and operate.

✓ **Supported use case and security**
✗ **Unsupported use case and security**

		Internal apps	**External apps**		
		Self-hosted private DC, *colo or cloud (non-Web)*	**Self-hosted public cloud** *(AWS, GCP, Azure)*	**SaaS and email** *(M365, GSuite)*	**Internet** *(FB, Reddit)*
Before Cloudflare	**Internal users** (office and remote)	✓ **"Trusted" location, device, or employee role** ✗ **"Untrusted" location, BYO device, contractor role**		✓ **Corporate IdP** ✗ **Social IdP**	**n/a**
	External users	✗ **"Untrusted" IoT device or B2B customer role**		✗ **Social IdP**	**n/a**
	On-network connectivity	**"Trusted" direct LAN**	**"Trusted" private link**	**One "Untrusted" egress point**	
	Off-network connectivity	**"Trusted" VPN**	**"Untrusted" VPN split channel**		
	Access security stack	✓ **FW, IDS** *(w/ LB, DNS)* ✓ **FW** *(with LB)* ✗ **WAF, DDoS, ZTNA, SWG, SEG, RBI, DLP**		✓ **SWG, SEG, DLP** *(sometimes)* ✗ **CES, CASB, RBI**	
With Cloudflare	**Internal users** (office and remote)	✓ **Any verified identity (role-based optional), any device (posture-based optional), any location (context-based optional)**			
	External users	✓ **Any verified identity via any IdP (context-based optional, e.g. mTLS, OTP)**			*n/a*
	On-network connectivity	**Direct breakout egress points to Cloudflare**			
	Off-network connectivity	**Direct to Cloudflare**			
	Access security stack	✓ **FW, IDS, WAF, DDoS, ZTNA, SWG, SEG, RBI, DLP** *(with LB, DNS)*		✓ **SWG, SEG/CES, CASB, RBI, DLP** *(with ZT rules)*	

Before Cloudflare: Hub-and-spoke architecture



Additional cost and complexity

Backhauling traffic to one centralized egress point to enforce security is increasingly inefficient and ineffective.

Difficult to adopt new technologies

Public cloud and SaaS app adoption forces security or performance and user experience tradeoffs.

Difficult to grow the business

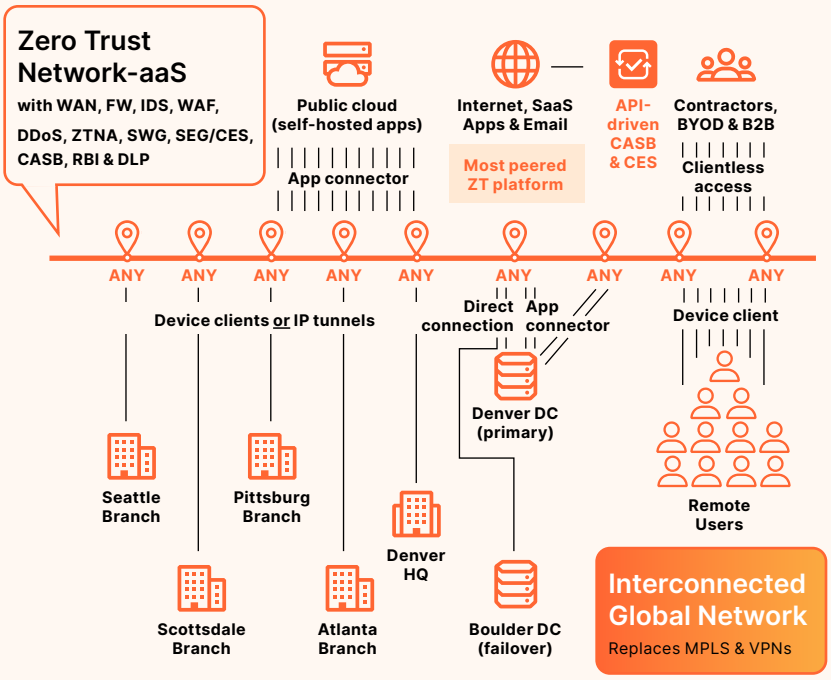
Hard decisions for where to deploy new hardware and how much capacity to ensure all users can access all apps.

Unfriendly model for remote work

The pandemic, climate, or geopolitical issues cause businesses friction as they rethink their resourcing models.

Figure 1: Hub-and-spoke architecture

With Cloudflare: Internet-native transformation



Improved experiences, reduced costs

Distribute enforcement points close to all users, reducing reliance on MPLS circuits at offices and hardware in DCs.

Reduced damage caused by breach

All users are conceptually 'off-net' and only access apps explicitly permitted, eliminating lateral movement.

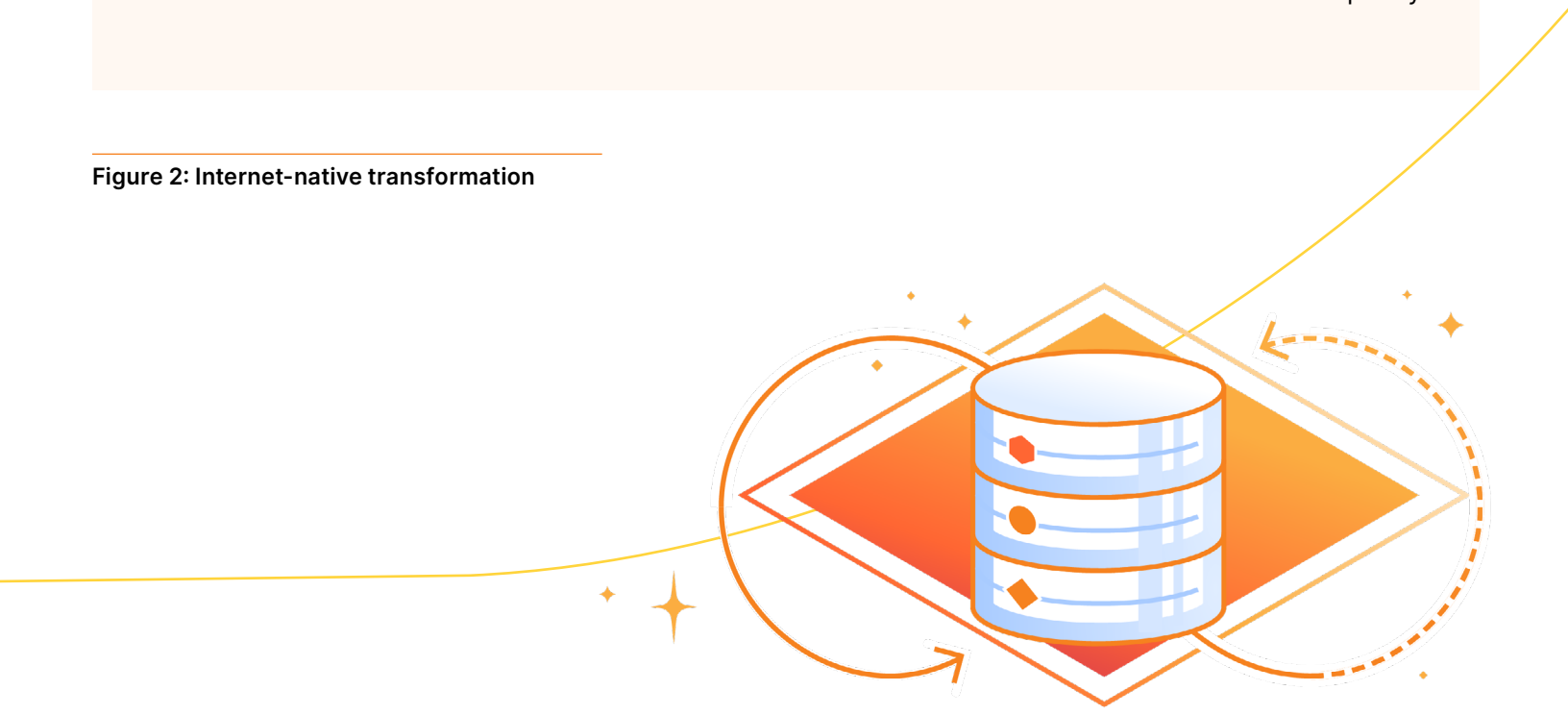
Hybrid workforce & multi-cloud ready

Simple reverse proxy and API setups enable secure access for contractors, BYOD, public cloud, SaaS apps & email.

Faster innovation & revenue growth

Accelerate digital transformation now that the Internet is faster, more reliable & more secure with unlimited capacity.

Figure 2: Internet-native transformation



Note: 1 to 5 are references on page 4's diagram

1 Corporate network benefits

Before Cloudflare

Users, devices, apps, and data have traditionally been grouped in a single location — your headquarters. It remained the central hub as businesses expanded geographically. Apps and data are hosted and maintained there, so it made sense for users to connect to that location to do their job. To reduce hardware costs, it also makes sense to center your security perimeter there. To protect the network, all traffic enters and leaves that one location. Yet, as users are increasingly more distant from these apps, it creates a bottleneck for productivity with many costly, complex band-aids to resolve this issue.

With Cloudflare

Instead of centralizing your network around your physical security and application infrastructure, Cloudflare becomes your 'first hop' for all security and networking functions for both users — on any device, in any location — and network locations. Users and networks have a shared-state connection to any Cloudflare data center wherein Anycast auto-selects the lowest-latency route. All traffic enters and leaves one customized Linux server where L3 firewall and L4-7 Zero Trust policies are applied in a single pass. This not only simplifies your existing hardware investments at your data centers, but distributes security infrastructure across the world, close to users, networks, and apps.

2 Remote user benefits

Before Cloudflare

Users outside of the 'secure' perimeter must connect back typically through a VPN connection terminating on a firewall. Traditionally, this represents challenges in (1) consistency and performance of user connectivity, (2) excessive access permissions for users on the network, and (3) inbound open ports in the firewall exposed to DDoS attacks. As user Internet traffic increases, businesses have to either accept the performance loss and increased backhauling costs or accept the loss of visibility and control by split tunneling remote user traffic around the perimeter.

With Cloudflare

Users benefit from a low-latency (<50ms) shared-state connection. They then transit our Internet-native backbone whether they are bound for internal or external apps, reducing performance hiccups, improving consistency, and eliminating the architecture capacity constraints and design concerns that come from backhauling user traffic. If you were split tunneling, this allows you to recapture all user traffic from anywhere in the world without backhauling, improving visibility and control without negatively impacting end user experience.

3 Branch office benefits

Before Cloudflare

As your office footprint becomes more distributed, there are difficult decisions for preparing each office for both internal WAN and Internet access:

- How do you ensure consistency and reliability supporting both? Or, do you overlay MPLS circuits (and maybe SD-WAN) to send office Internet traffic through your centralized security infrastructure.
- With global supply chain challenges, how long will it take to procure and deploy appliance hardware to increase throughput capacity?
- Do offices have interoperability requirements such as shared or local systems that each needs to access to justify the expensive and complexity of MPLS circuits and software-defined routers?

With Cloudflare

Instead of a heavy-handed, MPLS ripout approach, Cloudflare recommends an incremental roadmap to improve visibility and control plus reliability and performance. By using a combination of our device client and app connector software or configuring Anycast GRE and IPsec tunnels on existing routers, you can enable both internal WAN and Internet access to applications with more secure Zero Trust policies and cross-network connectivity on an as-needed basis without building overly permissive network policies. It enables you to remove office users (and IoT devices) from the traditional hub-and-spoke network, instead enabling them with a better cafe-like experience. All offices immediately gain a simple, fast software defined path to the Internet without expensive firewall (or SD-WAN) hardware. Apply the same comprehensive IP firewall, DNS filter, and Secure Web Gateway policies used to gain visibility and control for end users from the same simple management interface to reduce TCO.

4 Security perimeter benefits

Before Cloudflare

The moat that protects the castle is generally hardware derived. To ensure your sensitive data stays internal, and to protect your users and devices when engaging with the Internet, it made sense to centralize your security infrastructure — often firewall, intrusion detection, VPN, secure web and email gateway, and DLP appliances — at the egress point where a majority of your traffic needed to leave to the Internet. As the network expanded, and as both users and apps increasingly moved outside of the perimeter, this architecture becomes a chokepoint for adopting new technologies (e.g. Microsoft 365) and network paradigms. Downstream from this egress point, the MPLS circuits and hardware- or software-defined IP tunnels transporting corporate WAN traffic through your data center will also have hardware-based bandwidth limitations that must be taken into account.

With Cloudflare

As networks expand, application consumption matures and distributes, and users become increasingly geographically heterogeneous, Cloudflare transforms this hub and spoke architecture to distribute policy enforcement across our Internet edge, closer to all your users and applications they consume. Cloudflare can now provide the services provided by your FW, IDS, VPN, SWG, SEG, and DLP appliances plus DDoS, WAF, and newer technologies including ZTNA, CES, CASB and RBI. Since it also serves as the “first hop” termination point for both internal and external users, you get the benefit of this modern Zero Trust security applied in-line to ensure the transformation is effective and efficient.

5 SaaS app and email security benefits

Before Cloudflare

Most businesses are part way through their SaaS adoption journey, especially Microsoft 365 and Google Workspace that includes every office suite tool including email. SaaS represents both increased productivity and new challenges because it lives outside the perimeter. Often there is no security of data-in-transit between users and SaaS apps due to VPN split tunneling, unaffordable or non-scalable TLS inspection, or because it's an external user. And often there is no or fragmented visibility and control across all SaaS apps' configurations and data-at-rest profiles. Email is still the number one way that attackers get in without any network intrusion or malware download due to our implicit trust of inboxes — making everyone an insider. For things that are permanently outside the perimeter, how can you regain some of this visibility?

With Cloudflare

Security modernization frameworks — whether you call them Zero Trust Architecture (ZTA), Security Service Edge (SSE), or Secure Access Service Edge (SASE) — are all about unifying security posture in the face of continually distributed application and data usage. Cloudflare helps realize this vision by providing multiple modes of security; in addition to our in-line CASB delivered via the combination of our client or clientless SWG, ZTNA and RBI deployments we can also provide out of band API-driven CASB and cloud email security (CES). This delivers deep scans within SaaS apps, including Microsoft and Google's suites, with just a few clicks for profile discovery with findings that will prevent data exfiltration and identify new risks continuously — notably, phishing and BEC attacks that evade traditional secure email gateway methods.

With Others: Many stitched together architectures

Many offer piecemeal network and security infrastructure that cannot rapidly scale and evolve to connect all users to apps end to end. Visibility and policies are inconsistent to secure access against modern threats. Operations are complex and non-agile. User experiences are degraded.

Remote and external users

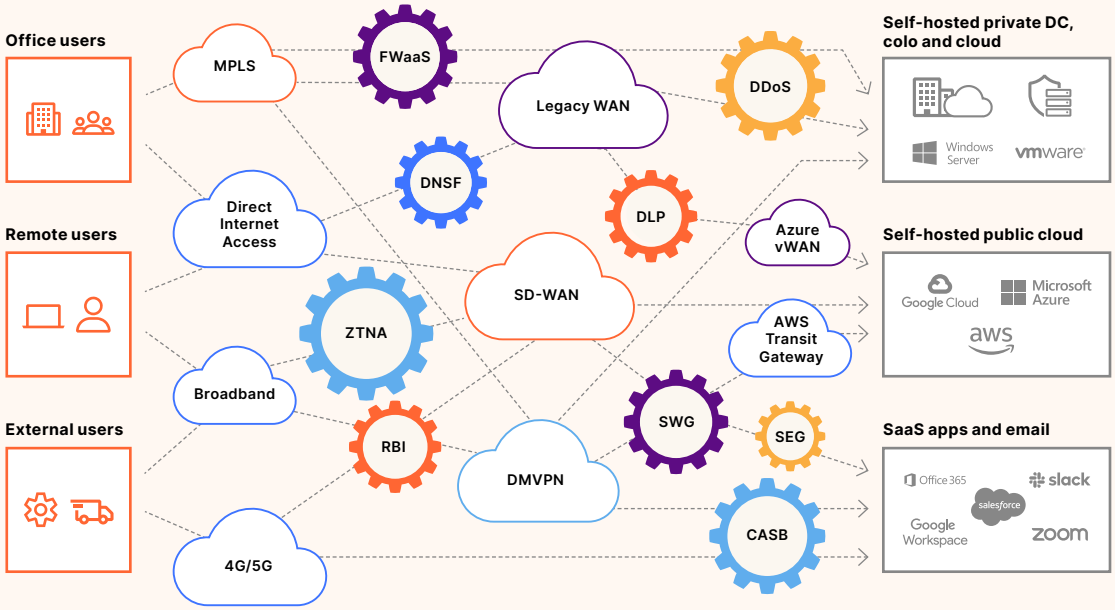
New Internet connectivity expands beyond our offices. New Zero Trust security is bolted on with reverse proxy and isolation modes to secure access for untrusted users, devices, and locations.

Public cloud, SaaS apps & email

New Internet connectivity breaks out of our offices. New Zero Trust security expands to combine API-driven with inline proxy modes to secure access to apps and email beyond our private network.

Modern threats

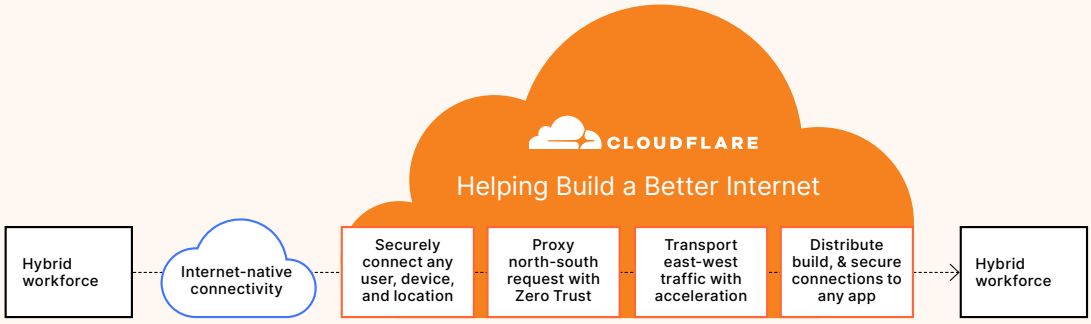
Excessive trust within offices and data centers is exploited. New Zero Trust security is bolted on with forward proxy and isolation modes to secure access against lateral movement.



With Cloudflare: One unified and composable architecture

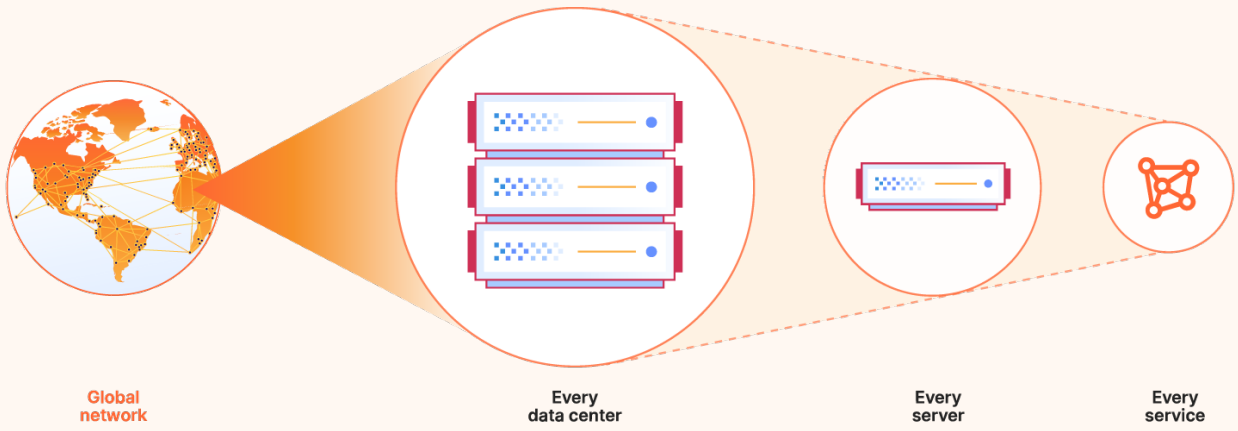
Your corporate network is as ubiquitous as the Internet

All connectivity and security services live in the cloud alongside applications within Cloudflare's network platform, ready and waiting to plug in and work together seamlessly. Now, any user across your hybrid workforce can consistently access any application across your hybrid multi-cloud environment — without security and performance tradeoffs.



One network, one control plane — everywhere

With Cloudflare, your corporate network can run with greater speed, reliability and security, than the Internet. Every service operating at the edge is built to run in every data center, so your users have a consistent, lightning-fast experience everywhere — whether they are in Chicago or Cape Town. This means all customer traffic is processed in a single pass at the data center closest to its source, with no backhauling or service chaining that adds latency.



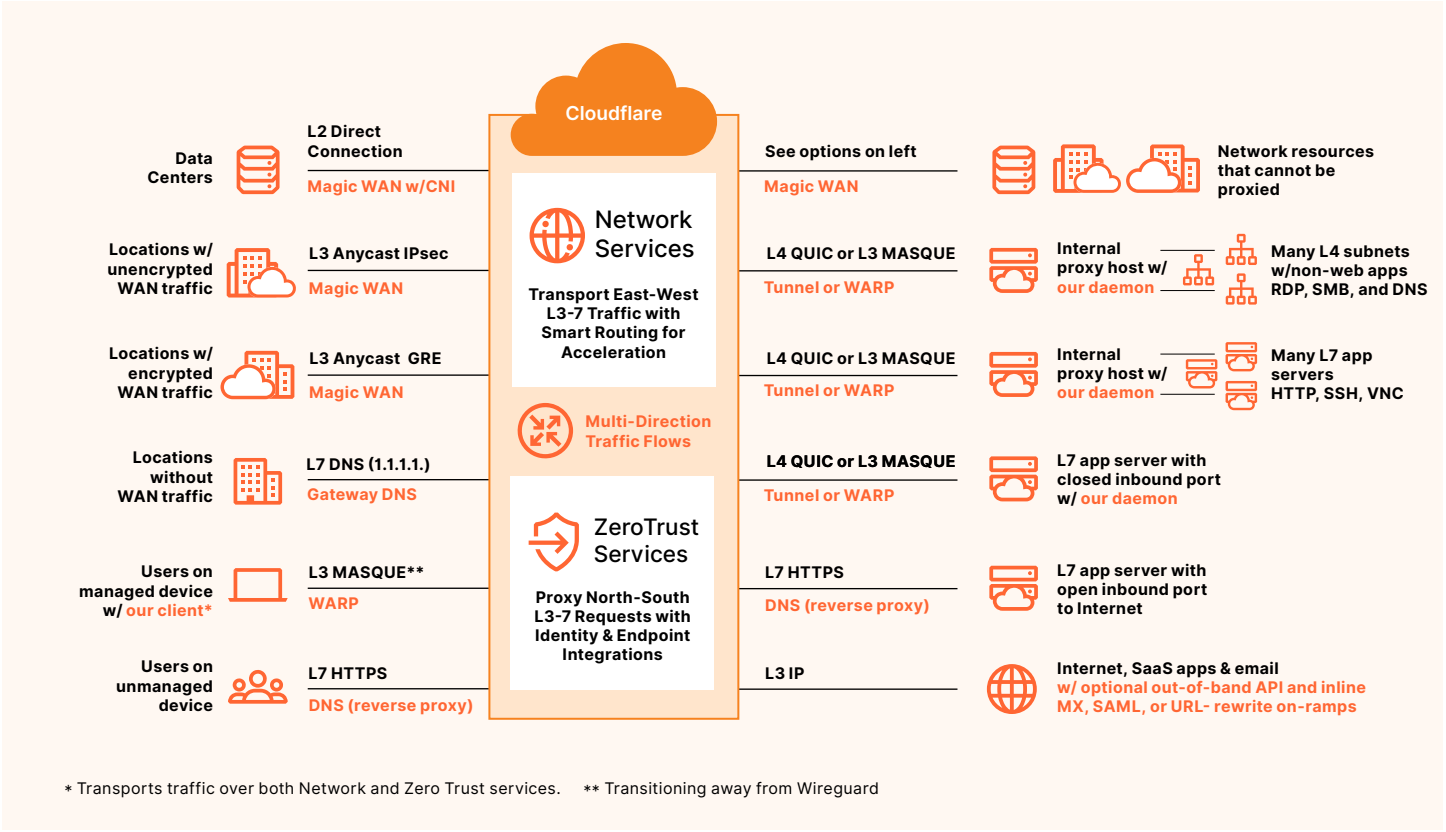
330+ cities available to everyone
296+ Tbps of network edge capacity
12,500+ interconnects to service and cloud providers, plus major enterprises
~50ms from 95% of Internet users

100% uptime SLA with Anycast
FedRAMP authorized at the Moderate level
IPv6 and TLS 1.3 processing and inspection without security tradeoffs

How our Zero Trust Network as a Service works

Composable on-ramps for any-to-any, end-to-end connectivity

Cloudflare network on-ramps use a shared-state connection via one unified control plane. So, data centers with network interconnects, offices with Anycast IPsec or GRE tunnels, users with wireguard clients, and app servers with Cloudflare Tunnels can transport and/or proxy traffic between each other and the Internet through every Cloudflare service.



* Transports traffic over both Network and Zero Trust services. ** Transitioning away from Wireguard

Zero Trust services

- Access control: Access and Gateway w/CASB
- Traffic filtering: Gateway and Cloud Email Security
- Content inspection: Gateway and Cloud Email Security
- Threat and data protection: Cloud Email Security and Gateway w/Browser Isolation, CASB and DLP

Network services

- Access control: Magic Firewall
- Traffic routing optimization: Magic WAN
- Intrusion detection: Magic Firewall
- DDoS protection: Magic Transit

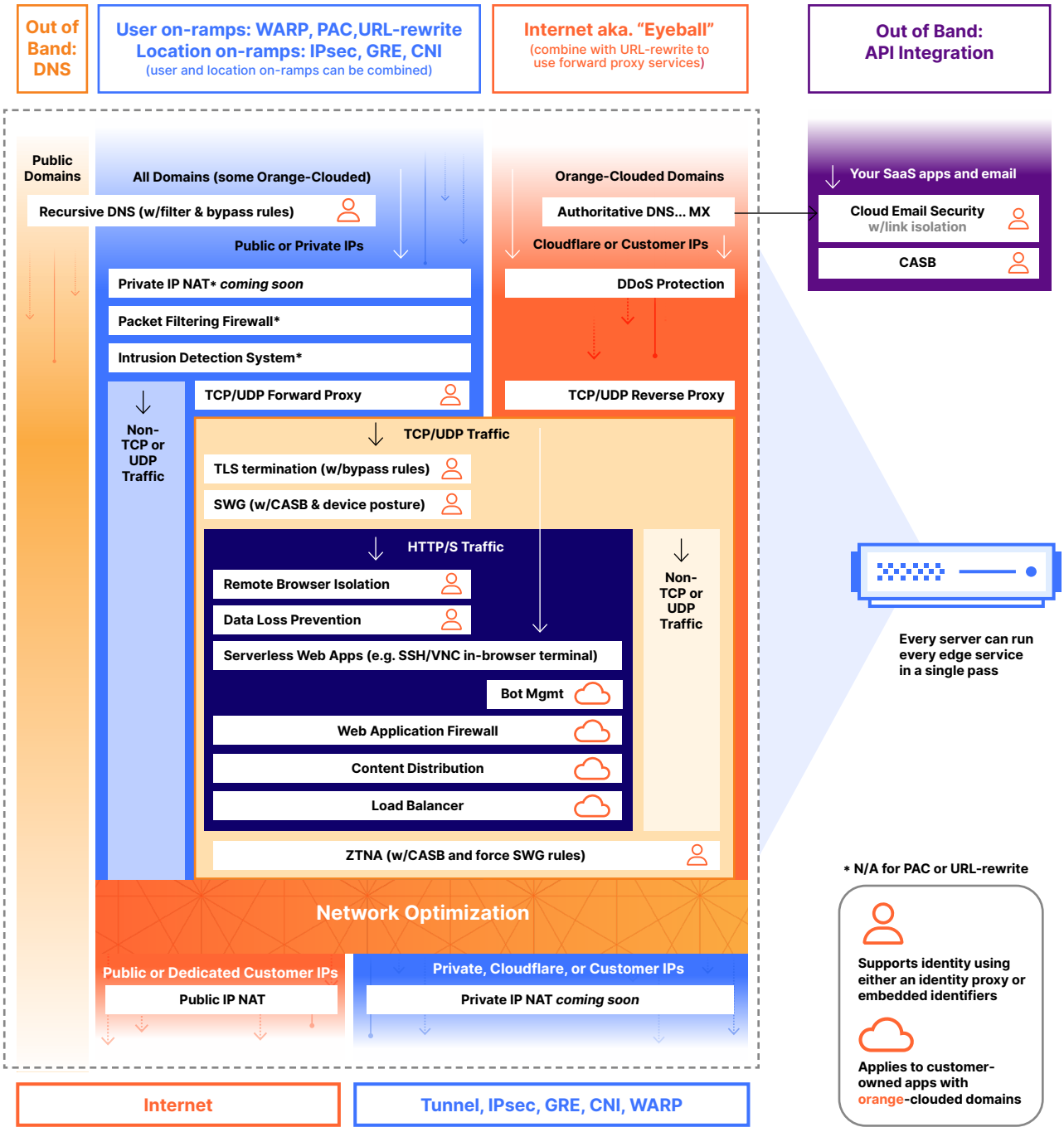
Built-in application security and performance

Customers also benefit from our application services that run inline with our Zero Trust services. Many are already enabled by default within your license.

- Protect apps with open ports: L7 DDoS Protection
- Prevent contractors from exploiting apps: WAF
- Simplify on-ramping traffic to apps: DNS
- Increase app reliability with zero downtime: LB
- Reduce bandwidth costs and improve UX: CDN

No security vs. user experience tradeoffs

Our entire edge service stack — plus, out of band services — are natively built to work together. Zero Trust, network, and application services sit between the appropriate on-ramps based on the domain, IP, and protocol. Requests and traffic are filtered, inspected, isolated, and verified in a lightning-fast single pass closest to its source; then routed and accelerated across the Internet to its destination.



Three reasons to transform your architecture with Cloudflare

Deployment simplicity

Cloudflare customers value a uniform and composable platform for easy setup and operations. They do not want piecemeal services that lead to a more time-consuming, error-prone experience.

Network resiliency

The Cloudflare global network is built with end-to-end traffic automation for reliability and performance that customers trust. No one wants manual connectivity to many cloud networks that forces security tradeoffs.

Innovation velocity

Cloudflare is architected to integrate innovations into the same network that customers use to evolve fast. No one wants new services bolted on or stagnating adoption of new standards that delays their future.

Start your journey to a faster, more reliable, more secure network

Request an architecture workshop

Not ready for your architecture workshop?
Keep learning more in our SASE reference architecture

Acronyms:

- BEC = Business Email Compromise
- CASB = Cloud Access Security Broker
- CDN = Content Delivery Network
- CES = Cloud Email Security
- DDoS = Distributed Denial of Service
- DLP = Data Loss Prevention
- DNS = Domain Name System
- DNSF = DNS Filter
- FW = Firewall
- IDS = Intrusion Detection System
- LB = Load Balancer
- MPLS = Multiprotocol Label Switching
- RBI = Remote Browser Isolation
- RDP = Remote Desktop Protocol
- SD-WAN = Software-Defined WAN
- SEG = Secure Email Gateway
- SMB = Server Message Block
- SWG = Secure Web Gateway
- WAF = Web Application Firewall
- WAN = Wide Area Network
- VPN = Virtual Private Network
- ZTNA = Zero Trust Network Access

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-6350.2024AUG26