Comparing Cloudflare vs. Zscaler
Which better fuels transformation?

Zero Trust implementation doesn't have to be so hard

Don't lock yourself out of your own future

Cloudflare helps you move quickly and nimbly as the future of networking evolves.

Simple deployment, network resiliency, and swift innovation provide a stronger foundation for true transformation of networking, security, and applications.

Three reasons customers choose Cloudflare over Zscaler

1.

Simplicity
to deploy fast

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.

2.

Trusted connectivity
to protect reliably

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.

3.

**Future-proof**
to evolve rapidly

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.

Pick an architecture designed for the future of networking

When choosing Cloudflare over Zscaler, you will benefit from a network built to run every edge service on every server — globally. We bring the entire network to the cloud and enable Zero Trust with single-pass inspection, quickly connecting users, devices, workloads, offices, clouds, and data centers to resources, wherever they are located. It is easy to deploy and run, so you can take control and start modernizing your environment at your desired pace, without needing an infinite IT budget, a parade of expensive POCs, and multiple complex deployments to get there.
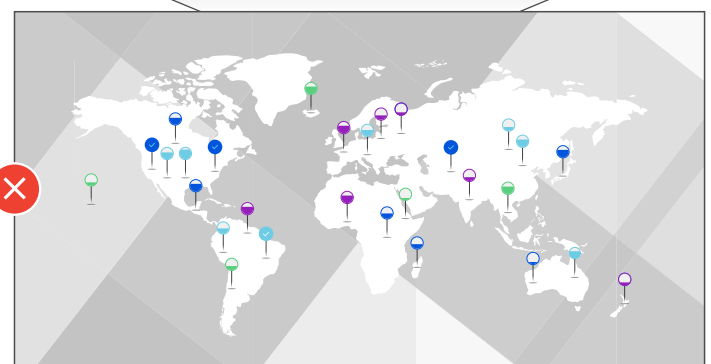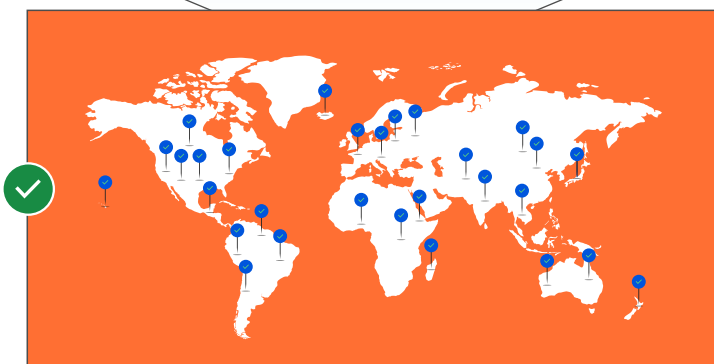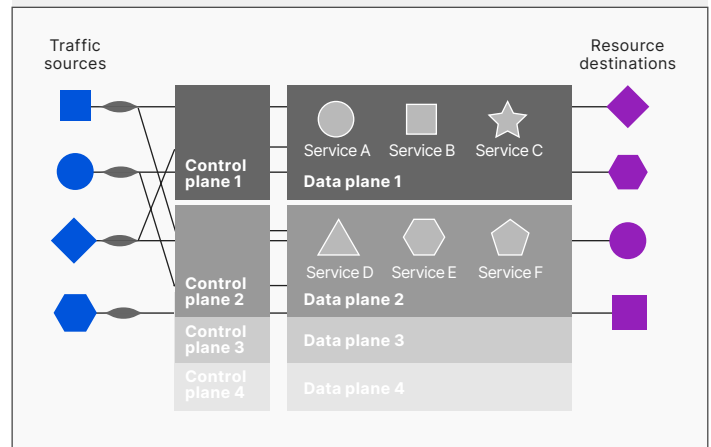
Cloudflare - Unified

A unified control plane provides single-pass inspection and trusted connectivity.
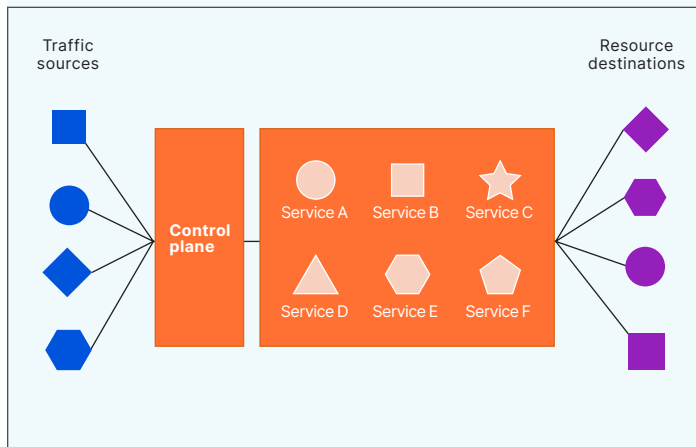
VS

Zscaler - Fragmented

Meanwhile, a fragmented and stitched architecture increases complexity and can introduce additional risk.

Traffic sources | Resource destinations

Control plane — Service A, Service B, Service C, Service D, Service E, Service F

Traffic sources | Resource destinations

Control plane 1 / Data plane 1 — Service A, Service B, Service C
Control plane 2 / Data plane 2 — Service D, Service E, Service F
Control plane 3 / Data plane 3
Control plane 4 / Data plane 4

In a comparative sampling of data center locations, each Zscaler service runs in a subset of the locations, and only a subset of locations are available to every customer.*****

*As of Jan 2022: According to cloudflarestatus.com and cloudflare.com/network, Cloudflare has public data centers in 250+ cities. Many cities are served by more than one data center. According to trust.zscaler.com and config.zscaler.com, Zscaler has 73 public data centers in 55 cities with 13 data centers in no published clouds and 11 data centers with auto geo proximity disabled. The other claimed 77 data centers do not appear to be publicly documented.

![Cloudflare logo]

Fast-track your journey to secure any-to-any connectivity

While Zero Trust principles remain the same across providers, implementation and ROI vary widely.

Cloudflare uniformly connects and secures end-to-end using one network and control plane to provide a better experience for both your IT practitioners and end users.

Is the deployment simple enough?

- Who would pick siloed services as a first choice? No one. That is why all Cloudflare on-ramps and edge services actually work together.

- Don't wait weeks on white-glove support to start adoption. Our services platform is composable, so in just minutes and hours you are solving real use cases.

- Avoid bloated virtual machine deployment logistics. Speed setup time with software-only connectors and one-time integrations.

Cloudflare - Simple

Cloudflare's network, Zero Trust, and application edge services are natively integrated through a unified backend architecture.
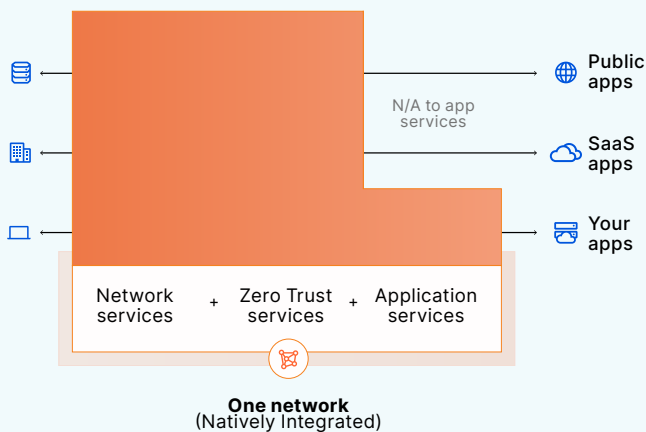
VS

Zscaler - Complex

Zscaler's network and Zero Trust services are stitched together and don't completely cover remote users, plus application services are entirely siloed across multiple vendors.

N/A to app services

Public apps

SaaS apps

Your apps

Network services + Zero Trust services + Application services

One network
(Natively Integrated)

N/A to app services

Public apps

SaaS apps

Your apps

Network services | Zero Trust services | Application services

Network 1
(Bolted on)

Network 2
(Native)
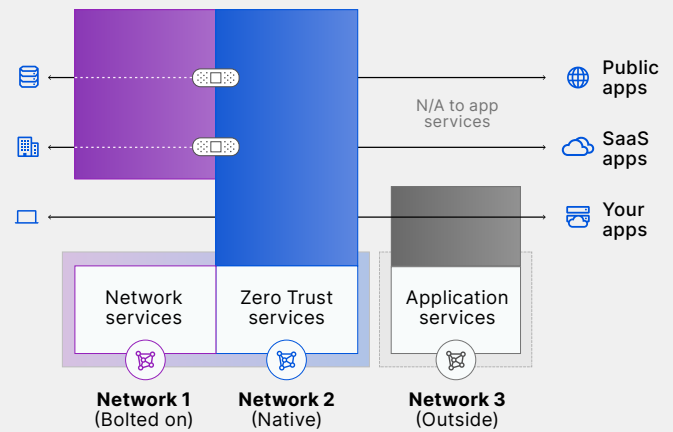
Network 3
(Outside)

## Only a better Internet can consistently protect your business

Today, roughly 20% of all websites are routed through the Cloudflare network — using the same proxies that deliver Zero Trust for your business.

Our end-to-end traffic automation ensures reliable and scalable network connectivity with consistent protection from any location.

Is the network resilient enough?

- Security should not feel like a puzzle. Every edge service is built to run in every network location, available to every customer.

- We feature a 100% uptime SLA for paid plans that only an Anycast architecture can deliver. Other vendors cannot just add this to their platform later.

- Direct private interconnects keep your traffic away from the public Internet. This should be non-negotiable, but Zscaler does not offer it.
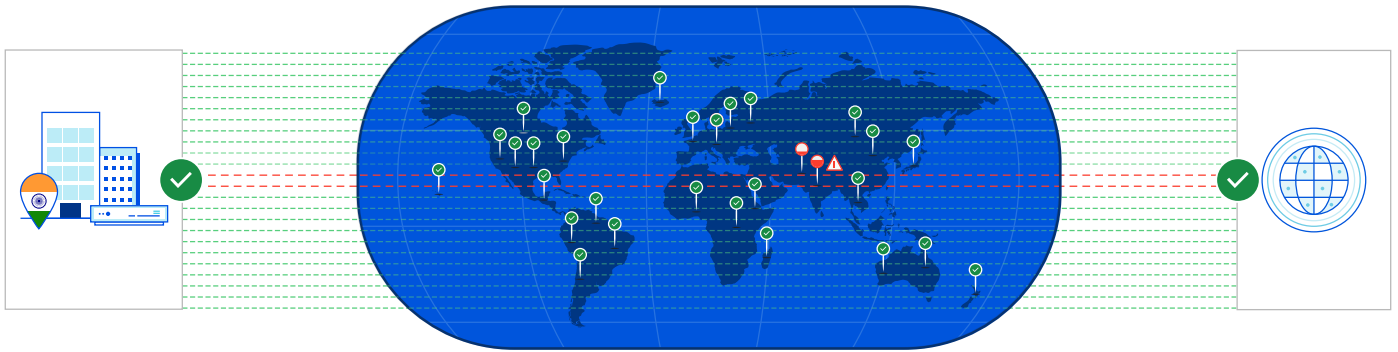
Cloudflare - Resilient

The Anycast architecture of the Cloudflare network delivers peace of mind. Should a regional issue occur, traffic automatically reroutes to keep edge services online.

VS

Zscaler - Vulnerable

When service locations are limited, this can leave you vulnerable should a regional issue arise. If planned or unplanned outages co-occur across primary and secondary data centers, Zscaler services could experience avoidable downtime.
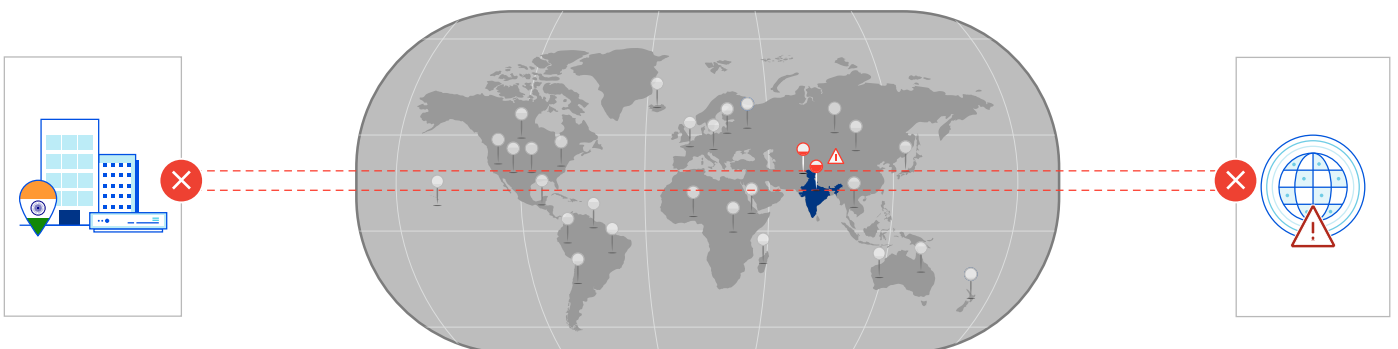
Relentlessly stay ahead of modern business needs to secure your future

Our future-proof architecture helps us build and ship very quickly — something we have established a solid reputation around.

Check out our blog for proof! Pick a customer-led, agile provider with a lightning fast rate of change to innovate new networking, security, and application capabilities.

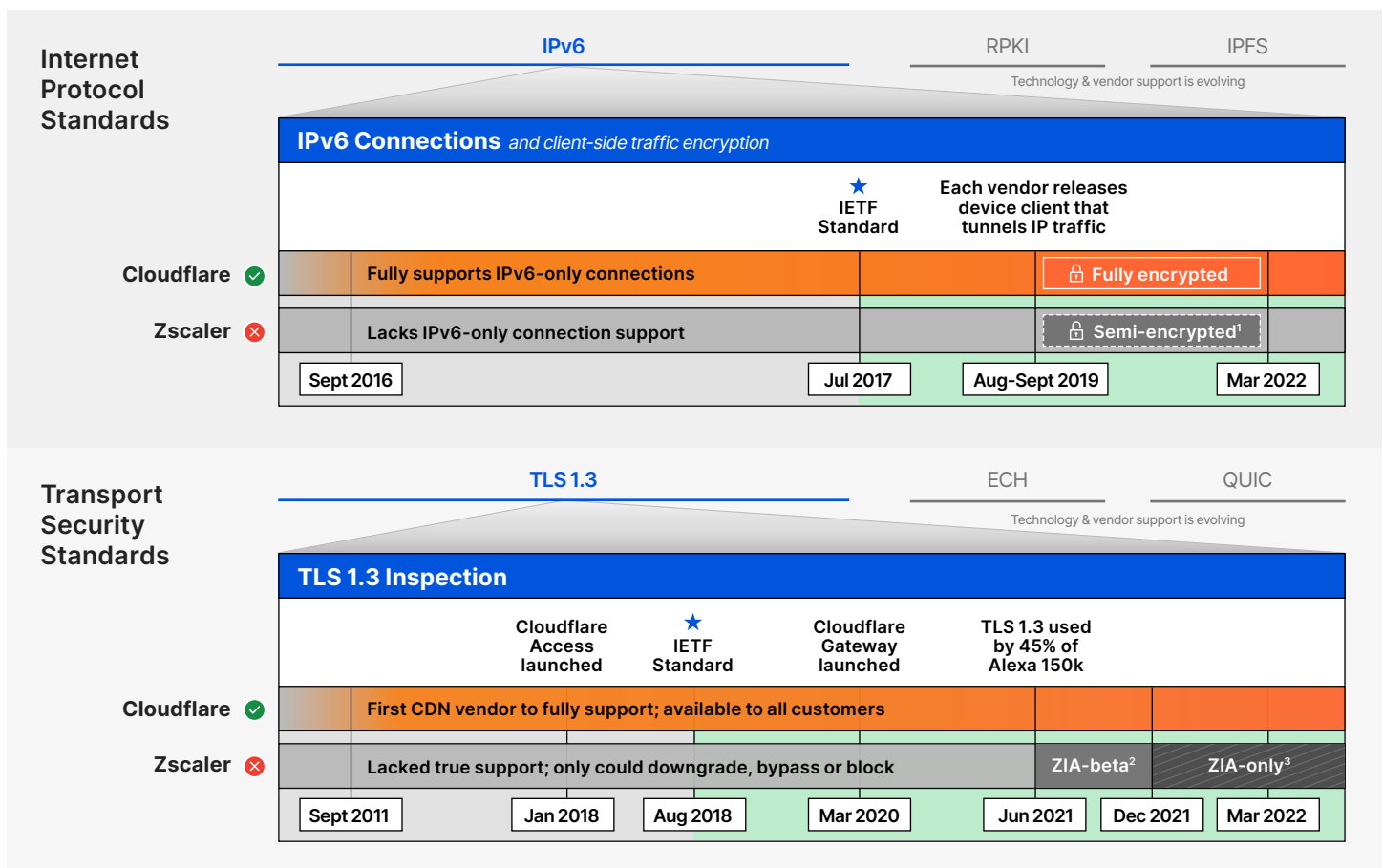## Is the pace of innovation fast enough?

- We have one composable, developer-friendly cloud platform, not multiple fragmented clouds, that is extensible with any future edge service.
- We achieve rapid, native adoption of new Internet and security standards.
- Our history of technical prowess and growth speaks for itself, and our foundation provides extreme optionality.

✓ Cloudflare - Innovate

You need fast innovation and flexibility to secure your future, whatever that might be. Cloudflare is known for executing quickly when adopting new technologies.

✗ Zscaler - Stagnate

You shouldn't have to prolong your wait for important new technology adoption, like fully integrating support for TLS 1.3 or IPv6.

Internet Protocol Standards

IPv6 | RPKI | IPFS
Technology & vendor support is evolving

IPv6 Connections *and client-side traffic encryption*

	★ IETF Standard	Each vendor releases device client that tunnels IP traffic	
Cloudflare ✓	Fully supports IPv6-only connections	🔒 **Fully encrypted**	
Zscaler ✗	Lacks IPv6-only connection support	🔒 **Semi-encrypted[1]**	
	Sept 2016	Jul 2017	Aug-Sept 2019	Mar 2022

Transport Security Standards

TLS 1.3 | ECH | QUIC
Technology & vendor support is evolving

TLS 1.3 Inspection

	Cloudflare Access launched	★ IETF Standard	Cloudflare Gateway launched	TLS 1.3 used by 45% of Alexa 150k		
Cloudflare ✓	First CDN vendor to fully support; available to all customers					
Zscaler ✗	Lacked true support; only could downgrade, bypass or block				**ZIA-beta[2]**	**ZIA-only[3]**
Sept 2011	Jan 2018	Aug 2018	Mar 2020	Jun 2021	Dec 2021	Mar 2022

---

1. Device client uses null-encrypted data channel for ZIA traffic. Only the TLS control channel is encrypted. **2.** The Zscaler Beta cloud for ZIA only has three data centers. **3.** Only applicable to ZIA traffic. For ZPA traffic, the device client uses a TLS 1.2 tunnel to encrypt data channel, but their cloud proxy does not inspect app-encrypted TLS 1.3 traffic.

See how Cloudflare stacks up →

	Cloudflare	Zscaler
Deployment Simplicity	✅	❌
On-ramps and services	Composable and work together	Many run separate from others
Security and connectivity	End-to-end: User/workload-to-app plus WAN and apps	Limited: User/workload-to-app only
Network and control plane	Uniform, one network, one control plane	AWS/Azure-augmented network, many control planes
Setup requirements	Often clientless, VM-free software, one-time integrations	Often clients, VM sizing logistics, repeated integrations
Network Resiliency	✅	❌
Global connectivity	Yes: Anycast architecture	No: Active/active local termination
Bypass public Internet	Yes: Private interconnects per customer to Cloudflare network	No: Private service VMs bypass Zscaler cloud, not the Internet
Network location availability	Every location available to every customer	Only a subset of locations available to every customer
Service availability	Every edge service built to run in every network location	Each service runs in a subset of network locations
Innovation Velocity	✅	❌
Cloud-native architecture	One cloud platform with uniform edge service availability	Many clouds with fragmented service availability
Developer-friendly platform	Composable and extensible with any future edge service	Bolted on for too long, loosely integrated years later
New Internet and security standards	Rapidly adopted, often contribute to designing them	Some introduced years later
ZTNA and SWG development	Built in four and two years, respectively	Built in six and 14 years, respectively

Why wait and pay to try Zscaler when you can start our free plan in minutes?

See how simple it is