CLOUDFLARE

SOLUTION BRIEF

Extend ZTNA without going all-in on Zscaler

Secure remote access without disrupting your web inspections — no extra device client required.

Best-of-breed to embrace Zero Trust

Overcome hesitations with Zscaler

Even with a web proxy like Zscaler Internet Access (ZIA) in place, many organizations hesitate to extend Zero Trust Network Access (ZTNA) controls. Doubling down with the wrong long-term vendor can lead to complexity juggling new dashboards, poor end user experiences, and limited support at rising price tags.

Run Cloudflare's clientless ZTNA with ZIA

If you are hesitating, let Cloudflare start modernizing access for priority apps and risky users — without adding another software client.

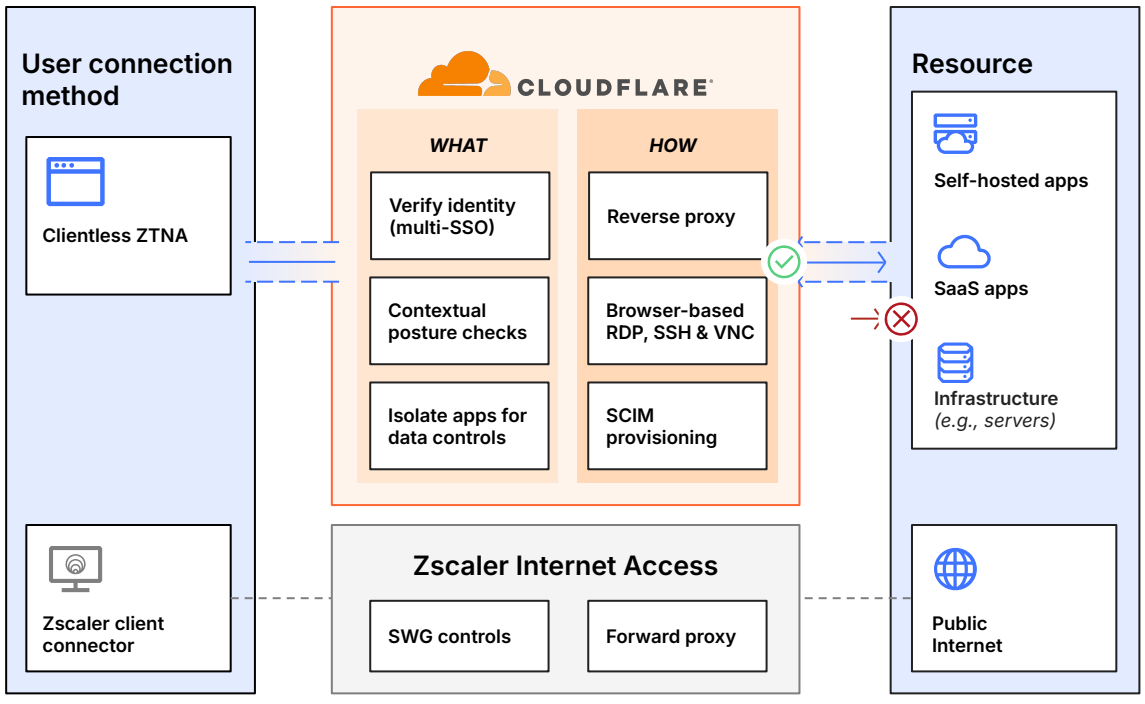
Cloudflare's clientless ZTNA is simple to scale and runs seamlessly in parallel with web protections from ZIA, so you can replace legacy tools and navigate hybrid work with a best-of-breed approach.

84% of IT & security leaders say that clientless ZTNA significantly accelerated Zero Trust adoption.[1]

The Cloudflare difference

- **Simple management** with browser-based access to self-hosted apps and infrastructure. One intuitive API and Terraform provider help you scale automation. No virtual machines needed to connect resources.
- **Consolidate more** with the only vendor to secure both public-facing infrastructure for your customers *and* internal infrastructure for your workforce.
- **Seamless user experiences,** proven faster in first- and third-party testing vs. Zscaler. A private global backbone optimizes East-West connectivity, wherever your users and apps are.

Start offloading VPN traffic with Cloudflare's clientless ZTNA



How it works

Avoid setting up VPNs for contractors, third parties, developers, and users on unmanaged devices.

Get support for web apps and browser-based SSH, RDP, and VNC.

Isolate to enforce data controls and L7 DLP policies through the browser.

1. Enterprise Strategy Group custom research commissioned by Cloudflare, "Considerations for Implementing Zero Trust for the Workforce", July 2024

Advancing Zero Trust posture for app access

	Use cases	Sample controls	ZIA impact
Step 1: Clientless access	• Augment VPN • Secure contractors / BYOD • Secure GenAI tools • Secure privileged access to infrastructure (SSH, RDP)	• Identity checks (enterprise / social) • Isolate apps to block copy / paste, up / download, and inputs • Lightweight app connector to connect resources without VMs	• No action required
Step 2: Full proxy ZTNA with device client	• Retire VPNs by extending ZTNA to legacy apps and private networks • Support peer-to-peer connectivity between devices • Set up longer-term SASE migration	• Device posture with device client or third-party integrations • Location-aware policies for office users on managed networks • Troubleshoot with digital experience monitoring	• Split tunnel Internet-bound traffic to ZIA and private app traffic to Cloudflare

APPLIED

Insurance technology
Read case study

Replaced Zscaler ZIA and Cisco VPN to unify remote access controls across 2,500+ workers.

THG

Global e-commerce
Read case study

Replaced Zscaler ZIA and ZPA for 7,000+ workers.

1 week to automate migration of ZIA policies.

Extend Cloudflare security with other clientless use cases

DNS filtering for threats and content

Block Internet threats, secure guest WiFi, and enforce acceptable use policies with clientless DNS filtering.

For offices: Point network routers to Cloudflare for DNS resolution and location-based policies.

For remote users: Filter DNS over HTTPS (DoH) requests using a user-specific authentication token.

Protect email inboxes

Integrate Cloudflare's email security with your existing email provider — within minutes — to block phishing attacks, malware, business email compromise, and vendor email fraud.

Augment your built-in email controls with Microsoft and Google with flexible inline, API-based, or hybrid deployment options.

Want to learn more about modernizing remote access? See our implementation guide or request a conversation.

