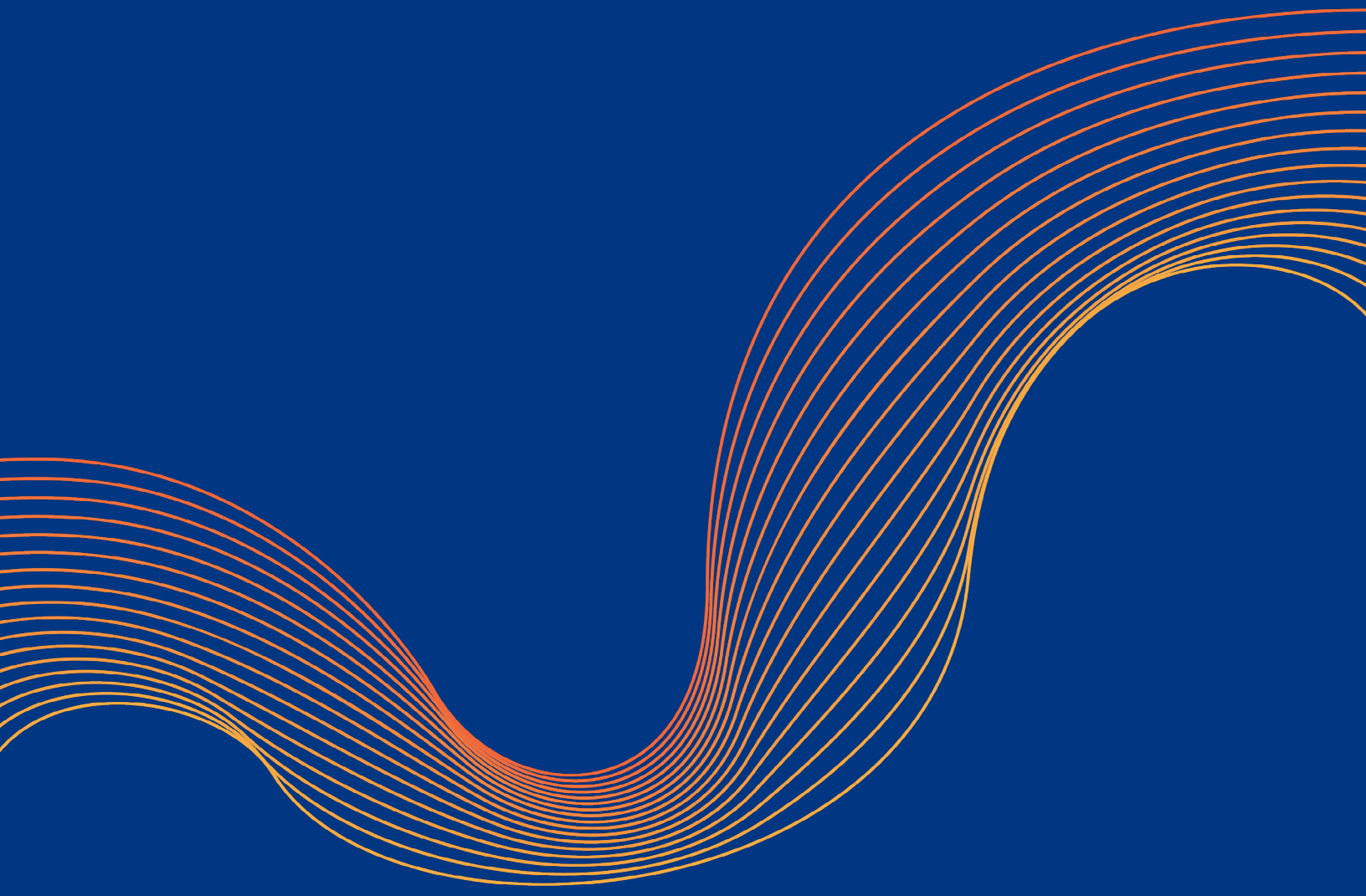
WHITEPAPER

CLOUDFLARE

Can ZTNA replace your VPN? Compare 3 remote access approaches



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

INDEX

INTRODUCTION

Secure, seamless remote access is a business enabler — boosting remote user productivity and reducing the time spent by IT teams to onboard and maintain user-to-application connectivity with agility and resilience. And yet, remote access remains a challenge for many organizations.

Once upon a time, VPNs offered a simple way to connect a few remote users to corporate networks for brief periods of time. As workforces became more distributed, however — and organizations needed to keep remote users securely connected for longer periods of time — the flaws in this approach became evident, from sluggish performance and increased security risks to scalability concerns.

As remote access needs grow, organizations are increasingly shifting away from traditional VPN implementations and toward more secure and performant remote access solutions. Zero Trust network access, or ZTNA, creates secure boundaries around specific applications, private IPs and hostnames, replacing default-allow VPN connections with default-deny policies that grant access based on identity and context.

In 2020, approximately 5% of all remote access usage was predominantly served by ZTNA. Due to the limitations of traditional VPN access and the need to deliver more precise access and session control, that number is expected to jump to 40% by 2024.[1]

While ZTNA offers enterprises several clear advantages — and expanded functionalities — over VPNs, many organizations have found it an incomplete replacement for VPN infrastructure. But as ZTNAs become more robust and VPNs become more problematic, that's changing fast. This paper contrasts VPNs and ZTNA remote access solutions to illuminate their benefits and limitations, while shedding light on the most important considerations for migration projects. It explains how Cloudflare offers ZTNA, and recommends a set of action steps for transitioning legacy VPN infrastructure to faster and safer Zero Trust connectivity for remote users.

[1] Riley, Steve, MacDonald, Neil, and Orans, Lawrence. "Market Guide for Zero Trust Network Access." Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. Accessed 21 June 2021. See Table 1 for details.

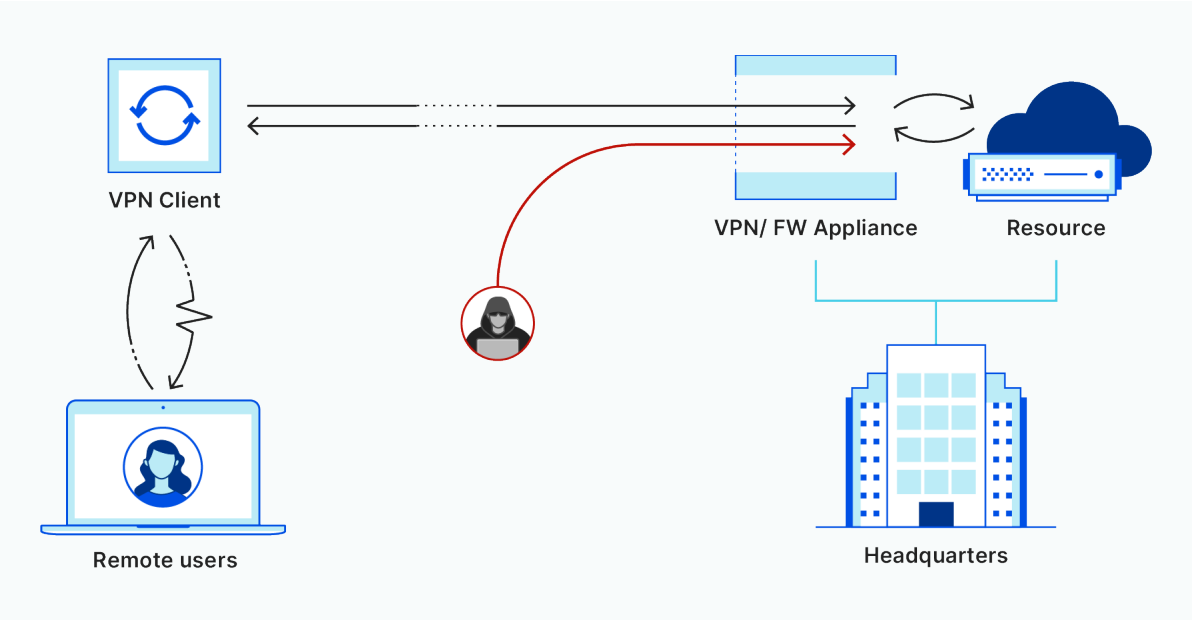
APPROACH #1: LEGACY VPN

For decades, VPNs have enabled organizations to connect their remote users to corporate networks with some measure of privacy and security. Instead of accessing sensitive information over the public Internet, where any attacker might snoop or steal data, VPNs allow users to safely access internal resources via an encrypted connection.

The two most common modes of VPN implementation are client-based VPNs and clientless SSL-VPN. Each comes with their own benefits and challenges:

Client-based VPNs connect remote users to a private network via an encrypted tunnel. This connection is established through a software application, or client, which requires users to authenticate once with a username and password in order to gain persistent access to any resource within that network.	**Benefit:** Once connected, free lateral movement makes it easy for users to quickly access multiple resources by accessing applications and connecting to internal hosts. **Challenges:** • **Not designed for roaming users and mobile devices**. As users roam about, both their laptops and mobile devices seamlessly reconnect as wireless networks change from location to location. However, VPN clients are not adept at fluidly handling these reconnections, requiring users to repeatedly force the VPN client to restart and re-authenticate — causing lost productivity and creating IT tickets. • **Poor visibility.** With this method, the VPN infrastructure terminates the encrypted tunnel from the VPN client behind the data center's internal firewall. Although these connections are logged, there are no application-specific centralized logs that reveal which applications users have accessed or the actions they have taken within the application.

Clientless SSL-VPN portals allow a few remote users to connect to a few browser-based applications within a private network. This connection is made possible using a web server built into the network appliance running the VPN service.	**Benefit:** Instead of using a client on a device, any web browser can use the portal's SSL certificate to establish an encrypted HTTPS connection to support contractors on unmanaged devices. **Challenges:** • **Security concerns.** Most VPN setups within the data center grant total access to users, which poses a problem for organizations that do not want non-employees, like contractors, to gain unrestricted access to sensitive resources and applications. • **Not built to support a high number of concurrent users.** Unlike modern cloud services, the portal's web server cannot be elastically scaled up to meet higher demand. Instead, more network appliances must be installed and load-balanced to scale the portal, which is often expensive, complex, and ineffective, since the rest of the appliance's functionality may be underutilized. • **Clientless SSL-VPN portals expose firewall ports and web servers to attacks.** In order to allow the web server hosting the portal to reach internal applications, administrators must open inbound firewall ports, exposing them to external attacks. Both the open ports and the web server itself must be shielded from DDoS and web application attacks, which requires more complex configuration and higher costs in order to secure this connectivity method.



While VPNs provide a basic level of privacy for remote users, they were not designed with security or scalability in mind. Traditionally, organizations have used VPNs to connect a few remote users to the corporate network for short periods of time. As remote work becomes more prevalent, however, VPN issues begin to multiply:

- **Users experience sluggish performance.** If the VPN infrastructure does not have the capacity to handle the traffic throughput and concurrent connections created by their workforce, users experience a slowdown in their Internet connection. Additionally, when VPNs are located a great distance from both the user and the application server they are trying to access, the resulting travel time creates latency.
- **Corporate networks are left vulnerable to attack.** VPNs typically use a castle-and-moat model, in which a user is given unfettered access to all corporate resources once they connect to a network. With no built-in method of restricting access to critical infrastructure and data, organizations are forced to configure costly, complex security services like next-generation firewalls and network access control — or left vulnerable to malicious lateral movement, resulting in larger data breaches.

The challenge of hosted VPN services

Some vendors have shifted the network appliance running the VPN service into the public cloud, where it runs as a virtual machine at one or more data centers. The VPN may or may not be bundled with (or daisy-chained to) additional security services.

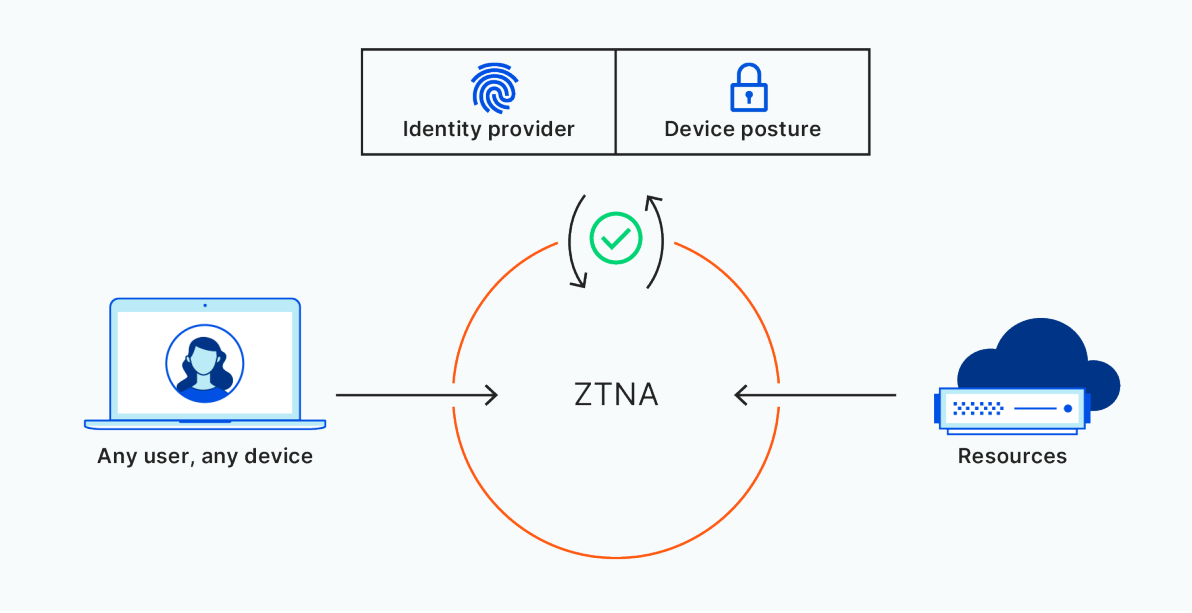
Placing a VPN in the cloud may appear to solve some of the scalability issues inherent in hardware VPN appliances. However, doing so also presents some significant security and scalability challenges.

For instance, consider an organization that hosts a full NGFW (next-generation firewall), which combines the VPN with a firewall and additional security functionalities. Since the NGFW is offered as a bundled service, it is impossible to independently scale any specific functionality on demand. Scaling up one function requires scaling up the entire service; to do so, more VMs must be spun up in order to load balance a small amount of compute being performed in each VM. Not only is this an impractical and unwieldy solution, but it is likely to incur high costs as the organization's remote access needs continue to expand.

APPROACH #2: ZERO TRUST NETWORK ACCESS

Zero Trust security circumvents many of the challenges inherent to VPNs. It is based on the principle that no user or device inside or outside of a network can be trusted by default. In order to reduce the risk and impact of data breaches, internal attacks, and other threats, a Zero Trust approach...

- authenticates and logs every login and request,
- requires strict verification of all users and devices,
- limits the information each user and device can access based on identity and context,
- and adds end-to-end encryption to isolate applications and data within the network.



As with VPNs, there are several ways ZTNA can be configured:

1. **Clientless (or service-initiated) ZTNA** uses the existing browser, instead of a client, to create a secure connection and authenticate user devices. Traditionally, clientless ZTNA has been limited to applications with HTTP/HTTPS protocols, but compatibility is evolving fast.[2]
   - **Benefit:** Clientless ZTNA uses a reverse-proxy connection to prevent direct access to applications, blocking users from accessing applications and data they may not have permission to view and allowing administrators greater control and flexibility in management.
2. **Client-based (or endpoint-initiated) ZTNA** installs software on a user device before an encrypted connection can be established between the controlling agent and authorized applications.
   - **Benefit:** Client-based ZTNA allows administrators greater insight into the device posture, location, and risk context of users accessing applications, so more granular policies can be created and enforced. And, because this method is not restricted to HTTP/HTTPS, it can be used to access a wider range of non-HTTP applications — such as those that rely on SSH, RDP, VNC, SMB, and other TCP connections.

[2] As of June 2021, Cloudflare's ZTNA solution supports clientless access to SSH and VNC applications, with support for RDP planned in the future.

Challenges of ZTNA implementation

While ZTNA provides clear advantages over traditional VPNs, it is not a flawless approach to securing network access for remote users. As enterprises weigh the pros and cons of Zero Trust adoption, they may run into one or more of the following challenges:

Solutions aren't truly cloud-native.

If a vendor does not offer cloud-based ZTNA — meaning their customers are required to deploy the software in their own data centers — then users lose out on key benefits like instant scalability and unlimited throughput.

Vendors may not offer client-based and clientless ZTNA options.

This limits the value for organizations that need to connect users to non-HTTP applications like remote desktops, SSH applications, or fileshares.

Configuration can be complex and time-consuming.

Vendors that don't offer support for policy orchestration and automation (via tools like Terraform) may introduce more manual work for administrators — in addition to configuration already happening in an identity provider.

CLOUDFLARE'S APPROACH TO REMOTE ACCESS

Securing and scaling remote access should be a seamless process, one that doesn't layer clunky security solutions, create performance tradeoffs, or incur unnecessary costs. Cloudflare empowers teams to handle all remote access use cases, with the following benefits:

- **Easy, no-risk onboarding for users and administrators.** Cloudflare easily integrates with existing identity providers and endpoint protection platforms to enforce Zero Trust policies that limit access to corporate applications and resources.
- **Flexibility for client-based and clientless ZTNA deployments**. Cloudflare provides clientless support for connections to web, SSH, VNC, (and soon, RDP) applications, and client-based support for non-HTTP applications and private routing to internal IPs (and soon, hostnames).

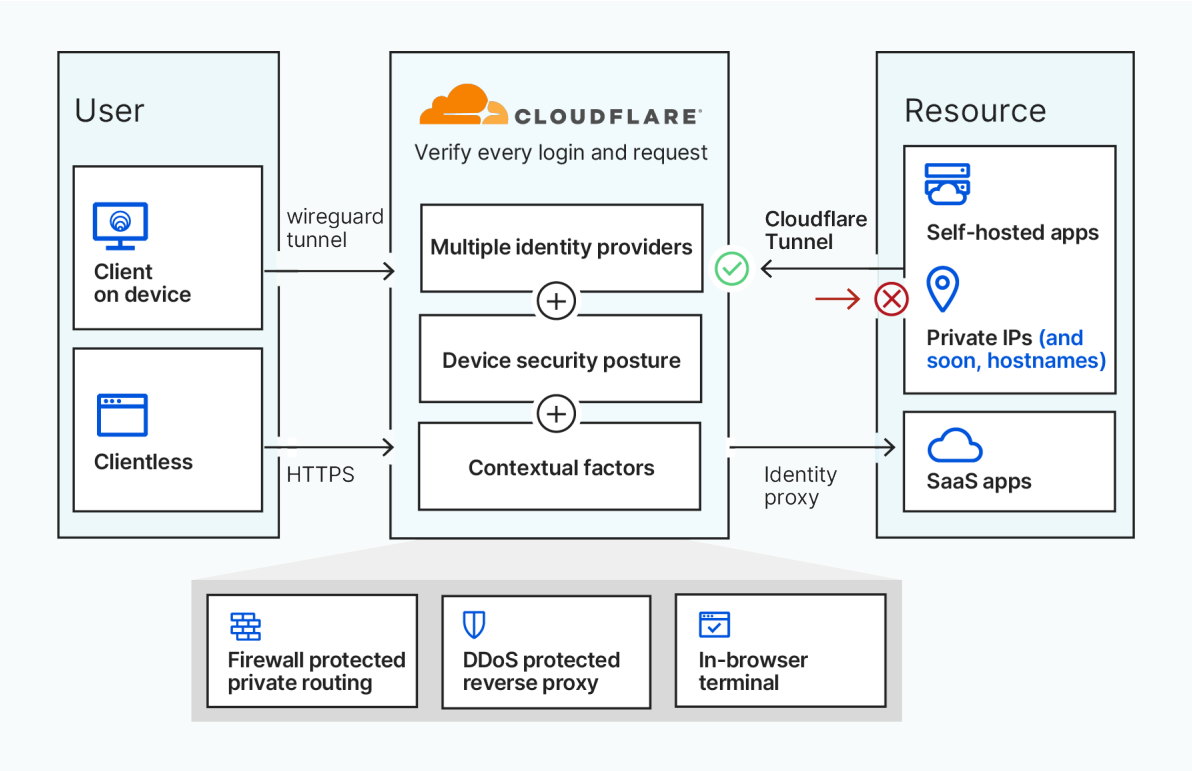


Table 1: How Cloudflare addresses remote access challenges

⚠ Problem	✓ Solution	⚙ Cloudflare Implementation
Difficult to scale	Global edge network	Scalability issues plague both VPNs and ZTNA services that are not cloud-native, making it difficult for remote users to access applications and data. Cloudflare's global Anycast network not only makes user connections faster than a VPN, but also ensures that remote workforces of any size can securely and swiftly connect to corporate resources as needed — without requiring additional time-consuming configuration by administrators.
Poor compatibility with mobile devices	Lightweight client	VPNs and ZTNA solutions that utilize IPSec and SSL protocols often have poor performance on mobile and roaming devices. The Cloudflare WARP client utilizes the more modern Wireguard protocol, which runs in user space to support a broader set of OS options with faster user experience than traditional options. Cloudflare's WARP client can be configured on Windows, MacOS, iOS, Android, and soon Linux devices.
No integrated or weak DDoS protection	Industry-leading DDoS protection built in	Without integrated DDoS protection in place, organizations are often forced to daisy-chain additional security services that can create configuration headaches, scalability issues, and security challenges. Cloudflare's 67+ Tbps network provides built-in DDoS protection for any ZTNA mode, defending networks against the largest volumetric attacks.
Protocol limitations	Non-web app support	✓ Mode compatibility: clientless ZTNA for SSH/VNC applications; client-based ZTNA for all other non-web applications.
No integrated network firewall	Built-in network firewall	As corporate networks grow, so does the stack of security hardware that organizations have to balance — causing trade-offs in cost, performance, and security. Cloudflare enables administrators to enforce network firewall policies at the edge, giving them fine-grained control over which data is allowed in and out of their network and improving visibility into how traffic flows through it. ✓ Mode compatibility: client-based ZTNA
Lack of fine-grained control	Built-in secure web gateway (SWG)	Unsanctioned use of applications can cause significant security issues for organizations; without rigorous policies in place, users may access and tamper with sensitive data and other corporate resources. Combining ZTNA with SWG, Cloudflare allows administrators to exert finer-grained control over user and device access rights within applications, so users and role-based groups only have access to the resources they need. ✓ Mode compatibility: client-based ZTNA

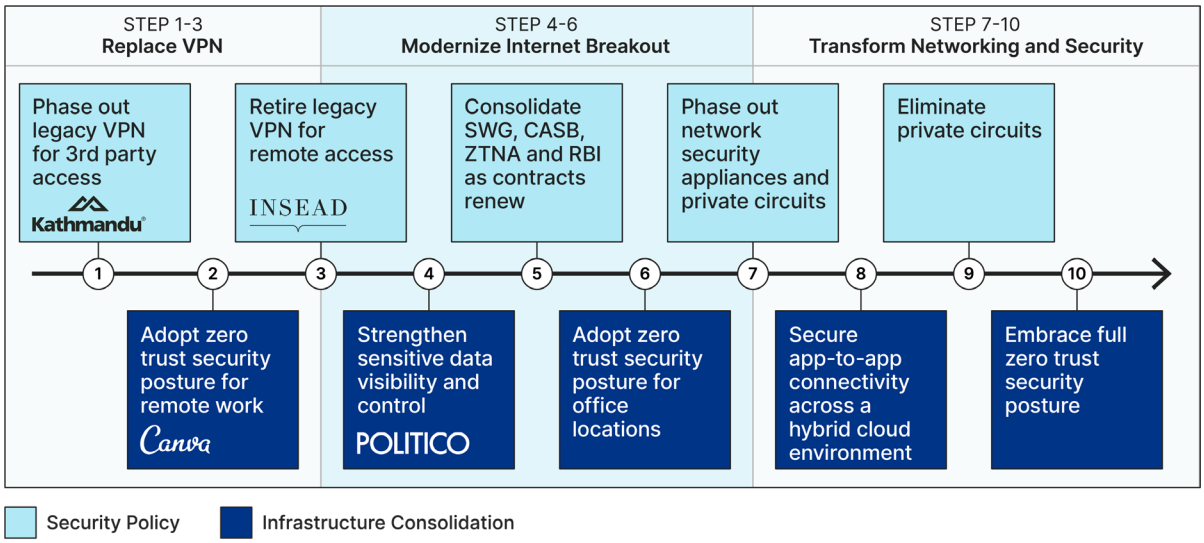
REPLACE YOUR LEGACY VPN WITH ZERO TRUST NETWORK ACCESS

The promises of Zero Trust can feel empty to IT security leaders in the midst of a long, painful transition to VPN-less security. But it is possible to replace your VPN with Zero Trust Network Access without making trade-offs in protocol support or functionality.

The recommended migration path varies based on the business priorities driving your project:

- If faster connectivity to applications is your priority, deploy **client-based ZTNA for non-web apps** first.
- If enhancing the security of your application access rules is more important, start with **web applications**.

Replacing your VPN is just the first step in a full network transformation. Because the transition to a SASE model can be overwhelming, we've broken down a common path to Zero Trust security based on the approach our customers have taken:



Learn more about how Cloudflare's Zero Trust platform can help you reduce reliance on your VPN and eventually replace it.

Learn more

See a real-world comparison between VPN and ZTNA and how Cloudflare Access enhances security for application access.

Watch the demo

APPENDIX

Modernize your Internet breakouts

Implementing ZTNA is an important step in deploying a secure access service edge (SASE) model. **Cloudflare One** is a comprehensive network-as-a-service (NaaS) solution that simplifies and secures corporate networking for teams of all sizes. With Cloudflare One, organizations can:

- **Embrace Zero Trust access.** Replace broad security perimeters with one-to-one verification of every request to every resource. Enforce Zero Trust rules on every connection to your corporate applications, no matter where or who your users are.
- **Secure Internet traffic.** When threats on the Internet move fast, the defenses you use to stop them need to be more proactive. Cloudflare One protects remote employees from threats on the Internet and enforces policies that prevent valuable data from leaving your organization by enforcing zero trust browser isolation on any site — with a smooth, lightning-fast user experience.
- **Protect and connect offices and data centers.** Corporate networking has become overly complicated, which means user traffic often has to travel through multiple hops to get to where it needs to go. With Cloudflare One, enterprises can protect offices and data centers through one consistent, unified cloud platform.

To learn more about Cloudflare One, watch a 10-minute introduction and demo.

Transform your network

Coming soon, Cloudflare's Zero Trust and WAN as-a-service offerings will converge as one, enabling your employees to access corporate resources consistently — wherever they're working.

Today, your VPN and WAN products allow your employees to access resources located within your private corporate network, but they force you to manage connectivity and security policies differently.

Now, Cloudflare provides a unified control plane, giving you more flexibility to apply the same Zero Trust security policies to your entire workforce and workplace without needing to juggle multiple point products.

To learn more, visit https://www.cloudflare.com/cloudflare-one/.