CLOUDFLARE

WHITEPAPER

The path to VPN replacement

Why and how to modernize secure remote access now

Content

Introduction

VPNs have reached their limit. As trends such as hybrid work, multi-cloud, evolving data compliance rules, and mergers and acquisitions (M&A) activities multiply, VPNs cannot keep up with the demand for fast, secure, and resilient internal access.

On the security side, VPNs make it difficult to stop evolving threats and achieve compliance mandates. On the connectivity side, they are clunky to maintain, slow down onboarding, and degrade user experiences. These challenges leave security and connectivity teams — spanning IT, networking, and infrastructure roles — constantly frustrated.

Most organizations now recognize that migrating to Zero Trust Network Access (ZTNA) offers a better way forward, especially for securing remote access.

Despite that recognition, there's been a prevailing market complacency and a slower move to change. This can be due to lack of clarity around where to start offloading VPN reliance, and what to do, in what order.

This guide can help. It offers:

- **Practical steps to building consensus among internal stakeholders**
- **A phased approach for VPN replacement**
- **Key vendor technology considerations**
- **Success stories from organizations who have made the crucial switch to ZTNA**

If you're ready to reduce risk, enhance efficiency, and future-proof your network, today is the day to start moving beyond VPNs.

74% of organizations have or will replace VPN with ZTNA.

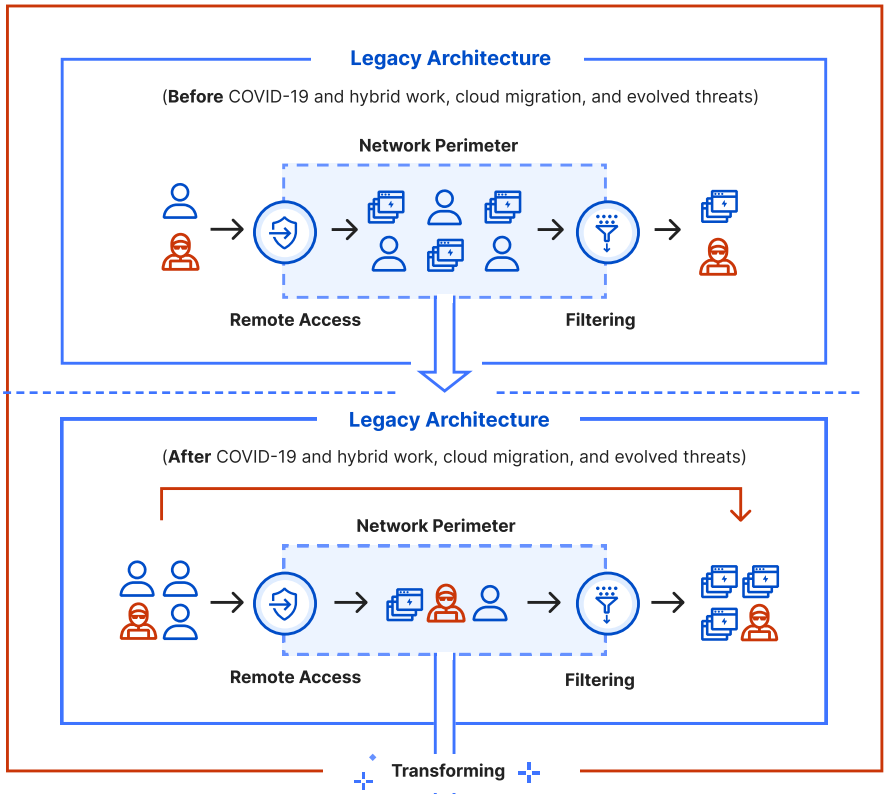
98% of IT security decision-makers agree: connecting users to applications directly — rather than the broader network — is important.[1]

> **"During COVID-19, we realized it made no sense to bring everything back on site via our VPN. Instead, we wanted a unified set of tools that would take us into the cloud to mitigate threats, improve performance, and provide our clients and users with the same security they would have if they were actually in the building."**
>
> **Danny Lilley**
> Vice President and Chief Technical Officer, Werner Enterprises

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

Beyond VPNs: The modernization journey

Because most **users and resources are located within the perimeter**, risks are either kept out or breaches minimized.

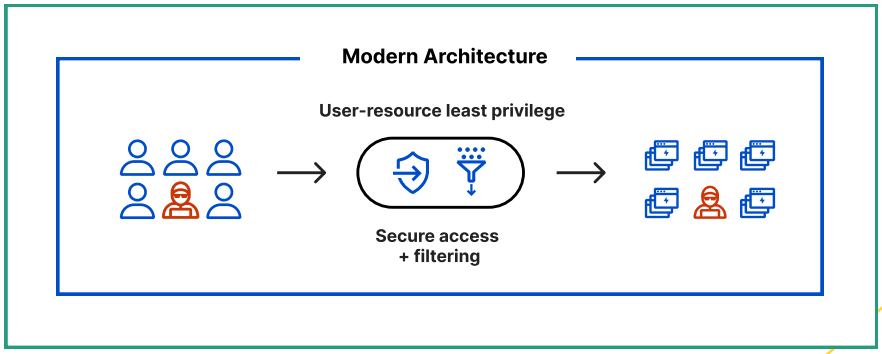


YOU ARE HERE

Most **users and resources are now located beyond the perimeter.** However, with legacy architecture, risks get in, move laterally, and cause large breaches.

Location no longer matters — identity and context do.

Since risk is always assumed, organizations gain visibility and enforce granular Zero Trust controls.



Making the business case: Why change now?

Making VPN replacement a reality begins with making the business case. For a start, this calculator is useful for understanding the return on investment for integrating security and network connectivity on one platform.

However, there are also costs associated with continued VPN complacency. Below are a few examples that may apply to your organization.

Frequent security vulnerabilities

It is well-known that VPNs are under constant attack. The zero-days previously found in Ivanti, Palo Alto Networks and Check Point VPN devices, and the brute-force attacks against Cisco's VPN solutions are just a handful of vulnerabilities that attackers have sought to exploit over the years.

While organizations can reactively wait for patches, the only long-term solution for eliminating these kinds of risks is to transition to an architecture that eliminates the network-level access and default trust granted by VPNs.

Breaches and compliance liabilities

According to Corvus Insurance data, attackers leveraging VPNs for initial access led to nearly 30% of ransomware incidents in Q3 2024.

VPN vulnerabilities have financial consequences beyond breach costs, too. For instance, the U.S. Department of Health and Human Services, SEC, New York State Attorney General, and Australian Government have all imposed multimillion dollar compliance fines against organizations following VPN-related attacks.

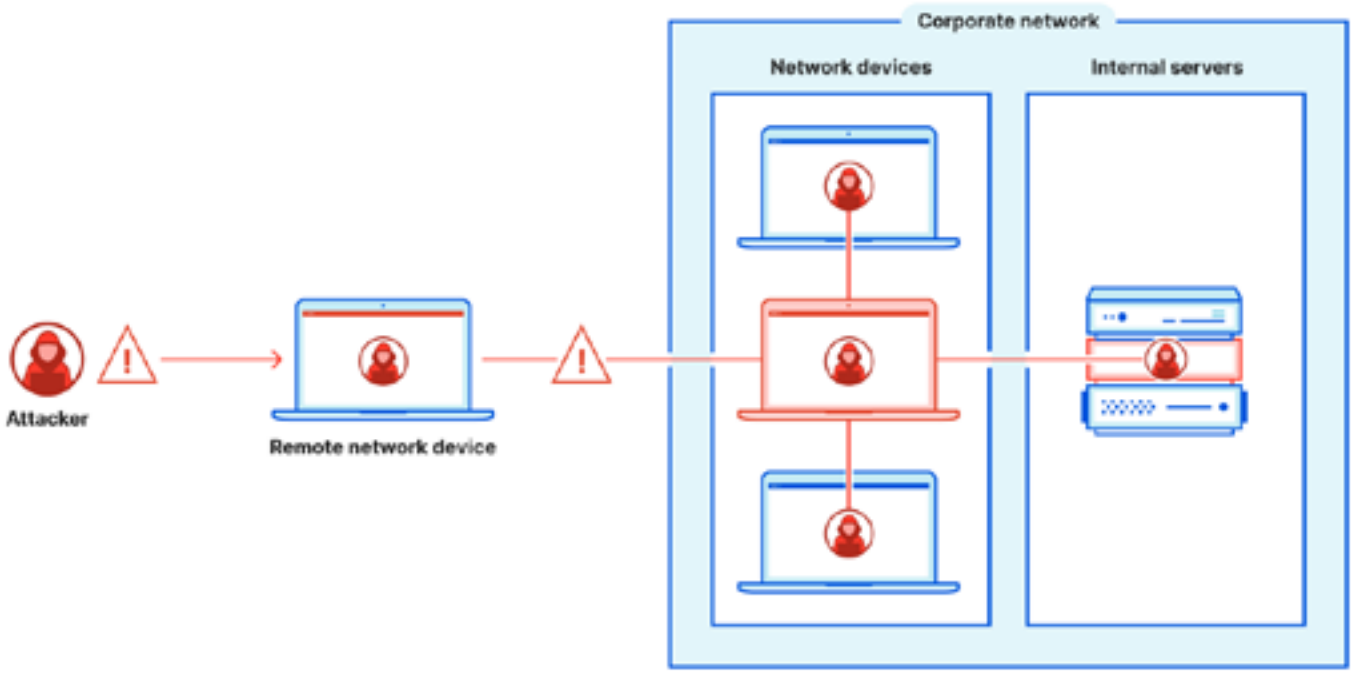


Figure 1: The network-level access and default trust granted by VPNs

Personnel and operational inefficiencies

Poor VPN experiences have a measurable impact on productivity — for both the IT teams responsible for managing VPNs and the rest of the workforce that use VPNs for remote connectivity.

In one example, a fintech company's Development Operations (DevOps) team discovered that — after implementing ZTNA — they saved almost 90% of the time previously spent on preparing an application for safe deployment.

VPNs can also increase the time it takes to onboard new employees and contractors, as they wait for hardware to be shipped, and to be connected to apps and programs manually.

Poor onboarding hinders productivity as well as retention: nearly three in 10 employees who were dissatisfied with their onboarding plan to seek new employment within three months.

However, as one global educational tech company found, using a ZTNA service instead of VPNs reduced their employee onboarding time by 60%.

Rising bandwidth costs

A survey of IT decision-makers conducted by Forrester Consulting found that 72% of global companies exceeded their set cloud budget for their most recent fiscal year.

One of the key problems with controlling cloud costs? Overconsumption of bandwidth, according to 42% of those surveyed.

More data transfer means more costs, yet it is already difficult for some organizations to granularly understand the full reach of their VPN usage. Organizations risk having bandwidth usage spiral out of control if they continue to rely on VPNs alone for connecting hybrid workforces, remote software developers, and other cloud-based resources.

Accelerating internal buy-in

Better security and connectivity experiences haven't always co-existed, but the fundamental architecture of ZTNA does improve both compared to legacy VPNs.

Therefore, ensuring internal alignment across security and connectivity teams (which can span IT, networking, and infrastructure roles) is key to successfully phasing out VPNs.

For example, introducing ZTNA must account for existing tools for identity management, endpoint security, and other existing security or networking on-ramps and services.

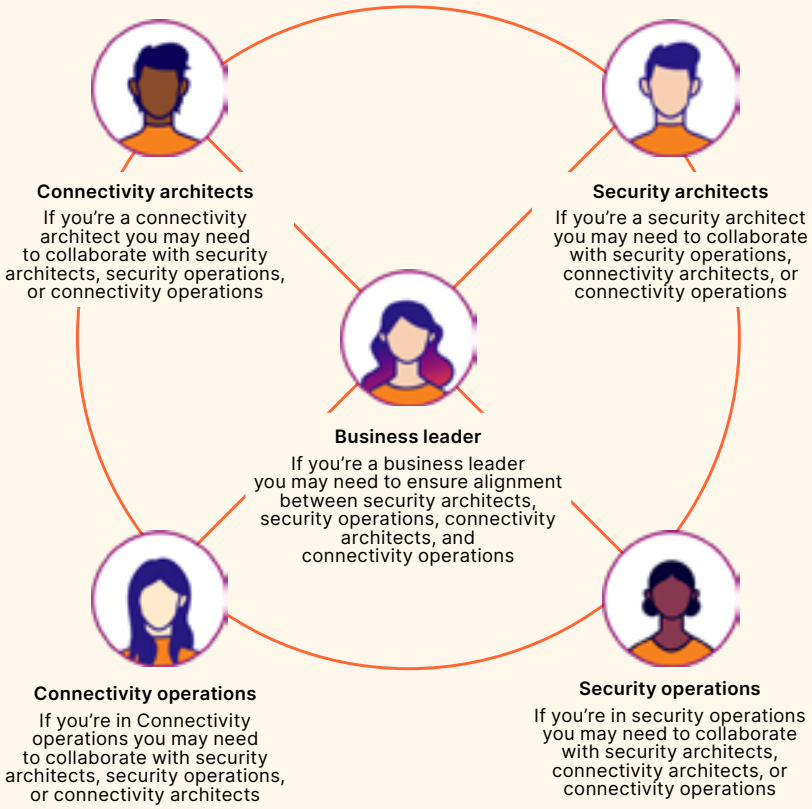
Executive sponsorship can also play a key role in helping to align teams.

While Zero Trust can mean different things to different people, if you first understand teams' business drivers for change (as explored in the next section), you will be better prepared to collaborate and assess vendors together.

You may need to collaborate with:

- Connectivity architects
- Security architects
- Business leaders
- Security/Connectivity operations

These teams must work together to align on VPN replacement ownership and implementation.



A complimentary Whiteboarding Architecture Workshop with Cloudflare's security specialist team can also assist — book one here.

Office of the CISO | Overcoming legacy security challenges

Why do they need to move away from VPN?	
Security architect	**Security operations (SecOps)**
For security architects, fragmented legacy security architectures lead to: • Increased complexity • Potential vulnerabilities • More difficulty meeting compliance requirements As Indeed's senior manager of information security, Matthew Ortiz, noted, "We have an obligation to be the best data stewards possible." However, their legacy architecture relied on implicit trust — "meaning, employees had access to more data and resources than we wanted." Plus, their VPN "could be slow or add friction in ways that annoyed users and made them turn off the connection, which created blind spots for us."	For SecOps, traditional VPNs mean: • Too much exposure of the network, especially when user credentials are compromised • Potential security gaps • Difficulty inspecting traffic with the increasing number of connections For example, when EQT underwent a major cloud migration and rapid workforce expansion, they relied briefly on a mix of custom proxies and an on-premises VPN for employee access to internal resources. However, according to the EQT Group site reliability engineering (SRE) team lead, this was "a lot of pain to maintain" and "not always secure."

What is the value that VPN replacement can deliver them?	
Security architect	**Security operations (SecOps)**
Shifting to ZTNA helps security architects: • Centralize management of all key resources • Simplify testing and visibility over connectivity and access across environments For example, Ortiz described that after replacing Indeed's VPN with Cloudflare's ZTNA service, "This Zero Trust approach helps us adapt to risk and gives us way more confidence than our legacy architecture … Cloudflare has helped resolve blind spots in our security and ultimately allows us to make better decisions in what access policies to set."	Shifting to ZTNA helps SecOps teams: • Limit network exposure and protect sensitive data • Provide consistent security across corporate and home networks • Effectively scale cloud-hosted workloads EQT's chief information security officer (CISO) described that, with ZTNA now: "The experience for end users is very smooth, and using a centralized service like Cloudflare to manage application access policies makes it easier for our IT and security teams. Plus, we now have visibility into who is using each of our services, which helps us improve our security holistically."

Office of the CIO | Overcoming legacy connectivity challenges

Why do they need to move away from VPN?	
Connectivity architect (IT, networking, or infrastructure roles)	**Connectivity operations** (IT, networking, or infrastructure roles)
For connectivity architects, legacy VPNs create: • Inconsistencies between in-office and remote IT systems • Complexity with juggling multiple VPN configurations and/or vendors • Business slowdowns, such as lengthier MandA IT integrations For example, Delivery Hero's rapid growth from ~9,000 to ~30,000 employees introduced IT and security challenges. They found relying on a VPN for secure access inefficient to manage and slow for end users. Wilson Tang, their director of platform engineering, Platform Core Services, described, "With so many different new people and infrastructures to manage, the complexity added up. That limited how efficiently we could innovate."	For connectivity operations, VPNs often mean: • Juggling multiple device agents, multiple identity and endpoint protection providers, and unmanaged private devices • Blame for network performance issues • Time-consuming, manually configured devices that generate user tickets For example, Conrad Electronics' Head of SRE and Cloud Technology, Janek Wonner, noted, "Everyone who wanted to access an internal system had to install a VPN client and configure it according to a specific VPN profile … Just keeping people online created a series of administrative bottlenecks."

What is the value that VPN replacement can deliver them?	
Connectivity architect	**Connectivity operations**
Shifting to ZTNA offers connectivity architects: • Scalable, flexible, agile, reliable, and resilient architecture • More streamlined security and compliance workflows • Cost savings and operational efficiencies Now with ZTNA deployed to over 40,000 employees, Tang said, "Being able to onboard new teams quickly and easily shift our new brands onto a consolidated, easily administered platform like Cloudflare, improved our efficiency and time-to-market with new products."	Shifting to ZTNA offers operational teams: • Fewer tools and integrations to manage • More automated IT workflows • A faster, reliable experience for end users Now with ZTNA, Wonner described, "All internal and external resources that have an account with our identity provider can quickly connect to specific systems using a single sign-on… Not having to maintain 1,000 VPN profiles improves our security and saves us time and money."

Where to start: A phased approach

The next step after aligning internal teams is to make a plan for how to approach ZTNA implementation.

In practice, there is no right number of phases or ways to approach ZTNA deployment. VPNs are so entrenched in some organizations that their VPN and ZTNA infrastructure may even co-exist indefinitely. However, any momentum toward modernization is a step in the right direction.

According to a Cloudflare-commissioned survey of 200 senior IT decision-makers across North America and Europe conducted by Enterprise Strategy Group (ESG), implementing Zero Trust for the workforce is best undertaken in phases.

For example — while there are key differences in adoption across different organization types — this journey can be broken down into the following:

Phase 1: Initial rollout	Phase 2: Expansion	Phase 3: Advancement
The organization identifies key priorities and then targets a limited set of use cases or functionality (i.e., those that deliver high value in relation to time invested). According to the ESG survey, IT decision-makers include 25% of their apps (commonly ERP, communication and collaboration, and file storage/sharing) and users (commonly sales, IT, and C-suite) in this phase.	The organization rolls availability out to a broader set of employees, increases coverage across more applications, and takes advantage of additional Zero Trust capabilities. Prioritized apps at this point commonly include CRM, financial management, DevOps CI/CD workflows, and development and collaboration.	In phase 3 and beyond, as they evolve to adopt advanced Zero Trust capabilities, the organization broadly deploys the initiative to most employees and applications. After successful early phases, the organization further scales the implementation via initiatives such as full VPN replacement, unifying context-based access controls to SaaS apps, adding data controls, and more.

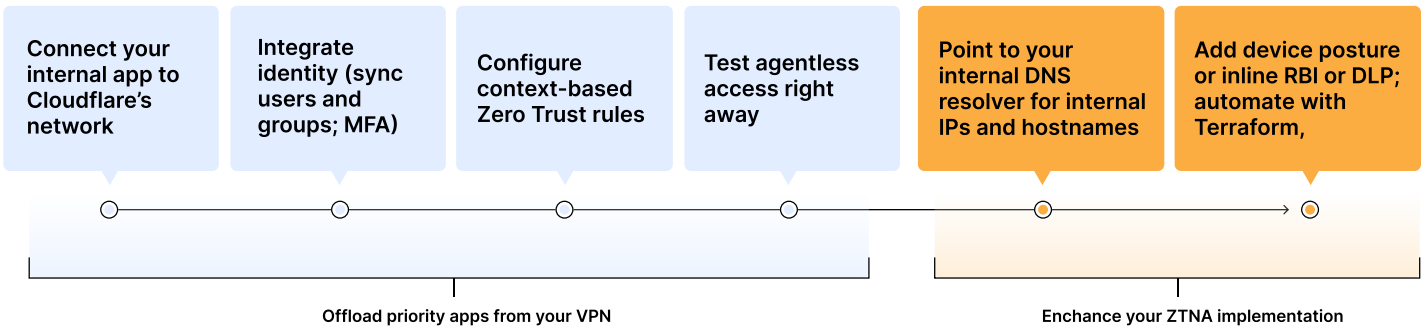


Figure 1: Example VPN replacement journey using Cloudflare Access.

A phased approach in action: Indeed and Cloudflare

Indeed modernizes IT and security by replacing its VPN with a Zero Trust approach

Within a few months of Indeed — the world's #1 job site — initially adopting Cloudflare's web application firewall (WAF) and bot management capabilities to its job platform, Indeed and Cloudflare began collaborating on a longer-term strategic effort to modernize connectivity and security across their workforce. This included reimagining how their employees accessed resources.

Indeed recognized the need to modernize an IT ecosystem that had grown increasingly complex. This complexity resulted in inconsistent traffic controls to the company's SaaS apps, data centers, and cloud resources. It also meant inefficient backhauling of traffic to data centers and an overreliance on traditional, perimeter-based tools like an on-premises VPN.

"As we grew, our technical debt grew with us," said Matthew Ortiz, senior manager of Indeed's Information Security, Engineering, and Operations teams. "We developed increasingly complex networking and security stacks which created risk and hurt productivity. We needed to simplify — complexity only leads to challenges and vulnerabilities."

Read the full case study

indeed

Phase 1: Initial rollout	Phase 2: Expansion	Phase 3: Advancement
To evaluate ZTNA for VPN replacement, Indeed rolled out Cloudflare Access progressively over a few weeks to dedicated test groups of hundreds of users — representing different device types and roles, including contractors. Testing helped Indeed become comfortable with how Cloudflare fit within its existing architecture and protected critical apps, developer environments, and its AWS infrastructure.	In just over three months, Indeed had deprecated its VPN entirely. This included migrating hundreds of preexisting access policies and rolling out Cloudflare to over 13,000 employees and contractors around the world. Cloudflare has also helped Ortiz and his colleagues identify which unsanctioned AI apps (known as "shadow AI") employees are using and establish controls when appropriate to prevent information exposure.	Today, Indeed uses the infrastructure-as-code tool, Terraform, to automate the vast majority of its ongoing management, including onboarding new users and configuring new policies. Another use case on the horizon includes identity-based verification for machine-to-machine workloads. Indeed is also exploring how Cloudflare can further protect data, secure SaaS environments, and defend against threats with DLP, CASB, and other SASE capabilities.

A phased approach in action: Delivery Hero and Cloudflare

Delivery Hero secures its global workforce in 70+ countries

Delivery Hero — the world's leading local delivery platform — rapidly grew its workforce from ~9,000 to ~30,000 employees over four years. They also expanded their global reach through various strategic M&As. Keeping pace with onboarding new users and integrating new companies with different tech stacks was increasingly taxing for Delivery Hero's internal teams. The shift to remote work during the pandemic placed even greater demands on security.

"When we adopted work-from-home and hybrid work models around the world, we needed to protect applications designed for access only on our internal office networks," said Delivery Hero's Wilson Tang, director of Engineering, Platform Core Services. "Securing everything and giving employees access from home, or anywhere else they chose to work, became much more challenging and complex."

Previously, Delivery Hero had relied on a VPN solution, but had found the technology inefficient to manage and slow for end users (including contractors, engineers, and developers). They turned to Cloudflare One, a platform that includes ZTNA, to secure access to internal apps.

Read the full case study

Delivery Hero

Phase 1: Initial rollout	Phase 2: Expansion	Phase 3: Advancement
Delivery Hero focused first on applying identity-based checks for web apps — a common initial use case that does not require deploying any device client software. They prioritized offloading riskiest users, such as developers and contractors, first. They found that, with ZTNA, they could "skip the pain points of setting up access with traditional VPNs" and protect an application within minutes, instead.	Delivery Hero began scaling their Cloudflare One deployment across more users and more apps, including key developer tools and backend customer systems. They now use Cloudflare to secure access for over 40,000 employees to all applications across self-hosted, SaaS, and non-web environments.	The company began a similar process for security across their public-facing resources, including websites, desktop and mobile customer apps, and vendor-facing administrative portals. Delivery Hero has also extended Cloudflare protections to app development; all new features for websites and apps, including new API endpoints, are built with Cloudflare's security protections.

To learn how other organizations from different industries adopted ZTNA with Cloudflare, visit our Zero Trust case studies.

Vendor technology considerations

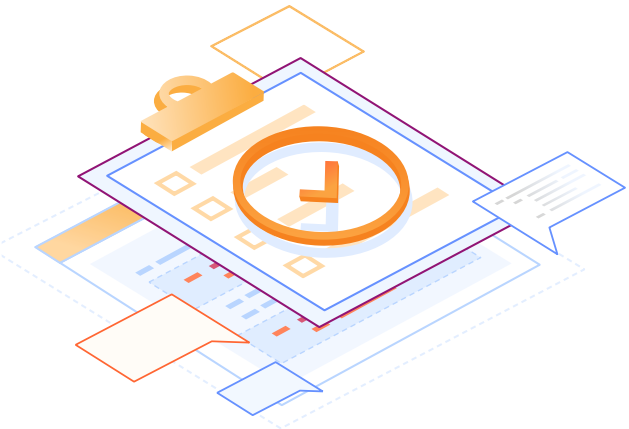
Once you are ready to create a shortlist of vendors to evaluate, a simple way to rule in (or out) potential providers is to review their:

- Reference architectures, policy design guides, and free trial (if available)
- Customer testimonials, including those found on Gartner® Peer Insights™
- Relevant analyst reports, including independent cost-benefit studies

While many vendors provide a similar ability to create Zero Trust access policies, not all providers are created equal. Consider whether their underlying technology will be flexible and scalable enough to meet future security, connectivity, and compliance mandates.

For example, security teams may ask vendors:

- Are any security functions bypassed based on the network on-ramp used?
- Can we use your service to enforce a range of controls over how users interact with content — such as rendering self-hosted apps in a remote browser for less trusted, third-party users?
- How do you ensure customer traffic is isolated and private across your multi-tenant cloud architecture?
- Do you provide data localization capabilities? Will enabling these capabilities add latency for remote users that connect outside the localized region?
- Can you allow access to our private resources without requiring that the user install software on their device (i.e., agentless ZTNA)?



IT, networking, and infrastructure teams may ask vendors:

- What are all the different options for connecting my network to yours?
- Do we integrate our identity provider to your service one time or many to enable identity-based access policies to every application (web, SaaS, and private)?
- Can your user device agent connect composably to any other network on-ramp (e.g., WAN connectors, app connectors, and mesh/P2P connectivity with other device agents)?
- Can we leverage your service for broader network connectivity with an endpoint? Do you support arbitrary Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) traffic, including bidirectional traffic, while still enforcing Zero Trust rules?
- Is every connect option available at every data center location on your network map — without paying extra fees or bandwidth surcharges?

Benefits of agentless deployment

The majority (84%) of IT decision-makers said that agentless deployment helped them significantly accelerate Zero Trust adoption through simplified deployment. Benefits realized include:

- Reduced admin burden and potential points of failure
- Easier scalability by eliminating individual agent installs on every device
- Effectively meeting organizations' use cases and scale for desired number of users and apps

Cloudflare helps teams move faster to remove VPNs

Many organizations are modernizing their secure access with Zero Trust as part of a broader Security Service Edge (SSE) or Secure Access Service Edge (SASE) strategy. However, if they are stitching together services from fragmented clouds, they can struggle with complicated implementations and policy management. Initiatives such as VPN replacement then stagnate or deliver lower-than-expected return on investment (ROI).

For organizations who value modernizing their security and network architectures the "right way," Cloudflare delivers simpler, more consistent controls built on a faster, more resilient network. Cloudflare's SASE platform, Cloudflare One, is built on our connectivity cloud — the next evolution of the public cloud, providing a unified, intelligent platform of programmable services.

Tech-enabled teams can replace VPNs faster and accelerate their Zero Trust journey, with first-class identity infusion throughout our offering, simplifying policy management. This drives momentum to achieve additional SASE use cases using Cloudflare — with less time and effort.

Using Cloudflare for VPN replacement is:

Simple to set up and automate

- Use clientless access to start offloading traffic, then scale with composable on-ramps
- Centralize policy administration with a unified dashboard
- Intuitive APIs and Terraform provider accelerate automation

Seamless for end users

- Make on-premises apps feel just like SaaS apps with smooth authentication and authorization
- Ensure routing and enforcement are always local and fast, using Cloudflare's extensive global network

Agile for long-term modernization

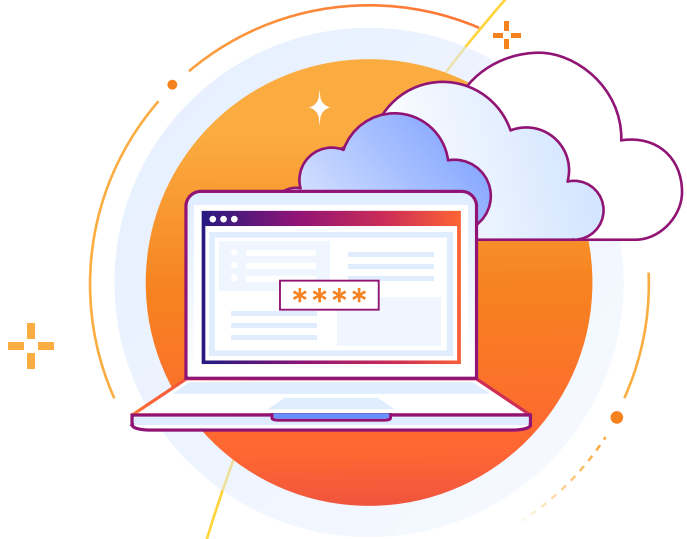
- Provide reliable any-to-any connectivity thanks to Cloudflare's Anycast-enabled architecture
- With our unified network and control plane of composable, cloud-native services, you can scale deployment anywhere

Next steps

Overcoming complacency and moving away from VPNs is imperative. And delaying the inevitable will only cost time and money, as well as increase risk and chances of business liability.

For more information on deploying ZTNA with Cloudflare, review our implementation guides for both clientless web access and replacing your VPN.

Ready to talk live? Book a complimentary Whiteboarding Architecture Workshop with our security specialist team here.



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

REV:BDES-6744.2025FEB12