CLOUDFLARE + VERSENT

The Path to VPN Replacement:

Explore when and how businesses are replacing outdated VPNs

Secure, Agile, and Future-Ready Connectivity

74% of organizations will reduce hardware by replacing VPN with ZTNA

VPNs are facing increased vulnerabilities, and organizations are grappling with three key challenges:

44%
of full-time employees are hybrid or remote users.

27%
of users accessing internal resources are third parties.

50%
of employees access internal resources from unmanaged devices.

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

While the vulnerabilities in VPN are well-known, there is a lingering complacency about switching to a Zero Trust alternative. However, with the security risk increasing and end user experience impacted more than ever, it's time to align internally and form a plan for VPN replacement now.

Introduction

VPNs are operating far beyond their original capacity and pose both a security risk and increase inefficiencies for businesses, from small and medium up to enterprise size. With changing work habits and the proliferation of apps and devices, employees are now working well beyond the traditional network perimeters. This is an ongoing headache for those working in both security and connectivity teams — where connectivity roles can span IT, networking, and infrastructure responsibilities.

VPNs make it difficult for security teams to comply with modern architecture mandates and to adequately prevent, respond to and remediate cyberattacks. And for those responsible for IT, networks and infrastructure, VPNs limit business agility and productivity, adding additional complexity around onboarding new employees and contributing to poor user experience.

VPN replacement is on the agenda for cyber leaders and transitioning to a Zero Trust Network Access (ZTNA) service is an excellent first step in empowering security and network teams to strengthen their security posture, reduce IT tickets, and improve team productivity.

However, there's prevailing complacency in the market and a slower move to change. This is often due to lack of clarity around where to start offloading VPN reliance, and what to in what order. But with security concerns and ongoing poor end user experience, it's critical to break this cycle and prioritize getting started now.

This guide will provide IT and security leaders with example considerations for where to start, clear steps to help transition to ZTNA, as well as give examples of how other organizations have made this crucial switch.

Contents

Costs of delay

VPN replacement is often filed in the 'someday' category. However, some simple calculations can help to quantify the true costs of delaying the inevitable and kickstart the move towards change.

For a start, this calculator is useful for understanding the return on investment for modernizing various parts of your security stack. Alternatively, below are some ideas of costs involved, which you can take and apply to your specific business.

Risk of security breaches

In February 2024, The Cybersecurity and Infrastructure Security Agency (CISA) in conjunction with agencies in UK, Canada, Australia and New Zealand, issued a joint advisory about threat actors exploiting vulnerabilities in Ivanti. Their advice was to limit outbound internet connections from SSL VPN appliances to restrict access to required service, and limit SSL VPN connections to unprivileged accounts.[1]

Writing in trade publication SecurityInfoWatch.com, a leading expert said this is a wakeup call to all organizations around the world to re-evaluate their secure remote access policies.[2]

Beyond the obvious costs of data breaches and reputational damage, there is also cyber insurance, which is not only becoming more expensive but more difficult to obtain.

Over the past few years, the cost of cyber insurance has rocketed. And while this has begun to stabilize, the list of exclusions is rising.[3]

Insurer Munich Re flagged in a recent report that "insurers and risk modelers continue to explore the limits and possibilities of insurability".[4]

"Against an extremely dynamic threat landscape, where geopolitical and technological stressors are setting new priorities, tackling insurability challenges and managing accumulation risk is key to the long-term sustainability and functionality of a still maturing market," the report said.

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b
2. https://www.securityinfowatch.com/cybersecurity/article/55019571/vpns-no-more-new-cisa-advisory-signals-need-for-secure-remote-access-amid-china-sponsored-attacks
3. https://professional.ft.com/en-gb/blog/cyber-insurance-rate-hikes-slow-but-exclusions-expand/
4. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

Poor user experience and onboarding

Inefficient technology can contribute to people resigning. In Workfront's 7th Annual State of Work Report, 49% of US workers surveyed said they would leave their job due to frustrations with technology[5].

And with Gallup[6] estimating that the cost of replacing an employee can range from one-half to two times the employee's annual salary, it's well worth thinking about whether poor VPN user experience might be impacting staff satisfaction.

This is particularly true for employees whose roles encompasses dealing with sensitive information accessed remotely, such as accountants, where research shows user experience and proper integration of systems are some of the biggest frustrations[7]. Or those who are constantly having to access different systems, such as software developers. If access is slow or inefficient, it can have a measurable impact on their productivity.

Business efficiencies and other business costs

By contrast, moving to a Zero Trust architecture can generate business efficiencies. For example, onboarding manually can create additional work and increase the time it takes for new employees and contractors to become productive, as they wait for hardware to be shipped manually and to be connected to apps and programs manually. In fact, one company reported a **60% decrease in onboarding time after implementing a ZTNA tool.**[8]

Other business costs that can be reduced include increased bandwidth due to backhauling costs, and increased hardware.

5. https://www.zdnet.com/article/nearly-half-of-workers-will-quit-their-job-if-their-workplace-technology-is-not-up-to-scratch/
6. https://www.gallup.com/workplace/247391/fixable-problem-costs-businesses-trillion.aspx
7. https://www.icaew.com/technical/technology/technology-and-the-profession/mastering-mid-tier-technology/icaews-mid-tier-research-highlights-shifts-in-technology-adoption
8. https://www.cloudflare.com/case-studies/eteacher-group/

Strategic costs of delay

Much business strategy, such as mergers and acquisitions (M&A) activity, is impacted by networks and systems.

For example, a report from Deloitte[9] estimated that about 60 percent of the organizations will consider cybersecurity posture in their due diligence process as a critical factor during any M&A.

"Technology also plays an important role by not only enabling the integration, but also driving the new business operating model. It brings in an entire gamut of cyberattacks, and a poor cybersecurity posture can slow down the company's acquisition process and, in some cases, also be a deal breaker," Deloitte says.

And, in a recent Enterprise Strategy Group Report, *Considerations for Implementing Zero Trust for the Workforce*, 78% of senior IT leader respondents agreed that M&A activity is driving the need to accelerate IT integration across multiple identity providers and networks.[10]

The strategic costs can also include delays in rolling out new apps, and even the loss of compliance certifications.

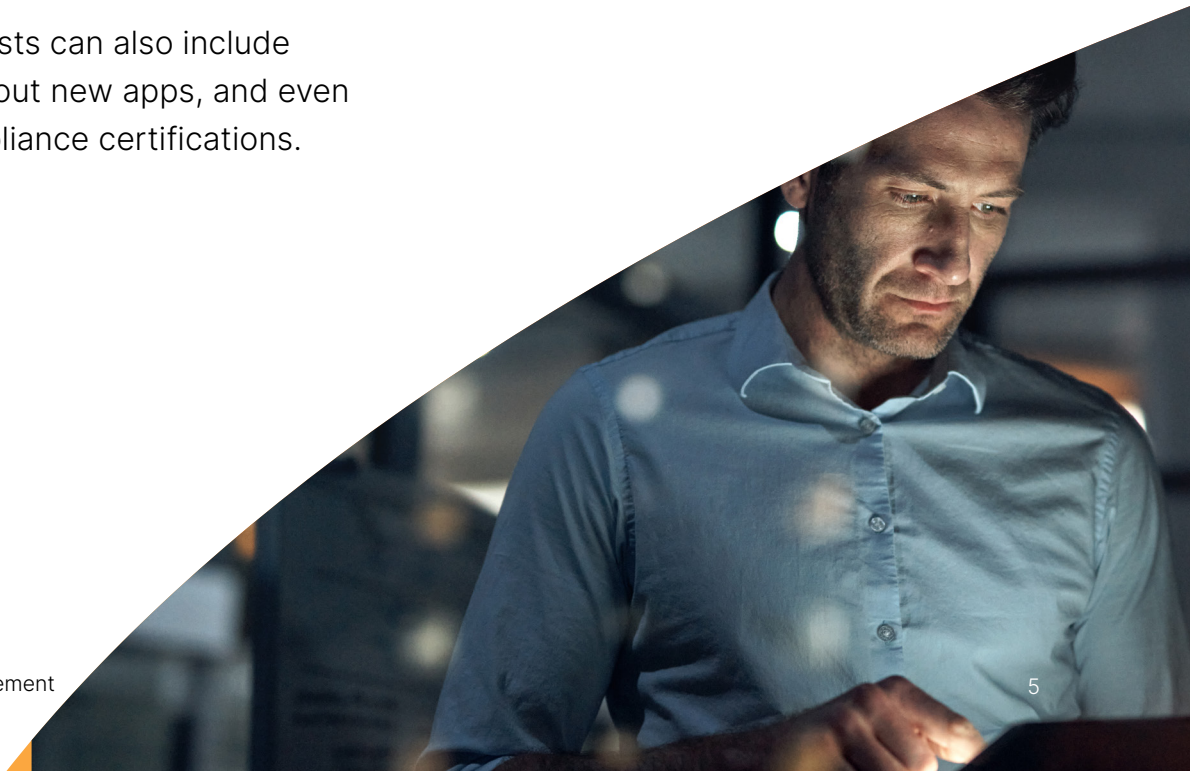
Personal costs of delay

A cyber breach can reflect badly on the reputations of all involved, from the directors of a company through to the security professionals responsible for preventing attacks. Researchers from Oxford University studied the impacts of a cyberattack – including psychological and reputational – identifying areas such as staff leaving and damaged relationships with customers.[11]

Not only that, but in many jurisdictions around the world, directors can and are being held personally liable[12].

Plus, an inefficient VPN only adds to IT staff workloads, both in terms of user inefficiencies and increased IT tickets.

9. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-for-mergers-and-acquisitions-noexp.pdf
10. https://cfl.re/esg-zero-trust-workforce-ebook-2024
11. https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks
12. https://www.whitecase.com/insight-alert/director-liability-cyber-breaches-transatlantic-warning-signs, https://www.allens.com.au/insights-news/insights/2022/04/cyber-risks-resilience-and-responsibilities/



Ensuring internal alignment

Replacing VPN is a cross-functional project, so ensuring that there is internal alignment is key to a successful and timely implementation.

VPN replacement projects can be initiated by both security and IT/networking/infrastructure teams — it depends on the needs of an individual business. What's crucial is these teams work together to align on ownership and implementation. A good place to start is to understand all the groups that are likely to be involved in a collaboration, and to align across the various business dynamics that impact their need to drive change.

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

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

Challenges of legacy security

Because VPNs are limited to the corporate perimeter, it's harder to prevent, respond to, and remediate security incidents due to lack of visibility and inability to restrict lateral movement and access permissions.

This results in workarounds that are inefficient to manage, and overly restrictive policies to meet security mandates. And if compliance fails, it can lead to fines, inability to close deals, and personal liability.

13. https://cfl.re/esg-zero-trust-workforce-ebook-2024

Challenges of legacy connectivity

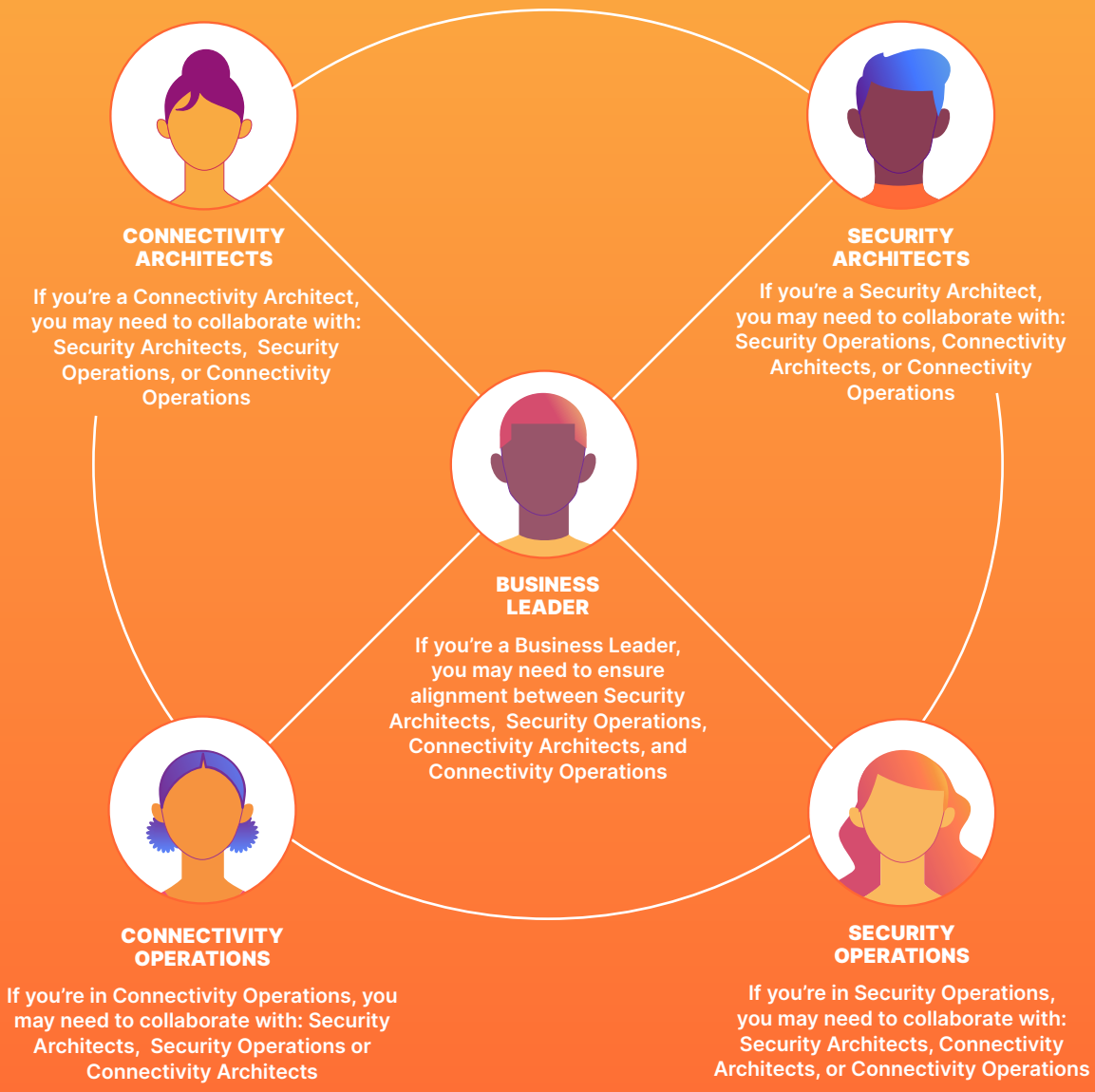
Meanwhile, for connectivity roles (that may span IT, network, and infrastructure responsibilities), a VPN impacts business operations, placing limits on business agility particularly during times of growth.

Firstly, it wastes their time in multiple ways — including onboarding new hires using complex manual processes, dealing with excessive tickets and complaints from end users, and setting up complex firewall policies to try and segment the network.

Also, the resulting time to productivity for new hires, loss of productivity for end users, and extended maintenance windows impacts their reputation and can lead to C-level executive frustration.

See below for more detail.

You may need to collaborate with:



	Why they need to move away from VPN	Value that VPN replacement will deliver
 **Security Architect**	For security architects, fragmented legacy security architectures mean increased complexity, potential vulnerabilities, and more difficulty meeting compliance requirements.	Moving to ZTNA provides security architects with centralized management of all key resources. Plus, simplified testing and understanding of connectivity and access across their entire environment.
 **Security Operations**	Traditional VPNs expose too much of the network, especially when user credentials are compromised. They're also less scalable and efficient. The increasing number of connections makes traffic inspection difficult for security operations. Plus, it is hard to upgrade and patch home networks and privately owned devices, creating potential security gaps.	Moving to ZTNA allows security operations to limit network exposure and protect sensitive data, even if user credentials are compromised. It also provides consistent security across both corporate and home networks, without them having to manage private devices. Also, it enables the ability to scale effectively with cloud-hosted workloads and to handle traffic inspection efficiently.
 **Connectivity Architect**	Using VPNs means inconsistencies between in-office and remote IT systems. Connectivity architects may be juggling multiple configurations and redundancies in their VPN – or even multiple VPN vendors – to accommodate different departments, regions, and subsidiary companies. Legacy hardware also causes headaches, particularly when it's not aligned to agility required by modern business.	Moving away from VPNs means an architecture that is scalable, flexible, modern, agile, reliable, and resilient. This move also brings additional security and compliance, and generates efficiencies in both costs and operations. Plus, a ZTNA service is more compatible and easily integrated with existing technologies
 **Connectivity Operations**	Connectivity operations, when using VPNs, is often juggling multiple device agents and multiple identity and endpoint protection providers, as well as dealing with unmanaged private devices. They also have to manage time-consuming, manually configured VPNs that generate user tickets. They are also responsible for managing bandwidth and traffic bottlenecks. They often get the blame for performance issues and outages and are increasingly held accountable for delivering apps to the workforce.	Transitioning away from VPNs means fewer tools and integrations for connectivity operations to manage. Plus, it eases their workload as they can automate workflows as much as possible and get end users to self-service their IT requests. Plus, a good end user experience reflects well on them — a fast, reliable service that enhances, rather than gets in the way of, productivity.

Where to start

Once internal teams are aligned, the next step is to make a clear plan for how to approach ZTNA implementation.

A recent Enterprise Strategy Group Report commissioned by Cloudflare, *Considerations for Implementing Zero Trust for the Workforce*,[13] surveyed senior IT security decision-makers across North America and Europe.

A key takeaway was that the breadth of users and applications make moving to ZTNA a process best broken down into phases.

For simplicity, the survey broke it into three phases: Phase 1: initial rollout, Phase 2: expansion and Phase 3: advancement. In practice, there is no 'right' number of phases or ways to approach ZTNA deployment, and some organizations may never reach 100% replacement perhaps due to niche, legacy resources or general change management worries. The key is starting small and building momentum toward modernization at an appropriate pace.

Initial rollout

In the first stage, the organization identifies key priorities and then targets a limited set of use cases or functionality before a broader rollout.

Organizations should try to find projects which deliver high value in relation to the time invested. This will help build momentum and keep the project moving forward.

Expansion

In Phase 2 the organization rolls availability out to a broader set of employees, increases coverage across a wider set of applications, or takes advantage of additional features or capabilities.

Advancement

In Phase 3 and beyond, the organization broadly deploys the initiative to most employees and applications, using advanced capabilities, and making sure the project meets the overall goals.

If you'd like help mapping your own plan, you can book a complimentary Whiteboarding Architecture Workshop with Cloudflare's security specialist team here.

13. https://cfl.re/esg-zero-trust-workforce-ebook-2024

Average percentage of users and apps covered during initial rollout

25%
Initial Rollout

Most common user groups
- Sales
- IT
- C suite

Most common app types
- ERP
- Communication and collaboration
- File storage and sharing

Benefits of agentless deployment

Nearly three-quarters (71%) of survey respondents said their current ZTNA tools supported agentless deployment and 84% said it helped them significantly accelerate Zero Trust adoption through simplified deployment.

Respondents also agreed that agentless ZTNA effectively addressed the use cases, users, and applications they wanted to cover, meaning they could expand coverage without deploying additional tools that use agents.

Benefits realized from agentless deployment

~84%
of the respondents

- **Simplified deployment reduced admin burden & potential points of failure**
- **Significantly accelerated zero-trust adoption**
- **Easier scalability by eliminating individual agent installs on every device**
- **Effectively meets our use cases and scale for desired number of users and apps**

How other customers embraced Zero Trust

As mentioned, security and connectivity teams both have their own drivers for wanting to replace VPNs, and the move towards replacement can be started from either – and then grown as more collaborators get on board. There's no set way to do this, as project ownership will vary company to company.

To provide some ideas of how this might look, here are some customer stories which highlight the main catalysts and value gained from VPN replacement from the points of view of security architects and operations, and connectivity architects and operations – although there is of course crossover. These customer stories look at how the companies moved from these starting points through the transition, and then highlight topline results for the organization.

CASE STUDY

Security architect

Media & advertising conglomerate protecting >50,000 knowledge workers

A need to address urgent security vulnerabilities led to long-term change

In 2022, a major media & advertising conglomerate decided to withdraw its operations from Russia following the invasion of Ukraine. Shortly thereafter, the company began experiencing attempts to attack its public websites. Concerns about these threats — including becoming a target for state-backed actors — escalated to the point that the company shut down all web properties and several critical internal applications on a Sunday evening.

Solution

Cloudflare, in collaboration with a major implementation partner, initiated a rapid response to mitigate threats directed at external websites. As a next step, the company rolled out Cloudflare's Zero Trust Network Access (ZTNA) service, to secure a handful of critical web-based applications that had been most severely disrupted for thousands of users.

Within 48 hours, the company was able to resume critical business operations. And within a few days, the company rolled out ZTNA to several thousand additional employees.

After reestablishing stable business operations, the company began to reconsider its longer term approach to securing access. Shifting access policy enforcement to a globally distributed cloud network offered an opportunity to deliver a more consistent experience for employees, who worked across many countries in both remote and in-office settings.

Over the next few months, the company extended identity-based and group-based policies for hundreds more applications and thousands of users. By May 2022, nearly 50,000 were using Cloudflare to authenticate to their most-used applications, offloading the majority of traffic from the company's existing VPNs.

Results

The company estimates that modernizing its security with Cloudflare Zero Trust across its entire organization can potentially reduce costs by over $5 million annually, thanks to time savings on IT administration, productivity gains for end users, lower spending on VPN and other legacy tooling, and the lower likelihood and reduced potential impacts of a data breach.

Choosing a provider

While many security vendors provide a similar ability to create Zero Trust access policies, not all providers are created equal.

Cloudflare's solution, for example, is faster and easier to deploy, using a simple agentless deployment setup with uniform operations for seamless expansion to more on-ramps and inline services.

And, once it's deployed, Cloudflare provides a better low-latency end user experience with security services delivered close to end users, available everywhere to everyone at global scale.

It's also resilient, providing end-to-end trusted connectivity and a private backbone with traffic routing and load balancing automated as code, plus built-in threat intelligence. Cloudflare's Anycast network architecture enables a 100% SLA for paid plans.

Plus, with Cloudflare's composable services available everywhere, you can easily move onto deploying the rest of an SSE or SASE strategy when you're ready. VPN replacement with Cloudflare's connectivity cloud drives momentum for broader IT/security modernization and consolidation.

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, have a look at our implementation guides for both clientless web access and replacing your VPN.

If you'd like to book a complimentary Whiteboarding Architecture Workshop with our security specialist team you can do so here.

Alternatively, contact us with any questions or for a more detailed discussion.

Book a White Boarding Architecture Workshop to learn more →

About Cloudflare

Cloudflare, Inc. (NYSE: NET) Cloudflare is a unified, intelligent platform of programmable cloud-native services that delivers unmatched security to protect people, apps and networks enabling organizations to regain control, lower costs, and reduce the risks of securing an expanded network environment.

Learn more about Cloudflare at **cloudflare.com/connectivity-cloud**. Learn more about the latest Internet trends and insights at **radar.cloudflare.com**.

Follow us: **Blog** | **X** | **LinkedIn** | **Facebook** | **Instagram**

Contact

Ph: 1300 748 959
www.cloudflare.com

CLOUDFLARE