eBook

The 6 Most Compelling Use Cases for Complete Legacy VPN Replacement

netskope

Introduction

Legacy remote access VPN infrastructure has long been a security liability. Its broad network connectivity attracts attackers and permits unauthorized lateral movement. Forcing remote users to backhaul non-local traffic through the VPN just to get back to the internet leads to poor user experience, and entails high cost and routing complexity.

For enterprises that plan to modernize connectivity for the hybrid workforce, ZTNA is the modern alternative to legacy remote access VPN. But not all ZTNA solutions successfully enable complete VPN replacement.

To successfully upgrade from legacy VPN to ZTNA, our recommendation is to identify and prioritize key use cases when planning for a full migration. Useful planning, combined with the right technology investments, will enable teams to finally meet the promise of full VPN retirement.

1. Empower Hybrid Workers

With most employees now favoring a hybrid work model, legacy VPN solutions prove inadequate for tackling the essential security and connectivity challenges necessary to empower the workforce. Remote access VPN provides little visibility into application-related activities, suffers from latency and performance issues through traffic backhauling, and provides broad, network-level access to authenticated users, expanding the attack surface because of unrestricted lateral movements. In addition to that, VPN concentrators with unpatched vulnerabilities act as major attack vectors for cyber attacks.

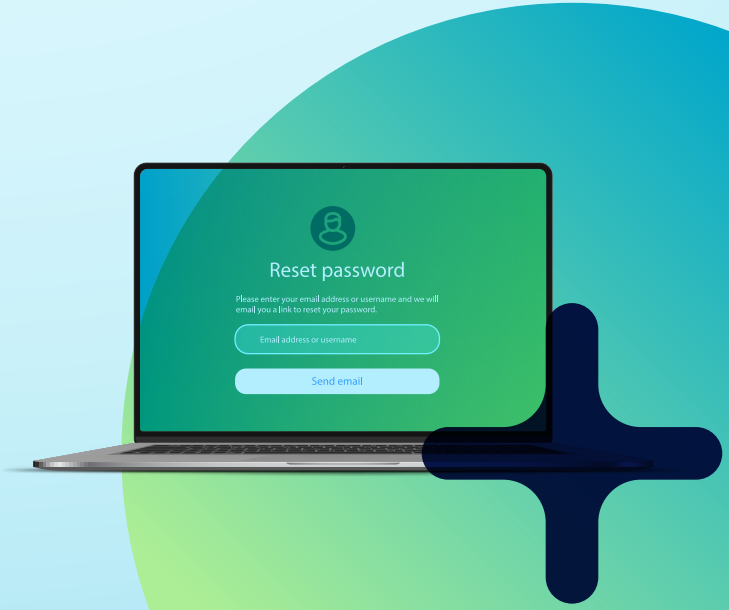
By upgrading from the legacy remote VPN solutions to a ZTNA solution such as Netskope Private Access, organizations will be able to address VPN-related security risks by enabling identity- and context-aware least privileged access to private applications while minimizing unauthorized lateral movements. NPA offers real-time visibility into detailed application traffic and user activities and allows for consistent policy enforcement for employees connecting from any location, whether remote or on-premises. Additionally, the solution can establish secure pre-log on connectivity, facilitating the secure onboarding of new devices and password reset for remote workers and ensuring that only sanctioned devices have access to critical internal resources such as directory services.

11 hours per year
lost by employees resetting passwords[1]

IMPLEMENTATION TIPS:

An inventory of VPN deployments is a good way to start on upgrading your infrastructure. This should include:

- **How many instances of remote access VPN services you operate today**
- **What application traffic is traveling through these remote access VPNs**
- **Named users with VPN access to these applications**



[1]Business Reporter, "How much time does your organisation spend on managing passwords?", Sept. 7, 2022. https://www.independent.co.uk/news/business/business-reporter/time-organisation-managing-passwords-b2161856.html

2. Accelerate Cloud Migration

Digital transformation has reached a tipping point: More workloads are now hosted in public clouds as opposed to private data centers. As a result, connectivity to IaaS, for users both on-premises and remote, has been at the top of mind and is one of the primary concerns as organizations plan their cloud strategy and deployment. In typical remote access VPN infrastructure, user traffic is routed through the private data center and then connected to IaaS clouds using MPLS or other pin-up tunnels such as AWS Direct Connect or Azure ExpressRoute. Backhauling traffic not only leads to poor user experience and drives up infrastructure expenses, but also requires complex network routing.

As a modern alternative to legacy remote access VPNs, Netskope enables efficient connectivity to the public cloud without that need to hairpin. The connection is secure, flexible, and highly scalable. NPA helps protect data and resources with application-level access control based on user identity and device security posture. With NPA, the connectivity is logical, not IP-based. As a result, it dramatically streamlines cloud and network operations, enabling automation while eliminating traffic backhauling.

IMPLEMENTATION TIPS:

Organizations looking to replace remote access VPN should also look for cloud VPN instances, such as AWS Client VPN or Azure VPN Gateway. They should leverage automation tools such as Terraform modules for automating the deployment, configuration, and scaling of NPA Publishers running in EC2 and other cloud environments.

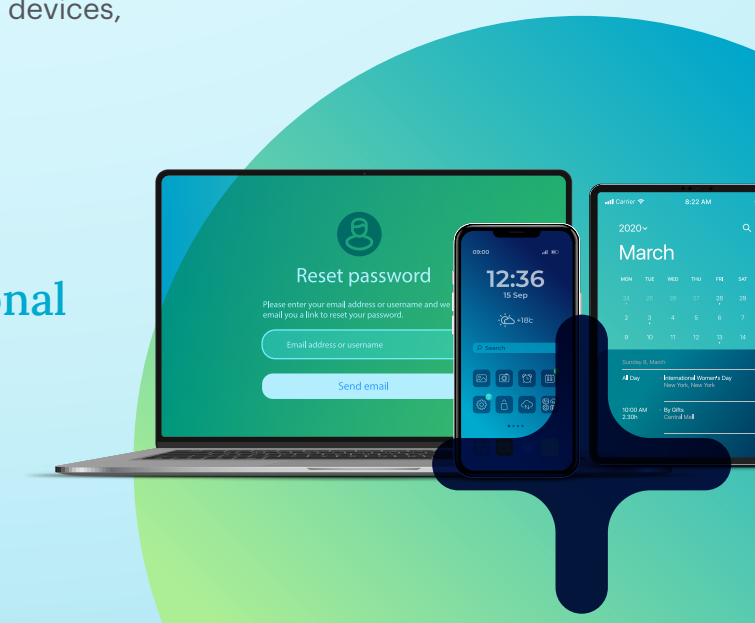
3. Facilitate Unmanaged Device Access (When It Makes Sense)

Organizations need to grant external contractors, service providers, and partners secure access to corporate resources. At the same time, employees also demand seamless access to private resources using their personal devices. This leads to the challenge of facilitating unmanaged device access without the risk of exposing the resources on the public internet or DMZ. Requiring special-purpose client software may not be feasible, as users may be reluctant to install software on their personal devices. Granting VPN access to unmanaged devices can result in too much access.

You can safely provision access to unmanaged devices for third- and fourth-party users and employee BYOD without the risks associated with VPN, DMZ, or exposing resources to the public internet. Netskope Private Access supports clientless deployment for unmanaged devices providing secure, zero trust access to private applications, hosted on-premises or in the cloud.

The clientless ZTNA deployment enables frictionless, browser-based access through a reverse-proxy architecture that is integrated with identity providers (IdP) for authenticating the users attempting to access private applications. Leveraging the same DLP controls on the Netskope SSE platform, organizations can maintain granular visibility and consistent data protection policy on all devices, managed and unmanaged.

On an average, an employee uses **2.5 devices at work**, that includes non-corporate devices such as personal laptops, smartphones and tablets.[2]



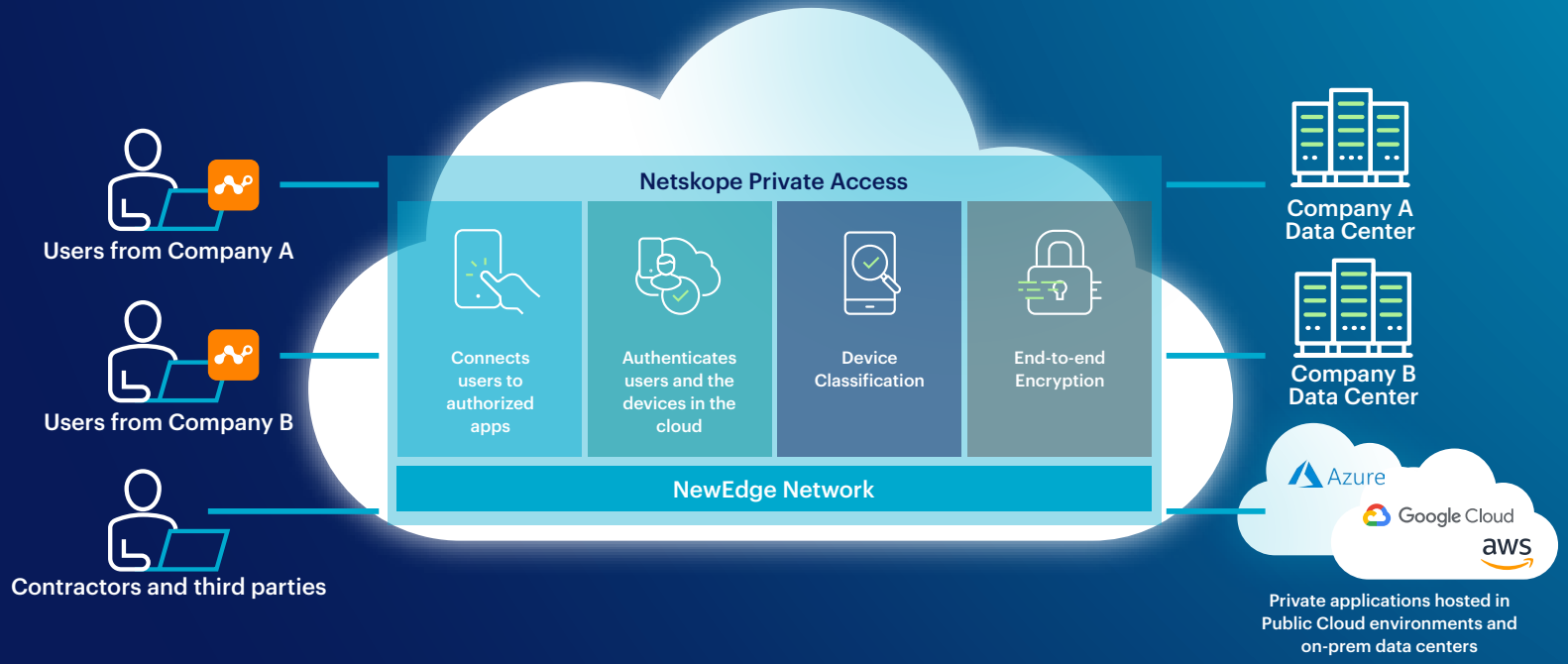
[2]Zippia. "26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace" Zippia.com. Oct. 17, 2022. https://www.zippia.com/advice/byod-statistics/

4. Accelerate M&A Integration

M&A activities are fast paced, high-stakes, time-sensitive events. For IT, networking, and security teams, M&A presents a unique set of challenges. M&A success is driven by how quickly the integration of the two firms can be completed.

IT operations teams are challenged to deliver day-one access, connecting users from both entities to mission-critical internal applications and at the same time ensuring the security of sensitive data. The traditional methods of merging two networks is a costly, time-consuming, and complex process that often results in IP conflict and requires re-numbering of addresses. The firewall rules often cannot offer granular access control, making both networks vulnerable.

Netskope recently introduced ZTNA Next, integrating cloud-delivered ZTNA with endpoint SD-WAN. A unified SASE client automatically steers user traffic to its destinations, whether it is cloud apps, private apps, IaaS, or web. ZTNA Next enables organizations to realize business value in M&A activities by enabling organizations to connect employees, contractors, and advisors to only the critical resources they need on day-one, even for legacy applications and without waiting for VPN infrastructure to be set up and eliminating the need for merging networks. This allows the firms to immediately begin combining their businesses in a secure way. The adaptive trust criteria for granting access considers the user identity, device hygiene and other contextual data. By granting users selective application and data access, ZTNA Next minimizes the risk of lateral movement and sensitive data exposure.



Provide day-one access to internal resources without the complexity of combining networks, configuring site-to-site VPN and firewall rules.

5. Support Remote Contact Centers

There are **1.8 million** call center employees worldwide and 52% of call centers in the US alone employ remote agents.[3] These agents are customer service representatives, travel booking agents, healthcare advice providers and other roles. While many call centers are upgrading to cloud-based unified communication as a service (UCaaS), many organizations are still using legacy on-premises hosted VoIP and often are routing calls through remote access VPN. For remote call center employees, VoIP quality can be hit-and-miss when relying on VPNs. They tend to be overwhelmed, contributing to added jitter and latency with VoIP calling which can be frustrating for people on both ends of the lines.

Until now, most cloud-delivered ZTNA solutions do not support on-premises hosted VoIP systems forcing organizations to maintain both ZTNA and VPN infrastructure.

52%
of call centers in the US alone employ remote agents

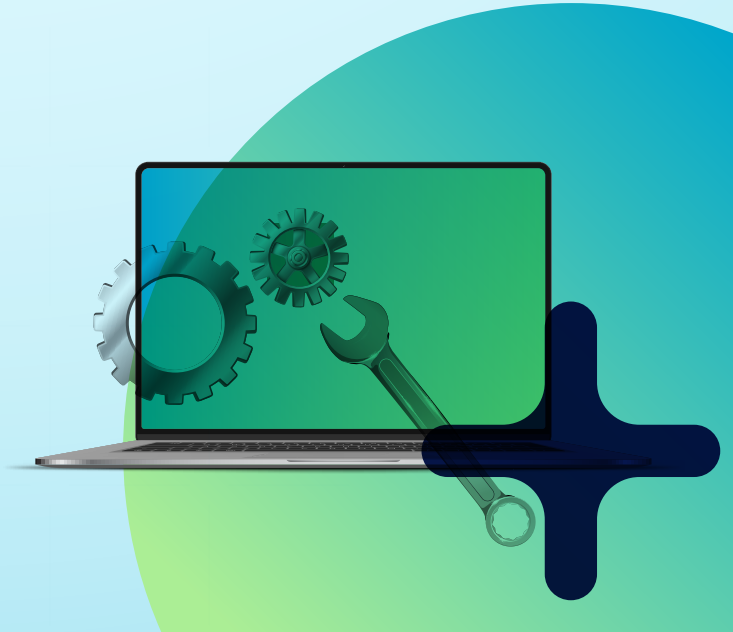
Netskope ZTNA Next offers converged ZTNA and SD-WAN capabilities delivered as a single solution. With dynamic traffic steering and context-aware QoS, boosting remote call center employees productivity with assured voice and video application experience while enhancing security posture with zero trust access to all internal resources.

[3]Source: "Call Center Statistics – 2023" Truelist.com. Jan. 1, 2023. https://truelist.co/blog/call-center-statistics/#:~:text=The%20number%20of%20people%20working,million%20currently%20to%201.8%20million.

6. Accommodate Legacy Applications

Testing for compatibility is a critical step in technology upgrade. Organizations that are deploying ZTNA also need to test applications for compatibility. During this process, organizations will likely discover some legacy applications that are incompatible with most current ZTNA solutions. For example, legacy applications that require server-initiated traffic don't work well with a modern ZTNA solution's "inside out connectivity" which requires the traffic to be endpoint-initiated. These legacy systems are often proprietary and require time, resources and careful planning to re-design and modernize (and often this means migrating to cloud hosted IaaS environments).

Netskope ZTNA Next solves for all of these legacy application examples, however, by providing secure and optimized access to all private applications from a single-integrated client. Organizations can therefore extend the longevity of legacy applications, reduce the cost of managing multiple remote access solutions and provide fast, reliable application access, regardless of where they are hosted.



Conclusion

Whereas they were once cutting edge technology, legacy remote access VPNs now challenge security teams—for whom they are a source of much threat vulnerability—and infrastructure & operations teams, for whom they affect network performance and, as a result, degrade overall user experience.

But most ZTNA solutions today aren't a panacea; if they don't solve for all relevant use cases, organizations find themselves able to do only partial VPN replacement, leaving them with a mix of infrastructure—legacy VPN plus "some" ZTNA—that may be even more complicated than before.

Netskope ZTNA Next is designed to help organizations accelerate their adoption of ZTNA zero trust using a fully integrated solution that catalyzes the successful replacement of all VPN infrastructure. It provides a clear path to complete replacement of remote access VPNs for all application access use cases, reducing the digital attack surface, enhancing security posture with zero trust principles, and boosting remote worker productivity with seamless and optimized application access experience.

About ZTNA NEXT

ZTNA Next combines our award-winning Netskope Private Access for ZTNA with the power of software-only Netskope Endpoint SD-WAN, allowing organizations to:

- Modernize connectivity, boost security.
- Enhance the user experience.
- Ensure highly reliable, optimized access to voice and video applications.
- Reduce complexity and operational cost.
- Accelerate plans to retire legacy remote access VPN infrastructure eliminating the need to maintain separate remote access tools.
- Achieve unprecedented visibility and control over applications traffic.

With ZTNA Next, Netskope can enable the complete retirement—not just partial replacement—of remote access VPN for all relevant application access use cases, while enhancing security posture and delivering seamless and optimized application access.

ZTNA next

OUT WITH THE OLD → IN WITH THE NEW

About Netskope

Netskope is a leader in Secure Access Service Edge, redefining cloud, data, and network security and helping organizations apply zero trust principles. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and protects people, devices, and data no matter where they are. Netskope helps organizations reduce risk, increase effectiveness, and gain unparalleled visibility into all cloud, web, and personal application activity.

Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to mitigate threats and address technological, organizational, network, and regulatory changes.

netskope