



VPN Replacement

Introduction

The era of “work from anywhere” demands a fundamental shift away from legacy remote access technologies. Traditional VPNs, designed for a different time, now represent a critical bottleneck to productivity and a significant security risk. They create a poor user experience, expand the corporate attack surface, and leave IT teams blind to resolving end user performance issues. A true VPN replacement strategy must address both security and employee experience. The Zscaler Zero Trust Exchange™ offers a unified platform solution, combining Zscaler Private Access (ZPA) for best-in-class Zero Trust security and Zscaler Digital Experience (ZDX) for end-to-end performance visibility. This integrated approach secures your workforce, delights your users, and empowers your IT teams.





THE CHALLENGE

Why Traditional VPNs Fail the Modern Enterprise

Legacy VPNs are failing to meet the demands of a distributed, cloud-centric workforce, creating friction for users and introducing unacceptable risks for the business.

- **Expanded Attack Surface & Security Risk:** VPNs place users directly on the corporate network, granting over-privileged access. A single compromised user or device becomes an entry point for attackers to move laterally, discover sensitive assets, and deploy ransomware.
- **Poor User Experience and Productivity:** By backhauling all traffic through a centralized data center, VPNs introduce significant latency. This results in slow performance, dropped connections, and frustrated, less productive employees.
- **High Cost & Operational Complexity:** Managing, patching, and scaling physical or virtual VPN appliances is a constant operational drain. Capacity planning is a guessing game, and supporting a fully remote workforce requires immense capital investment and administrative overhead.
- **Complete Lack of Visibility:** When users complain about a slow application, IT is left blind. Is it the user's home Wi-Fi, their ISP, the corporate network, or the application itself? This lack of insight leads to lengthy troubleshooting cycles, high mean-time-to-resolution (MTTR), and a strained helpdesk.

THE SOLUTION

A Platform Approach with the Zero Trust Exchange

The Zscaler Zero Trust Exchange platform provides a comprehensive solution that not only replaces VPNs but transforms how your organization approaches secure access and performance monitoring.

1. SECURE THE CONNECTION WITH ZSCALER PRIVATE ACCESS (ZPA)

ZPA is the world's most deployed Zero Trust Network Access (ZTNA) solution. It fundamentally inverts the legacy access model by connecting users directly and securely to private applications, never to the network.

- **Zero Trust Security:** Access is granted based on verified identity and business policy before a connection is made. Users are never placed on the network, and applications are made invisible to the internet, significantly reducing the attack surface. Device access from unsanctioned locations (e.g., logins from sanctioned vs. unsanctioned sites) can be identified and remediated.

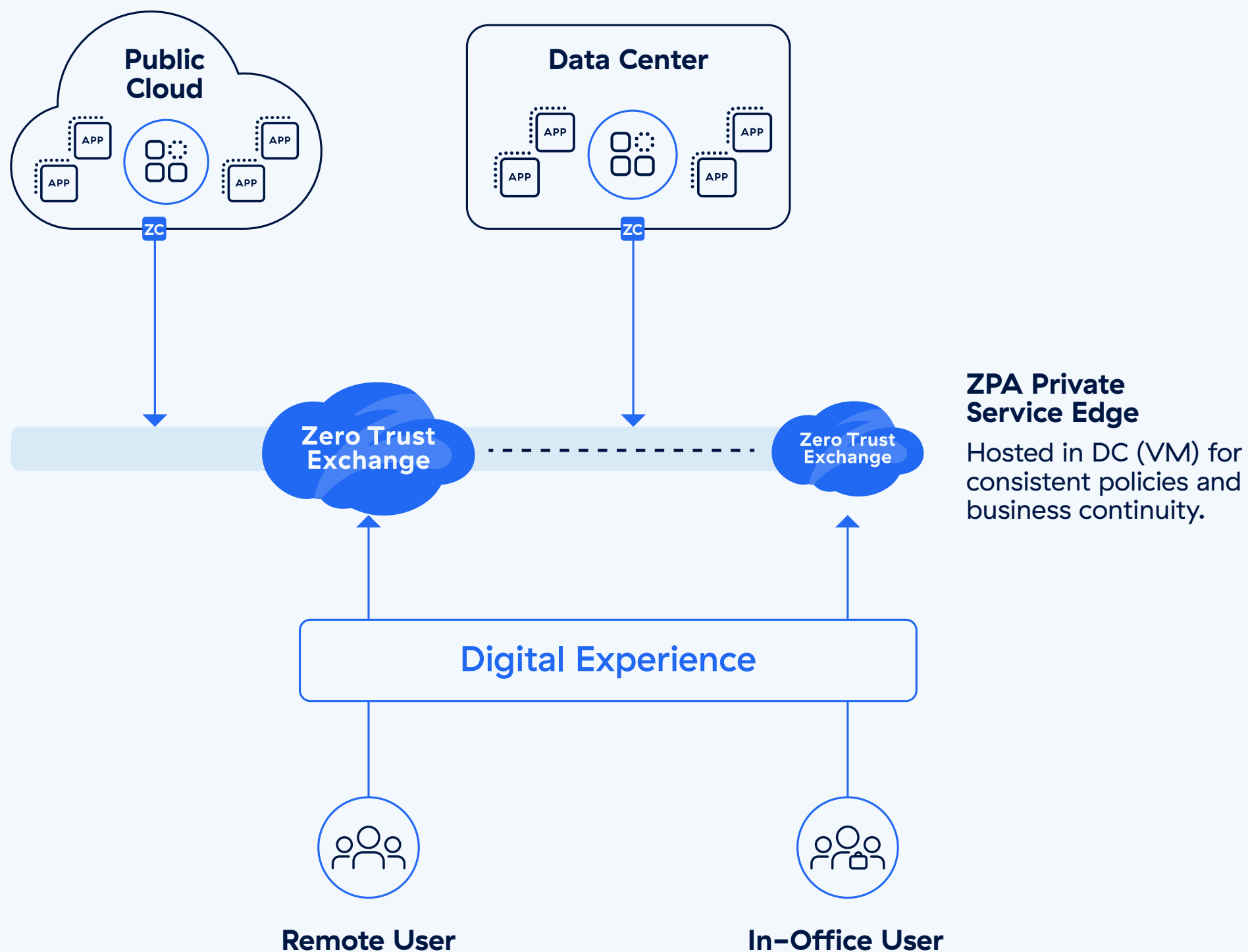


- **Autonomous User-to-App segmentation:** ZPA segments access at the application level. A user authorized for one application has zero visibility or access to any other, completely preventing lateral threat movement. ZPA uses AI and machine learning to autonomously create and enforce granular, application-level segmentation policies, dramatically simplifying operations and ensuring least-privileged access at scale without manual policy configuration.
- **Inside-Out Connections:** Lightweight connectors establish outbound-only connections to the Zscaler cloud, meaning there are no inbound firewall rules to manage and no exposed entry points for attackers.

2. ENSURE OPTIMAL EXPERIENCE WITH ZSCALER DIGITAL EXPERIENCE (ZDX)

ZDX is an integrated digital experience monitoring service that provides unprecedented, end-to-end visibility into device, network, and application performance, complementing ZPA to keep private access fast and reliable.

- **End-to-End Visibility:** ZDX monitors the entire connection path—from the user's device, across the last-mile and intermediate ISP, through the Zscaler cloud, to the application—pinpointing the source of any performance issue in seconds. It detects suboptimal routing and guides optimal Zscaler data center selection to reduce latency.
- **Proactive Monitoring:** ZDX proactively detects performance degradation and alerts IT teams, often before users are even impacted, allowing for faster resolution and reduced downtime. It identifies ISP latency and congestion (including DDoS-related slowdowns) between users and specific Zscaler data centers and enables traffic rerouting to alternate data centers to bypass impacted ISPs.
- **Actionable Insights:** With a simple, unified ZDX Score for every user, application, and location, helpdesk teams can instantly understand performance quality and rapidly triage support tickets, drastically reducing MTTR. ZDX also surfaces anomalous device behavior such as widespread CPU spikes from processes hijacked by malicious DLLs to accelerate security response and protect user experience.



NJ Transit successfully replaced their VPNs to connect their 100% mobile workforce to authorized apps and resources.

Enabled a productive, secure work-from-anywhere experience while significantly decreasing the volume of help-desk tickets.

Ensures safe and dependable transportation services by securing critical infrastructure.



Learn more: www.zscaler.com/customers/nj-transit

“With Zscaler, we’ve been able to reduce support tickets by 50%,” said Franciscone.

“It not only lightens the load for our help desk, it also ensures a seamless user experience.”

JOHN FRANCISCONE

Senior Director of Cybersecurity, Architecture, and Engineering, NJ TRANSIT



The Zscaler Advantage:

METRIC	WITH TRADITIONAL VPN	WITH ZSCALER (ZPA + ZDX)
Security	Network-Level Access: Places users on the network, creating a massive attack surface and enabling lateral movement.	Application-Level Access: Connects authenticated users to specific apps, never the network. Makes apps invisible to the internet. Autonomous User-to-App segmentation prevents lateral movement. Integrated monitoring adds location and device health signals to improve policy enforcement and threat detection.
User Experience	Slow & Inconsistent: Backhauls traffic, causing high latency and frustrating users.	Fast & Optimized: Provides direct, low-latency connections to on-prem and cloud apps for a seamless, “in-office” experience. Detects routing inefficiencies and ISP issues and recommends data center changes to maintain performance.
Visibility	Blind Spots: No visibility into the user-to-app path. IT cannot easily diagnose performance issues, leading to finger-pointing.	End-to-End Visibility: Real time insights into segmentation, automatically discover all apps and visualize which users and groups can access them. Pinpoints the source of performance issues (user device, Wi-Fi, ISP, app) for rapid troubleshooting and proactive monitoring.
Cost & Complexity	High: Expensive hardware, complex management, and significant operational overhead for patching and scaling.	Low TCO: A 100% cloud-delivered service eliminates appliance costs, simplifies management, and scales elastically with demand. A single agent for internet access, application access and monitoring reduces agent sprawl and minimizes CPU/memory impact.

Key Benefits



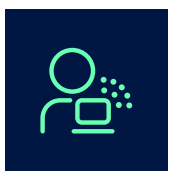
Comprehensive VPN Replacement: Securely connect your entire workforce to private applications while simultaneously ensuring a fast, reliable user experience.



Consistent security and user experience: Deliver consistent, robust security and an optimal user experience for all employees, whether they are working remotely, in the office, or as hybrid users.



Boost IT Helpdesk Productivity: Empower your helpdesk with the visibility of ZDX to slash troubleshooting times, reduce ticket escalations, and lower MTTR from days to minutes.



Secure Third-Party Access: Grant granular, application-specific access to contractors and partners without giving them any network access, minimizing supply chain risk.



Accelerate M&A Integration: Rapidly onboard employees from acquired companies by providing secure access to critical applications in days, not months, without complex network integration. Compare DNS resolution times and Wi-Fi health pre/post migration, demonstrating faster resolution and improved user experience, while gaining enterprise-wide visibility.

Take the Next Step

Don't just replace your VPN—transform your security and user productivity with a modern, integrated platform. The Zscaler Zero Trust Exchange provides superior security and visibility for all users accessing private applications.

Contact us today to see how Zscaler can eliminate your VPN challenges.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.



**Zero Trust
Everywhere**