Solution Brief

Enforcing Universal ZTNA with Netskope One Private Access

Netskope One Private Access ensures secure, least-privilege access to private applications for users, regardless of location—whether in the office, at home, or on the go. Serving as a key driver of digital transformation, it offers organizations the ideal framework for advancing Zero Trust initiatives.

Quick Glance

- Unified, Context-Aware ZTNA Policy Everywhere: Enforce a single, risk-based policy for secure access, based on identity, device posture, and context.
- Boost Productivity: All users—remote, at HQ, branches, or third-party—get fast, secure access to private apps, ensuring seamless productivity and security.
- Full Visibility and Control: Administrators gain a dashboard for monitoring user connectivity, device posture, location, and application usage.
- Reduce Costs and Simplify Management: Reduce costs and complexity by eliminating multiple solutions for remote and on-campus users.

"By 2026, 80% of ZTNA spend will occur as a part of a broader SASE, managed SASE or SSE purchase, up from 40% in 2022."

source: Gartner, Competitive Behaviors in the ZTNA Platform Market, 2024"; instead of source: Emerging Tech: How to Differentiate in the Fast-Growing but Crowded ZTNA Market, 2022.

The Challenge

As hybrid work becomes standard, organizations face challenges with legacy virtual private networks (VPNs) impacting security, performance, and management. These issues include:

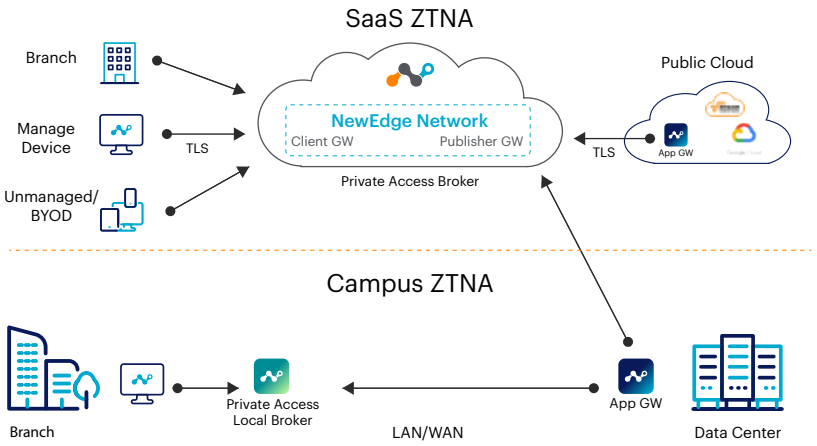
- Expanded Attack Surface: Legacy VPNs rely on implicit trust, increasing the risk of lateral threats.
- Complexity and Costs: VPNs add operational complexity and costs, particularly in cloud-first environments.
- Network Performance: Backhauling traffic to VPN termination devices causes delays and poor user experience.
- Lack of Visibility: Limited visibility into network events makes troubleshooting difficult.
- Compatibility Issues: VPNs struggle to support hybrid workforces and cloud applications.

SaaS ZTNA removes implicit trust, granting access based on context, device posture, and location. However, for on-premises users, it may cause performance issues like hairpinning and inconsistent policies. With Universal ZTNA for branch and campus environments, organizations can ensure secure, reliable access, simplified management, and consistent performance for all users, regardless of location.

The Solution

Netskope One Private Access ensures secure, least-privilege access to private applications for users, regardless of their location—whether in the office, at home, or on the go. Leveraging Zero Trust principles, it provides consistent authentication, authorization, and risk-based controls to protect against threats. With intelligent traffic routing, performance is

Figure: Universal ZTNA with Netskope One Private Access



optimized, and a unified client seamlessly integrates ZTNA and VPN functions. The solution enforces granular access controls for both on-premises and remote users, continuously updating policies in real time based on risk scores. Additionally, it reduces the reliance on network access control (NAC) by incorporating essential features like device and user authentication and access control.

Supported scenarios and use cases

- On-premises users accessing internal apps via an on-prem broker
- Branch users accessing internal apps via an on-prem broker
- Remote users accessing apps in the public cloud or internal apps via the Netskope One Private Access Broker or the customer broker hosted in the cloud
- Private Dataplane via an on-prem broker for compliance audits (PCI), data sovereignty, and operational technology (OT) use cases

Consistent Zero Trust policy enforcement across all locations

Netskope One Private Access ensures consistent Zero Trust policy enforcement across all locations by shifting from traditional network-based controls to granular, application-specific access for individual users and groups. A unified ZTNA policy engine enforces policies for both on-premises and remote users. Granular access rules restrict users to specific enterprise applications, with real-time updates based on risk score changes from the SASE platform. This approach accelerates the decommissioning of legacy applications and mitigates security risks like unauthorized lateral movement.

A unified ZTNA policy engine enforces consistent Zero Trust policies for both on-premises and remote users.

Key capabilities include:

- Least-privilege access to private applications, based on identity and context, whether hosted in public clouds or on-premises data centers
- Facilitating connectivity through the broker in the security cloud. By concealing applications from unauthorized discovery and granting access exclusively to approved users, the risk of lateral movement by threats is greatly reduced, along with the potential damage that could be caused.
- Removing reliance on public-facing VPNs or open inbound firewall ports for application access, safeguarding networks from threats and DDoS attacks.
- Enabling unmanaged devices to access corporate resources using reverse proxy capabilities (supported by the SaaS Private Application broker)
- Continuous device posture assessment strengthens security by ensuring all devices meet compliance standards and blocking risky or compromised endpoints from accessing the network. This proactive approach minimizes the chance of data breaches.

Seamless and optimized user experience

Netskope One Private Access provides a frictionless user experience for remote and on-campus environments, including HQ, branch offices, or third-party partners. Remote users enjoy fast, secure access to private applications, preventing any lateral movement across the network, reducing the impact of social engineering or phishing attacks. On campus, whether at HQ, a data center, or a branch, users experience seamless access to private applications and network resources, all while maintaining least-privilege access.

Netskope One Private Access provides a frictionless user experience for remote and on-campus environments, including HQ, branch offices, or third-party partners.

- Netskope One Client intelligently routes traffic to connect authorized users directly to required resources, regardless of their hosting location.
- By positioning the brokers close to the end-user, Netskope reduces latency and ensures high performance. With broker interconnections, traffic can bypass the WAN, taking advantage of lower-latency paths when available.
- By using the Netskope NewEdge Network, the largest cloud security infrastructure, along with advanced routing optimization techniques, it minimizes latency and round-trip time for both cloud and on-premises access.
- The solution applies Zero Trust principles while maintaining a smooth user experience, adapting dynamically to real-time factors like user identity, device posture, and location. It also ensures consistent policy enforcement across all environments—cloud, hybrid, and on-premises—simplifying management and providing reliable, uninterrupted access.

Both remote and on-campus users benefit from the same fast, secure access to private application access, ensuring a seamless user experience and maximum productivity without compromising security.

Deep visibility and centralized control

A unified solution provides deep visibility and centralized control by continuously monitoring user access, device posture, and application activity across the network. It consolidates access management through a unified dashboard, allowing administrators to enforce granular, context-based policies and track real-time events for both remote and on-premises users. This centralized control ensures that security teams can quickly detect anomalies, respond to threats, and maintain consistent security policies across all environments, from on-premises to cloud, providing a clear and comprehensive view of user interactions and network activity.

Netskope One Private Access combined with Netskope One DEM provides real-time visibility into application traffic and user activities across distributed environments, with AI/ML alerts for performance degradation or policy violations to mitigate risks and safeguard data.

Key features include:

- Unified 360-degree visibility, combining user and application performance data, covering everything from device health to network links and applications
- Comprehensive visibility into user access, application usage, security policies usage and impact, and traffic patterns to detect anomalies and prevent threats
- Context-aware policy enforcement, based on user identity, device posture, and application risk
- Streamlined operations with automated troubleshooting, proactive support, and visibility into traffic flows and policies

Cost and complexity reduction

Netskope One Private Access provides secure, bidirectional connectivity through a single client that enables secure access to both legacy and modern private applications.

Key capabilities include:

- Eliminating the need for separate solutions like VPN and ZTNA by offering unified access to private applications for both remote and on-campus users, which reduces both capital and operational costs
- Providing a single, unified agent and platform that streamline administration and ensure consistent policy enforcement across all private applications
- Continuously evaluating user traffic for threat prevention and data protection using a single-pass inspection with multiple integrated security engines such as FWaaS, SWG, IPS, CASB, DLP, and AV software. Malicious traffic is promptly identified, audited, and blocked.

This solution helps organizations simplify remote access, improve security, and reduce complexity, eliminating the need for complex routing and integration projects.

FEATURE	DESCRIPTION
Superior business agility and user experience	Lightning-fast secure access to private apps extends seamlessly across remote users, HQ, branch offices, and third-party partners.
Minimize security risk	Context-driven visibility into applications, paired with least-privilege access, reduces security risks by limiting the attack surface and preventing lateral movement across resources.
Gain operational efficiency	Consolidating ZTNA policy enforcement across all users, devices, and locations simplifies operations and management.
Cost savings	A unified solution for private application access eliminates the need for on-premises traditional VPN and NAC appliances, significantly reducing both capital and operational costs.