Solution Brief

Netskope ZTNA Next

Netskope delivers the industry's first VPN replacement solution that combines ZTNA and SD-WAN with a single client. Address the application visibility and security challenges associated with VPNs while optimizing the user experience and reducing the cost and complexity of managing multiple solutions for securing private application access.

Quick Glance

- Enable zero trust access to all private applications hosted across distributed environments
- Reduce the cost and complexity of managing multiple solutions for accessing legacy and modern applications
- Eliminate performance inefficiencies and elevate the user experience
- Reduce the risk of data loss due to lack of visibility and control over application usage

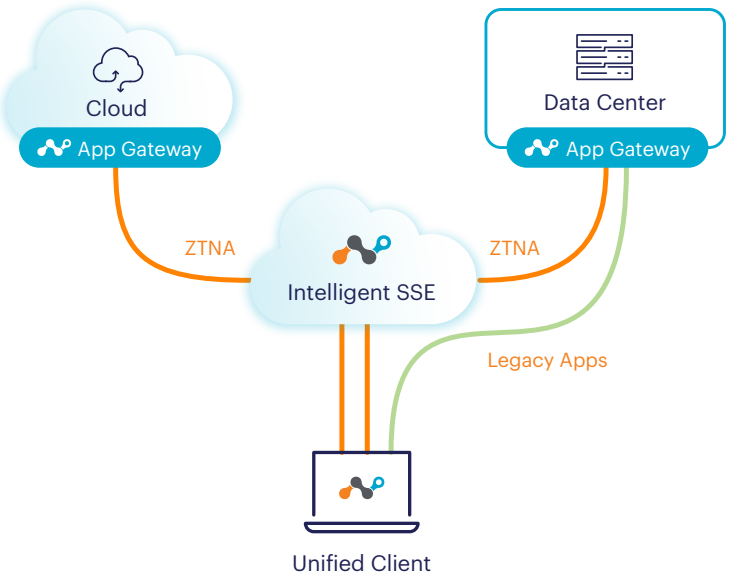
Gartner predicts that by 2025, at least 70% of new remote access deployments will be served predominantly by ZTNA as opposed to VPN services, up from less than 10% at the end of 2021.

The Challenge

With hybrid work becoming a fundamental mainstay, organizations need to modernize their network and security infrastructures for enabling seamless and secure access to data and applications. In this regard, the legacy remote VPN solutions have proven to be woefully inadequate in solving the remote and hybrid workforce requirements and instead have led to the following challenges:

- Expanded attack surface through excessive implicit trust and the risk of unauthorized lateral movement of threats
- Increased network cost and complexity due to over-reliance on VPN infrastructure to support the modern cloud-first deployments
- Increased network latency with traffic backhauling to VPN terminating devices at the corporate data centers
- Lack of application visibility, network awareness, and the ability to deal with degradations impacting the quality of service

Many organizations agree that cloud-based ZTNAs are a modern alternative to remote access VPN solutions. However, some of them face compatibility issues between ZTNA and legacy applications during the upgrade process. Therefore, these organizations must maintain a smaller footprint of VPN infrastructure during the transition period of upgrading their legacy application infrastructure. Unlocking the full potential of the hybrid workforce requires overcoming the security, cost, and performance obstacles associated with VPNs, and providing the required support for legacy applications.



The Solution

Netskope ZTNA Next brings SD-WAN capabilities to ZTNA for enabling secure and optimized connectivity to all private applications, including on-premises hosted VoIP, video, and remote assistance, allowing organizations to completely replace their remote access VPN solutions and modernize connectivity for the hybrid workforce. The solution utilizes zero trust principles to enhance the security posture and eliminate the lateral movement of threats, reduces deployment complexity, optimizes performance, and enables ubiquitous access to corporate resources hosted anywhere through intelligent traffic steering. With ZTNA Next, organizations can avoid maintaining separate ZTNA and VPN clients and instead address all the relevant use cases with a unified client deployment.

Path to zero trust access

Legacy VPN solutions place implicit trust on authenticated users and allow them broad network access, expanding the attack surface and increasing the risk of excessive data exposure through unauthorized lateral movements.

Netskope ZTNA Next incorporates zero trust principles and proposes a shift from traditional network-centric access control to granular application-centric access control on a per-user or user group basis. The solution accelerates the time frame for decommissioning legacy applications and minimizes associated security risks, including unauthorized lateral movement. Key capabilities include:

- Identity- and context-aware, least-privileged access to private applications hosted in public clouds or on-premises data centers
- Facilitating the connectivity through the ZTNA broker in Netskope security cloud. The applications are hidden from discovery, and access is restricted only to authenticated and authorized users.
- Reducing the opportunities for lateral movement of threats within the private networks and limiting the blast radius
- Eliminating the dependence on public-facing VPNs or open inbound firewall ports for application access, securing networks from threats and DDoS attacks

Reduce cost and complexity through vendor consolidation

While cloud-based ZTNA solutions are architected to support inside-out connectivity and shield private applications from discovery, their capabilities are greatly limited for supporting legacy applications that require bi-directional connectivity, such as VoIP services.

Netskope ZTNA Next supports server-to-client or bi-directional traffic connectivity, enabling access to both legacy and modern private applications through a single client. Key capabilities include:

- Eliminating the need to maintain two separate solutions—VPN and ZTNA—for accessing all the private applications and achieving greater cost savings by reducing capital and operational expenditure
- Unified agent and platform to greatly simplify the administrative process and ensure consistent policy enforcement across all the private applications

Seamless and optimized user experience

Remote access VPN backhaul user traffic to centralized data centers for traffic inspection and policy enforcement, increasing the network latency and impacting the user experience.

Netskope ZTNA Next provides fast, direct, and reliable access to private applications, regardless of where they are hosted. Key capabilities include:

- Automatic traffic steering by Netskope client for connecting authorized users directly to specific resources regardless of where it is hosted. Strategically positioned New Edge point of presence (PoP) helps achieve lowest possible latency and round-trip time for application access.
- Assured voice and video application experience with dynamic traffic steering and context-aware QoS. For example, prioritizing traffic for VoIP users, such as remote call center employees, improving their experience and productivity.

Deep visibility and control

Remote access VPN solutions obfuscate the user traffic at the network layer, providing no visibility into the application-related activities and creating a blind spot for IT and operations teams.

Netskope ZTNA Next provides real-time visibility into detailed application traffic and user activities across the highly distributed environments, as well as alerting on policy violations, to reduce business risks and protect data. Key capabilities include:

- Deep visibility into user access, applications usage, and traffic patterns to detect unusual user activity and prevent threats
- Enforcing context-aware policies with deep understanding of content and context including user identity, user risk, device identity, device posture, and app risk
- Simplifying operations with automated troubleshooting, proactive support, and insights into traffic flows and policies

BENEFITS	DESCRIPTION
Improved business agility and user experience	Accelerate hybrid work deployments and enable superior user experience with direct, optimized, and secure zero trust access to applications in public cloud environments or private data centers.
Minimized security risk	Deep application visibility with context-based least-privileged access to the resources to mitigate security threats.
Reduced cost and complexity	Unified solution for all private application access, preventing installation and maintenance of VPN appliances on-premises and reducing capital and operational expenditure.

	LEGACY REMOTE ACCESS VPN	ENDPOINT SD-WAN	PRIVATE ACCESS FOR ZTNA	ZTNA NEXT
Remote connectivity	Yes	Yes	Yes	Yes
Broad legacy application	Yes	Yes	Unidirectional traffic (client-initiated only)	Yes
Support ZTNA architecture	No	No	Yes	Yes*
Minimize lateral movement	No	No	Yes	Yes
Reduce attack surface	No (public facing, exposed to attackers)	No	Yes, shield resources from discovery	Yes, shield resources from discovery
Direct access to resources	No	Yes	Yes	Yes
Application visibility	Limited	Yes	Yes	Yes
Private app traffic inspection	No	No	Yes	Yes*
Optimize VoIP performance	No	Yes	No	Yes

* Applies to ZTNA compatible applications

netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.