wipro | netskope

True Zero Trust should mean VPN retirement



It has been decades since network infrastructure offered a single clearly defined perimeter. But many enterprises still approach security as though a perimeter still exists, even in the face of AI-enabled cyberattacks and a growing need to enable and secure cloud and hybrid work models that include a range of devices, data types and endpoints.

As remote work has increased, the limitations of virtual private networks (VPN) and other legacy approaches have become more apparent: they can lower productivity, cause unreliable performance, and increase attack surfaces by allowing network-based access while failing to provide secure and seamless access to applications in public cloud, SaaS and PaaS. Many are multi-vendor solutions that increase cost and complexity while reducing visibility and control — and they often do not scale well.

Even more concerning, legacy solutions provide a convenient way for malware to effortlessly cross into an enterprise's most sensitive areas. This is because a VPN is nothing more than an encrypted tunnel. It has no security-scanning functions (no anti-virus capabilities, for example) which means malware can get into the tunnel without being challenged.

Zero Trust — A modern alternative

Cloud-delivered Zero Trust Network Access (ZTNA) is a better alternative to VPN. ZTNA is an evolving set of cybersecurity tools that move defenses from static, network-based perimeters to focus on users, assets and resources.



It assumes no trusted zone in networks



Identity-based authentication and authorization are strictly enforced for all connections



Machine to machine (M2M) authentication and authorization are strictly enforced for communication between servers and applications



Risk profiles from near-real-time monitoring are assessed based on user and device behaviors and are then used for authentication and access



All sensitive data is encrypted both in transit and at rest



Centralized governance and policy management are standard



All events are monitored, collected, stored, and analyzed to help assess, deliver and maintain compliance

As businesses adopt and refine hybrid work models, many have begun to replace legacy approaches with modern programs built on ZTNA architecture. These organizations cite VPN replacement as their primary motivation for evaluating ZTNA offerings, but they often find that risk reduction is a bigger benefit than cost savings. ZTNA enables them to significantly improve security and provide faster access to data and applications, whether in the cloud or on-premises. This enables huge transformation as businesses work to bring employees back to the office in a secure hybrid model.

AI-enabled attacks demand AI-enabled defenses

Malware developers and attackers are now using AI to bypass traditional security controls. ZTNA uses deep learning AI algorithms, AI-enabled analytics and automation to detect and respond to these sophisticated threats. ZTNA also provides contextualized reports and auto-healing functionalities to resolve issues. This makes underlying networks and logistics transparent to users.

Managed ZTNA enables users to access applications hosted anywhere with a single agent though Netskope cloud. ZTNA can also provide considerable license cost savings by reducing the number of virtual desktop infrastructure (VDI) and reducing dependencies on hardware.

Protecting the entire organization

ZTNA protects infrastructure, data, devices, apps and users no matter how the attack surface evolves. It also enables continuous policy definition and continuous policy enforcement.

Unlike a VPN, ZTNA delivers access to specific applications instead of networks. Using a cloud-hosted broker between users and enterprise resources, ZTNA services authenticate and validate a user's authorization before connectivity. The user and application traffic meets in the middle, creating a secure connectivity that is an isolated user-to application segment. Benefits include scalability, simplified connectivity, and most importantly, enhanced performance and security thanks to direct, logical connectivity and Zero Trust principles.

As in any technology upgrade, ZTNA and VPN must often co-exist during transition. But many enterprise IT teams find themselves maintaining two connectivity approaches for much longer than planned and without a clear timeline for eliminating legacy VPN. In some cases, they may have to wait until the enterprise has fully modernized their application infrastructure, which can take years.

This is because most ZTNA architectures use an "inside-out connectivity" where private applications must make outbound-only connections to the ZTNA broker to shield it from discovery on the public internet.

Because ZTNA only permits client-initiated application traffic, it poses challenges for on-prem VoIP applications, peer-to-peer connectivity, and other use cases that require server-initiated traffic flow. Endpoint IP addresses are also masked, so ZTNA won't work for applications that require direct access to the endpoint using its public IP address, such as legacy forensic tools.

As a result, many organizations use ZTNA and VPN in tandem until they upgrade their application infrastructure.

The unified Netskope SASE client enables enterprises to prepare for a future when they can permanently retire their VPNs. ZTNA Next is an application that integrates ZTNA/SD-WAN architecture to enable VPN retirement. It sits in front of a converged architecture comprising ZTNA for access to

private and cloud-based applications, and software-defined wide-area networking (SD-WAN) capabilities to securely connect applications that require bi-directional, server-to-client traffic

The virtual client automatically routes application data to the appropriate infrastructure based on whether it is a modern (private access) or legacy/bi-directional (SD-WAN) application as defined by the enterprise's application policies. This realizes the full potential of a SASE-based approach to remote work and unlocks many benefits including:

- Accelerated ZTNA adoption by enabling organizations to identify their bi-directional apps and create a transformation roadmap
- Improved security by replacing VPNs with end-to-end encryption across an organization's networks
- Reduced complexity for legacy apps in multi-cloud environments, as SD-WAN enables more flexible traffic routing compared to VPNs
- Improved user experience with routing to ZTNA/SD-WAN taking place behind the scenes, providing users with seamless and immediate access to their applications
- Reduced costs of multiple security appliances by eliminating VPN holes in the corporate firewall
- Enhanced performance for video and voice traffic, which can be routed via the SD-WAN for reduced latency

When deploying a converged ZTNA/SD-WAN remote working capability, look for an approach that:



Reduces overall cost and complexity, prevents technology sprawl, and consolidates separate products into a modern approach using a single agent—with no hardware required



Addresses legacy application compatibility issues with ZTNA



Extends the longevity of legacy applications such as on-premises VoIP by optimizing performance



Unlocks AI-driven operations with automated troubleshooting and insights into traffic flows, policy violations and anomaly



Connects users anywhere, using any device, to corporate resources everywhere, continuously evaluating context and adapting in real time to protect data

The scope of these changes is huge and complex, so adopting ZTNA requires careful planning and a phased, integrated approach that builds the right principles into planning, architecting, deploying and managing networks.

Traditional tech-focused roles like the CISO, CTO and CIO are involved in making this shift but other roles should provide key input. These can include operations-focused roles like the COO, CHRO, Chief Legal Officer, Chief Risk Officer, Chief Compliance Officer and others. ZTNA also has profound implications for revenue, innovation, and growth, so the CMO, CXO, CDO, Chief Revenue Officer and Chief Innovation Officer should also be involved.

The process starts by assessing your current cybersecurity maturity with a due diligence to assess and design migration of applications to ZTNA. From there, organizations must rationalize their tools and strengthen their controls to create a cohesive architecture with the appropriate ecosystem of security tools. The goal should always be to gain complete visibility and insight into your cybersecurity environment, to identify risks prioritized by context and to automate remedial actions.

ZTNA is proving to be a holistic, practical, and adaptable solution to the cybersecurity challenges that all enterprises now face. The Zero Trust approach offered by Wipro and Netskope solves the problem of wide-open, un-policed internal IT systems by leveraging analytics and automation to provide visibility and access based on a trust-but-verify model.

Learn more about Wipro's Managed ZTNA solution powered by Netskope

Wipro + Netskope

Wipro is a Netskope reseller and Platinum partner, providing managed services and professional services. Netskope is a strategic Alliance Partner for Infrastructure and Cloud Security, a CoE for SDWAN, Zero Trust, and cloud security, and are certified and trained professionals in Wipro strategic technology solutions. Together, we ensure that enterprises secure their digital transformation initiatives by delivering customized, integrated, and fully managed solutions and services that protect users, data and businesses.



Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses.

With nearly 245,000 employees and business partners across 65 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world.

For additional information, visit us at www.wipro.com

AMERICAS/CRS/NOV2024