Solution Brief

Universal ZTNA with Netskope One Private Access

Netskope's Universal ZTNA represents a holistic approach to securing modern, distributed IT, IoT, and OT environments. It delivers zero trust visibility and control over users and devices from any location, ensuring consistent, identity- and risk-based access across the enterprise.

Quick Glance

- **Accelerates legacy retirement:** Fully replaces outdated VPNs, NACs, VDI/DaaS, and PRA.
- **True least-privilege access:** Delivers granular, real-time, identity- and risk-based adaptive access for users and devices across IT, OT, and IoT.
- **Integrated security:** Inspects all web traffic with advanced threat protection and DLP controls.
- **Intelligent automation:** AI-powered Copilot continuously discovers apps, defines policies, and optimizes configurations, eliminating manual complexity.
- **Optimized user experience:** Ensures seamless application access and high-performance connectivity via NewEdge intelligent steering and the shortest-latency path.

Universal zero-trust network access (ZTNA) is expected to grow to widespread adoption, greater than 40%, by 2027.

Gartner®, Emerging Tech: Universal ZTNA Drives Secure Access Consolidation, by Charanpal Bhogal, Andrew Lerner, John Watts, Marissa Schmidt, 20 December 2024

The Challenge

Existing ZTNA solutions offer fragmented coverage, addressing only specific user types, locations, or access scenarios, and often creating new silos rather than removing them.
As a result, they:

- Are built for user-initiated access, making it difficult to support server-initiated services like SCCM, VoIP, Remote Assistance, and security scans in campus or branch environments.
- Are ineffective for headless IoT and OT devices, which lack a human user to initiate secure connections.
- Create silos across users and environments, forcing separate solutions for remote workers, campus users, contractors, and IoT/OT devices, adding complexity, inconsistency, and risk.
- Lack continuous, dynamic posture enforcement, limiting their ability to adapt to changing risk conditions.

The Solution

Netskope One Private Access is the foundation of Netskope's Universal ZTNA. When combined with Netskope One Device Intelligence, it unifies secure access across IT, OT, and IoT environments. This comprehensive solution replaces legacy VPN, NAC, and VDI, delivering least-privilege controls, built-in threat and data protection, and high-performance connectivity. To make operations even simpler, the AI-powered Copilot automates policy definition and optimization, while intelligent traffic steering ensures a seamless and superior user experience, strengthening security and streamlining IT.

Netskope's Universal ZTNA delivers secure hybrid access for users across remote and on-prem environments while extending Zero Trust protection to OT and IoT ecosystems. It helps organizations retire legacy VPN, NAC, and VDI/DaaS solutions, securely enable third-party and BYOD users, accelerate M&A integrations, and support VoIP and remote assistance.

netskope

Beyond complexity: Simplifying access with a user-first experience

Netskope One Private Access delivers the most comprehensive, user-first secure access experience available today. By consolidating multiple legacy technologies, it replaces VPN, NAC, VDI/DaaS, and Privileged Remote Access solutions. Whether users connect remotely, on campus, or from unmanaged and third-party devices, Netskope One Private Access provides frictionless application access that enhances productivity while eliminating the complexity and risks of traditional tools.

Local broker support extends ZTNA to on-premises users with local traffic steering and policy enforcement, thereby eliminating cloud hairpinning and to OT environments that have limited internet connectivity. It also acts as a disaster recovery (DR) mechanism, maintaining resilience and continuity.

Key capabilities include:

- **Flexible access methods,** including agent-based, and browser-access methods with granular policies to intelligently route traffic through cloud or local brokers.
- **Native integration with Netskope One Enterprise Browser** to provide secure, browser-based access to private applications; ideal for unmanaged or third-party devices.
- **Continuous, adaptive zero trust enforcement** with consistent, real-time policies across users, devices, apps, and data. Permissions adjust automatically as context changes, instantly terminating risky connections to maintain strong security posture.
- **Intelligent traffic steering** via NewEdge cloud or local brokers to ensure low latency, resilience, and global scale for a seamless user experience everywhere.

56% of organizations experienced at least one VPN-related security incident in the past year.

Source: "VPNs Under Siege: Why you need zero trust access in 2025, by Cybersecurity Insiders"

- **Built-in end-to-end monitoring** with Netskope One Digital Experience Management (DEM) to provide continuous insight into private app performance, reducing mean time to resolution (MTTR) and simplifying troubleshooting.

Beyond manual: Continuously optimized ZTNA

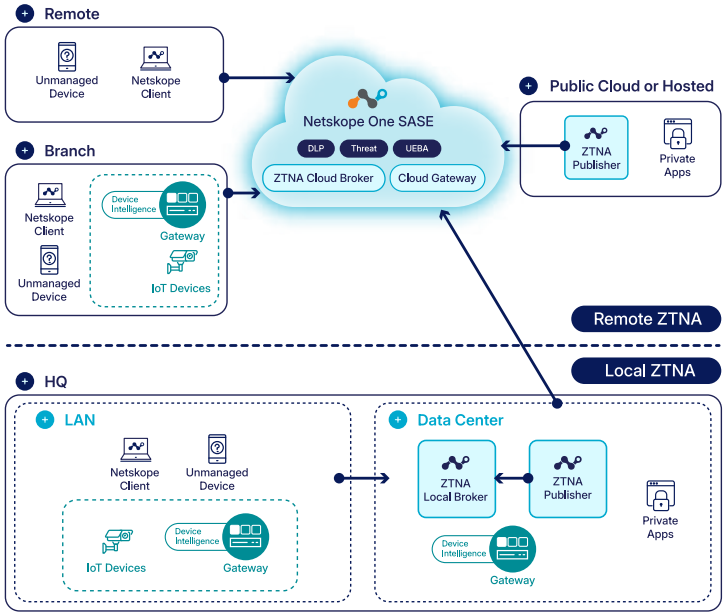
Netskope One Private Access redefines secure access by moving beyond the manual, time-consuming, and error-prone processes of traditional ZTNA. A key innovation is the Netskope One Copilot for Private Access, an intelligent assistant that automates the manual and time-consuming process of ZTNA administration, and provides actionable recommendations across three core areas:

- **ZTNA posture from day one:** Accelerates the shift from VPN-like access to true ZTNA by redefining application discovery and creating granular application segments and policies for newly accessed applications.
- **Ongoing ZTNA posture improvement:** Replaces broad network destinations with more precise definitions, specific IP addresses, or FQDNS.
- **Continuous audit:** Regularly reviews existing ZTNA configurations to identify and remove dormant app segments, destinations, or policies.

This AI-driven approach enables security teams to move faster, reduce their attack surface, and scale ZTNA strategies effectively across large scale environments.

By 2027, 60% of enterprises will replace network access control (NAC) and/or embedded switching security features with ZTNA on corporate-owned campus LANs, up from nearly 10% in 2024.

Gartner®, Emerging Tech: Universal ZTNA Drives Secure Access Consolidation, by Charanpal Bhogal, Andrew Lerner, John Watts, Marissa Schmidt, 20 December 2024



Universal ZTNA, delivered by Netskope One Private Access and Netskope One Device Intelligence. Built on a unified platform, it eliminates silos by converging identity-based access with the full SASE security stack, providing consistent protection across all locations, users, devices, and applications.

Beyond validation: Built-in threat and data protection

Modern secure access requires more than identity validation, it demands deep inspection and consistent enforcement to protect the private application landscape against evolving threats. Netskope One Private Access integrates foundational threat and data protection directly into private application traffic flows.

It inspects all web traffic with advanced threat protection (ATP) and data loss prevention (DLP) controls. ATP stops threats like malware and ransomware from reaching your network, while DLP enables policy-based controls across unmanaged or third-party devices. This ensures sensitive data remains protected, regardless of how users connect or what devices they use.

Netskope One Private Access utilizes the same Threat Protection and DLP engines powering Netskope's Next Gen SWG and CASB solutions, ensuring consistency across the platform while minimizing operational complexity.

These capabilities transform ZTNA from a basic access solution into a comprehensive security framework, offering deep visibility, unified policy enforcement, and enterprise-grade protection.

Key capabilities include:

- **Integrated threat inspection:** Built-in IPS, AV, and ML classifiers, Phishing Engines, Heuristics Analysis, and Sandboxing.
- **Comprehensive DLP controls:** Full coverage for client and browser-based access.
- **Unified security engine:** Shared threat and DLP engines ensure consistent enforcement across SWG, CASB, and ZTNA.

Beyond users: Secure connectivity across IoT/OT devices

With the proliferation of IT, IoT, and OT devices, ZTNA must extend beyond users to secure every connected endpoint, especially in branches, campuses, and factory environments. Netskope addresses this need through Netskope One Device Intelligence, a capability that brings visibility, context, and control to your device ecosystem.

Powered by HyperContext®, an agentless smart device security platform, Device Intelligence discovers both managed and unmanaged devices, analyzes hundreds of parameters, and delivers real-time classification and risk scoring, enabling dynamic access controls and segmentation for zero trust at scale.

Key Capabilities:

- **Comprehensive device classification and visibility:** Agentless discovery and classification deliver deep insights into device activity and behavior across all IT, OT, and IoT environments.
- **Integrated cybersecurity asset management:** Built-in asset inventory engine provides granular search and reporting, with seamless integration to platforms like ServiceNow CMDB.
- **Continuous device risk assessment:** Ongoing monitoring detects anomalies, assigns dynamic risk scores, and generates alerts for streamlined SOC automation.
- **Context-aware access control & segmentation:** Real-time device grouping and micro-segmentation policies are enforced at the gateway and via seamless integration with multi-vendor switches and access points.

BENEFITS	DESCRIPTION
Eliminate legacy complexity with unified access	A single solution that delivers consistent, secure access for all users, whether remote, on-campus, or third-party, and across all device types, including managed, unmanaged, BYOD, and agentless. It spans IT, OT, and IoT environments, eliminating the need for fragmented tools.
Full VPN replacement, strong alternative for NAC, and VDI	Deliver secure, least-privilege access to private apps with granular policies that route traffic intelligently through cloud or local brokers. End users get a smooth, reliable experience on any device or location, while built-in Digital Experience Management (DEM) provides visibility and monitoring to simplify operations and reduce troubleshooting.
Adaptive access for users and devices across IT, OT, and IoT	Continuously evaluates user identity, device posture, location, activity, behavior, threat intelligence, and data risk to grant least-privilege access. Secures managed and unmanaged devices, such us laptops, IoT, and OT systems, with consistent protection everywhere.
Built-in data and threat protection	Protects sensitive data and private applications against evolving threats without adding complexity. By embedding advanced threat detection and DLP directly into secure access, organizations reduce risk, ensure consistent protection across all users and devices, and maintain confidence that sensitive resources stay safe everywhere.
Enhanced operational efficiency and agility	Simplifies operations and accelerates secure access adoption by replacing manual, error-prone processes with intelligent automation. With Copilot for Private Access continuously optimizing ZTNA policies and a single unified console for all operations, organizations reduce administrative overhead, shorten time-to-value, and accelerate zero trust adoption.
Optimized user experience	Delivers seamless, app-level connectivity with intelligent steering, auto-failover, and shortest-latency path routing. Users gain fast, reliable access from any location or device, while IT benefits from reduced support overhead and improved visibility through built-in DEM. The result is stronger productivity and consistent experiences across all locations.
Unified visibility	Get real-time, end-to-end insights into private app performance with Netskope One Digital Experience Management (DEM). Path-level metrics accelerate troubleshooting, reduce MTTR, and simplify compliance, ensuring high-performance, secure access with a single source of truth.

10/25 SB-930-1