netskope

6 Reasons Universal ZTNA is a Smart Escape from VPN and NAC Chaos

Table of Contents

Introduction

Virtual private network (VPN) and network access control (NAC) solutions once anchored enterprise access. They now struggle in organizations where applications span data center, SaaS, and public cloud environments, and where endpoints range from unmanaged laptops to IoT and OT systems. The outcome is operational drag, inconsistent user experience, and exploitable gaps, resulting in higher costs, reduced productivity, and increased exposure to attackers.

Zero trust network access (ZTNA) offers a path forward by enforcing least privilege at the point of access. However, outcomes vary widely. If implemented as another point solution, ZTNA may add complexity instead of reducing it, fall short of delivering the true zero trust protections organizations expect, and even slow down access in ways that drag on productivity.

Universal ZTNA addresses the potential for complexity with traditional ZTNA. It applies a single policy framework across every user and device—whether managed or unmanaged, and across all locations, including IT, OT, and IoT environments. This reduces silos, lowers reliance on legacy access technologies, and creates a consistent control plane that improves security, performance, and manageability across an organization's systems.

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

Why we need Universal ZTNA

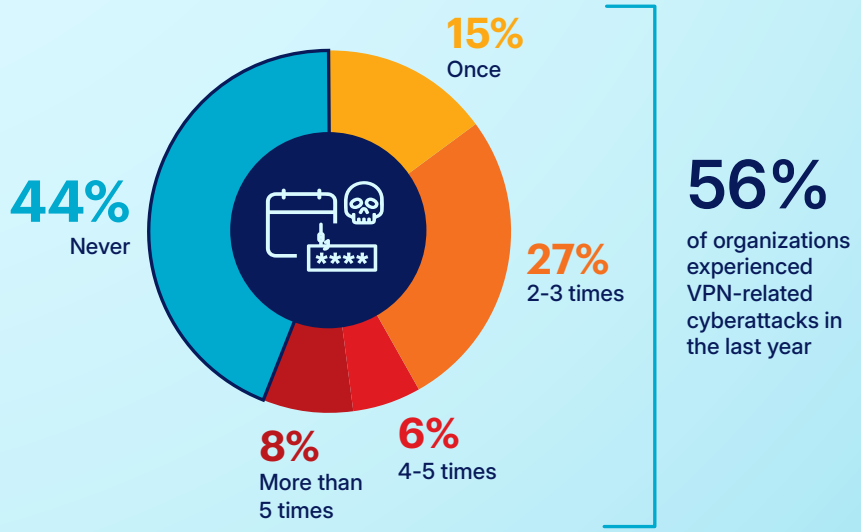
In recent years, the way employees access company resources has changed dramatically, reshaping the digital threat landscape. As more workers connect from outside the office, legacy VPNs are stretched to their limits. Meanwhile, the rise of cloud, OT, and IoT environments has overwhelmed many NAC solutions with too many devices to secure.

Managing these technologies consumes IT resources, while performance and stability issues degrade the user experience. Worse, VPN and NAC systems expose companies to risk: once users gain entry, they often have nearly unlimited lateral movement.

Concerns about security, performance, and complexity are fueling adoption of ZTNA, which promises least-privilege access to private apps, anywhere, on any device. Yet many ZTNA tools fall short. Fragmented, complex, and incomplete, they often fail to cover all use cases.

Organizations need a truly universal ZTNA solution, such as Netskope One Private Access, to close these gaps.

In the last 12 months, has your organization experienced an attack that took advantage of security vulnerabilities in your VPN servers?



+ 56% of companies experienced a cyberattack within the past year that took advantage of VPN security vulnerabilities. 41% experienced more than one such attack.*

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

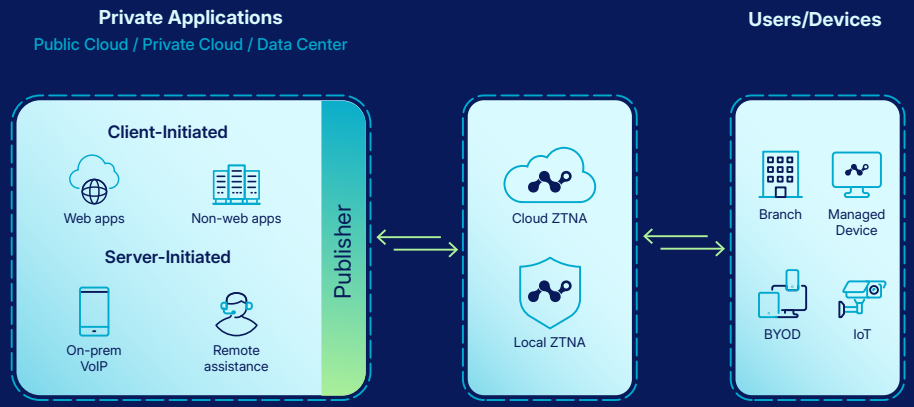
Reason 1 - Adaptive granular access control can replace VPNs entirely.

Despite known security weaknesses, 21% of IT professionals cite poor user experience as their biggest VPN issue.* VPNs slow performance, complicate remote workflows, and create troubleshooting headaches that burden IT. Fragile and high-maintenance, VPNs are increasingly unfit for hybrid work.

Traditional ZTNA solutions were meant to resolve these issues, but most focus only on remote users, leaving gaps for those on premises.

Universal ZTNA solves both sides. By replacing fragile tunnels and static network-level controls with identity- and context-based access, it delivers fast, consistent connections to approved apps from any device, whether remote or onsite. For IT teams, it reduces tickets, simplifies management, and adds resilience, streamlining secure connectivity, cutting risk, and enabling today's hybrid workforce.

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



How we do it

Netskope One Private Access delivers adaptive, identity- and risk-based access to corporate resources on-premises or in the cloud. By continuously evaluating user identity, device posture, location, activity, behavior, threat intelligence, and data risk, it ensures least-privilege access from anywhere in the world.

Reason 2 - Universal ZTNA reduces dependency on legacy NAC by delivering dynamic, posture-driven access control.

Originally designed to govern the on-premises workforce's access to on-premises solutions, NAC platforms struggle to govern remote access. The unsuitability of using NAC to govern "off-prem" users typically drives organizations to rely on a different solution for branch or remote-user access.

Even for onsite connectivity, NAC systems create a security risk: After authentication, they implicitly trust the user and grant broad network access. This approach, which NAC shares with VPN systems, fundamentally conflicts with zero trust principles.

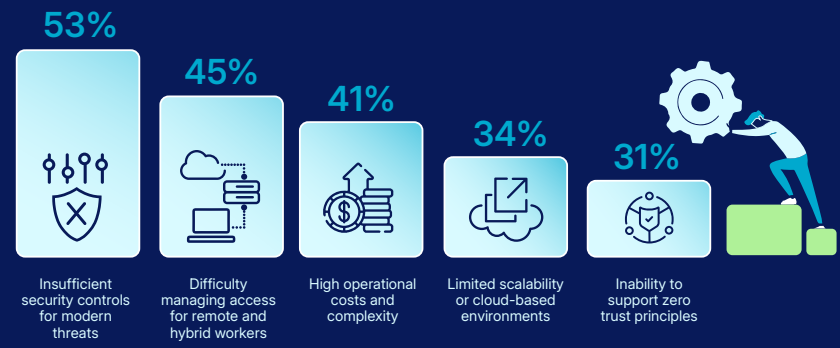
NAC solutions also lack visibility into many IoT/OT devices, so they have trouble blocking unsafe connections from those systems.

Universal ZTNA shifts security from this static, network-based model to a dynamic, identity-centric paradigm. By continuously verifying users and devices, it grants granular, least-privilege access to specific applications, regardless of the user's location. This unified approach secures all devices, including remote, IoT, and OT, reducing the organization's attack surface and improving operational efficiency.

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

+ 76% of organizations consider replacing their NAC to be a high priority.

What challenges does your organization face with its current NAC (network access control) solution?



How we do it

Netskope augments legacy NAC with adaptive, context-aware ZTNA that unifies device authentication, visibility, and control for both on-premises and remote users. Local Broker extends secure access on-prem, eliminates cloud hairpinning, and adds built-in Disaster Recovery resilience. Device Intelligence extends zero trust enforcement across east–west traffic through integrations with leading NAC vendors.

Reason 3 - Extend zero trust to every device, even IoT and OT.

A major gap in many traditional ZTNA solutions is the lack of support for OT, IoT, or device-initiated network access. As a result, companies are forced to maintain legacy VPNs for on-premises, server-initiated services, creating gaps in security, adding risk, and burdening IT with managing two inconsistent systems instead of retiring outdated infrastructure.

Since Gartner® coined the term “Universal ZTNA” in 2022*, many vendors have claimed to offer these capabilities. Netskope defines “universal” as full coverage across all users and devices, including unmanaged endpoints and device-to-service communications, something most solutions fail to achieve.

Truly universal ZTNA consolidates both user-to-app and device-to-service access across environments into one centrally managed platform, applying least-privilege, granular access controls consistently to everything from remote endpoints to supervisory control and data acquisition (SCADA) controllers.

Gartner, Emerging Tech: Universal ZTNA Drives Secure Access Consolidation, 20 December 2024.

How we do it

Access controls in Netskope One Private Access integrate device intelligence to assess device risk and posture in real time. With agentless discovery and classification across OT and IoT environments, it delivers deep visibility, continuous risk assessment, and context-aware segmentation for stronger security and control.

Reason 4 - One unified, intelligent platform replaces patchwork access and complexity.

Most IT and security teams are juggling an alphabet soup of security tools, from VPN and NAC to privileged access management (PAM), secure web gateway (SWG), data loss prevention (DLP), and more. Each tool creates a silo with its own management console and policy framework, making it difficult to enforce consistent controls across the enterprise.

Moving from VPN to ZTNA introduces new challenges. VPNs use broad policies, while ZTNA requires precise, app-specific controls. Mapping users, apps, and dependencies is complex, and without a unified approach, organizations risk policy sprawl and inconsistent enforcement.

Universal ZTNA addresses these pain points by consolidating policy creation, enforcement, and monitoring into a single platform. Delivered through a secure access service edge (SASE) architecture, it integrates access control, device and user authentication, threat protection, and data security into one intelligent system. This eliminates silos, simplifying operations and providing end-to-end visibility for IT and security teams.

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

+ 13% of IT professionals said their biggest headache in VPN management is juggling VPN compatibility with various devices, operating systems, and applications.*

How we do it

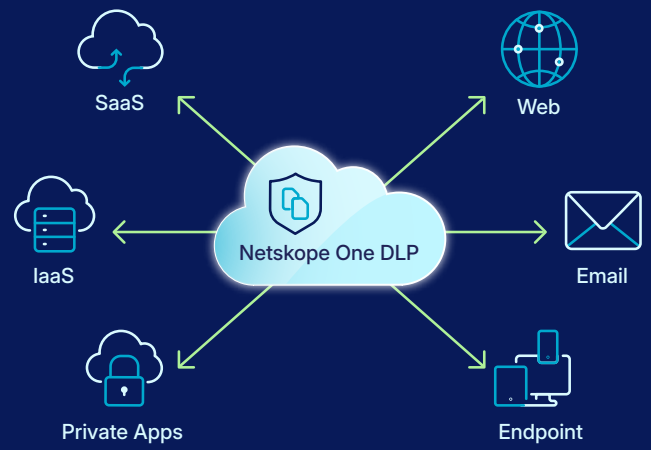
Netskope One Copilot is an AI-powered ZTNA assistant built into Netskope One Private Access that simplifies and accelerates ZTNA adoption. It discovers applications, recommends granular app segments and policies, optimizes broad configurations, and removes stale rules, continuously improving security posture.

Reason 5 - Universal ZTNA applies zero trust principles, universally.

Truly universal ZTNA delivers identity-centric access control, continuous monitoring, and seamless integration across any environment. Resources can be on premises or in the cloud; users can be at headquarters, a branch, a home office, or literally anywhere with internet access. Every device is covered, managed or unmanaged, agent-based or agentless, user-initiated or machine-level.

This is not theoretical zero trust. Universal ZTNA applies real-time, dynamic policies based on identity, posture, activity, behavior, threat signals, and data context. Unified security policies, centralized management, and distributed enforcement extend to every asset, with built-in threat and data protection.

Where traditional ZTNA covers only part of the problem, universal ZTNA standardizes granular, application-specific access to the individual user. By applying unified policy across all access methods, it eliminates blind spots, reduces complexity, and ensures secure, consistent access for every user and device.



How we do it

Netskope One Private Access goes beyond fast, secure access for remote and local users, delivering advanced threat protection (ATP) and data loss prevention (DLP) across private application traffic. ATP blocks malware and ransomware before they reach the network, while DLP enforces policy-based controls—even on unmanaged or third-party devices—keeping sensitive data protected everywhere.

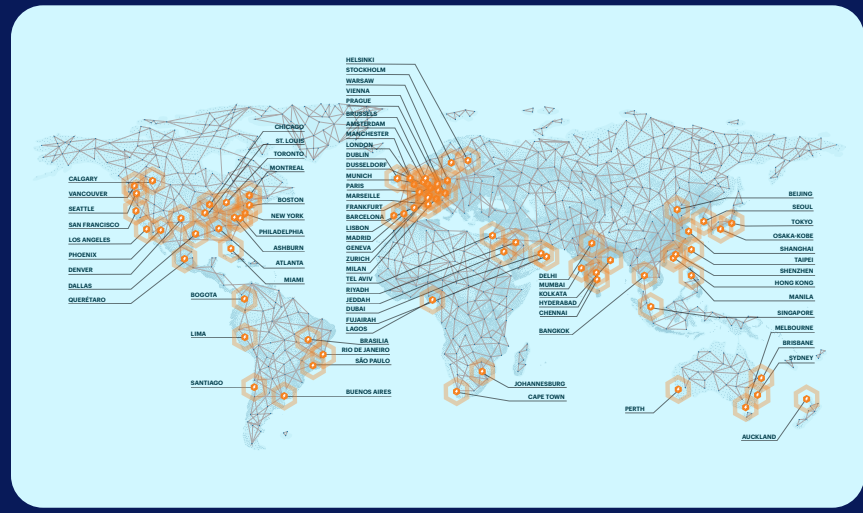
Reason 6 - Universal ZTNA provides a simplified experience for the end user.

Organizations still struggle with VPN performance and user experience. A Cybersecurity Insiders' survey* found that end users are frustrated by VPN sluggishness (22%), complex authentication (19%), login issues (18%), connection drops (15%), and inconsistent experiences across devices (12%). These problems generate IT tickets and drain valuable staff time.

Universal ZTNA eliminates these challenges. Users no longer need multiple access methods, authentication is the same everywhere, for every app. The result: higher productivity and fewer IT support calls.

Better yet, a universal ZTNA solution with built-in digital experience management (DEM) provides IT with unified visibility and monitoring. With a single source of truth for end-to-end connections, IT can resolve issues faster, streamline troubleshooting, and keep employees focused on their work.

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



NewEdge Network, the world's most performant private cloud, powers Netskope One

How we do it

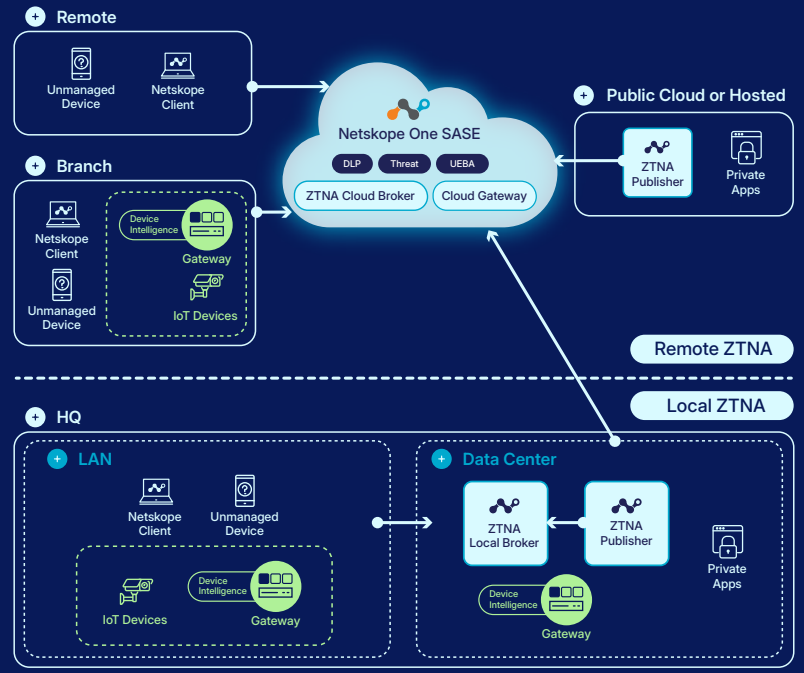
Netskope One Private Access cuts help desk tickets by streamlining access and reducing latency. Powered by the global NewEdge Network, traffic is routed closer to users and applications for faster performance. Built-in Digital Experience Management (DEM) monitors private traffic in real time, simplifying troubleshooting and improving user experience.

Conclusion - Smarter access, stronger protection for users and devices everywhere.

VPN and NAC tools built on principles of implicit trust are in direct conflict with zero trust strategies. ZTNA, by design, removes implicit trust from the network security architecture. Universal ZTNA platforms that include integrated threat and data protection further ratchet down security across the corporate environment.

Netskope One Private Access is the foundation of Netskope's Universal ZTNA, unifying access across IT, OT, and IoT environments. Together with Netskope One Device Intelligence, Netskope One Private Access enables a truly universal ZTNA approach that goes beyond traditional ZTNA.

Part of the Netskope One SASE platform, this solution fully replaces legacy VPN, and offers a strong alternative for NAC, virtual desktop infrastructure (VDI)/desktop as a service (DaaS), and privileged remote access (PRA) solutions with least-privilege controls, built-in threat and data protection, and high-performance connectivity.



Netskope's Universal ZTNA solution

Learn more

If these six reasons to adopt universal ZTNA sound familiar, you're not alone. Netskope's solution, powered by Netskope One Private Access and Device Intelligence, helps organizations fully retire VPNs and reduce their dependency on NACs—all while gaining greater visibility, simplicity, and security.

About Netskope

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.

Security & Networking ReAImagined


netskope