eBook

10 Things Your ZTNA Must Do

netskope

Table of Contents

Introduction 3

Back to basics: What is ZTNA 4

How is ZTNA instrumental to SSE? And how does this integration help customers? 5

The 10 must-haves for an advanced ZTNA solution: 6

- Identity-based Least Privilege Authentication 6
- Comprehensive Device Posture Assessment 7
- Advanced Micro-segmentation with Identity-based Policies 8
- Universal ZTNA 9
- Support for legacy applications 11
- Security controls closer to where user and applications connect 12
- Integration with broader security ecosystem 13
- Full network visibility and analytics 14
- Ensuring scalability and agility 15
- Effective administrative tools 16

Summary 17

Introduction

The rise of cloud technologies, decentralized infrastructures, and remote workforces has made traditional security perimeters obsolete, exposing the limitations of VPNs. VPNs are now often inadequate, struggling with expanded attack surfaces, high costs, increased latency, and limited visibility into application performance.

Zero Trust Network Access (ZTNA) offers a cloud-based alternative tailored to today's security needs. By granting controlled, role-based application access based on user identity and device context, ZTNA minimizes risks, reduces attack surfaces, and prevents unauthorized lateral movement within networks. Unlike VPNs, ZTNA uses a trusted broker to connect users to applications without exposing them to the public internet. With seamless integration into Security Service Edge (SSE) solutions, ZTNA ensures secure, flexible connectivity across on-premises, cloud, and hybrid environments, enhancing both security and performance.

Not all ZTNA solutions are equal—discover the 10 must-haves that make a ZTNA solution exceptional.

Back to basics: What is ZTNA?

ZTNA provides controlled, role-based, least privilege access to applications and resources by evaluating the identity of users and their devices, as well as contextual factors like time, date, geolocation, and device posture. It creates a secure perimeter around assets and manages network flow, where even small changes, such as a shift in device posture, can trigger near-real-time revocation of access.

ZTNA operates with a default-deny approach and adheres to zero trust principles, such as granting just-in-time access to specific resources. Users are granted access only to authorized applications, and this access is continuously monitored and re-evaluated. The objective is to reduce risk by shrinking the attack surface and placing security controls closer to the protected resources.

Additionally, ZTNA eliminates the need for direct exposure of applications to the public internet. Instead of connecting directly, a trusted broker facilitates the connection between users and applications. This broker can be a managed cloud service, a self-hosted service in a data center, or a virtual appliance in an IaaS cloud. After verifying the user's credentials and device context, the broker communicates with an app connector, located near the application. The app connector then establishes a secure connection back to the private application and an outbound communication path to the broker.

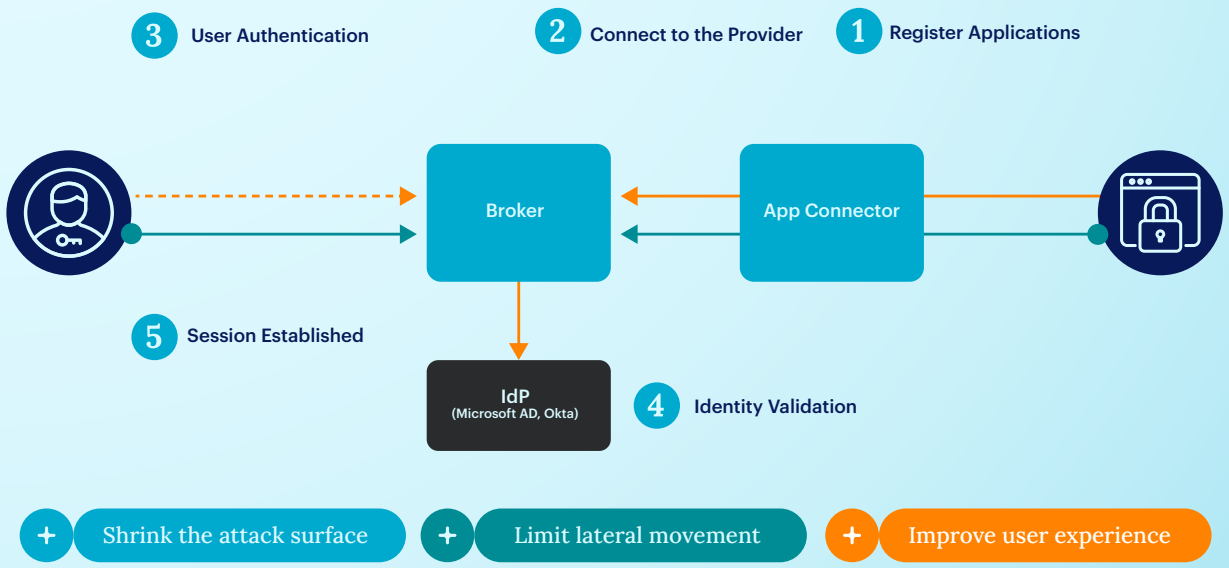


Figure 1: How zero trust network access works

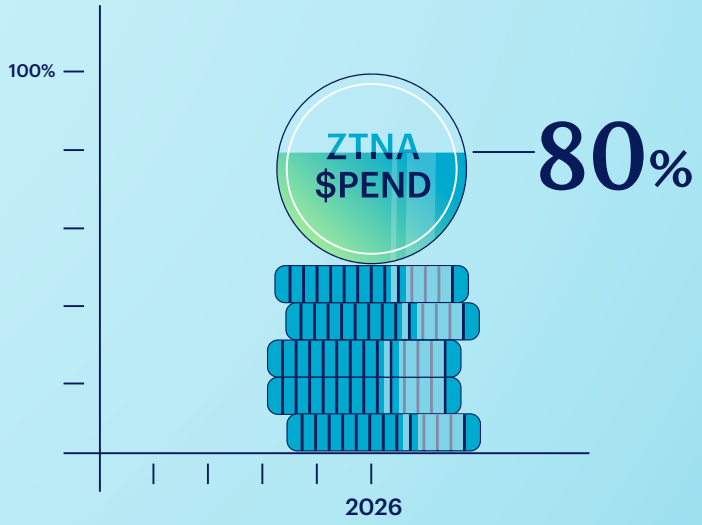
How is ZTNA instrumental to the SSE? And how does this integration help customers?

Security service edge (SSE) consolidates key security services—including ZTNA, secure web gateway (SWG), cloud access security broker (CASB), and data loss prevention (DLP)—into a unified, cloud-delivered platform.

As a central component of SSE, ZTNA provides secure, granular, and conditional access to applications and services. It manages access controls and authentication for both on-premises and cloud-based resources. ZTNA applies adaptive, contextual access controls based on user behavior, device health, location, and other risk indicators, ensuring consistent protection across all security services within the SSE framework. According to Gartner, 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[1].

SSE uses real-time data from ZTNA to make dynamic security adjustments. For instance, if a device becomes compromised, SSE can automatically modify access controls and activate additional services, like DLP, to prevent data breaches or unauthorized access.

The use of ZTNA within SSE enhances security, improves user experience, simplifies management, and supports scalability. This alignment enables organizations to adopt a modern zero trust security model, protecting their resources and adapting to the evolving threat landscape.



> According to Gartner, 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[1]

[1] Gartner, Competitive Behaviors in the ZTNA Platform Market, By Evan Zeng, Charanpal Bhogal, 12 August 2024

1 | Identity-based Least Privilege Authentication

01

Authentication provides security, but its static nature can lead to gaps, compliance issues, user dissatisfaction, and weakened security for an organization.

Compromised credentials are a common threat, and traditional security methods often apply uniform protection to all users, leading to vulnerabilities in high-risk situations or unnecessary friction in low-risk ones. While authentication is crucial, its true value lies in being flexible and context-aware. Without proper adaptive authentication, organizations are at greater risk of security breaches, compromised accounts, and insider threats, as they lack the ability to respond to contextual factors in real time.

Identity-based Least Privilege Authentication addresses these challenges by applying a dynamic, context-aware approach to authentication. It adjusts security measures based on the assessed risk level of a user's login attempt. In a ZTNA solution, this method enhances security by continuously evaluating the risk of each access request and adapting authentication requirements accordingly. By integrating real-time risk assessments with access control, this approach supports a strong zero trust security framework.

Implementing Identity-based Least Privilege in ZTNA involves defining security policies, integrating multi-factor authentication (MFA), and configuring contextual risk assessments. ZTNA must include identity-based least privilege authentication, granting users access only to what they need, when they need it, based on their identity and access context. This minimizes risk, reduces the attack surface, and strengthens security.

HOW?

Netskope One Private Access enforces strict identity-based access, granting users only the necessary permissions, with support for both managed (agent- based) and unmanaged (agentless) devices.

2 | Comprehensive Device Posture Assessment

02

The absence of posture management of devices in use significantly increases the risk of cyberattacks, data breaches, compliance failures, and inefficient security operations for organizations.

With the rise of remote work and bring your own device (BYOD) practices, device posture management has become increasingly crucial. Without continuous monitoring and enforcement of security standards, organizations are vulnerable to threats from unsecured devices. Device posture management ensures that all devices, managed or unmanaged, comply with security policies before accessing sensitive resources.

With ZTNA, device posture management verifies compliance before granting access to network resources, dynamically assessing device health and context to allow only secure devices access to critical data. This approach reduces risk and enhances overall network security.

Device posture management is a must-have in any ZTNA solution to address security, compliance, threat mitigation, and incident response while enforcing zero trust principles. For instance, if a device with corporate credentials is stolen, posture checks detect non-compliance and trigger alerts during access attempts.

By ensuring only secure devices access their networks, organizations maintain a robust zero trust security posture.

HOW?

Netskope One Private Access continuously assesses device health and compliance for managed and unmanaged devices, offering real-time risk evaluation before granting access.

3 | Advanced Micro-segmentation with Identity-based Policies

03

Conventional network security models and segmentation methods frequently fail to manage the complexities of modern IT environments, leading to increased risks and greater exposure to vulnerabilities.

Organizations lacking advanced security controls face increased risks of data breaches, unauthorized access, and inefficient network resource use, making it difficult to protect sensitive data, comply with regulations, and defend against evolving threats. Advanced micro-segmentation with identity-based policies addresses these challenges by offering precise control over network access and enforcing security based on user identity, device posture, and application context.

This approach divides the network into secure micro-segments, controlling access to each based on user identities and contextual factors. It strengthens security by adhering to the principle of least privilege and applying dynamic, granular access controls for users, devices, and applications. This prevents lateral movement, reduces implicit trust, supports compliance, mitigates third-party risks, and secures hybrid and multi-cloud environments.

When combined with ZTNA, advanced micro-segmentation becomes a critical component of a zero trust architecture. While ZTNA verifies identities at the network perimeter, micro-segmentation provides deeper protection by controlling interactions within the network, restricting user activity based on identity and role even after access is granted.

Implementing advanced micro-segmentation requires a combination of technologies, best practices, and continuous management. To fully leverage this in a ZTNA solution, organizations should integrate identity-based access controls, continuous monitoring, automation, and regular policy updates to maintain secure segmentation and enforce dynamic policies based on user and device identities.

HOW?

Netskope One Private Access enforces identity-based policies that limit access to specific applications, not the entire network.

4 | Universal ZTNA

04

Traditional ZTNA solutions often focus on web or cloud apps, leaving gaps in securing legacy systems, non-web applications, and unmanaged devices. This causes inconsistent access control across on-premises, cloud, and hybrid environments, and a poor user experience.

ZTNA solutions must tackle the challenges of legacy applications, which often rely on outdated VPN technology, creating security risks and a poor user experience. Many ZTNA solutions route traffic for legacy or on-premises apps through centralized VPN gateways, causing bottlenecks and latency, undermining ZTNA's advantage of direct, identity-based access. Additionally, inconsistent application of the zero trust principle, especially with legacy systems, leaves organizations exposed to security vulnerabilities.

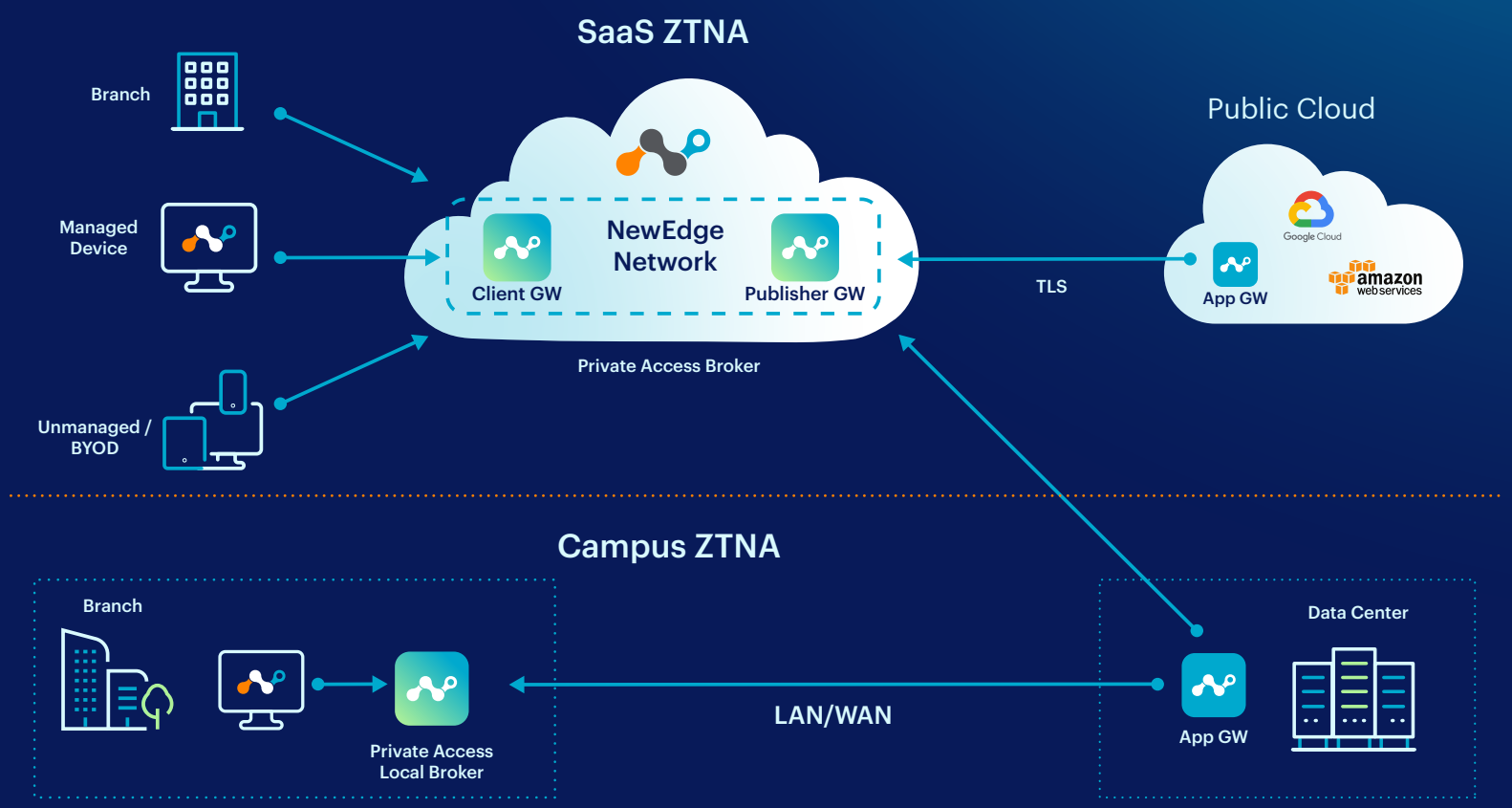
Universal ZTNA is key to overcoming these challenges. It provides secure access to all types of resources—whether legacy, modern, cloud-based, or on-premises—regardless of the user's location or device. Universal ZTNA allows organizations to manage access to all applications in on-premises and hybrid environments while maintaining consistent security policies. It ensures comprehensive protection by uniformly applying zero trust principles, offering full visibility into user activity, and simplifying access management. This approach delivers a seamless experience for users with frictionless access, and for administrators with unified policy enforcement, simplified management, and streamlined monitoring and auditing across the entire environment.

HOW?

Netskope One Private Access integrates advanced ZTNA capabilities with core NAC features, enforcing consistent, least-privilege access across all environments—remote, on-campus, branch offices, and even for third-party users.

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. Leveraging zero trust principles, it provides consistent authentication, authorization, and risk-based controls, mitigating lateral threats and simplifying deployment. Intelligent traffic steering optimizes performance, while a unified client consolidates ZTNA and VPN functions. A single policy engine enforces granular access for both on-premises and remote users, with real-time updates based on risk scores.



5 | Support for legacy applications

05

Lack of legacy application support in ZTNA hinders efforts to modernize infrastructure and transition to cloud-based services.

ZTNA solutions must support legacy applications to ensure comprehensive security, operational efficiency, and a smooth transition to modern infrastructure.

Many organizations still rely on legacy applications for critical business functions that handle sensitive data and essential processes. Examples include Remote Desktop Protocol (RDP), on-premises ERP systems like SAP or Oracle, Industrial IoT systems, VoIP platforms, and more. These older systems, built before wide adoption of cloud computing and many modern security protocols, are often difficult to replace or upgrade due to cost, complexity, or technical dependencies.

Without ZTNA support, legacy applications depend on outdated access methods like VPNs, which introduce vulnerabilities, create security gaps, and weaken the zero trust model. Centralized VPN access also causes network bottlenecks and latency, especially for remote users, leading to poor performance and decreased productivity.

Additionally, using separate access methods for modern and legacy applications complicates security management, increasing administrative overhead and weakening policy enforcement. By supporting legacy applications, ZTNA solutions provide consistent security policies across all environments, simplify management, and ensure critical operations remain uninterrupted during modernization. This allows organizations to transition to newer systems gradually while maintaining strong security and operational continuity.

HOW?

Netskope One Private Access brings SD-WAN capabilities to ZTNA for enabling secure and optimized connectivity to all private applications, allowing organizations to completely replace their remote access VPN solutions and modernize connectivity for the hybrid workforce.

6 | Security controls closer to users and applications

06

When ZTNA lacks security controls near users and applications, it causes latency, bottlenecks, and weakens zero trust enforcement, leading to poor user experience and security gaps.

Centralized controls can slow cloud app performance, increase latency, and create security gaps, especially for remote users. Without distributed security, traffic is routed through a central gateway, delaying access and complicating policy enforcement.

In a ZTNA solution, security controls should be placed at the connection point between users and applications, ensuring per-application policies are enforced without exposing the broader network. This approach enhances scalability as user and service demands grow, while enabling real-time access decisions based on factors like identity and device posture. To reduce latency and improve performance, strategies include deploying local brokers on-premises, positioning ZTNA gateways at key locations, embedding security controls in the cloud, and integrating ZTNA with SSE. Additionally, leveraging edge computing and local points of presence (PoPs) helps optimize performance and compliance.

Leading ZTNA vendors address these challenges by deploying global PoPs to meet latency-sensitive demands and regional compliance requirements.

HOW?

Netskope One Private Access enforces policies through a broker, whether local or cloud-based, positioned near users to enable quick connections to applications, reducing latency and boosting performance.

7 | Integration with broader security ecosystem

07

If ZTNA events aren't linked to broader network activity or endpoint behavior, security teams may miss early warning signs of a compromise, giving attackers more time to spread or steal data. This delay in detection increases the risk and exposure to breaches significantly.

Seamlessly integrating ZTNA with other IT, security, and network systems enhances security, streamlines operations, and improves the user experience. Key integrations include IAM (SSO and MFA), endpoint detection and response (EDR), SIEM, CASB, SD-WAN, VPN, traditional firewalls, threat intelligence, and application or cloud infrastructure tools.

Integrating ZTNA with broader monitoring tools like SIEM or log management systems is essential for complete visibility into ZTNA traffic and user behavior. Without this integration, security teams may miss abnormal access patterns or threats, increasing the risk of breaches. By connecting ZTNA with other systems such as network security and endpoint protection, teams can correlate events more effectively, improving incident detection and response times. Integration with IAM and SSO also simplifies user identity and access management.

These integrations make ZTNA more efficient, scalable, and responsive to modern business needs, improving security, flexibility, and user experience.

HOW?

Netskope One SASE, integrates with CASB, SWG, DLP, and key partners across security, identity, ITSM, mobile, and SecOps, delivering unified policies, real-time threat protection, and visibility across data and applications.

8 | Full network visibility and analytics

08

Lacking full network visibility creates security blind spots, compliance issues, and inefficiencies, weakening an organization's zero trust security posture and increasing vulnerability to potential threats.

Maintaining full network visibility and analytics in a ZTNA framework is essential for protecting organizations from security risks. Without it, they face compromised zero trust enforcement, difficulty detecting insider threats, and challenges in managing BYOD and remote work risks.

Real-time monitoring of all network traffic helps detect anomalies and security breaches, and evolving threats. With comprehensive visibility, security teams can identify lateral movement, malicious behaviors, and use advanced detection algorithms. Network analytics and machine learning further enhance detection, improve compliance, and optimize performance.

Continuous monitoring, real-time analysis, and dynamic policy enforcement are key to addressing evolving threats, and are essential to a ZTNA solution. To achieve this, organizations must implement monitoring tools, behavioral analytics, and access control, integrated with existing security infrastructure like SIEM, CASB, and threat intelligence.

HOW?

Netskope One DEM, provides a 360-degree view of digital experiences from users to applications, covering user scores, device health, local connectivity (Wi-Fi), SD-WAN onramps, SSE services, and more.

9 | Ensuring scalability and agility

09

As organizations grow or remote access demand increases, lacking a scalable ZTNA solution can limit user capacity, hinder connections, and restrict access to cloud applications, making the organization vulnerable and inefficient.

Many organizations today operate with a mix of on-premises infrastructure, public and private clouds, and various SaaS applications. Managing separate security solutions for each environment can be complex and costly, and often leads to inconsistent policies. ZTNA simplifies this by providing unified visibility and control over user access across all environments, reducing complexity and enhancing security.

In hybrid environments where applications and data span both on-premises and cloud systems, ZTNA solutions must enforce consistent security policies and adapt to dynamic workloads. A cloud-native ZTNA solution is key to scaling with user growth or new applications, ensuring seamless scalability without requiring physical changes.

ZTNA should also offer APIs and SDKs for integration with cloud platforms, enhancing control and visibility. To manage resources across diverse environments effectively, ZTNA must provide unified security policies, adaptive controls, seamless user experiences, and integration capabilities. A robust ZTNA solution should leverage cloud-native infrastructure, automated provisioning, and adaptive policies to ensure scalability, performance, and responsiveness to changing demands, such as more users, new applications, or emerging threats. These features are essential for delivering both security and agility in today's dynamic IT landscape.

HOW?

Powered by Netskope NewEdge Network with its cloud-native, scalable architecture and global reach, enabling seamless expansion, fast deployment, and secure access for remote workforces.

10 | Effective administrative tools

10

The absence of strong administrative tools in legacy ZTNA solutions limits security teams' ability to enforce granular access controls, respond quickly to incidents, and continuously enhance the organization's security posture.

An inefficient administrative interface in a ZTNA solution complicates management, leading to fragmented oversight and delays in incident response. Slow access to security logs and cumbersome policy management can result in inconsistent enforcement across the organization.

Optimizing the administrative experience in ZTNA involves improving usability for both end-users and administrators. A unified console for managing users, devices, applications, and policies simplifies monitoring, configuration, and troubleshooting, ensuring consistent security policies and easy onboarding.

Implementing the least privilege model further streamlines management by limiting resource access based on roles and conditions, making policies simpler to implement and audit. Autodiscovery, analytics, and troubleshooting tools enhance this process. Additionally, using policy templates, automation, and detailed dashboards boosts security and operational efficiency in a ZTNA environment.

HOW?

Netskope One Private Access delivers a unified console to manage users, devices, and policies, ensuring consistent enforcement and auditing across environments.

The shift to hybrid workforces and adoption of cloud and SaaS applications have reshaped the modern enterprise, altering how, where, and what resources are accessed.

As organizations move to cloud services and adapt to remote work in distributed environments, they need a more scalable, flexible, and secure solution. A modern ZTNA solution meets these demands by providing adaptable, secure access, helping organizations tackle the evolving security challenges of today's digital landscape.

Experience the power of Netskope One Private Access.

The Netskope One Platform

Netskope One SSE is built on the **Netskope One Platform**, a platform that provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites and private apps from anywhere, on any device.

Cloud Access Security Broker
Secure Web Gateway
Zero Trust Network Access
Data Protection + DLP
Threat Protection
Posture Management

SD-WAN
SASE Client
Digital Experience Mgmt.
Firewall and IDS/IPS
Intelligent IoT

About Netskope

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.

Interested in learning more? Request a demo

netskope

©2024 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized “N” logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners. 24-11 EB-783-1