DATA SHEET

Netskope Private Access for ZTNA

Frictionless and Secure Access for Remote Workers

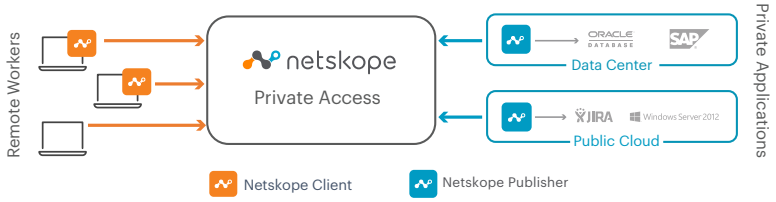
Zero Trust Net Access (ZTNA) is the modern remote access solution built on the principle of Zero Trust. ZTNA provides streamlined and secure access to private resources hosted in data centers and public cloud environments. Authenticated users gain direct access only to authorized applications, not the underlying network.

WHY NETSKOPE PRIVATE ACCESS (NPA):

Private Access seamlessly connects users anywhere to private resources everywhere. Built on the NewEdge security private cloud, it ensures a superior user experience. A modern alternative to VPN, Private Access reduces business risks, simplifies IT infrastructure and enables organizations to move toward a secure remote access architecture built with Zero Trust.

TOP USE CASE AT A GLANCE:

- **Security Transformation:** Zero Trust Network Access (ZTNA) that connects authenticated users to authorized applications, not the underlying network.
- **Augment Remote Access VPN:** Reduce the risks and exposure associated with remote access virtual private network (VPN).
- **Support Hybrid Cloud:** Deliver a seamless end-user experience for accessing applications in private data centers and public cloud environments.
- **Third-party Access** with clientless Browser Access for private web applications.
- **M&A Integration:** Provide day-one access to internal resources without the complexity of combining networks.
- **DevOps Access:** Native access to resources hosted in the virtual private cloud (VPC) environments.



KEY BENEFITS AND CAPABILITIES

Zero Trust Network Access to Private Applications
ZTNA provides access to private applications, not the network. With granular application-level access control policies, trust is granted based on user identity, group membership, and the security posture of the devices. .

Superior User Experience With Direct & Fast Connectivity
Bypass complex network routing and boost user productivity with fast and frictionless connectivity to applications. Leverage NewEdge security private cloud, a high performance, highly available, and extensively peered with cloud service providers.

Reduce Attack Surface
Enhance security posture and reduce overall attack surface by eliminating the exposure of protocols and services to the public internet.

Simplify Operations
Built on the Netskope SASE platform that unifies ZTNA, CASB, SWG, and Cloud Firewall with one client, one policy engine, and a single management console, providing consistent policy enforcement, ease of management, and visibility.

"By 2024, at least 40% of all remote access usage will be served predominantly by zero trust network access (ZTNA)."

Gartner® Press Release, Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021, 22 June 2021.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

YOUR NEEDS	THE NETSKOPE SOLUTION
Broad Application Support	Support for client-initiated traffic using both TCP and UDP protocols on almost all associated ports, thus enabling access to web applications and non-web / thick clients (e.g. SSH, RDP, Microsoft Windows Active Directory).
Clientless Browser Access	Support for clientless Brower Access for private web applications (e.g. HTTP or HTTPS applications) for 3rd party access or employee BYOD.
Granular Policy for Access Control	Access control policy with user identification and device posture. Integration with Identity Providers and Microsoft Active Directory provides user context. The device posture profile monitors information such as operation systems, registry setting, running process, encryption status, presence of a file or certificate, and domain membership.
Real-time Visibility	Discover private applications, plus real-time visibility into detailed private application traffic and user activities, as well as alerting on policy violations.
Direct and Fast Connection	The user-to-application traffic is optimally routed through the Netskope NewEdge security private cloud, with its global coverage, premium transit selection, and extensive peering to cloud providers, to deliver a superior user experience and fast application performance.
Ensures Privacy	Connectivity between remote users' devices and private applications is secured by an end-to-end TLS (v1.3) encrypted tunnel.
DEPLOYMENT COMPONENTS	
Netskope Client	Utilizing the unified lightweight Netskope Client installed on the device running Microsoft Windows, Apple MacOS, or Android device, the Netskope Client steers Private Access application traffic to the Netskope Security Cloud using either DNS or the IP address. For the iOS devices, the client is deployed as an on-demand or a per-app VPN configuration profile.
Private Access Publisher	The publisher initiates outbound connection to the Netskope Security Cloud, eliminating the risk of inbound network access. Publishers can be deployed on networks where private applications are hosted, supporting AWS, Azure, GCP, VMWare ESX, and CentOS-based virtual machine (VM) environments.

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.

©2021 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 08/21 DS-376-2