DATA SHEET

Netskope Private Access for ZTNA

EVERYCLOUD IT SECURITY

Frictionless and Secure Access for Remote Workers

Zero Trust Network 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 is Netskope the best choice?

Netskope Private Access (NPA) seamlessly connects users anywhere to private resources everywhere. An integral component of the Netskope Security Service Edge (SSE) solutions, NPA reduces business risks, protects data, simplifies IT infrastructure, and enables secure remote access with a superior user experience.

Top use case at a glance:

- **Security Transformation:** Zero Trust Network Access (ZTNA) that connects authenticated users to authorized applications, not the underlying network.
- **Replace 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, a high-performance, highly available security private cloud that is 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.

Protect Data and Mitigate Insider Risk

Detect data usage, activities, and behavior anomalies (UEBA), enforce advanced DLP rules and policies, and apply adoptive access policy based on user risks.

Simplify Operations

Built on the Netskope SSE 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 2025, at least 70% of new remote access deployments will be served predominantly by zero trust network access (ZTNA) as opposed to VPN services."

– Gartner®, Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access, Nat Smith, Mark Wah, Christian Canales, 8 April 2022

YOUR NEEDS	THE NETSKOPE SOLUTION
Broad Application Support	Support for client-initiated access to enterprise applications built on TCP and UDP protocols, thus enabling access to web applications and non-web / thick clients (e.g., SSH, RDP, Microsoft Windows Active Directory).
Third-Part and BYOD Access	Support for clientless Browser Access for private web applications (e.g. HTTP or HTTPS applications) for third-party access or employee BYOD, with optional inspection withDLP rules for data protection.
Granula Policy for Access Control	Leverage user and device identity along with unified risk information to enable access to privte applications.
Application Discovery	Accelerate ZTNA adoption by streamlining the process of application discovery, policy definition, and access authorization. Network administrators gain detailed insights into the private application landscape, utilization, users, and traffic patterns. Combined with the API automation tools, enterprises now can scale the delivery of application access with adaptive controls and policies.
Private Infrastructure Management	The Publisher Dashboard provides insight into application traffic, publisher health, and utilization, enabling decision on resource allocation, connection optimization, and troubleshooting.
Analytics and Reporting	Advanced Analytics provides real-time visibility into detailed application traffic and user activities, as well as alerting on policy violations.
API Automation	Administrators can automate the entire process of application discovery and management using APIs. APIs are also available for Publisher management. The APIs offered are full featured and have parity to the Netskope UI.
Data Protection	NPA supports DLP controls to prevent data exfiltration, leveraging Netskope's DLP engine. This means that data is classified only once, and the same DLP profiles and incident response can be used for SaaS, Public, and private applications.
Secure Connectivity at Pre-logon	Quickly onboard new employees and enable self-service provisioning on a new PC. Administrators can leverage enterprise device certificates to ensure only sanctioned devices have access to internal applications.
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.
Auto Update	Enable administrators to schedule software updates thus ensuring NPA publishers and host OS are always on the latest software version.
Unified Platform	One client, one policy engine, and single Admin UI for app configuration, policy, analytics, and reporting across all Netskope services.

DEPLOYMENT COMPONENTS

Netskope Client	NPA is enabled in the unified lightweight Netskope Client. Netskope Client supports Microsoft Windows, Apple Mac OS and iOS, Chrome OS (Chromebook), and Android. With Browser Access, NPA works with any devices running a supported web browser.
Private Access Publisher	The Publisher is an application gateway that initiates outbound connection to the Netskope Security Cloud, eliminating the risk of inbound network access. Publishers can be deployed on servers running Ubuntu, in virtualized environments using VMware and Hyper-V, and in public cloud environments such as AWS, Azure, and GCP.