Netskope Private Access

TOP USE CASES AT A GLANCE

- Provide remote users with secure zero trust access to authorized applications, not your entire network
- Deliver a seamless end user experience for accessing applications in public clouds and data center environments
- Provide employees with remote access to apps in the public cloud without needing to expose them publicly
- Retire inefficient and complex VPN routing architectures used to access applications in public cloud
- Combine Private Access with the wider Netskope Security Platform and extend security to cloud apps and web, using a single transparent client

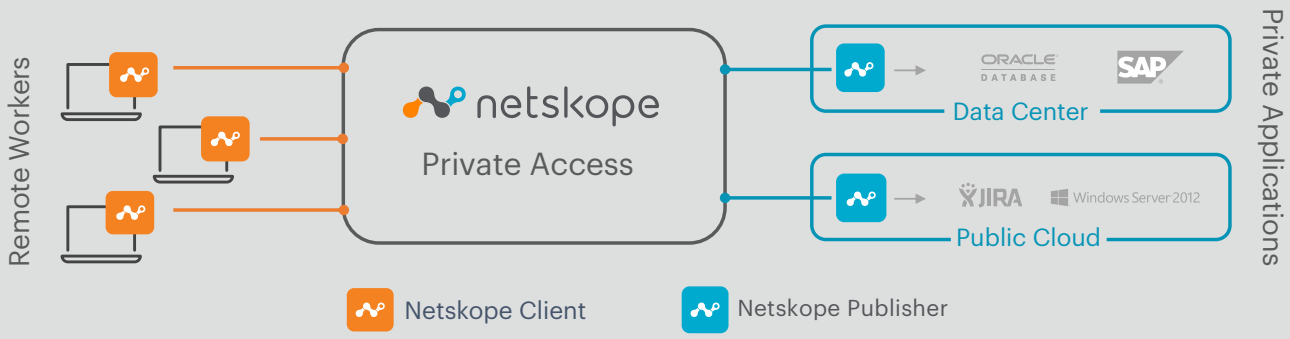
Traditional remote access VPN solutions require capital expenditure on on-premises appliances. These appliances lack scale, fail to limit remote users' lateral movement within the corporate network, require hairpinning over the corporate WAN when accessing public cloud, and are cumbersome to maintain. A modern remote access solution built on the principles of zero trust can instead provide streamlined and secure access to private applications hosted within data centers and public cloud.

PRODUCT OVERVIEW

Netskope Private Access (NPA) is a cloud-based Zero Trust Network Access (ZTNA) solution that is a fully integrated component of the wider Netskope Security Cloud platform and delivered through the global Netskope NewEdge network. NPA directly connects remote workers to private applications running in public cloud environments or private data centers; reducing risk and simplifying security operations.

NPA allows an organization to begin retiring legacy VPN hardware, and move towards a more secure, cloud-first, remote access architecture. End the high capital investment, refresh cycles, and ongoing management costs of VPN appliances —and adopt ZTNA for your remote access needs.

Netskope Private Access



NETSKOPE PRIVATE ACCESS BENEFITS

Zero Trust Network Access

ZTNA gives employees access to applications, not the network. This protects private applications and other network assets from malicious insiders or compromised accounts. NPA has application-level access policies, which are strictly controlled by user or group identity, and the security posture of remote devices.

Optimized and Direct End User Experience

NPA connects remote users directly to applications hosted in public cloud and private data centers using NewEdge—a high-performance, scalable global network infrastructure. Netskope offers an always-on end user remote access experience and avoids backhauling (or hairpinning) remote users through the corporate network to access applications in public cloud environments.

Secure Access to Public Cloud Applications

If applications in public cloud environments are exposed publicly to allow remote access for employees then there is an increased risk of compromise through unauthorized access. Avoid the brand damage, fines, or remediation costs associated with a breach—deploy NPA to provide employees with remote access without needing to expose apps publicly.

Begin your network and security transformation

The Netskope cloud-native architecture ensures scale, agility and elasticity and provides a single administrative console for simplified security policies, analytics, and incident investigation for employee use of web, cloud, and private applications. Netskope takes you to the cloud-based future of network security, combining ZTNA with Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB), and aligning with the Gartner-defined Secure Access Service Edge (SASE) architecture—**www.netskope.com/about-sase**

Netskope Private Access Features

ZERO TRUST NETWORK ACCESS	
Secure Access	Connectivity between remote users' devices and private applications is secured by an end-to-end TLS (v1.3) encrypted tunnel and optimally routed through the Netskope NewEdge network—a low-latency, high-capacity, scalable global network infrastructure. Built on the principles of zero trust, NPA policies ensure that remote users are directly connected only to the applications they are authorized to use and do not have broad network-level access to environments.
Application Support	Support for browser-based access to web applications (e.g. HTTP or HTTPS applications) and for non-web / thick applications (e.g. SSH, RDP, Microsoft Windows Active Directory). Support for both TCP and UDP protocols on almost all associated ports.
User Authentication	Following the principles of Zero Trust, NPA ensures that only authenticated and authorized users can gain access to applications. Netskope is able to integrate with Microsoft Active Directory and Single Sign-On (SSO) providers to understand users, groups and organizational units.
Device Security Posture	Ensure that only corporate devices meeting a specific security posture can access private applications. A corporate device can be identified by monitoring the encryption status, registry setting, running process, presence of a file or certificate, or Active Directory Domain membership.
DEPLOYMENT COMPONENTS	
Netskope Client	Private Access utilizes a lightweight Netskope Client installed on a Microsoft Windows or Apple macOS device. The Netskope Client steers Private Access application traffic to the Netskope Security Cloud using either DNS or the IP address. Note: The same Netskope Client is used to steer website and cloud application traffic when subscribed to the Netskope Next Gen Secure Web Gateway solution (for data loss prevention and threat protection).
Netskope Private Access Publisher	NPA requires a Publisher be deployed on any network where private applications are running that need to be securely accessed. The NPA Publisher can be deployed on AWS, Azure, VMWare ESX, and any CentOS based virtual machine (VM). Publishing makes private enterprise applications available to authorized users through the Netskope Security Cloud. Importantly, the connection to the Netskope Security Cloud is initiated outbound by the Publisher. There is, therefore, no requirement for any inbound network access to the data center or public cloud networks. Netskope does not limit the number of Publishers that may be deployed to meet the requirements of an environment's network topology and/or network partitioning. For example, Publishers may be placed where VPN concentrators have historically been installed, or they may be deployed in individual AWS VPCs to improve security by isolating those VPCs from one another.
Netskope Inline Policies	NPA policies are created and managed through the Netskope Security Cloud's admin console. Granular policies for blocking or allowing access to private applications can be built on criteria including User, Group or Organizational Unit (OU); Device Classification; or Operating System.
Events and Alerts for Private Apps	Network Events enable visibility of private application traffic and relevant details, such as who has accessed what, from where, and for how long. Alerts highlight where private app policy violations occur (i.e. when an attempt to access a private app is explicitly denied by a policy). Both Events and Alerts are retained for analysis within the Netskope platform for 90 days (optionally up to 1 year).

NETSKOPE SECURITY CLOUD	
Securing Remote Workers	In addition to connecting remote workers to their private applications using ZTNA, Netskope also provides a globally available, cloud-based security platform for securing remote workers' access to websites and cloud applications. Netskope has the unique ability to decode cloud application and website traffic to understand remote workers' activities, inspect data movement, and detect threats hidden in SSL/TLS traffic. Netskope uses the same, lightweight client installed on a device to manage web and cloud traffic, and tunnel private application traffic.
Further Security for Cloud Applications	The Netskope Cloud Security Platform extends beyond remote access and securing remote workers access to cloud and web. Netskope API-enabled Protection can discover advanced threats and sensitive data-at-rest within managed cloud applications, and identify and remediate files that are inappropriately shared publicly. Furthermore, APIs into public cloud environments can perform Cloud Security Posture Management (CSPM) to ensure the secure configuration of Infrastructure as a Service (IaaS) environments.

THE NETSKOPE DIFFERENCE

Data-centric

The rapid adoption of cloud apps, services, and mobile devices has resulted in data going to places where traditional security technology is blind. Netskope takes a data-centric approach to cloud security, following data everywhere it goes. From data created and exposed in the cloud to data going to unmanaged cloud apps and personal devices, Netskope protects data and users everywhere.

Cloud-smart

Cloud usage dominates the web, with cloud services making up the majority of enterprise web traffic. Securing this environment, without slowing down the business, demands a new security model based on contextual knowledge of the cloud. Netskope enables you to take advantage of our intimate, contextual understanding of the cloud to apply effective security controls that enable you to safely use the cloud and web.

Fast

When it comes to security, performance and scale are often the biggest challenges. Reliance on the public Internet to deliver inline security causes performance challenges, and an appliance-based approach to deploying security does not scale. Netskope delivers real-time, cloud-native security, without the traditional performance trade-off. As we continue to build one of the world's largest and fastest security networks, you can be certain your security is always on, always present, and never a roadblock.