Solution Brief

Securing Third-Party Access with Netskope One Private Access

Netskope One Private Access enables contractors, partners, and vendors to securely and seamlessly access critical resources from any device. Simplify connectivity, boost productivity, and safeguard applications and data from external threats—all without the delays of legacy solutions.

Quick Glance

- Simplifies third-party access management with a client-based or clientless, cloud-native architecture that scales with your business.
- Extends zero trust access to contractors, partners, and vendors, enhancing security and minimizing exposure to threats.
- Integrates Data Loss Prevention to monitor sensitive information, and prevent unauthorized access and data leakage from unmanaged devices.
- Delivers a frictionless, high performance access experience that accelerates workforce productivity and fuels business growth.

> "Unauthorized network access is the leading cause of third-party attacks, responsible for more than 53% of third-party breaches."
>
> Black Kite, March, 2024

The Challenge

Businesses have come to rely heavily on the services of third parties to increase operational agility and drive cost savings. While they offer clear value, giving third-party users access to the network can expose organizations to significant security risks, including:

- Overly permissive access that allows third parties to move freely within your network.
- Unmanaged third-party devices that introduce malware and ransomware, potentially disrupting operations and endangering workers.
- Unchecked data usage that leads to accidental or malicious data loss, resulting in a third-party data breach.

To harness the benefits of third parties without exposing the business to added risks, IT and security teams are adopting Zero Trust Network Access (ZTNA) as a modern, secure alternative to traditional remote access methods such as VPN and VDI.

The Solution

Netskope One Private Access elevates Zero Trust Network Access (ZTNA) with its dual-mode functionality, offering both seamless client-based access via the Netskope One Client and clientless access through Browser Access. This flexible, cloud-based solution enables contractors, partners, and vendors to securely access private applications directly through their web browsers. Browser Access supports secure protocols such as HTTP, HTTPS, RDP, and SSH, while the Netskope One Client extends access to any application over TCP/UDP. Together, these capabilities provide businesses with robust tools to securely manage third-party access, minimize the attack surface, and reduce the risk of security breaches.

Accelerate third-party productivity

Traditional third-party onboarding is a significant burden on your team and a roadblock to productivity for your users. Netskope One Private Access eliminates the complexities and delays, providing frictionless access to the applications your contractors and vendors need to hit the ground running. No more shipping devices, installing agents, or troubleshooting connectivity issues. Just consistent zero trust access that empowers your extended workforce from day one.

The clientless option through Browser Access offers two convenient access methods. The intuitive Browser Access User Portal provides one-click access to all authorized applications, tailored to each user's specific job functions. This personalized experience streamlines workflows and minimizes the risk of unauthorized access. For technical users who prefer direct access, the solution also supports access via hostname, offering flexibility and convenience.

The client-based access through the Netskope One Client enables a user to access partner applications without requiring the user to first logout of the existing user session in the Client. A user can securely switch private application access to the partner tenant, while their internet bound traffic continues to flow through the primary tenant.

Additionally, client-based access is also available for more advanced scenarios with complex partner requirements. This is ideal for scenarios involving thick-client applications or enhanced security needs. The Netskope One Client ensures seamless connectivity with advanced authentication and policy enforcement.

Secure server and machine with optimal user experience

RDP and SSH connections are prime targets for attackers as initial entry points into corporate and industrial networks. Netskope One Private Access reduces the risk of compromise by enabling secure access to sensitive internal environments over the internet without opening inbound ports in the DC Firewall. The AnyApp feature provides secure RDP and SSH access to servers and machines, allowing contractors and vendors to perform remote operations, maintenance, and upgrades. This gives you greater visibility and control over third-party access to critical systems.

Reduce third-party security risks

Netskope One Private Access ensures that only authorized users can access resources on a least-privilege, need-to-know basis, reducing the risk of over-entitled third parties exposing your network to full lateral access. By combining granular access controls with continuous adaptive trust and inline data protection, Netskope One Private Access dramatically reduces the risk of lateral movement and data breaches stemming from your partners. Sensitive data within private apps remains safeguarded when accessed by third parties and even employees using personal devices. Inline data loss prevention controls actively monitor and control web browser traffic, and prevent unauthorized downloads, uploads, and form submissions.

> Netskope offers a secure, seamless access experience, maximizing the productivity of your extended workforce while minimizing risks to your business.

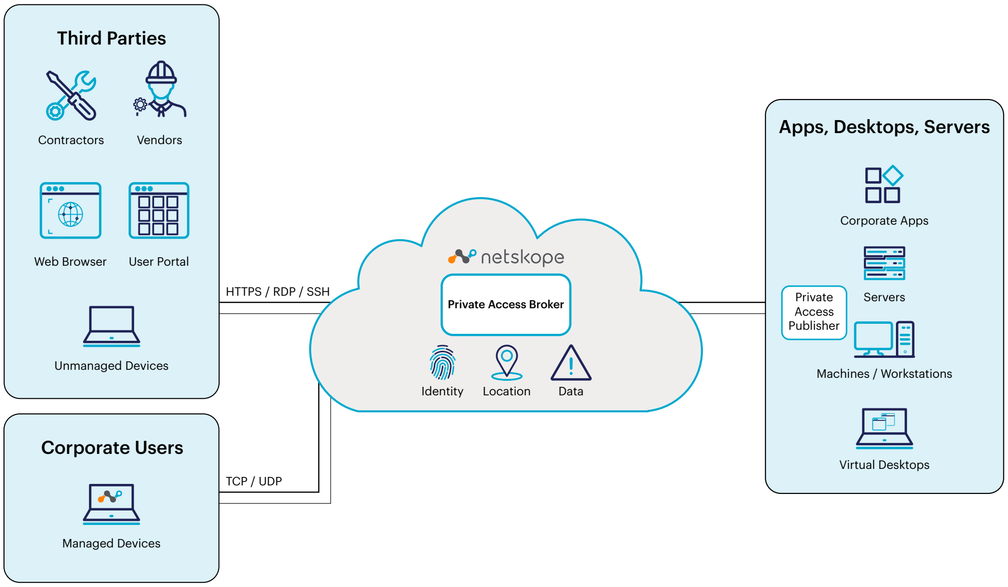

Figure 1 **Netskope One Private Access: Third Party Access with Netskope One Client or with Browser Access (clientless)**

Streamlined third-party access: How it works

Clientless option with Browser Access

1. Admins define and configure Browser Access for private apps, the User Portal, and Real-time Protection policies to allow/block access for their users.
2. Users simply open a web browser on their device and enter the User Portal URL.
3. The access request is automatically directed to the Browser Access service, which seamlessly integrates with your corporate Identity Provider (IdP) for authentication.
4. Upon successfully authenticating to the User Portal, users can view only the private apps they are authorized to access, based on admin-configured policies.
5. Users simply click on the tile of their desired app. Since they're already authenticated via the User Portal, traffic for the selected app is securely directed to a Private Access Broker within the Netskope NewEdge network..
6. The Private Access Broker dynamically enforces granular, per-user, and per-app security policies defined by the admin.
7. The Private Access Broker intelligently selects the Publisher instance closest to the requested private app for optimal performance and user experience.
8. The Private Access Publisher instance forwards traffic to the requested private app, thereby successfully allowing access to the resource within the User Portal.

Client-based option with Netskope One Client

1. Primary tenant's admin, defines the partner's tenant information in the primary Netskope tenant.
2. The user can view and select the target partner tenant from the Netskope One Client.
3. Following this, the Netskope One Client presents the authentication challenge for the partner tenant's IDP.
4. Upon successful authentication, all requests for partner private applications, will be evaluated by user policies in the partner tenant.
5. Netskope's Private Access Broker dynamically enforces granular, per-user, and per-app security policies defined by the admin.
6. The Private Access Broker intelligently selects the Publisher instance closest to the requested private app for optimal performance and user experience.
7. The Private Access Publisher instance then forwards traffic to the requested private app, thereby successfully allowing access to the partner application.

FEATURE	DESCRIPTION
Browser Access	Enables clientless remote access to private applications from any web browser on any device, including personal devices (BYOD). Enforces user authentication and grants access on a need-to-know, least-privileged basis. Supports remote access using web (HTTP/S), Remote Desktop Protocol (RDP), and Secure Shell (SSH).
User Portal	Provides a convenient and intuitive web portal where users can access all the applications they need to be productive. Users simply navigate to a User Portal and are presented with only the applications they are approved to see—and nothing more.
AnyApp	Provides granular controls for IT and security teams to restrict server access via RDP and SSH. Enables technical users to remotely manage machines and equipment with their CLI and GUI tools, while reducing the risk of attackers using compromised RDP/SSH sessions to move laterally.
Data Loss Prevention	Actively monitors and controls web browser traffic with inline data protection controls. Prevents unauthorized downloads, uploads, and form submissions.
Source IP Allowlisting	Strengthens security for private applications by restricting access to users connecting from approved source IP address ranges. Blocks unauthorized users and malicious traffic, further reducing your attack surface.

BENEFITS	DESCRIPTION
Accelerate business productivity	Streamlines the onboarding process by providing immediate zero trust access to essential business applications and data, enabling third parties to be productive from day one.
Reduce exposure to threats and data loss risk	Enhances visibility and control over third-party behavior with real-time protection policies. Monitors and manages application usage, restricts lateral movement, controls downloads and server access to minimize the risk of unauthorized activity.
Simplify operations and management	Provides a client or clientless, cloud-native architecture that scales with your business. Eliminates the need to ship corporate laptops or set up VPN or VDI accounts for third parties.

netskope

Netskope, a global SASE leader, uses zero trust principles and AI/ML innovations to protect data and defend against cyber threats, optimizing both security and performance without compromise. Thousands of customers trust the Netskope One platform and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity. Learn more at netskope.com.

©2024 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. 07/24 SB-757-1