DELL Technologies

Dell SafeData

Netskope Private Access

Benefits

Zero Trust Network Access

Provides 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 the 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 a public cloud or a private data centers using NewEdge, a high-performance, scalable global network infrastructure. Offering an always-on end-user remote access experience and avoids backhauling (or hairpinning) remote users through the government network to access applications in public cloud environments.

Begin your network and security transformation

The Netskope cloud-native architecture helps to ensure scale, agility, and elasticity. It provides a single administrative console for simplified security policies, analytics, and incident investigation for employee use of the web, cloud, and private applications.

Federal Transformation with FedRAMP and TIC 3.0

The Netskope Security Cloud Platform meets the Federal Risk and Authorization Management Program (FedRAMP) requirements and has achieved FedRAMP Authorization for its SASE-based TIC 3.0 Solutions

A cloud-based zero trust network access solution that provides fast and secure access to private applications hosted in public clouds or enterprise data centers.

Product Overview

Netskope Private Access, NPA is more secure than a traditional VPN because it connects users to authorized apps instead of networks where they can move laterally. As a cloud-based solution, NPA is simpler to administer and operate vs. on-premises products. NPA is part of the Netskope Security Cloud, leveraging the NewEdge globally distributed private network to ensure fast and reliable connectivity.

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 Zero Trust Network Access, ZTNA, for your remote access needs.

Netskope takes you to the cloud-based future of network security, combining ZTNA with Secure Web Gateway and Cloud Access Security Broker, CASB. Aligning with Gartner defined Secure Access Service Edge, SASE, architecture.

A Secure Access Services Edge (SASE) architecture makes it possible to identify users and devices, apply policy-based security controls, and deliver secure access to the appropriate applications or data. These capabilities directly align with the foundation of Netskope's cloud-native Security Platform, built to understand and protect SaaS, web, and IaaS environments while accessed from any device. All done from a single console, with a single architecture and integrated policies for all of the SASE services, including CASB, SWG, and Private Access.

netskope

Key Product Features

Secure Access

Connectivity between remote users' devices and private applications are secured by an end-to-end TLS 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 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 can integrate with Microsoft Active Directory and Single Sign-On (SSO) providers to understand users, groups, and organizational units.

Device Security Posture

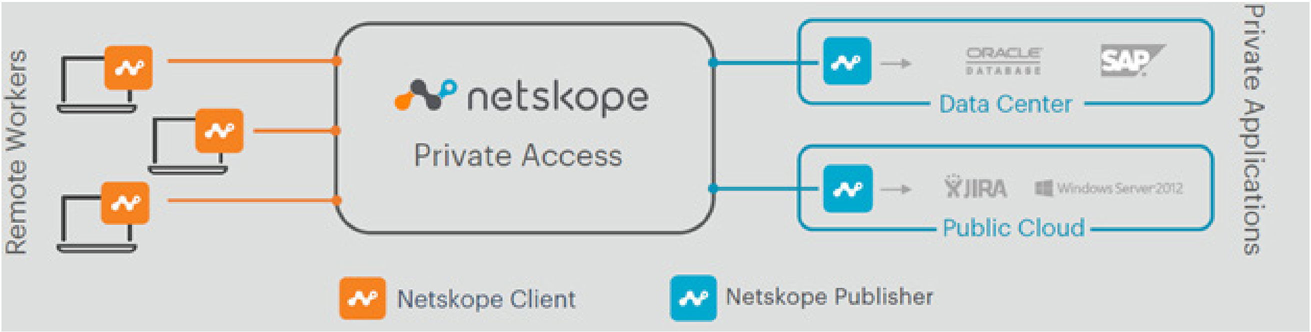
Helps to ensure that only agency devices meeting a specific security posture can access private applications. A agency device can be identified by monitoring the encryption status, registry setting, running process, presence of a file or certificate, or Active Directory Domain membership.

What is included

Netskope Client - steers Private Access application traffic to the Netskope Security Cloud using either host-name or the IP address.

Netskope Private Access Publisher - Publisher, is deployed on any network where private applications are running that need to be securely accessed. The NPA Publisher can be used on AWS, Azure, GCP, VMWare ESX, or Hyper-V.

Events and Alerts for Private Apps - Enables the visibility of private application traffic and relevant details, such as who has accessed what, from where, and for how long. Events and Alerts are retained for analysis within the Netskope platform for 90 days (optionally up to 1 year).



Contact your dedicated Dell Endpoint Security Specialist today at, endpointsecurity@dell.com, about the SafeData products that can help improve your security posture