SOLUTION BRIEF

Netskope with Okta

Extend step-up authentication beyond managed apps and cloud services to thousands of apps by integrating Netskope with Okta. Automate policy decisions based on rich content and context including app risk, user risk, and data sensitivity. Integration also covers provisioning, monitoring, enforcement, and identity services across SASE architecture including ZTNA.

KEY USE CASES

- **Extend MFA step-up authentication.** Leverage rich cloud and web activity, content, and context for policy-driven step-up authentication requests.
- **Provision users and groups.** Leverage AD and SCIM to share users and groups between Okta and Netskope.
- **Monitor identity for all apps.** Define and track federated identities across all apps with Okta and Netskope.
- **High-risk user enforcement.** Based on Okta and Netskope activity and events, place users into high-risk groups until remediation.
- **Integrate across SASE architecture.** Integrate Okta identity services into Netskope Next Gen SWG, CASB, CSPM, and ZTNA solutions.

"Less than 3% of apps are managed"

Netskope Cloud and Threat Report
February 2021

THE CHALLENGE

Identity and data are new attack surface areas legacy web defenses are challenged to defend. They use allow/deny controls lacking app content and context to determine when policy-driven step-up authentication should be utilized. The average large enterprise accesses 2,415 apps while a mid-sized company with 500-2,000 users accesses 690 distinct apps[1]. As cloud app adoption continues with 20% year over year growth, less than 3% of apps are managed today and the rest are shadow IT apps freely adopted by business units and users. Extending MFA to all apps with policy-driven step-up authentication is a challenge facing many organizations transforming to the cloud.

NETSKOPE WITH OKTA

Netskope integration with Okta extends SSO and MFA with policy-driven step-up authentication based on rich content and context to thousands of apps and cloud services. The Okta Identity Cloud and Multi-factor Authentication integrate with the Netskope Security Cloud to enforce real-time continuous context and identity-based Zero Trust access to cloud resources, services, and apps. Provision users and groups to monitor identity across all apps and enforce high-risk restricted policy controls based on user activity and events.

[1] Netskope Cloud and Threat Report, February 2021

CAPABILITIES

STEP-UP AUTHENTICATION BASED ON CONTEXT

The value of invoking step-up authentication is directly related to the context you have for apps and cloud services, users, devices, and data sensitivity. Building your SASE architecture with a web-only proxy defeats the purpose of having step-up authentication. Netskope Next Gen SWG analyzes five types of user traffic including web, SaaS, Shadow IT, public cloud services, and custom apps in the public cloud.

Applying SSO and MFA to only managed apps is missing more than 97% of the target. Given identity is the new perimeter, extending Okta with Netskope to all possible apps and cloud services with policy-driven step-up authentication based on rich context is the security posture you need to protect your data. While managed apps benefit from API and inline analysis, the runaway train of Shadow IT requires inline analysis to decode these cloud apps, a challenge most legacy SWGs cannot address.

Integrating Netskope and Okta extends SSO and MFA to thousands of apps with granular controls based on rich context for policy-driven step-up authentication.

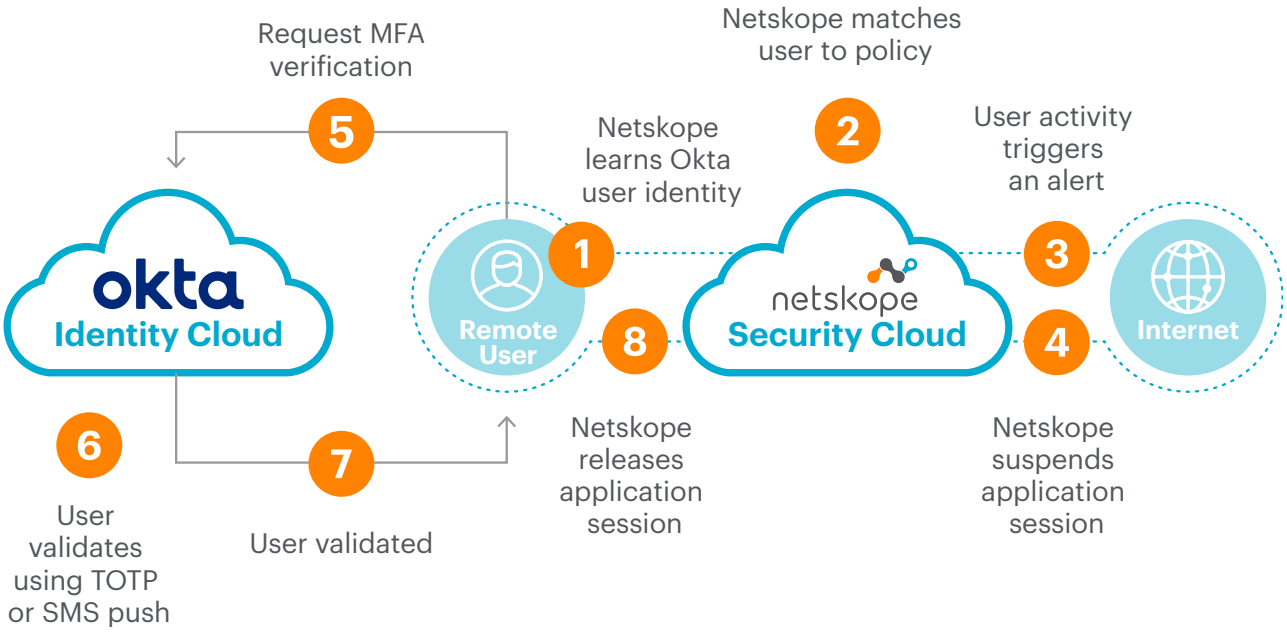
Extending Okta with Netskope with policy-driven step-up authentication based on rich context is the security posture you need to protect your data.

LEADING CLOUD FIRST SOLUTIONS

Okta and Netskope are leading cloud first vendors built in the cloud, for the cloud, with cloud performance and scale. Identity and data context are at the core of SASE architecture as users, apps, and data transform to the cloud. Okta has seven years of leadership for access management while Netskope has four years of leadership for inline and API cloud security of apps and cloud services. Together, they provide an integrated cloud services platform for identity and data use cases including employees, contractors, partners, and customers for infrastructure, apps, and APIs.

Okta has seven years of leadership for access management while Netskope has four years of leadership for inline and API cloud security of apps and cloud services.

Netskope and Okta enable customers to modernize their IT infrastructure delivering new digital experiences with rich contextual policy controls protecting against threats and data exposure. Netskope can enable policy-driven step-up authentication with Okta based on content and context including app risk, user risk, data sensitivity, activity, device posture, to/from, instance awareness, alongside managed or unmanaged app and device status to enable granular policy controls unmatched by legacy defenses.



ENTRY POINT FOR BYOD TO MANAGED APPS

Next Gen SWGs and cloud inline solutions include both forward and reverse proxy capabilities. Integrated with Okta for identity services, Netskope reverse proxy supports access to managed apps for unmanaged devices and BYOD where a client or agent is not possible. The same granular policy controls with the ability to invoke step-up authentication are available including data and threat protection.

When users access Okta for identity services including SSO and MFA, the Okta cloud service then transparently sends their traffic to the Netskope Security Cloud for managed app security policy controls, including step-up authentication based on content and context details. The same leading cloud services that secure thousands of apps with forward proxy for managed devices, also protect unmanaged device access to managed apps with reverse proxy.

RICH METADATA FOR ANALYTICS AND MACHINE LEARNING

At the core of SASE architecture is data context, and two of the most valuable cloud sources of metadata for analytics and machine learning are for identity and access, plus activity analysis for apps and data. Together Okta and Netskope provide rich alerts, events, and metadata to drive investigations, remediation, threat hunting, and machine learning analysis.

As users, apps, and data transform to the cloud, the rich details drive analytics and insights, highlight the effectiveness of policy changes, and uncover unknowns about risks to data and identity access. Okta covers a wide breadth of identity service use cases, while Netskope Next Gen SWG covers five types of user traffic for cloud and web unmatched by legacy SWG defenses.

ABOUT OKTA

Okta is a publicly-traded identity and access management company based in San Francisco. It provides cloud software that helps companies manage and secure user authentication into applications, and for developers to build identity controls into applications, website web services, and devices. More than 10,000 organizations trust Okta's software and APIs to sign in, authorize, and manage users.