netskope
+
CITRIX®

Netskope and Citrix

At a glance:

- Comprehensive solution that helps secure mobile devices, native mobile apps, and access to both sanctioned and unsanctioned cloud apps.
- Secure data sync and sharing service with flexible storage options and integration with your on-premises KMIP-compliant key management system.
- Seamless integration to deliver Netskope agent to mobile devices.

The Cloud and Enterprise Mobility

Now, more than ever, users are using the cloud and mobile devices as a major part of their daily lives. This trend allows employees to be more engaged, more collaborative, and more productive, with the added benefit that employees feel an unprecedented freedom to work from anywhere, at any time. Regardless of who owns these mobile devices, employees use them for work as well as personal use, which introduces risk in the enterprise. Clearly, the security landscape has changed and IT must now adapt to ensure that their strategy includes both cloud and mobile.

Netskope and Citrix come together to provide you with the perfect combination to comprehensively address your enterprise mobility and cloud security needs.

Understand usage and secure access

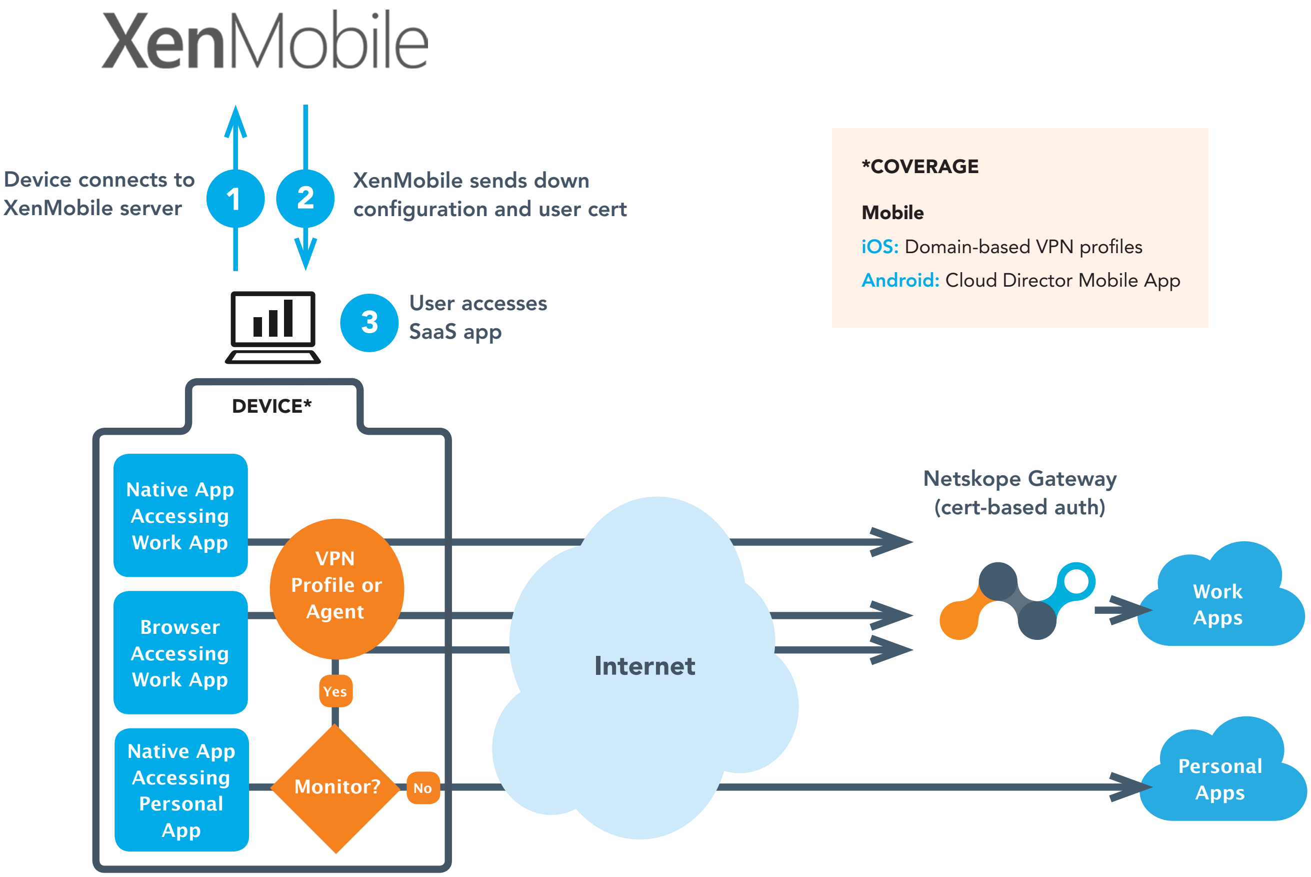
As the traditional enterprise network perimeter dissolves, users access work data while on the go, from remote locations and using cloud apps, on various devices, in order to get their jobs done. At the center of their work is the content they're dealing with, which often contains sensitive information such as Personally Identifiable Information (PII), Payment Card Industry (PCI) data, or Protected Health Information (PHI). IT needs a way to ensure that they access this content in a secure and compliant method without sacrificing productivity.

With Citrix and XenMobile, you first understand your users, the apps they are using (both sanctioned and unsanctioned), and what devices they use to access both apps and data. You get access to rich contextual details such as the user's Active Directory group or OU membership, their device OS, the location of their device, the app they're accessing and the content they're accessing. You can classify devices based on a variety of parameters such as their ownership, enrollment status, and encryption status. The solution then provides you with controls to provide secure access to enterprise resources, set policies granting differing levels of access based on the device classification, and ensuring unrestricted private access for personal use. Additionally, you can monitor devices for compliance and even issue a selective or complete device wipe when it is found to be out of compliance.

How the solution works

With Citrix XenMobile and Netskope, organizations are provided with a comprehensive enterprise mobility solution with coverage for all internal enterprise apps as well as cloud apps, both sanctioned as well as unsanctioned. You can monitor all cloud app access and use Netskope's powerful noise-cancelling DLP solution to ensure that sensitive enterprise content does not leak to personal or unsanctioned cloud apps. This is accomplished by automatically distributing the Netskope agent to your mobile devices so that you have complete cloud traffic coverage, including coverage for all native mobile app traffic. You can even inspect ActiveSync traffic to ensure that users are not sending sensitive data via email to unauthorized recipients.

With Citrix ShareFile and Netskope, organizations have a secure data sync and sharing service with flexible storage options that allows IT to mobilize all enterprise data while retaining full control. You can also take advantage of automatic encryption of content while on-premises, in-transit to or from the cloud, or while resident in the cloud, without compromising the user experience. The solution utilizes AES-256 with a per-file key controlled by fault-tolerant, FIPS 140-2 Level 3 certified HSMs. Additionally, you can optionally integrate Netskope Active Encryption with your on-premises, KMIP-compliant key management system to ensure that you retain control of the keys and their lifecycle.


XenMobile
1
Device connects to XenMobile server
2
XenMobile sends down configuration and user cert
3
User accesses SaaS app
DEVICE*
Native App Accessing Work App
Browser Accessing Work App
Native App Accessing Personal App
VPN Profile or Agent
Yes
Monitor?
No
Internet
Netskope Gateway (cert-based auth)
Work Apps
Personal Apps

***COVERAGE**

Mobile

iOS: Domain-based VPN profiles

Android: Cloud Director Mobile App

Netskope and Citrix together allow you to answer questions such as: “Is anyone downloading sensitive content onto a personal mobile device?” or “Who is sharing sensitive data with people outside of the organization,” and then drill down to a more granular level of “What devices and methods are people using to share data, such as email from a personally-owned device, or via collaboration/storage cloud apps?” After uncovering these details, you can easily put in place policies to prevent risky activity.

Enforce real-time, surgical controls

Once you’ve determined the activities being performed, make that intelligence actionable by enforcing real-time granular policies for individual sanctioned and unsanctioned apps or across app categories such as cloud storage, human resources, etc. When crafting these policies, utilize the power of the platform’s context engine by incorporating rich details available such as the user’s identity, Active Directory group, access method, devices, location, activity, and content.

Additionally, Netskope provides you with the ability to distinguish between app instances, allowing you to tell whether you see activity on a personal instance, corporate instance or differentiate between multiple personal/corporate instances of an app. This provides IT with truly granular options when crafting policies. For instance, IT can simply choose to ignore all non-corporate app traffic for privacy reasons, they can block all personal cloud storage app instance traffic, or they can monitor all traffic to personal instances, ensure no loss of sensitive data and guide users to the corporate-owned instance of an app.

Prevent loss of sensitive data with noise-cancelling cloud DLP

Netskope has the only “noise-cancelling” cloud DLP solution in the market. This starts with the out-of-the-box pre-defined DLP profiles such PII, PCI, PHI, and source code etc. Breaking it down, Netskope also makes available over as 3,000+ data identifiers, over 500 file types, support for language-agnostic double-byte characters, custom regular expressions, proximity analysis, document fingerprinting, and exact match.

Admins can use these building blocks to form DLP rules and create their own custom DLP profiles with one or more DLP rules to create precise, contextual, noise-cancelling DLP policies in the Netskope Active Platform. These policies can be applied to real-time activities, such as uploads, downloads, and shares, as well as applied offline to content already resident in cloud apps no matter when it was put there.

Furthermore, the solution boasts the unique ability to use context such as user, group, device, access method, location, activity, and content classification to reduce the surface area of potential DLP violations. Critical DLP workflows such as content quarantine, legal hold, automatic elimination of public access to sensitive content, event visualization in corporate SIEM systems, and featuring an elegant integration with your on-premises DLP and incident management systems, enable IT to remediate and report on violations.

Coach users

Promote a culture of transparency and awareness when it comes to security. When you enforce policies or the system initiates automatic workflows, instead of simply blocking apps, block risky activity, use Netskope’s custom alerts to inform them why it was blocked, and then direct them to sanctioned and safe cloud alternatives.

Continuously monitor for anomalous behavior and address risk

Get an at-a-glance view of a variety of factors that contribute to enterprise security risks and potential threats. From risky apps and users to risky devices and activities, get a handle on potential security exposure and risk associated with your organization. The joint solution allows you to first establish a baseline of user behavior and then understand anomalies so that IT can react in real-time to otherwise difficult to detect malicious activity.

Further evaluate your risk by understanding which users might have compromised credentials or a compromised device and put in place policies that can automatically remediate the risk. Finally, in the situation that something goes wrong, use the solution to get a comprehensive audit trail, including logs and pertinent information from the device(s), in order to recreate the occurrences surrounding the event.

FEATURE	BENEFIT
Device classification	Classify your devices, differentiate between BYOD versus corporate-owned and mobile versus desktop, and ensure that you're providing the right level of access to each.
eDiscover, control, and secure sensitive data with noise-cancelling cloud DLP	Mitigate your security risk and ensure data governance by protecting sensitive data in no matter the device or content type.
Real-time, surgical visibility and control of risky activities	Allow, don't block. By focusing on identifying specific risky activities and blocking them, instead of the app, you can allow safe cloud usage and confidently allow the sharing of data.
Instance identification and consolidation	Clearly distinguish between personal and corporate instances of cloud apps and drive users to the sanctioned corporate instance.
Anomaly detection	Use powerful machine learning to help streamline excessive downloads or shares, logins from multiple locations, or other activities that could signal a security threat.
Cloud forensic analysis	Create an audit trail to help in the investigation of risky activities.
Risk dashboard	Mitigate your exposure to security risks and potential threats.
User coaching	Involve users. Make them a part of the solution rather than a factor of risk.

Citrix XenMobile + Citrix ShareFile

XenMobile is the most comprehensive Enterprise Mobility Management solution delivering mobile device, mobile app and mobile content management along with business optimized productivity apps (including secure email), that enhance the user experience without compromising security.

ShareFile is a secure data sync and sharing service with flexible storage options that allows IT to mobilize all enterprise data. ShareFile enables mobile productivity with read-write access to data, workflows and collaboration, allows users to securely share files with anyone, and sync files across all of their devices.

About Netskope

Netskope™ is the leading cloud access security broker (CASB). Netskope gives IT the ability to find, understand, and secure cloud apps. Only Netskope empowers organizations to direct usage, protect sensitive data, and ensure compliance in real-time, on any device, for any cloud app so the business can move fast, with confidence.