

Data Security on Mobile Devices with Netskope Mobile Client

Netskope mobile client extends Netskope security protection to mobile devices and harmonizes security controls between desktop and mobile environments. With the Netskope mobile client, customers can access a range of Netskope security services, including Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Secure Web Gateway (SWG),

Quick Glance

- Unified client offering Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Secure Web Gateway (SWG), Netskope Private Access (NPA), and Netskope Cloud Firewall (CFW) capabilities for securing mobile workspace.
- Compatibility with various Mobile Device Management (MDM) solutions such as Intune, VMware Workspace One, Jamf, Ivanti Neurons facilitates a true Zero-touch deployment, ensuring a user-friendly experience.
- Consolidate and secure remote access with Netskope Private Access (NPA) instead of standalone VPN or MDM attached remote access solutions.
- Extend data protection to support BYOD (Bring Your Own Device) use cases.

“Netskope’s swift and comprehensive mobile client solution empowered a French public sector organization to securely deploy iPads for 60,000 students while complying with stringent content regulations and ensuring robust protection and data security.”

Systems Engineer
French Public Sector Organization

The Challenge

Mobile devices, tablets, and BYOD arrangements have emerged as the fundamental support for the rapidly evolving hybrid work model, ensuring swift, secure, and dependable access to applications across countless devices worldwide. Although they have empowered users to access apps from anywhere and enhance productivity, they also bring forth certain security challenges related to:

- **Data Privacy:** BYOD often blurs the line between personal and corporate data. Ensuring the privacy of personal data while managing corporate data on the same device can be challenging.
- **Secure Network Access:** Enabling company network access from diverse mobile devices increases the risk of unauthorized access and breaches.
- **Policy Enforcement:** Enforcing company policies on personal devices while respecting personal freedom can be a constant challenge.
- **User Coaching:** Effectively educating users about behaviors that may result in data breaches or unauthorized data sharing is an ongoing necessity.

The Solution

The Netskope mobile client expands data security to mobile devices in an innovative way. It integrates with various MDM solutions for seamless deployment on iOS and Android. This extends Netskope’s CASB and DLP security to mobile workspaces and allows monitoring of non-web traffic with Netskope Cloud Firewall. It provides secure access to corporate apps through NPA, eliminating the need for standalone VPN clients. The client also examines data traffic, aiding in threat detection and mitigation, especially for unmanaged cloud services, sync clients, mobile apps, and TLS-encrypted websites.

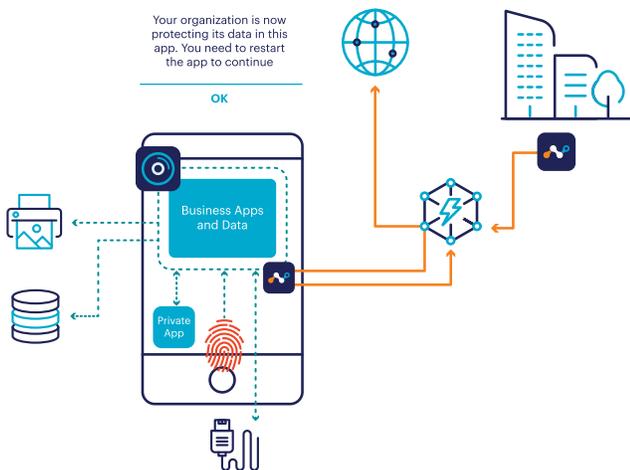
Data Loss Prevention

Tracking and safeguarding sensitive data as it circulates beyond the conventional corporate boundaries becomes increasingly challenging, making it susceptible to both deliberate and accidental exposure. The mobile workspace exacerbates this issue further.

The Netskope mobile client consistently identifies, oversees, and safeguards sensitive data whether it's in transit, at rest, or in use, spanning SaaS applications, IaaS, corporate networks, branch offices, and email services accessed via users' mobile devices. It delivers unified data protection policies for all data locations, and these policies are managed from a centralized cloud service.

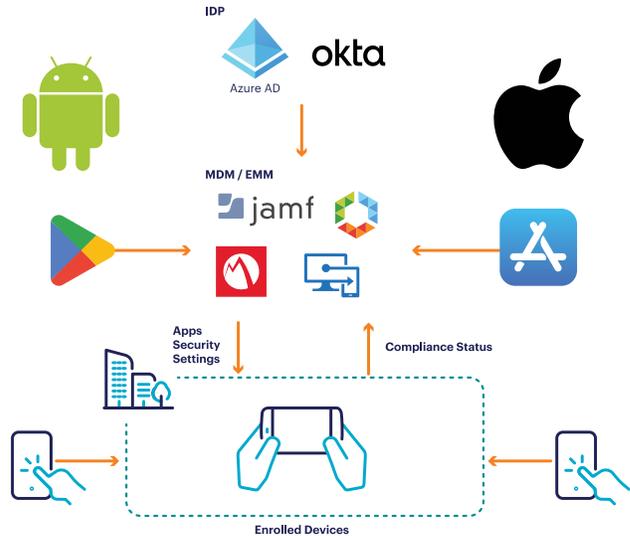
Organizations employing BYOD arrangements can find solace in the Netskope client, as it effectively addresses their foremost concern of data protection.

The Netskope mobile client consistently secures sensitive data in transit, at rest, and in use across various platforms and devices, delivering unified data protection policies managed from a centralized cloud service.



Zero Touch Deployment

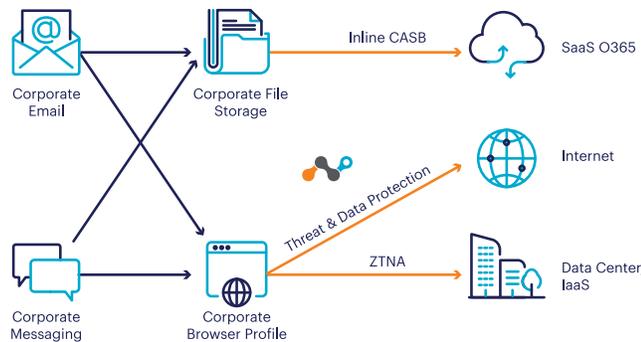
Thanks to the integration with diverse MDM solutions, the Netskope mobile client can be effortlessly installed on mobile devices with zero user involvement. MDM aids in achieving operational efficiency through consistent and repeatable deployments, swift and straightforward onboarding, segregation of personal and corporate apps and data.



Corporate-owned iOS and Android devices are subject to MDM enrollment after their initial activation. This allows MDM administrators to deploy necessary applications, configurations, and policies, including the Netskope client. Consequently, the Netskope service governs external connections for corporate devices during their entire operational lifecycle. Corporate devices are configured with stringent lockdown settings, preventing users from disabling Netskope controls or removing the client.

Netskope mobile client, through MDM integration, automates device installation, secures corporate devices' external connections, and ensures privacy for BYOD users

For BYOD devices, the enrollment process is essential to gain access to corporate applications, privileges, and connectivity through the Netskope service. The Netskope client is deployed in Per-App VPN mode for iOS devices or as a VPN for designated Work profiles on Android. This method ensures that only business-related traffic is monitored, preserving the user's privacy.



Secure Access to internet and private applications

The Netskope mobile client effectively counters the constantly evolving cyber threats encountered by mobile users by harnessing the power of the Next-Generation Secure Web Gateway (SWG). Industries such as healthcare and Higher Ed, which heavily rely on extensive mobile device usage, greatly benefit from the diverse capabilities provided by the Next-Generation Secure Web Gateway.

Higher education institutions, renowned for their open learning environments, face considerable cloud security challenges. An array of tools for productivity, research, management, and e-learning have migrated to cloud-based applications, with easy accessibility via mobile devices. These institutions frequently struggle to ensure the safe internet browsing of students and protect them from sophisticated malware threats.

The Next-Generation Secure Web Gateway offers a comprehensive suite of capabilities, spanning malware prevention, advanced threat detection, categorically filtered website access, data protection, and control over applications and cloud services. These features safeguard data for users, regardless of their location or the device they use.

Similarly in the healthcare sector the Netskope mobile client enables organizations to embark on digital transformation initiatives with confidence, ensuring they maximize organizational value while minimizing security risks.

The Netskope mobile client, powered by the Next-Generation Secure Web Gateway, safeguards data for education and healthcare sectors amid evolving threats, ensuring organizational value without security compromises.

BENEFITS	DESCRIPTION
Zero touch Deployment	Netskope mobile client integration with various MDM solutions enable a seamless deployment.
Unified Client for CASB, DLP, SWG, CFW	Netskope offers a single mobile client for diverse security services
Secure Network Access with NPA	Netskope helps organizations to securely access business applications without accessing the entire network.
Holistic data protection	Netskope offers solutions for safeguarding the complete data perimeter.



Interested in learning more?

Request a demo

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit [netskope.com](https://www.netskope.com).