

# Netskope for Workplace

Workplace by Facebook is the enterprise version of the popular social media service. With its familiar interface and features, Workplace has quickly become the standard collaboration platform in organizations worldwide. Netskope for Workplace protects sensitive data and defends against threats so teams can work together while remaining safe and compliant.



## QUICK GLANCE

- Gain visibility into usage of Workplace with deep contextual details
- Apply granular controls to risky activities and sensitive data
- Prevent the loss of PII, PHI, PCI, and other sensitive data
- Detect and remediate threats such as login anomalies and data exfiltration

## NETSKOPE FOR WORKPLACE

Netskope for Workplace offers granular access controls, data loss prevention, and cloud threat and malware protection. With Netskope, you have a complete risk dashboard on users, devices, and activities within Workplace groups, chats, and files. Enforce policies on messages and files that may contain sensitive

information in real-time activities to prevent compliance violations. For example, prevent users from uploading confidential data into a chat or alert on potential sensitive data already stored in Workplace in an uploaded file.

# Netskope for Workplace Feature Table

FEATURE	BENEFIT
Granular visibility of Workplace usage	Assess your security risk associated with usage of Workplace
Granular control of Workplace activities	Stop risky activities from taking place in Workplace
Advanced, enterprise cloud DLP	Alert on sensitive data in Workplace or prevent its upload in real time
Cloud threat and malware protection	Detect and remediate malware and prevent its propagation in real time and be alerted to anomalies like compromised credentials

## FEATURES

### Granular visibility into Workplace usage and risk

Drill down on users, activities, devices, and more accessing Workplace by Facebook. Delve into files and messages that contain data violations and be alerted to these violations. Perform ad-hoc queries or create reports of relevant access and usage information for compliance.

### Granular control of Workplace users, activities, and data

Create granular, contextual policies based on app, user, activity, device, and more. Perform actions like coaching with custom user messages or blocking of activities — all in real time. Create policies such as “Users cannot upload sensitive data such as PII into Workplace.”

### Advanced, enterprise cloud DLP

Netskope lets you detect data violations in transit or at rest in Workplace with industry-leading cloud DLP. Uncover and protect content containing sensitive data using pre-built profiles such as personally identifiable information (PII), payment card industry data (PCI), protected health information (PHI), source code, profanity, and more.

Alternatively, you can custom-build DLP profiles using Netskope’s robust set of advanced cloud DLP features such as 3,000+ data identifiers, 500+ file types, support for language agnostic double-byte characters, custom regular expressions, pattern matching, proximity analysis, fingerprinting, and exact match. Alert on potential violations on files already resident in Workplace or block in real-time activities such as uploads and downloads.

### Cloud threat and malware protection

Detect and respond to usage anomalies using Netskope’s machine learning- and rules-based anomaly detection. See logins from different locations, be alerted to data exfiltration, know when users’ credentials have been compromised, and understand privileged user threats. Using Netskope’s anti-malware capabilities, detect and block cloud malware in real-time activities to prevent upload of infected files.



Netskope is the leader in cloud security. Trusted by the world’s largest companies, Netskope’s cloud-scale security platform enables security professionals to understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work. Netskope — security evolved.