# Netskope for Google Workspace

Managing risk tied to data loss and threats in Google Workspace is a shared responsibility between Google and organizations adopting Google Workspace. Netskope provides deep visibility and granular control to protect sensitive data and defend against threats, helping organizations get the most out of Google Workspace while staying safe and compliant.

## QUICK GLANCE

- Gain deep visibility into usage of Google Workspace and its 3rd party app ecosystem
- Apply granular controls to reduce risk and optimize usage
- Protect sensitive data in Google Workspace with advanced cloud DLP and encryption
- Detect and remediate threats such as anomalous user behavior and malware
- See and control apps that have been granted access to Google Workspace

## NETSKOPE FOR GOOGLE WORKSPACE OVERVIEW

Google Workspace by Google Cloud is a popular productivity suite, with services like Gmail and Google Drive consistently appearing in the list of top cloud services used by Netskope's customers. Google Workspace provides a secure platform for its cloud services, but Google Workspace security is a shared responsibility between Google and its customers. Improper use of secure services like Gmail and Google Drive can still put an organization at risk. Netskope helps Google Workspace customers understand and control risky activities, protect sensitive data, and stop cloud threats.

Netskope for Google Workspace offers real-time, granular visibility and control of Google Workspace as well as its ecosystem of connected services. Netskope provides rich, contextual details around Google Workspace usage including users, devices, activities, data, and more. Automated workflows include options for encrypting sensitive content, quarantining sensitive or malicious files, or interrupting users attempting risky activities with customized coaching messages. With Netskope, organizations can take full advantage of Google Workspace while staying safe and compliant.

# Netskope for Google Workspace Feature Table

| FEATURE | BENEFIT |
|---|---|
| **Deep, contextual visibility for Google Workspace and its ecosystem** | • Get a clear picture of risk tied to activities and data movement in Google Workspace<br>• Understand your compliance posture from GDPR to PCI-DSS |
| **Flexible policy enforcement options** | • Enforce policies that zero in on specific risky activities rather than taking a coarse-grained allow or block approach<br>• Distinguish between managed and unmanaged Google Workspace instances to optimize policy and coaching workflows<br>• Keep end users in the loop for awareness or to enable self-remediation |
| **Advanced cloud DLP** | • Accurate and precise detection of sensitive data in Google Workspace and across its ecosystem to reduce false positives<br>• Stop data exfiltration from Google Workspace to unmanaged or shadow IT cloud services or personal Google Workspace instances<br>• Ensure compliance with 40+ compliance templates including PII, PCI-DSS, PHI/HIPAA |
| **Strong and flexible encryption** | • Protect data in Google Drive with AES-256 file encryption<br>• Use Netskope's FIPS 140-2 Level 3-certified KMS or utilize your on-premises KMIP-compliant HSM so you keep the keys<br>• Improve encryption targeting by incorporating Netskope cloud DLP to determine sensitive data to encrypt |
| **Multi-layered detection for cloud threats and malware** | • Stop malware and cloud-enabled threats in real time going to and from Google Workspace via browser or sync client<br>• Find and quarantine malware and ransomware in Google Workspace<br>• Detect anomalous activities in Google Workspace that could signal a compromised account, data exfiltrationn, or insider threat |

## KEY CAPABILITIES

**Deep visibility into Google Workspace and its Marketplace ecosystem**

Netskope offers deep visibility into Google Workspace as well as the ecosystem of services that share data with Google Workspace. View important contextual details around Google Workspace usage—including users, devices, and activities—and assess risk by identifying sensitive files in Google Workspace and seeing how they are being shared. Find all Google Workspace instances running in your environment, whether managed by IT or being used by individual employees or workgroups. Perform real-time queries to answer specific questions about Google Workspace usage, or develop reports for regular security and compliance reporting.

**Granular control reduces risk and optimizes Google Workspace usage**

Netskope applies granular policies to Google Workspace, its ecosystem, and other cloud services by combining deep cloud context with flexible options for policy enforcement. Beyond simply allowing or blocking a cloud service, Netskope offers real-time, fine-grained control. Block downloads for users accessing the managed Google Workspace instance from unmanaged devices. Allow downloads from personal instances of Google Drive, but block uploads of sensitive data. Provide proactive coaching to use the managed instance of Google Workspace when users try to access similar unmanaged cloud services.

### Advanced enterprise data protection

Discover and control sensitive data across Google Workspace services with Netskope cloud DLP, which accurately detects sensitive content across 1,500+ file types, using 3,000+ pre-defined data identifiers, metadata extraction, proximity analysis, fingerprinting, exact data match, and more. DLP policies are applied to real-time activities, such as sends, uploads and downloads, and also to sensitive content already stored in Google Drive. Leverage sophisticated activity-level decoding methods to prevent data exfiltration from Google Workspace to unmanaged cloud services. Respond quickly and effectively with automated actions such as encrypting or quarantining a sensitive file. Netskope Encryption adds another layer of protection, automatically and transparently protecting sensitive data stored in Google Workspace with the highest level of AES encryption.

### Comprehensive cloud threat protection

Netskope delivers comprehensive threat protection for Google Workspace and its ecosystem, with multi-layered threat detection and response capabilities. Uncover sophisticated attacks with machine learning-driven anomaly detection, advanced malware inspection, heuristics-based detection, and multi-stage sandbox analysis. Netskope threat detection is further enhanced with the latest cloud threat intelligence from Netskope Threat Research Labs, a dedicated team of cloud security researchers. Respond with automated actions to block or quarantine discovered threats, and use integrated workflows to further analyze and remediate the effects of new attacks, which too often evade existing security solutions.

## FLEXIBLE DEPLOYMENT OPTIONS

| | | API PROTECTION | REAL-TIME PROTECTION | |
|---|---|---|---|---|
| | | | Forward Proxy | Reverse Proxy |
| USE CASES | Out-of-band, near real-time integration with Google Workspace providing:<br>• Detection and policy-based remediation of sensitive data or malicious files at rest within Google Drive<br>• Detection and policy-based remediation of files incorrectly exposed publicly within Google Drive<br>• Alerting and incident management for sensitive data discovered in Gmail Draft, Bin, and Sent folders<br>• The ability to revoke high-risk Marketplace apps that are integrated with Google Workspace by employees | X | | |
| | Inline, real-time visibility and granular policy-based control* for users accessing Google Workspace applications<br>Real-time inspection of data transfers between users and Google Workspace with detection and remediation of threats and DLP violations | | X | |
| | Inline, real-time visibility and granular policy-based control* for users accessing Google Workspace applications—including from unmanaged devices<br>Real-time inspection of data transfers between users and Google Workspace with detection and remediation of threats and DLP violations | | | X |

*Examples of real-time Google Workspace applications and activities recognized by Netskope include:
Google Drive: Create | Delete | Download | Edit | Mark | Move | Post | Send | Share | Upload | View | View All
Google Gmail: Create | Download | Post | Send | Share | Upload | View All
Google Hangouts: Create | Delete | Edit | Join | Login Successful | Logout | Mark | Post | Unblock | Upload | View All

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.

To learn more visit, https://www.netskope.com.