netskope

Netskope for Google Apps for Work

Protect sensitive data and ensure compliance in Google Apps and the cloud

Google Apps for Work has become the productivity suite of choice for many enterprises as services like Gmail have been heavily adopted by consumers due to ease of use and popularity. With Netskope for Google Apps, you can let users take advantage of one app like Google Drive or Hangout, or the whole suite, to get their jobs done. Maintain the visibility and security controls you need to protect sensitive data, prevent its loss, and ensure compliance.

Understand usage in Google Apps and its ecosystem

Get visibility into activity- and data-level usage details within Google, along with the cloud apps that are part of Google's app ecosystem. This allows you to answer questions like "Who's sharing sensitive content outside of the company, and with whom?" across any app with a single query. IT can get visibility for security or compliance purposes without disrupting business processes.

Standardize on Google Apps

Consolidate redundant instances of Google Apps to save cost, reduce complexity, and encourage collaboration. Discover unsanctioned cloud storage and collaboration apps and migrate those users to Google Apps. Use the Netskope Cloud Confidence Index to make data-driven decisions about which apps to promote, which to limit, and which to consolidate.

Classify devices and control access

Ensuring that the devices being used to access Google Apps and its ecosystem are secure play an important part in your cloud security, risk, and compliance strategy. Device classification is continually evolving, often needing reclassification based on new parameters.

Netskope for Google Apps enables you to classify the devices accessing Google and its ecosystem based on parameters such as their encryption status, registry settings, processes running, files present, or even the device's Active Directory domain. Tight integration with a variety of single sign-on (SSO) vendors enables an easy way to bring new devices into the corporate fold. Using these granular identifiers and classification methods, enterprises can confidently differentiate between corporate and non-corporate devices, and define policies to grant differing levels of access to users.

At a Glance

Standardize on Google Apps

Get surgical visibility and control of usage in Google Apps and its ecosystem

Prevent loss of sensitive data with Netskope noise-cancelling DLP

Enforce real-time, granular control of Google Apps and its ecosystem

Utilize automated workflows to quarantine sensitive content or place it in legal hold

Additionally, Netskope provides you with information about activity for both admins and Google Apps users giving IT and the information security team true surgical visibility and control of Google Apps and its ecosystem. For example, IT can use Netskope to prevent Google Apps admins from being able to view all the users' documents or prevent them from accidently deleting user accounts. At the same time, IT can use Netskope to prevent Google Apps users from downloading or sharing a document that contains sensitive content.

Enforce real-time, granular control of Google Apps and its ecosystem

Instead of taking a coarse-grained allow vs. block approach, enforce granular policies in real-time within Google Apps and ecosystem apps. Apply contextual policies that account for: identity, location, activity, and content. For example, "Don't let financial 'insiders' share confidential reports outside of the company." Block risky behavior without blocking apps and protect sensitive content already resident in Google Apps from getting into the wrong hands.

Netskope inspects real-time activities, such as uploading, downloading, and sharing, and can inspect content already resident in Google Apps.

You can even get as granular as to track and restrict data access by domains and level of sharing: private, internally shared, externally shared, and public (accessible by anyone with the link).

Netskope for Google Apps also allows you to distinguish between personal and corporate-owned instances of Google Apps. This provides IT with several options when crafting policies. As an example, IT can simply choose to ignore all non-corporate Google Apps traffic for privacy reasons, block all personal Google Apps traffic, or they can monitor all traffic to personal instances of Google Apps, to ensure no loss of sensitive data and guide users to the corporate-owned instance of Google Apps.

Prevent loss of sensitive data using noise-cancelling cloud data loss prevention (DLP)

Netskope inspects real-time activities, such as uploading, downloading, and sharing, and can inspect content already resident in Google Apps. IT can find sensitive content using industry-leading DLP with 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 content detection.

These elements form DLP rules, which are comprised of DLP profiles that are used to set 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 and content already resident in Google Apps no matter when it was put there.

Furthermore, only Netskope enables IT to use context such as user, group, location, device, activity, and more to reduce the surface area of potential DLP violations, which further increases detection accuracy and efficiency. Critical DLP workflows such as content quarantine, legal hold, automatic elimination of public access to sensitive content, and event visualization in corporate SIEM systems, enable IT to remediate and report on violations.

Finally, Netskope's cloud DLP features integration with on-premises DLP and incident management systems, performing a first pass of sensitive content discovery in the cloud for efficiency, and then funneling suspected violations to an organization's DLP solution via secure ICAP. With Netskope noise-cancelling cloud DLP capabilities, it's possible to reduce the number of false positives that funnel into on-premises DLP solutions.

Encrypt sensitive data

Encrypt sensitive content stored in Google Apps. Netskope for Google Apps provides 256-bit encryption with support for cloud-based, fault-tolerant FIPS 140-2 Level 3 key management with an optional hardware security module or integration with your on-premises, KMIP-compliant key management. Special effort has been made to ensure that encryption takes place behind the scenes to seamlessly support mobile, native clients, and data synchronization.

Ensure smooth user experience with automated workflows

Netskope security controls kick off automated workflows for both the user and admin to ensure efficient follow up and a smooth user experience.

Netskope security controls kick off automated workflows for both the user and admin to ensure efficient follow up and a smooth user experience. Automatically quarantine content that meets your specific criteria or matches a DLP profile. Upon detecting a violation, Netskope automatically places the file in an admin-designated folder, whether the content is in process of being uploaded by the user or Netskope discovers it in your Google Apps environment. Based on your policy, Netskope can automatically encrypt that content for you in quarantine and notify the user and/or admin with a customized message.

Additionally, organizations have the ability to hold a copy of specific content, such as that matching specified content identifiers or created by a certain individual, for examination by a legal or regulatory reviewer using legal hold. Netskope automatically and silently places a copy (encrypted or not) of the file in a designated folder or on-premises. In keeping with the requirements of regulatory investigations, once content is designated for legal hold, Netskope will continue to discover and place files that users modify from the original in your reserved legal hold folder.

Furthermore, Netskope's integration with SSO vendors provides you with an automated method to mitigate risk when dealing with compromised credentials. With this method, Netskope detects that a user's credentials have been compromised and notifies the SSO system, which prompts the user to change their password. The SSO system can also be instructed to force the user to use two-factor authentication.

Coach users to success

When you enforce policies or initiate automatic workflows with Netskope, it's always a good idea to keep your users in the loop. That can mean simply letting them know that you've blocked them from an app or a particular activity within the app because it's against corporate policy. But even more useful is to give them an alternative, such as blocking them from uploading content to an unsanctioned app, and then coaching them with a URL (or simply redirecting them) to sign up for Google Drive.

Continuously assess and address your cloud risk

Get an at-a-glance view of a variety of factors that contribute to security risks and potential threats. From risky apps to risky users to risky activities, get a handle on what your potential security risk is when it comes to using Google Apps and its ecosystem of apps. Further evaluate your risk by using the 'Password Breach' visualization to see what users might have compromised credentials.

For organizations standardizing on Google Apps, Netskope provides rich detection of activity-level anomalies such as excessive downloading or sharing from Google Apps, unusually heavy uploads to an app other than Google Apps, or logins from multiple locations. These usage anomalies can indicate compromised credentials, out-of-compliance behaviors, and even the presence of malware and can help prevent possible data breaches.

With Netskope, you can create a granular cloud activity audit trail following a suspected event such as the theft of sensitive content upon employee departure. IT can reconstruct this activity inthe form of a forensic audit trail to understand what that user did with what content in which app, and if they shared the content, with whom they shared it.

For organizations standardizing on Google Apps, Netskope provides rich detection of activity-level anomalies such as excessive downloading or sharing from Google Apps, unusually heavy uploads to an app other than Google Apps, or logins from multiple locations.

Key Features / Benefits Table

FEATURE	BENEFIT
eDiscover, control, and secure sensitive data stored in Google Apps with noise-cancelling cloud DLP	› Mitigate your security risk and ensure data governance by protecting sensitive data
Device classification	› Ensure that only the right kinds of devices are accessing your sensitive data
Real-time, surgical visibility and control of risky activities in Google Apps and its ecosystem of apps	› Allow, don't block. By focusing on identifying specific, risky activities and blocking them, instead of the app, you can allow safe use of Google Apps and ecosystem apps
Instance identification and consolidation	› Clearly distinguish between personal and corporate instances of Google Apps and drive users to the sanctioned corporate instance while ensuring employee privacy
Cloud forensic analysis	› Create an audit trail to help in the investigation of risky activities
Anomaly detection	› Detect risky activities earlier with powerful machine learning to identify excessive downloads or shares, logins from multiple locations, or other activities that could signal a security threat
Data quarantine	› Enable a remediation-centric workflow that helps you mitigate risks, while ensuring minimal impact to users
Risk dashboard	› Mitigate your exposure to security risks and potential threats by identifying high-risk apps, activities, and users
User coaching	› Make users a part of the solution and not simply a part of the problem by driving them to sanctioned apps and compliant activities
Legal hold of sensitive content	› Streamline legal and regulatory review by holding a copy of specific content matching specified content identifiers (DLP profile) or created by a certain individual, for examination by a legal or regulatory reviewer in a designated folder

Only Netskope gives you:

Noise-cancelling DLP

Efficient cloud DLP that leverages existing on-premises DLP solutions and dramatically reduces false positives

Surgical Visibility and Control

Granular visibility and governance of all cloud apps' usage, whether sanctioned or unsanctioned

Future-proof Architecture

Largest variety of flexible deployment options to satisfy all current and future use cases and needs

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.