Netskope Introspection

Where is your data? Find and secure sensitive content stored in cloud apps

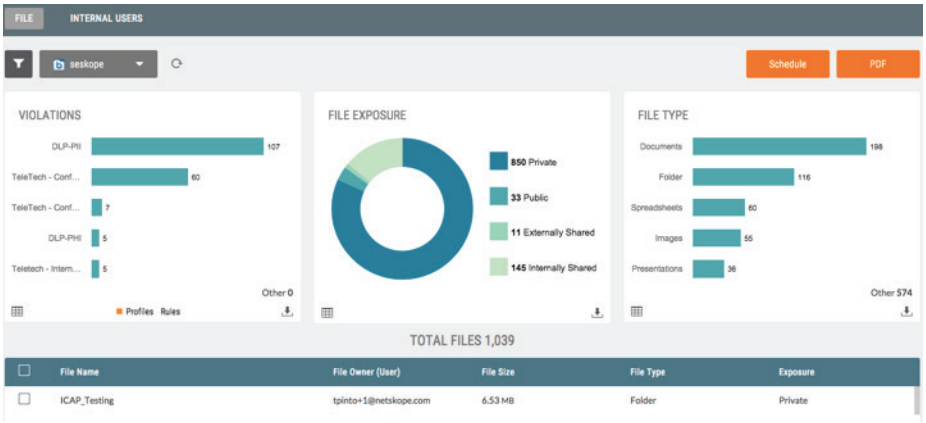
At a glance:

- Find and secure sensitive content stored in your cloud apps
- Inventory content and users
- Perform a variety of actions such as revoke access, quarantine, and encrypt
- Simple and frictionless offline deployment

Netskope Introspection (Introspection) inspects content that is already resident in a cloud app, irrespective of when it was uploaded or where it was created. Introspection inventories and classifies content, content owners, and collaborators as well as provides content sharing status. Additionally, it enables you to download files for review, and perform a variety of actions such as restrict access, revoke sharing, encrypt content, quarantine content, and place content on legal hold.

Effortless deployment

Introspection setup is simple and frictionless. After getting access to your private Netskope cloud tenant, the streamlined configuration leverages an API authorized by an OAuth transaction to create a secure connection to your cloud app. With that, you are only a few minutes away from seeing what sensitive data is inside your cloud app.



Determine exposure

Introspection gives you a detailed view into the data stored in your sanctioned cloud apps. Your files are classified and displayed in the following categories: Private – shared with no one, Shared internally – shared with people within the organization's domain, Shared externally – shared with people outside the organization's domain, and Shared publicly – typically shared with a link so anyone can access the data. They are also broken down and displayed by file type such as Google Doc, MS PowerPoint, PDF, CSV, XML, Box Note etc.

Additionally, you can manually use a fine-grained filter to drill down and view a specific file after searching for it by file type, file size, exposure, DLP profile, legal hold, quarantine, encryption, collaboration, date created and date last edited.

Introspection + noise-cancelling cloud DLP

When combined with with Netskope Cloud DLP, Introspection enables you to find and secure content that matches a DLP profile. Use the industry's most advanced DLP with a selection of pre-defined DLP profiles such as Personally Identifiable Information (PII), Protected Health Information (PHI), Source Code, etc. or create your own custom profiles using the available 3,000+ data identifiers covering nearly 500 file types, fingerprinting, keyword search, pattern-matching, proximity search, regular expression lookup, exact match, and language-agnostic double byte character support.

This ensures that you get the most accurate and efficient noise-cancelling ability — significantly reducing false positives and false negatives to create a balanced high-fidelity DLP solution. Additionally, Netskope's elegant integration with your highly tuned on-premises DLP solutions allows you to perform a first pass in the cloud and then funnel suspected violations to your on-premises solution via secure ICAP.

Take action

Leverage Netskope's powerful policy engine to take action such block, restrict, or revoke access and quarantine or place content on legal hold. Take one-click actions to restrict access to file owners, internal users, users belonging to one or more whitelisted or blacklisted domains, or to remove any public links found. Additionally, Netskope Introspection enables you to create policies and ensure that they're very surgically targeted.

You have the ability to select a particular sanctioned app instance, target folders belonging to all users or a specific set of users, filter whether the policy should apply to files based on sharing status, restrict access based on domain, select the file type(s) to scan, choose whether to apply scans to files moving forward and/or retrospectively, select a DLP profile to apply, and assign an appropriate action to take such as alert a user, encrypt the content, quarantine it or put it on legal hold. Additionally, you can choose to send notifications to file owners, collaborators, app admins, or a custom list of users, as these policies trigger. Alternatively, schedule the notification alerts to go out in batches ever 30 minutes, 60 minutes, 6 hours or 24 hours.

Netskope also provides you with dedicated quarantine and legal hold UIs to comprehensively view and act on quarantined files and files placed on legal hold, across all your sanctioned cloud apps.

Secure sensitive content with strong encryption

Protect your sensitive data using Netskope's strong 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 system.

Introspection + Netskope Active for 360-degree protection

Introspection secures content stored in cloud apps. Netskope Active helps you secure and control the activities (e.g. uploading and downloading) that happen in real-time. The combination of Introspection + Netskope Active makes sure that both stored content and real-time activities are protected, ensuring that your data is secure no matter what.

Built for scale

Some of the largest companies in the world have deployed Introspection in the most demanding environments with some deployments covering millions of files and more than 300,000 users. Introspection leverages patent-pending technology to ensure reliable data inspection regardless of how many files, folders, or users are present.

Deep visibility into your account

- File name/owner/size/type
- App and instance name
- File path
- Audit trail with activity, user, access date
- File version history
- Encryption status
- Shared link expiration
- DLP policy triggers
- External users (and access to internal files)
- Search and filter on a variety of conditions
- File access to external domains

Available actions (varies by cloud app)

- DLP policies
- Download files
- Restrict access
- Revoke access
- Change ownership
- Quarantine
- Legal hold
- Encrypt/decrypt
- Notify original owner / end user
- Secure collaboration

Capabilities supported per cloud app: Visibility and actions

Introspection gives you the visibility you need while arming you with actions you can take to mitigate your risk. Support for visibility and action capabilities varies based on what specific cloud app you are using. Netskope currently supports Introspection for Box, Dropbox, Egnyte, Google Apps, Office 365 (focused on OneDrive, and all SharePoint Online sites), and Salesforce. Please contact Netskope for details on what features on supported for your cloud app.

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.