Netskope CASB API Protection

Data Sheet

Observe, Monitor, and Protect Data in Managed Cloud Services

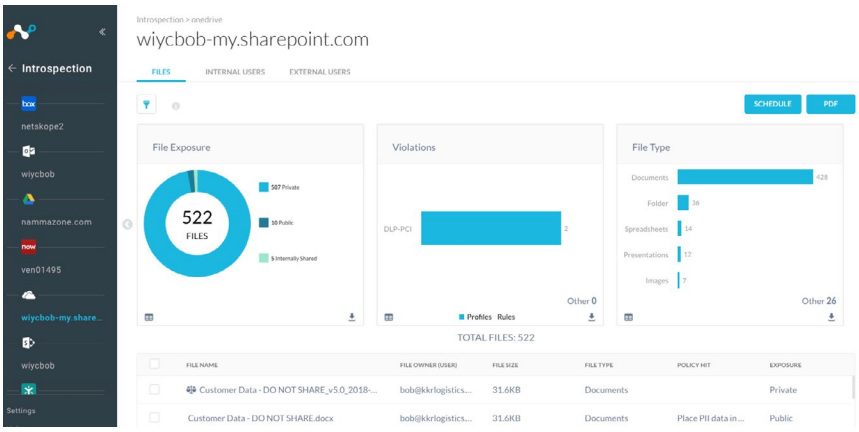
Netskope CASB API protection inspects content residing in managed cloud services. API protection identifies content, content owners, collaborators, and content sharing status, along with policy enforcement for sharing violations, sensitive data, and malicious files.

Why is Netskope the best choice?

Many cloud services already have published APIs that allow third-party access. CASB API protection leverages these APIs available from vendors like Box, Google Workspace, and Microsoft 365 for visibility into settings and data residing in the service. With Netskope, enforce powerful policies to control access and protect data in cloud services.

Enforce Policies, Control Access, and Protect Data in Cloud Services:

- **Visibility into Cloud Services:** Uncover and protect sensitive content stored in your cloud services.
- **Extensive Actions and Capabilities:** Including the ability to revoke access, quarantine, change access or ownership, place in legal hold, notify, and more.
- **Protect Against Cloud Threats:** Combined with Netskope Threat Protection, inspect cloud services for malware, including ransomware. Quarantine and replace malware with a tombstone file to indicate an action has been taken.
- **Industry's Most Advanced DLP:** Combined with Netskope DLP, Introspection enables you to find and secure content that matches a DLP profile. Includes pre-defined DLP profiles for regulatory compliance.



Key Benefits and Capabilities

Effortless Deployment

Setup is simple and frictionless. Streamlined configuration leverages an API authorized by an OAuth transaction to create a secure connection.

Determine Exposure

API protection gives you a detailed view into the data in managed cloud services. Understand when sensitive files are shared externally and publicly; and by file type.

Take Action

Use policy to take action, including block, restrict, or revoke access; quarantine or place content on legal hold. Use one-click actions to restrict access to file owners, internal users, users belonging to one or more allowed or blocked domains, or remove any public links. Create your own custom policies.

Built for Scale

Some of the largest companies in the world have deployed Netskope API protection in the most demanding environments, including deployments covering millions of files and more than 300,000 users.

Combine with Inline CASB for 360 Degree Protection

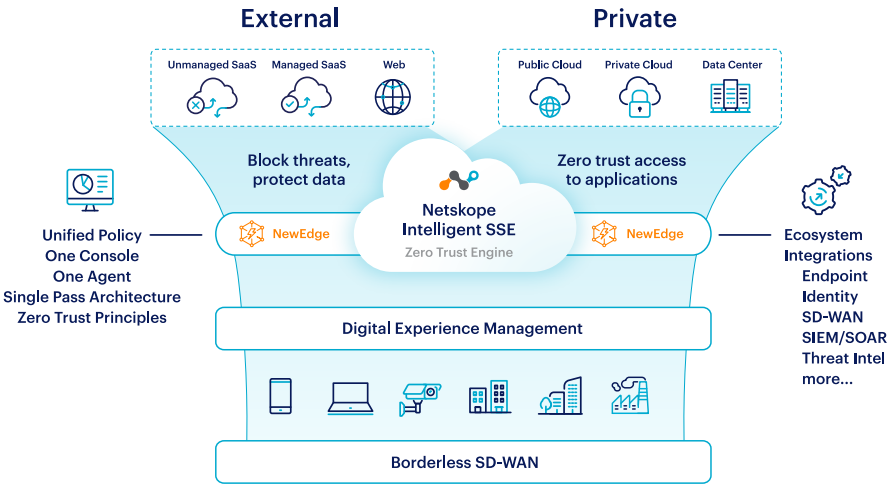
API protection secures content stored in cloud apps. Netskope Inline CASB (including Netskope Intelligent SSE and NG-SWG) helps control activities that happen in real-time (like uploading/downloading). API Introspection with CASB inline deployment ensures both stored content and real-time activities are protected.

"Visibility and DLP functionality of CASB through API is easy to setup and gives great results."

– Director, IT Security, Industry: Real Estate, Role: Security and Risk Management, Source: Gartner Peer Insights, Security Service Edge, CASB, September 2021

The Netskope Difference

Netskope helps you reduce risk, accelerate performance, and provide unrivaled visibility into any cloud, web, and private application activity. To empower safe collaboration, Netskope reliably balances trust against risk with granular controls that adapt to changes in your environment. The Netskope platform protects against advanced and cloud-enabled threats and safeguards data across all vectors (any cloud, any app, any user). A single-pass architecture delivers a fast user experience and simplified operations.



YOUR NEEDS	THE NETSKOPE SOLUTION
Ongoing and retrospective scans	Inspect content, including a full repository scan on an ongoing basis, based on multiple criteria, including sharing attributes and exposure and take a retrospective look at existing file stores.
UEBA/anomaly detection	API protection is integrated with UEBA and anomaly detection to identify new and specific insider risk scenarios.
RMS support	Integration and support for Microsoft Rights Management System.
Threat and data protection	Fully integrated with Netskope Threat Protection and Netskope DLP.
Full file metadata	Including cloud service, activity history, file name, owner, size, type, file path, DLP policy triggers, encryption status, exposure to external domains, shared link expiration, version history, users with access, and more.
Supported applications	AWS, Microsoft Azure, Google Cloud, Box, Cisco Webex Teams, Dropbox, Egnyte, GitHub, Gmail, Google Drive, Microsoft 365 OneDrive, Microsoft 365 Outlook, Microsoft 365 SharePoint, Microsoft 365 Teams, Salesforce, ServiceNow, Slack for Enterprise, Slack for Teams, Workplace by Facebook, Yammer, Workday, Okta, Sharefile. Available controls may vary by cloud service due to richness of published APIs.

netskope

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.