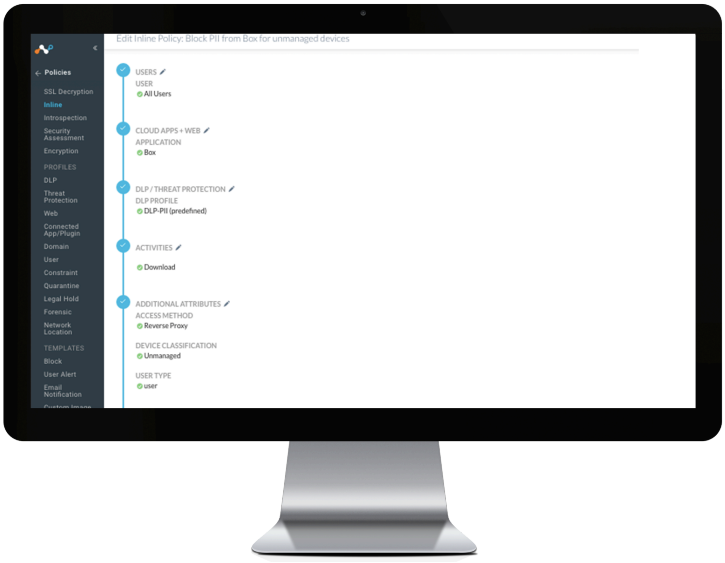
Netskope API Protection

AT A GLANCE

- Uncover and protect sensitive content stored in your cloud services
- Inventory content and users
- Perform a variety of actions such as revoke access, quarantine, and encrypt
- Simple and frictionless out-of-band deployment



Many well-established, enterprise-ready cloud services come with published APIs that allow third-party control. Netskope API protection leverages these APIs available from vendors like Box, G Suite, Office 365, and Slack to get visibility into usage and data already resident in the service. Through this access, Netskope can enforce powerful policies to control access and protect data.

PRODUCT OVERVIEW

Netskope API protection inspects content that is already resident in a cloud services, irrespective of when it was uploaded or where it was created. API protection 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

API protection 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 service. With that, you are only a few minutes away from seeing what sensitive data is inside your cloud service.

DETERMINE EXPOSURE

API protection gives you a detailed view into the data stored in your sanctioned cloud services. 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.

API PROTECTION + THE INDUSTRY"S MOST ADVANCED DLP

When combined with with Netskope 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. Additionally, Netskope's integration with on-premises DLP systems allows you to perform a first pass in the cloud and then funnel suspected violations to your on-premises DLP system 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, API protection enables you to create policies and ensure that they're very surgically targeted.

You have the ability to select a particular sanctioned service 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 based on any of the above.

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.

PROTECT AGAINST ADVANCED CLOUD THREATS

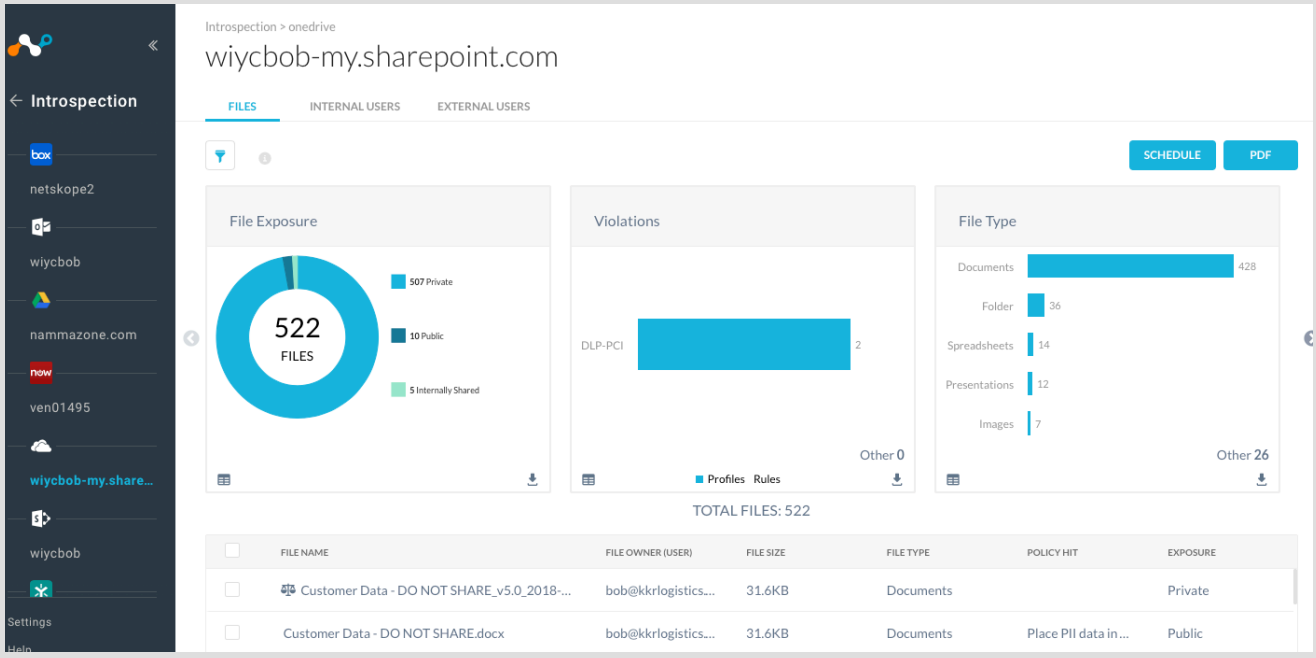
When you combine protection with Netskope Threat Protection, you are protected against various strains of malware such as ransomware that can hide and spread in cloud services. Malware is quarantined and replaced with a tombstone file that lets users know the action taken.

API PROTECTION + REAL-TIME DEPLOYMENT OPTIONS FOR 360-DEGREE PROTECTION

API Introspection secures content stored in cloud apps. Netskope's inline deployment options helps you secure and control the activities (e.g., uploading and downloading) that happen in real time. The combination of API Introspection plus inline deployment options 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 API protection in the most demanding environments, with some deployments covering millions of files and more than 300,000 users. API protection leverages patent-pending technology to ensure reliable data inspection regardless of how many files, folders, or users are present.



API Protection Supported Cloud Services

Netskope API Protection Features

VISIBILITY INTO CLOUD SERVICES	
Cloud Service	Instance name and ownership (corporate, personal, other)
Activities	Activity history
Files	File name Owner Size Type File path DLP policy triggers Encryption status Exposure to external domains Shared link expiration Version history
Users	Named account users with access details External users with access details
AVAILABLE ACTIONS — VARIES BY CLOUD SERVICE DUE TO RICHNESS OF PUBLISHED APIs	
Access	Change access or ownership Restrict access Revoke access
Data Protection	DLP policies Prevent download Encrypt/decrypt data
Advanced Threat Protection	Inspect services for malware
Workflows	Quarantine Place in Legal Hold Notify original / end users of action

netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.