netskope + Dropbox

Netskope for Dropbox

COLLABORATION WHILE ENSURING SAFE USAGE

At a glance:

- Standardize on Dropbox
- Get surgical visibility and control of usage in Dropbox and its ecosystem
- Prevent loss of sensitive data with Netskope noise-cancelling DLP
- Enforce real-time, granular control of Dropbox and its ecosystem
- Utilize automated workflows to quarantine sensitive content or place it in legal hold

Dropbox, with its great user experience, holds a strong attraction for everyone. With Dropbox for Business, organizations can take advantage of all of the productivity benefits of Dropbox while remaining in control of company data and ensuring collaboration between employees. Using Netskope for Dropbox, IT can gain an additional layer of security and control over sensitive data. Gain visibility and insight into usage of data in Dropbox and its ecosystem of apps, and secure that usage appropriately so employees remain happy and you can sleep soundly at night.

Understand usage in Dropbox and its ecosystem

Get visibility into activity- and data-level usage details within Dropbox, along with the cloud apps that are part of Dropbox'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.

Differentiate between personal and corporate sanctioned Dropbox usage

Security and privacy do not have to be at odds. Identify personal vs. corporate sanctioned Dropbox usage and optionally focus your policy enforcement on corporate use and take a hands-off approach to personal usage. Or, monitor personal instances of Dropbox for uploads of sensitive corporate data.

Standardize on Dropbox

Consolidate redundant instances of Dropbox to save cost, reduce complexity, and encourage collaboration. Discover unsanctioned cloud storage and collaboration apps and migrate those users to Dropbox. 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 Dropbox and its ecosystem are secure play an important part in your cloud security, risk, and compliance strategy.

Netskope for Dropbox enables you to classify the devices accessing Dropbox 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.

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

In addition to tight integration with SSO vendors, Netskope offers built-in, device-level access control policies that enable you to restrict access to Dropbox based on whether or not users are on a corporate device. Device-level access control is granular so you can perform actions such as restrict certain Dropbox activities to only corporate-managed devices.

Enforce real-time, granular control of Dropbox and its ecosystem

Instead of taking a coarse- grained allow vs. block approach, enforce granular policies in real-time within Dropbox and ecosystem apps. Apply contextual policies that account for: identity, location, activity, and content. e.g., "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 Dropbox from getting into the wrong hands.

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).

By distinguishing between personal and corporate-owned instances of Dropbox, IT has more flexibility when crafting security policies. As an example, IT can simply choose to ignore all non-corporate Dropbox traffic for privacy reasons, block all personal Dropbox traffic, or monitor all traffic to personal instances of Dropbox, to ensure no loss of sensitive data and guide users to the corporate-owned instance of Dropbox.

Enable safe collaboration

Dropbox for business allows for secure collaboration with control of links that are shared with others. Besides enabling you to put policies and controls in place to restrict or limit links that are shared, Netskope can view external users' activities and prevent them from doing anything malicious as well as make sure that only authorized users get to it. Stay secure even when sharing sensitive content with external collaborators.

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 Dropbox. IT can find sensitive content using industry-leading DLP with 3,000+ data identifiers, 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 for content already resident in Dropbox 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 Dropbox, retroactively or as it's being uploaded. Netskope for Dropbox 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 initiate automated workflows for both the user and admin to ensure efficient follow up and a smooth user experience. 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 Dropbox.

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 Dropbox 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 Dropbox, Netskope provides rich detection of activity-level anomalies such as excessive downloading or sharing from Dropbox, unusually heavy uploads to an app other than Dropbox, 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 in the 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.

Feature summary

FEATURE	BENEFIT
eDiscover, control, and secure sensitive data stored in Dropbox with noise-cancelling cloud DLP	Mitigate your security risk and ensure data governance by protecting sensitive data, even when it's shared with external stakeholders
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 Dropbox and its ecosystem of apps	Allow, don't block – regardless of whether users are on-premises or remote, on a PC or mobile device, in a web or native app. By focusing on identifying specific, risky activities and blocking them, instead of the app, you can allow safe use of Dropbox and ecosystem apps
Instance identification and consolidation	Clearly distinguish between personal and corporate instances of Dropbox 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 or suspected security events
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
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. Also, give them an opportunity to enter a business justification and proceed, or enter a false posititve.

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.