netskope
+
EGNYTE

- Standardize on Egnyte
- Get surgical view and control of usage in Egnyte and its ecosystem
- Enforce real-time, granular control of Egnyte and its ecosystem
- Prevent loss of sensitive data using Netskope's noise-cancelling DLP

Netskope for Egnyte

Enable Safe Enterprise File Sync and Share

The Evolving Storage Cloud

Organizations are adopting the cloud in a big way. This is especially true of cloud storage and enterprise file sync and share apps. Today, there are more than 200 such apps, with the average enterprise using 33 of them. While many of these cloud apps often house an organization's most sensitive content, our research shows that over 73% of these apps are not enterprise-ready, falling short of minimum standard for security, auditability, and business continuity.

As your needs evolve, you must ensure that the solution you choose evolves to meet your business needs, compliance requirements, is cost-effective, and performs according to your vendor service-level agreements. You also want to make sure you get the most out of your existing on-premises storage investments.

Egnyte uses a hybrid file services platform built to uniquely address the needs of IT and users by providing a hybrid cloud and on-premises file service to ensure that you can take advantage of a cloud storage solution that combines flexibility with security. Netskope complements Egnyte to provide you with surgical visibility, access controls and DLP capabilities you need to ensure its safe and compliant use for your organization.

Understand Usage in Egnyte and its Ecosystem

Netskope provides you with deep visibility into app usage and user activity supplemented with rich contextual details. You can quickly understand how your users are using sanctioned Egnyte, apps that are part of Egnyte's app ecosystem, and other competing unsanctioned cloud storage apps they're using to fulfill their cloud storage needs.

You can analyze and act on data at rest in Egnyte as well as data in motion, to or from the cloud, giving you the comprehensive coverage you need. Use Netskope's introspection to view all content resident in Egnyte no matter when it was uploaded. In a short while, get answers to questions like: who is sharing content outside of your company, what content they shared, and with whom. Using inspection, see whether confidential data are being uploaded to the cloud or being downloaded from the cloud, and what devices are being used for this activity. Simply put, with Netskope for Egnyte, IT easily gains visibility for security or compliance purposes without disrupting the business.

Standardize on and Consolidate Usage to Egnyte

After you discover unsanctioned alternatives, use Netskope's Cloud Confidence Index to make data-driven decisions about which apps to promote, which to limit, and which to consolidate. Additionally, use Netskope's ability to distinguish between different instances of apps to find redundant corporate instances of Egnyte.

Once you've discovered all the alternate Cloud Storage and Collaboration apps, use Netskope to migrate those users to Egnyte and consolidate redundant instances of Egnyte to save cost, reduce data exposure, management complexity, and encourage collaboration.

In order to make the migration to Egnyte simpler for your users, take advantage of Netskope's custom coaching ability to inform users that you've blocked them from an app or a particular activity within the app because it's against corporate policy. You can even go a step further by redirecting them to sign up for Egnyte.

Encrypt Sensitive Data

Encrypt your sensitive data without compromising the user experience. Netskope for Egnyte 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.

Utilize Contextual Real-time Controls in Egnyte and its Ecosystem

Only Netskope enables you to use context such as user, group, location, device, activity, and more while putting security controls in place. Use this context to enforce granular policies in real-time at the activity and content levels. Additionally, take into consideration the device being used by using Netskope's device classification ability. This feature uses a combination of one or more of the following attributes to distinguish between personally-owned and corporate devices: encryption level, registry settings, processes running, the existence of a file, or Active Directory domain.

Take advantage of these controls to bring to life the use cases you designed when creating your security and compliance policies. For instance, prevent sharing of documents containing financial information outside of the company, encrypt sensitive data such as PHI or PCI upon upload to Egnyte, or only allow the downloading of sensitive data to corporate-issued laptops. This allows you the flexibility to curb risky behavior without blocking apps.

Prevent Loss of Sensitive Data with Noise-cancelling Cloud DLP

Netskope has the most advanced cloud DLP in the market. The most differentiating feature is that it is "noise-cancelling." This starts with Netskope's robust set of advanced cloud DLP capabilities such as 3,000+ language-independent data identifiers, over 500 file types, and features capabilities such as support for language agnostic double-byte characters, custom regular expressions, proximity analysis, document fingerprinting, and Exact Match.

These elements come together to form DLP rules, which comprise 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 Egnyte no matter when it was put there.

Utilize critical DLP workflows such as content quarantine, and automatic elimination of public access to sensitive content, and take advantage of event visualization in corporate SIEM systems thus enabling IT to remediate and report on violations.

Finally, Netskope's cloud DLP features the most elegant 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 organizations' highly-tuned DLP solutions via secure ICAP.

Assess and Address your Cloud Risk

From the moment Netskope is introduced, it works on detecting and correlating activities to detect and alert on anomalies such as excessive downloading or sharing from Egnyte, unusually large uploads to an app other than Egnyte, logins from multiple locations, or an attempt to delete a large collection of files. These usage anomalies provide you with invaluable information that could indicate compromised credentials or the presence of malware, and can be used to prevent possible data breaches.

Get an at-a-glance view of a variety of factors that contribute to enterprise 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 Egnyte and its ecosystem of apps. Further evaluate your risk by using the 'Password Breach' visualization to see which users might have compromised credentials.

Furthermore, Netskope's seamless 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.

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

FEATURE	BENEFIT
Cloud app discovery and risk assessment	Know what apps are running, and make data-driven decisions about which apps to standardize on, block, limit, or monitor
Deep visibility into user activity	Quickly understand user activity at a granular level and be alerted to risky behavior, lapses in security, and non-compliance
Contextual policy enforcement	Improve your risk profile and safely enable cloud by shaping user behavior. Block risky activities, not apps
Discover sensitive content in Egnyte and take action based on risk and compliance requirements	Know what sensitive content is in your cloud through Introspection. Triage your remediation
Standardize on hybrid file services you can trust	Get the best of both worlds - the flexibility of cloud storage with assurance that files are stored and shared in the right place based on their size, type, and sensitivity
Disaster recovery and business continuity	Minimize downtime or data loss as a result of app failure or problem
Encryption	Ensure that all data that's stored and transmitted meets your data protection standards and policies
File Sharing	Ensure the app will meet employee requirements
Identity and access control	Secure app access in the same manner as the rest of your enterprise systems
Netskope Cloud DLP	Powerful DLP engine with 3,000+ data identifiers, support for 500+ file types, custom regex, proximity analysis, international support, and fingerprinting and use of context to narrow detection surface area to reduce false positives. Efficient DLP with critical workflows like quarantine and legal hold, and features the most elegant integration with on-premises DLP solutions, performing a first pass in the cloud and then funneling suspected violations to your on-premises solution via secure ICAP.
Netskope Introspection	Discover content against your key DLP profiles, inventory content and users, encrypt sensitive content, see sharing status (private, shared, or public), download content, and notify content owners.

Take the first step

Get your complimentary Cloud Risk Assessment today to understand the cloud apps in your environment and evaluate your risk. Visit https://www.netskope.com/cloud-risk-assessment/

About Netskope

Netskope is the leader in cloud security. Trusted by the world's largest companies, Netskope's cloud-scale security platform enables security professionals to understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work. Netskope — security evolved.