The Netskope Active Platform

Enabling Safe Migration to the Cloud

Netskope™ is the leader in safe cloud enablement. With Netskope, IT can protect data and ensure compliance across cloud apps so businesses can move fast, with confidence.

Massive Cloud Adoption

Organizations are adopting cloud apps, and for good reason. They help users get their jobs done more efficiently, quickly, easily, and flexibly than traditional software. While organizations are responsible for and in control of some apps, their users are now more than ever procuring and using these apps without IT's permission or involvement. This means you can't consistently manage and secure all of the cloud apps running in your organization.

Whether sanctioned or unsanctioned, cloud app usage is growing and C-suites, boards of directors, and audit committees around the world are beginning to ask whether the cloud technologies in their environments are safe, compliant with business policies, perform according to vendor service-level agreements, are cost-effective, and are optimized for business usage. In order to answer these questions, you need to consistently enforce and monitor the effectiveness of your security policies across all of the cloud apps in your environment, and report on their compliance, whether you sanction them or not. You need to do all this while enabling your users to move fast with the cloud. With the Netskope Active Platform, you can confidently do it all.

The Netskope Active Platform

The Netskope Active Platform™ gives IT the ability to find, understand, and secure cloud apps. Only Netskope empowers organizations to gain surgical visibility and control, protect sensitive data using "noise-cancelling" data loss prevention (DLP), and ensure compliance in real-time, on any device, for any cloud app so the business can move fast, with confidence.

There are three primary phases of safe cloud enablement that Netskope provides: find, understand, and secure.

Find

Find all of the enterprise cloud apps that are running in your enterprise and understand your risk. Netskope maintains detailed information for thousands of apps in the Netskope Cloud Confidence Index™, which draws on objective security, auditability, industry-standard certifications and business continuity criteria adapted from the Cloud Security Alliance. The apps' scores are combined with financial viability information from Dun & Bradstreet to help determine each app's risk and the overall cloud risk for your organization's specific usage.

Additionally, discovered apps are classified into categories such as Cloud Storage, Collaboration, Data & Analysis, HR, Marketing and Software Development but can also be custom tagged based on how they're used in your organization. Where possible, pricing associated with the application is made available. This helps determine the organizations cost associated with Shadow IT.

Understand

Beyond finding cloud apps, the Netskope Active Platform gives you rich activity- and data-level usage details. With Netskope, you can answer questions such as "Who's sharing sensitive content outside of the company, and with whom?," "Do we have any PCI residing in our cloud apps?," and "Are any of my non-U.S. users downloading PII from HR apps?".

In addition to answering specific questions, you can take advantage of Netskope's advanced anomaly detection to understand granular anomalies such as whether a user is excessively downloading and sharing, or logging in from multiple locations, which could indicate compromised credentials. These usage anomalies can indicate security threats, out-of-compliance behaviors, and even the presence of malware.

Furthermore, the Netskope Risk Dashboard provides you with an intuitive interface to quickly understand your organization's overall risk by viewing data such as your top risky apps, top risky users, and password breaches. You can drill down into each of these categories to gather more information to mitigate your risk.

Netskope lets you drill down into details such as:

- Apps, app instances, services, and sessions
- Users, roles, and enterprise directory groups
- Specific app activities, e.g., share or download
- Devices and browsers, e.g., IE, Firefox, and Chrome
- Time periods
- Geo-locations
- Content type, file type, file or object name, and DLP profile
- Anomalies

Secure

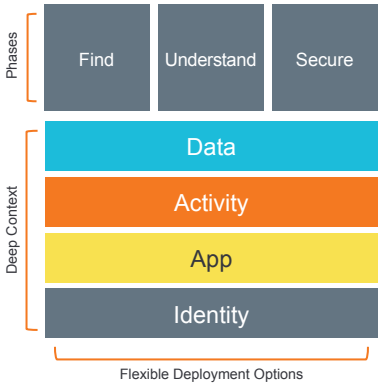
After you understand which apps you have and what activities people are performing in those apps, you can enforce granular policies to protect data and comply with regulations. You can enforce those policies in context, specifying policies like "Encrypt all content matching my 'confidential' DLP profile in cloud apps," "Block the download of any .exe file from a cloud storage app," or "Alert on the download of PII from any HR app to a mobile device." This helps you narrow the policy aperture to a particular activity or a particular type of content you're trying to protect. It also helps you effectively minimize false positives and be precise in your control. Beyond simply enforcing policies, Netskope lets you coach users to a desired behavior with customizable automated messages in the product. For example, you can say "You are uploading a sensitive document to Zippyshare. We have standardized on Box for corporate usage. Here is the URL to sign up," or even redirect the user to the correct app.

Netskope lets you enforce policies based on activities such as:

- Access Denied
- Admin activities
- Approve
- Attach
- Create
- Delete/delete all
- Detach
- Download/download all
- Export
- Follow
- Invite
- Join
- Logout
- Mark/Markup
- Move
- Invite
- Login Attempt/Login Successful/Login Failed
- Logout
- Print all
- Route
- Reboot
- Post
- Send
- Share
- Start
- Stop
- Sync/restore
- Unblock
- Upload/import
- View/view all

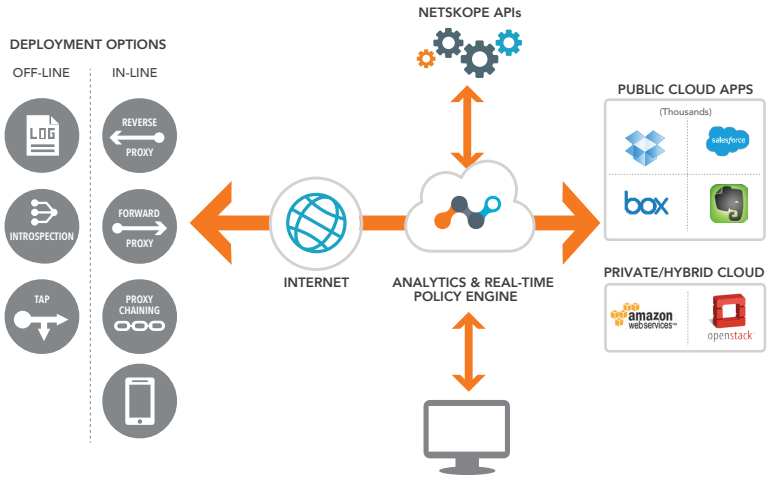
The Power of the Platform

The power of the Netskope Active Platform is brought about by the rich set of contextual details it surfaces. It starts with identity, which includes information about the user, their AD group membership, device, browser, and location. Then it layers in app information, at the app instance, or the category level. Then it takes activity into consideration: is the user sharing content outside of the company? Downloading PII? Uploading ePHI? Finally, it pulls in the data: What is the content? A record? A link? A file? If so, what kind of file? What is the name of this file? Does it trigger your DLP profile for PII? Anytime you perform a query or enforce a real-time policy, you can be very precise and granular with that contextual information in order to really understand your risk in its entirety and enforce policies that address the real risk, while still allowing the app.



Future-proof Architecture

Organizations may start with one safe cloud enablement use case today, but their needs will grow. They need a variety of deployment options and a scalable way to add additional apps to their visibility and control matrix so they can future-proof their investment. For example, you might want to start with a reverse proxy deployment to address your web users but then expand that to ensure that you address users with native clients too.



Unlike other vendors whose product capabilities are dependent on their deployment architecture, Netskope's core product engine is abstracted from the way the solution is deployed. We are the only vendor with customers in production across every deployment architecture offered in the market today, including log-based discovery, introspection, inline as a reverse proxy, inline as a forward proxy, inline with or without agents or mobile profiles, in secure TAP mode, in proxy-chaining mode, and even as a secure, on-premises appliance.

Furthermore, Netskope's modular data plane abstracts our analytics and policy enforcement engine from our support for cloud apps. This means that we can add new apps and facilitate additional deployment options now and in the future.

Secure, Highly-Available Cloud

The data analysis and policy enforcement components of the Netskope Active Platform are located in geographically distributed Equinix data centers around the world. Data centers have redundant, multi-Gbps Internet links that peer directly with all major carriers. The infrastructure is SSAE-16 certified and carries ISO and LEED certifications for safety and green data center standards. Netskope has certified its software deployment as SOC-1 Type I and II, and SOC-2 Type I and II through independent, third-party auditors.

Netskope Discovery, Active Platform, Active DLP, and Active Encryption

Netskope offers Netskope Discovery, an offline, log-based discovery solution, as well as the Netskope Active Platform, and Netskope for Featured Apps that provide safe cloud enablement for a variety of specific cloud applications such as Box, Dropbox, Egnyte, Google Apps, Office 365, and Salesforce. Netskope Cloud DLP and Netskope Encryption can be added to round out configurations. See table, below, for specific functionality of each.

CAPABILITY	NETSKOPE DISCOVERY	NETSKOPE ACTIVE PLATFORM	NETSKOPE FOR FEATURED APPS
	FIND		
Discover all cloud apps	•	•	•
Cloud Confidence Index	•	•	•
Baseline visibility of cloud app activites	•	•	•
Deep visibility of cloud app activities	Requires TAP interface or Active Deployment	•	Requires TAP interface or Active Deployment
Discovery of stored data		Requires App Introspection	•
	UNDERSTAND		
Risk Dashboard	•	•	•
Anomaly detection	•	•	•
Custom reports	•	•	•
Custom reports with AD integration	•	•	•
Alert watchlists	•	•	•
	SECURE		
Real-time, granular control of all cloud apps		•	•
Control stored data in sanctioned apps		•	•
Cloud DLP		Requires Netskope Active Cloud DLP	Requires Netskope Active Cloud DLP
Leverage on-premises DLP		•	•
Strong Encryption		Requires Netskope Active Encryption	Requires Netskope Active Encryption
Leverage on-premises HSM		•	•
Geo-location-based policy enforcement		•	•
Device-level access control		•	•
User coaching		•	•
Data quarantine		•	•
Legal hold		•	•
Ensure privacy with role-based access control, data obfuscation, and filtering of certain kinds of traffic (e.g., app activity using personal credentials)		•	•
Integrate with AD to manage and secure apps and data within the context of users and groups		•	•

FLEXIBLE DEPLOYMENT OPTIONS

- On-prem log parser
- TAP interface
- Agentless forwarder
- On-prem appliance (all data is maintained on customer premises)
- Reverse proxy
- Thin agent
- Mobile profile