netskope

The Netskope Advantage:

Three "Must-Have" Requirements for Cloud Access Security Brokers

Gartner has placed the CASB category as number one atop its information security priorities, emphasizing that "the time is now" for organizations to get their cloud security strategies ironed out.

Organizations are adopting the cloud in a big way. Cloud apps or Software-as-a-Service (SaaS), the most prevalent segment of cloud, are easy to procure, deploy, and use, letting people work faster and more flexibly than ever. Whether cloud apps are sanctioned or unsanctioned, IT remains responsible for safely enabling them. But how do you ensure security? Govern administrator and user access, activities, and privileges? Protect sensitive data?

Cloud Access Security Broker (CASB) is a new market category that addresses these issues. Cloud-adopting organizations of all sizes and industries are adopting CASBs. Gartner has placed the category as number one atop its information security priorities, emphasizing that "the time is now" for organizations to get their cloud security strategies ironed out at its recent Security and Risk Management Summit. While there are a handful of CASB vendors in the market, only one is built from the ground-up to give you three must-have requirements for successful cloud security: Noise-cancelling cloud data loss prevention (DLP), surgical visibility and control of sanctioned and unsanctioned apps, and a future-proof architecture.

This document will provide a short overview of these requirements and explain why Netskope is the best choice for your cloud needs.

Before we proceed, it's important to note that many vendors are essentially the same when it comes to discovering and rating cloud apps. That fact doesn't diminish the importance of this step, and Netskope handles it very well. That said, we see discovery as the starting point, and then take you to that crucial next step, enabling you to understand and mitigate risk, prevent data loss, and enforce policies in a holistic way, with or without an agent.

3 CASB Requirements

1. Noise-cancelling DLP

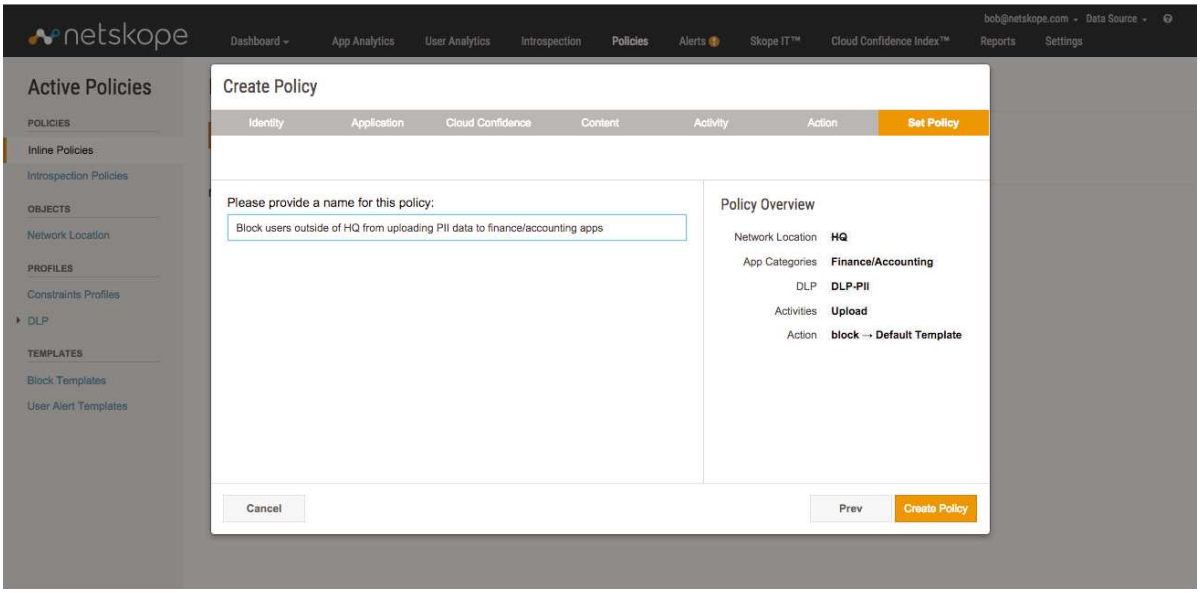
Organizations need to identify and protect sensitive data in the cloud accurately, efficiently, and in a way that takes advantage of their existing on-premises DLP solutions.

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+ data identifiers, support for 500+ file types, custom regular expressions, proximity analysis, international support such as double-byte characters, and document fingerprinting, which reduce false positives and increase detection accuracy.

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.

Another "only" is that we offer critical DLP workflows such as content quarantine, legal hold, automatic elimination of public access to sensitive content, and event visualization in corporate SIEM systems, which enable 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.



2: Surgical visibility and control for sanctioned and unsanctioned apps

Organizations need to say "yes" to apps while blocking risky activities and govern cloud app usage without disrupting business.

Organizations need to be surgical in what they look for and control. Rather than take an "allow" or "block" stance to cloud apps, why not say "yes" to useful apps, but just govern the access, activities, and data? This means offering granular access control to apps in a sanctioned suite by device classification or saying "no" to sharing content outside of the company if the user is an "insider." Organizations need to be able to do this across both sanctioned AND unsanctioned apps, and regardless of device type and whether users are on-premises or remote.

Only Netskope provides surgical, or fine-grained, visibility and control for both sanctioned and unsanctioned apps.

For sanctioned apps, only Netskope provides full-spectrum governance across access, activities, and data. This includes the ability to see all app activities, their surrounding context, and any anomalous usage in sanctioned apps and their ecosystems. It also means organizations can use device classification to enforce granular access policies – with or without an agent (e.g., "Offer full suite access to users on corporate-issued devices, but webmail only to those on BYOD").

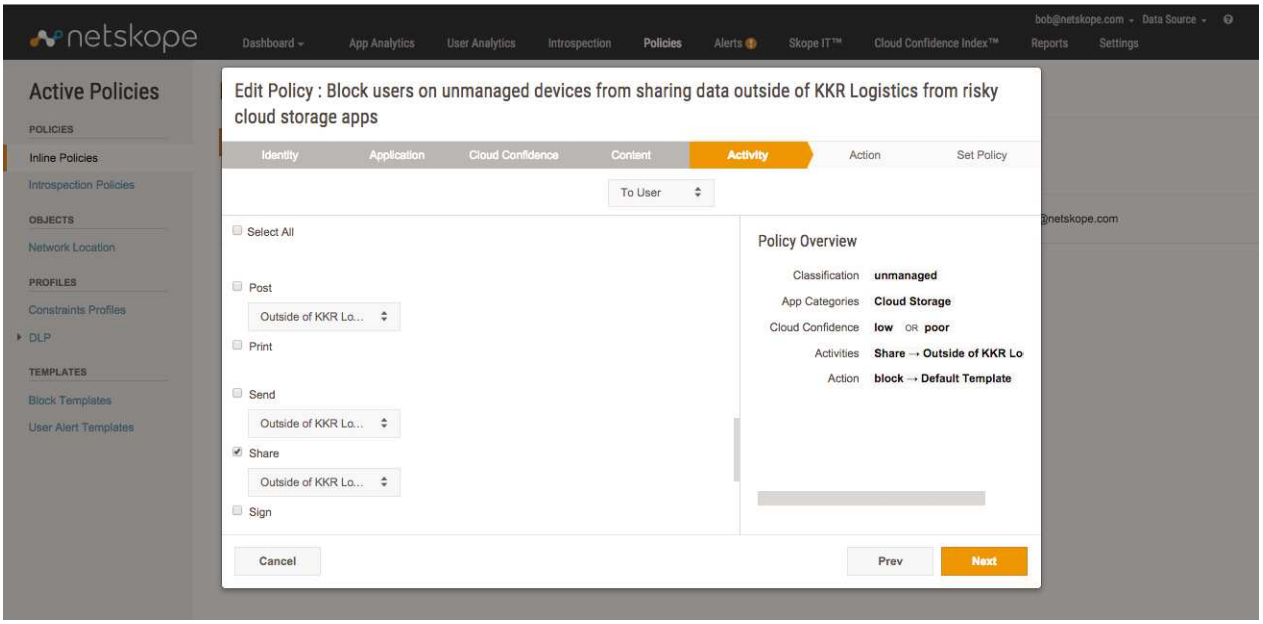
Furthermore, only Netskope enables organizations to govern activities in sanctioned apps and their ecosystems (e.g., "Don't let anyone in AD group 'corporate insiders' share content outside of the company."), and coach users with automated messages that provide insight into the policy violation, redirect them to an alternative app if needed, and allow them to enter a business justification or report a false positive.

Netskope discovers and protects sensitive data at rest within sanctioned apps, as well as en route to or from those apps and their ecosystems. Moreover, we enforce granular, contextual administrative privileges, enabling organizations to support a "least privilege" security model.

For unsanctioned apps, only Netskope provides visibility and control at the app, category, or globally. This includes the ability to see all cloud activities and their surrounding context, and pivot on any factor to see "Who shared data outside of the company from any app?" or "Did anyone from a remote Customer Support office download records from our CRM?" Also, Netskope can enforce access, activity, and data policies in a set-it-once way across an app or category, including on native clients on laptops, tablets, and smartphones, whether users are on-premises or remote, and even based on device classification.

Only Netskope enables contextual policies like "No sharing outside of the company," "No download of PII to a mobile device," and "No access to CRM if you're outside of the country," which let IT mitigate risk without breaking business process. Moreover, coach users with automated messages that provide insight into the policy violation, redirect them to an alternative app if needed, and allow them to enter a business justification or report a false positive.

Whether across sanctioned or unsanctioned apps, only Netskope provides this level of visibility and control whether the user is in a web-based app, on native clients on laptops, tablets, and smartphones, and on-premises or remote.



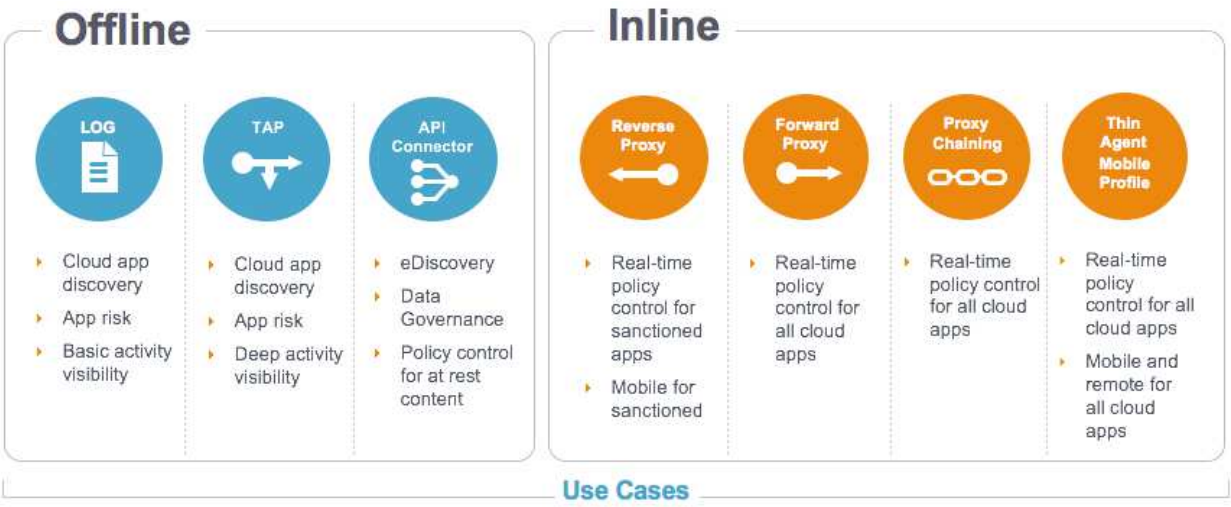
3: Future-proof architecture

Organizations need to address their cloud security needs today and in the future.

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.

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.



About Netskope

Netskope™ is the leader in safe cloud enablement, and the leading CASB vendor. We are a Gartner Cool Vendor, a top 10 CIO Magazine cloud security company, and have been featured in key media outlets including CBS News, the Wall Street Journal, and Forbes.