

At a glance:

Essential CASB pillars:

- › Visibility
- › Compliance
- › Data security
- › Threat protection

The Netskope difference:

- › Granular policies for all apps
- › Advanced, enterprise DLP
- › Architected for any use case
- › Threat protection built for the cloud

Safely enable sanctioned apps including

- › Box
- › Dropbox
- › Google Apps for Work
- › Microsoft Office 365
- › Salesforce
- › ServiceNow

...and secure shadow IT!

Cloud with Confidence

On average, enterprise organizations now have over 900 cloud apps in use by employees. Cloud apps are great for businesses because of their convenience, ease of use, and management, but present problems related to data breaches, failed audits, and potential for loss of sensitive data and corporate IP. Security professionals need a way to gain visibility into and secure cloud use for full employee productivity and collaboration.

As the leading cloud access security broker (CASB), Netskope™ helps organizations go cloud-first in a secure and compliant fashion.

Visibility

- › Provide visibility into all cloud apps in use by organization, including shadow IT
- › Understand all contextual details of cloud use including user identity, action performed (upload, share, download, etc.), location, device, and more

Compliance

- › Use cloud forensics to track and audit all cloud activity by employees, regardless of location or device
- › Comply with regulations such as SOX, FINRA, HIPAA, and more with security policies, auditing, and access controls
- › Fulfill data residency requirements with cloud, hybrid, and on-premises deployment options

Data security

- › Govern cloud usage with granular access controls over sanctioned and unsanctioned cloud apps based on activity, device, user, category, and more
- › Apply policies across all users and encrypt data regardless of device or location
- › Utilize advanced, enterprise Cloud DLP that integrates with on-premises DLP systems

Threat protection

- › Scan for malware in real-time or for data already at-rest in sanctioned apps
- › Remediate threats with integrated workflows to quarantine infected files
- › Identify anomalies using machine intelligence such as data exfiltration or compromised credentials

Leading enterprises trust Netskope



The Netskope Difference

Granular policies for all apps

Say “yes” to apps while blocking risky activities and governing cloud app usage without disrupting business.

Netskope sees all app traffic and can enforce policies such as encrypt, block, and more across all apps, sanctioned and unsanctioned. Netskope uses context like user, group, location, and data across 50+ activities performed in apps such as “download,” “share,” “edit,” and more.

Advanced, enterprise DLP

Identify and protect sensitive data across sanctioned and unsanctioned apps accurately, efficiently, and in a way that integrates with existing on-premises DLP solutions.

Utilize advanced capabilities such as 3,000+ data identifiers, support for 500+ file types, custom regular expressions, proximity analysis, international support such as double-byte characters, exact match, and fingerprinting. Netskope also reduces detection surface area using context (user, location, activity, etc.).

Architected for any use case

Address cloud security needs today and in the future.

Netskope’s multi-mode architecture supports any use case, including every possible offline and inline, including all agent-less, modes. Choose from a cloud, hybrid, or on-premises deployment with enterprise-grade scalability.

Threat protection built for the cloud

Find and remediate cloud malware and threats.

Netskope is the only CASB that combines threat intelligence, static and dynamic malware analysis, and remediation of threats that may originate from—or be further propagated by—cloud apps. Scan and remediate threats in real-time when an employee tries to share or upload an infected file or detect and prevent unauthorized access to cloud apps and data.

About Netskope

Netskope™, the leading cloud access security broker (CASB), helps enterprises find, understand and secure sanctioned and unsanctioned cloud apps. Through contextual awareness and a multi-mode architecture, Netskope sees the cloud differently. This results in the deepest visibility and control, the most advanced threat protection and data loss prevention and an unmatched breadth of security policies and workflows. The world’s largest companies choose Netskope, the only CASB that ensures compliant use of cloud apps in real-time, whether accessed on the corporate network, remotely or from a mobile device. With Netskope, enterprises move fast, with confidence. To learn more, visit <https://www.netskope.com>.