Netskope Active Platform

TOP USE CASES AT A GLANCE

- Discover cloud services in use and assess risk
- Safely enable cloud services instead of being forced to block them
- Gain visibility whether users are on premises, remote, or via sync clients or mobile apps
- Protect sensitive data with advanced, enterprise data loss prevention (DLP)
- Guard against cloud threats and malware
- Secure your sanctioned cloud service such as Office 365, Box, Amazon AWS, etc.

As people become more mobile, collaborate more freely, and shift more of their data to the cloud, enterprises need a security platform that governs usage and protects data while maintaining security and compliance.

PRODUCT OVERVIEW

Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real-time, whether accessed from the corporate network, remotely, or from a mobile device. This means that IT Security admins can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and an unmatched breadth of workflows, the largest companies in the world trust Netskope.

Understand

Understand all cloud services, activities, and data

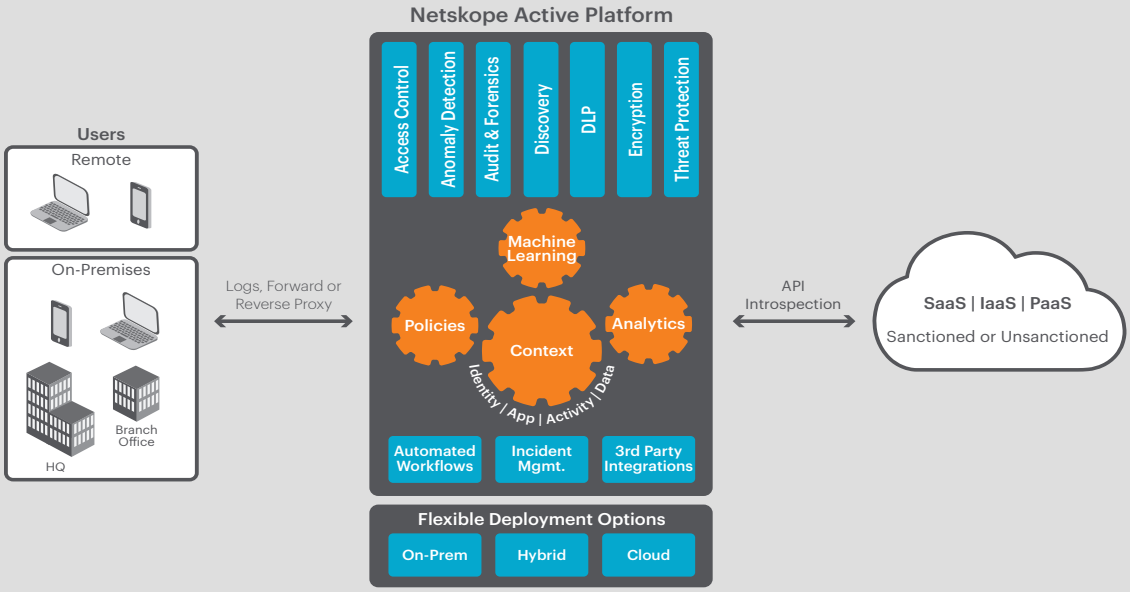
Protect

Protect sensitive data and stop online threats

Respond

Respond to incidents immediately and thoroughly

Security Evolved



Netskope offers the industry's only all-mode architecture that supports any use case from an API-only deployment mode to several inline options. Get complete visibility of the cloud, including traffic from sync clients and mobile apps and SSL-encrypted traffic. Leverage a 100% cloud deployment, an on-premises appliance, or hybrid deployment.

	Access method	Discover	Govern usage	Secure data	Protect against threats	
Logs	◔	● ●				NEAR REAL-TIME
API introspection	●		●	●	●	
Reverse proxy	◒		●	●	●	REAL-TIME
Forward proxy	●	● ●	● ●	● ●	● ●	

● Browser, remote, mobile and desktop apps, sync clients ◒ Browser and remote ◔ Browser ● Sanctioned ● Unsanctioned

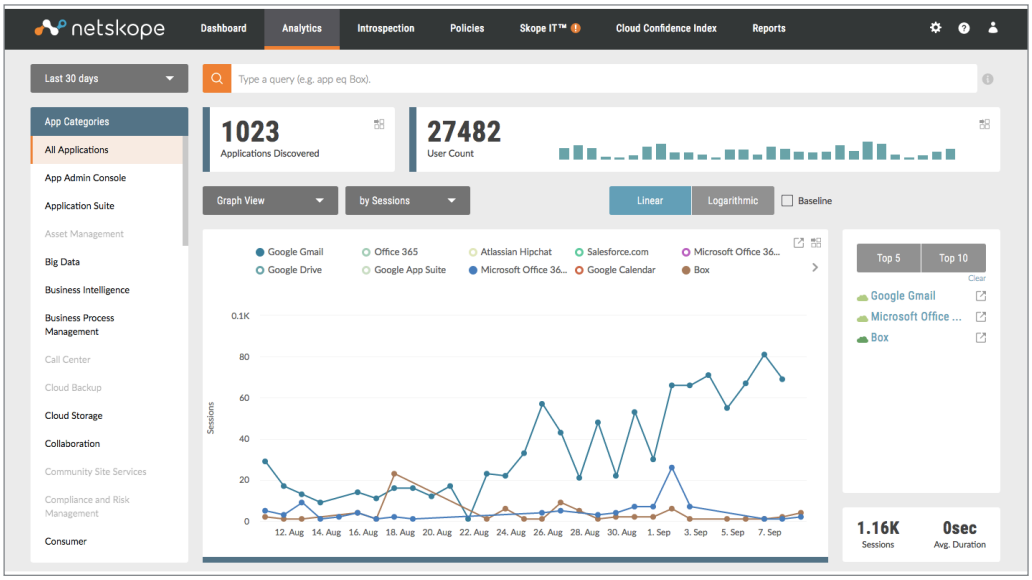
NETSKOPE DIFFERENTIATORS

Granular policies for all services
Use context — user, device, location, activity — for fine-grained control

Complete view of cloud transactions
All-mode architecture provides full use case coverage

Advanced, enterprise DLP
Protect sensitive data with the industry's most advanced DLP

Threat protection built for the cloud
Stop cloud threats and malware, including ransomware



Netskope Active Platform Features

CLOUD SERVICE DISCOVERY AND RISK ASSESSMENT	
Risk Dashboard	A comprehensive view of cloud risk from all cloud services (including ecosystem services, IaaS, and PaaS), activities, users, and devices. Granular enough to differentiate between instances of the same service.
Netskope Cloud Confidence Index (CCI)	The enterprise readiness of cloud services based on criteria like security, auditability, and business continuity. Serves as a guidepost to mitigate risk, influence usage and reduce costs.
Cloud forensic analysis	Deep visibility to understand user activities in services. Drill down into granular details including identity, device, browser, time, location, activity (e.g., 'share'), content, and more for a full audit trail.
Ad hoc queries and dynamic reports	Perform ad-hoc queries for on-demand analytics and reports, save queries as custom search results, or generate detailed custom reports using natural language inputs and Boolean operators.
GRANULAR VISIBILITY AND CONTROL OF SANCTIONED AND UNSANCTIONED SERVICES	
Real-time policies for all services	Security and access policies in context (e.g., service, activity, device). Policies can block, alert, bypass, encrypt, quarantine, and coach. Works with sanctioned or unsanctioned services, IaaS and PaaS.
Netskope Context Engine (NCE)	Real-time cloud activity details in context of users, devices, locations, dates, times, and content. Based on patented technology that decodes API transactions.
User and remediation workflows	Use built-in workflows such as quarantine, legal hold, and user coaching with custom messages. Workflows are specific to policies and capabilities, like automatic tombstoning of malware.
ENCRYPTION AND TOKENIZATION	
Encrypt structured data	Encrypt structured data at rest or in real time in sanctioned services through Netskope native format-preserving encryption with AES-256 encryption and a FIPS 140-2 Level 3-certified key management service and the option of leveraging your on-prem HSM.
Encrypt structured data via BYOK	Leverage pre-built integrations with cloud service provider bring your own key (BYOK) capabilities with AES-256 encryption and a FIPS 140-2 Level 3-certified key management service and the option of leveraging your on-prem HSM.
Encrypt unstructured data	Encrypt unstructured data at rest in sanctioned services or in real-time activities with AES-256 encryption and a FIPS 140-2 Level 3-certified key management service and the option of leveraging your on-prem HSM.
Tokenization	Tokenize data at rest or in real time in sanctioned services through Netskope native formatted-field tokenization

ADVANCED, ENTERPRISE DLP	
Context-aware DLP	Prevent data leakage from sanctioned, unsanctioned, and mobile apps. Supports 500+ file types, 3,000+ data identifiers, proximity analysis, fingerprinting, exact match, and more.
eDiscovery and control of sensitive data at rest	Find sensitive data resident in sanctioned services such as Microsoft Office 365 OneDrive, Box, Google Drive, Dropbox, and more. Take action on data that violates policy.
Closed-loop incident management	Respond quickly and thoroughly to cloud service policy violations, with workflows to facilitate end-to-end incident management process, detailed forensics, and event-by-event incident history.
Compliance templates	Leverage dozens of pre-defined policy templates to identify sensitive data in accordance with regulations. Templates include (but are not limited to): AMRA, EC Directive, EU-GDPR, GLBA, HIPAA, PCI-DSS, PHI, PII, PHIPA, PIPEDA, SSN Confidentiality Act, US FTC Rules, etc.
Role-based access controls	Customizable role-based access controls, including predefined admin. and analyst roles. Additional privacy controls include data obfuscation and automatic filtering of certain kinds of traffic.
CLOUD THREAT AND MALWARE PROTECTION	
Threat intelligence for malicious sites	Identify malicious sites that your employees may be visiting and block them. Threat intelligence is updated dynamically using multiple sources.
Anomaly detection	Identify and remediate anomalous user behavior such as compromised credentials, data exfiltration, insider threats, privileged account access abuse, and more.
Cloud malware protection and remediation	Detect and block or quarantine infected files and replace with tombstone files. Remediation options include blocking and quarantining as well as analysis and response workflows. Layered detection approach includes static and heuristic analysis, machine learning, and sandboxing.
ARCHITECTURAL ADVANTAGE	
All-mode architecture	Supports all out-of-band and inline modes. Industry's only visibility and control for unsanctioned services. Modes are often deployed in conjunction with each other to cover key use cases.
Cloud-scale infrastructure	Unlike traditional security tools limited by the compute, storage, and I/O available in a physical appliance, the Netskope platform has virtually infinite resources and scalability.

INTEGRATIONS

Productivity Suites
Microsoft, Google, Box

Single sign-on (SSO)
Ping Identity, Centrify, Okta, OneLogin

Cloud Storage
Microsoft Office 365 OneDrive, Google Drive, Box, Dropbox, Egnyte, Intralinks

Enterprise mobility management
AirWatch by VMware, Citrix, Microsoft, MobileIron

Data classification
Boldon James, Box, TITUS

Security and threat
Carbon Black, Cyphort, FireEye. For more general integration capabilities, Netskope supports STIX/TAXII standards.

On-premises DLP
Via secure ICAP with Digital Guardian, McAfee DLP Prevent, Symantec Network Prevent DLP, and Forcepoint (Websense) TRITON AP Data

Enterprise
Leverage your existing investment in enterprise tools like firewalls and proxies, SIEM, directories, and more as part of an integrated cloud security solution. Netskope also offers a REST API for general use.

Other
Amazon Web Services, Google Cloud Platform, ServiceNow, Slack, Salesforce

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.