# Netskope Security Cloud Platform
## Data-centric. Cloud-smart. Fast.

### TOP USE CASES AT A GLANCE

- Discover SaaS, IaaS, and web use details and assess risk

- Secure your managed cloud services such as Office 365, G Suite, Box, and AWS

- Safely enable unmanaged, business-led cloud services instead of being forced to block them

- Govern cloud and web use for users on-premises, mobile, and remote

- Guard sensitive data with award-winning DLP

- Stop elusive cloud threats and malware
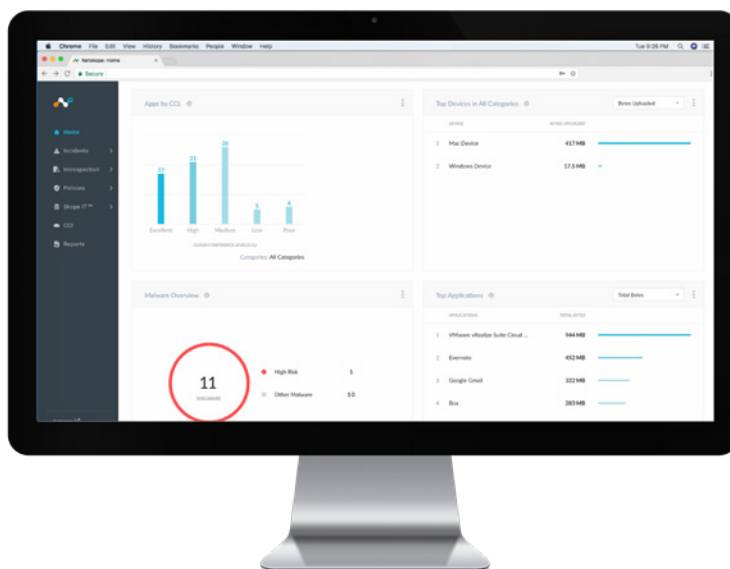


The cloud is transforming your organization. It's changing how you work as everything is becoming more intuitive, connected, open, and collaborative, and that change is rippling across SaaS, IaaS, and web environments. This creates new challenges and risks that legacy security solutions can't address. You need security that can protect your data and users, wherever they are.

### PRODUCT OVERVIEW

Using patented technology called Netskope Cloud XD™, the Netskope Security Cloud eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud (SaaS and IaaS) services and millions of websites. With full control from one cloud, our customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection that stops elusive attacks.

# The Netskope Security Cloud Platform
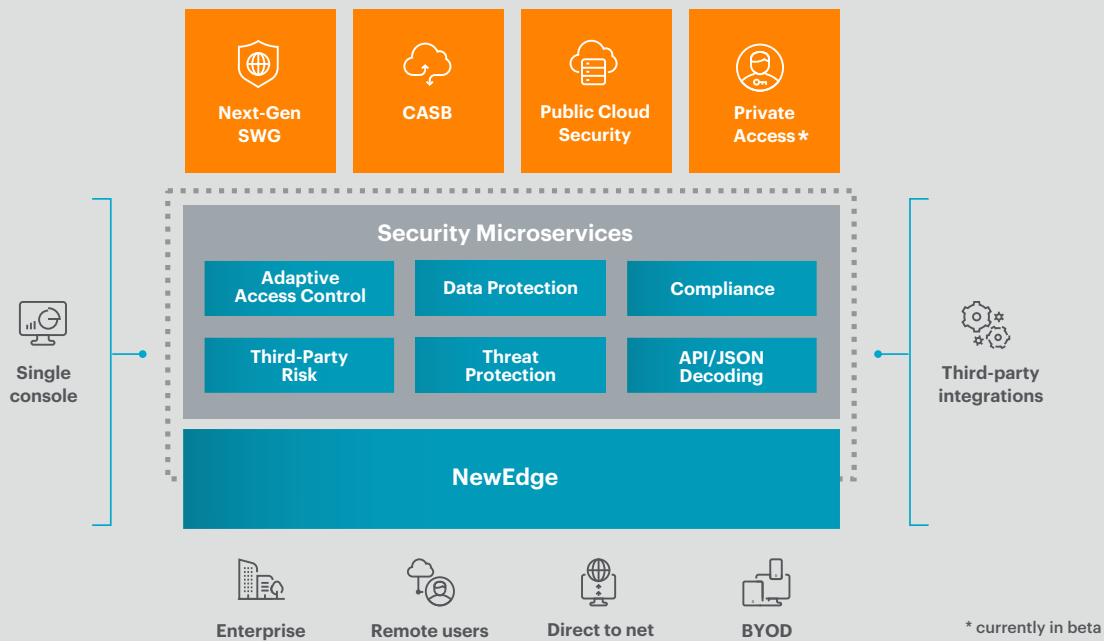


Netskope deployment options support any use case, from an API-only deployment mode to several real-time options. Get complete visibility of all SaaS, IaaS, and web traffic, including from sync clients, mobile apps and TLS-encrypted traffic. Deploy 100% in the cloud, with an on-premises appliance, or a hybrid option.



## THE NETSKOPE DIFFERENCE

### Data-centric

Netskope takes a 360 degree data-centric approach to cloud security, protecting data and users everywhere using award-winning DLP and encryption.

### Netskope Cloud XD

Netskope Cloud XD™ understands SaaS, IaaS, and web in extreme definition to monitor all cloud activity, eliminate blind spots and stop elusive attacks and malware.

### Fast

Netskope gives you optimal performance and responsiveness. Delivered through the NewEdge infrastructure, you benefit from one of the world's largest, high performance networks to protect your environment.
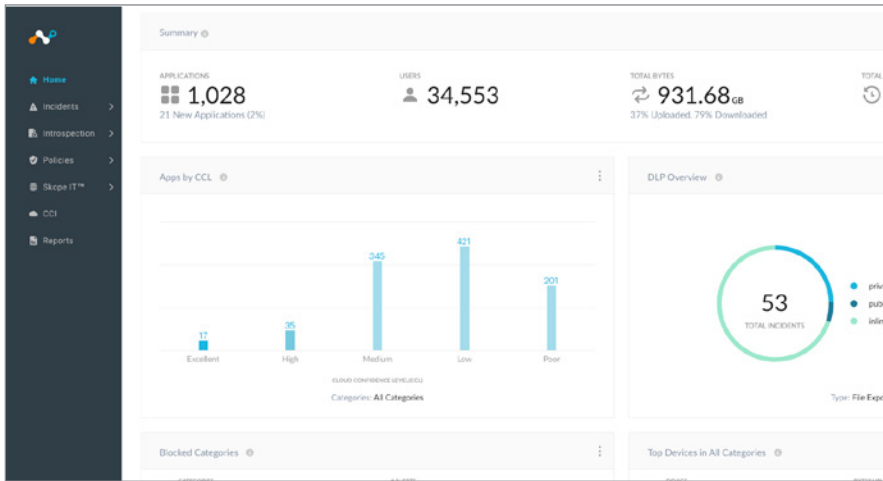
**THE NETSKOPE CONSOLE**

The industry's only unified SaaS, IaaS, and web security platform built from the start in one cloud that's easy-to-use. Unlike cobbled-together tools, Netskope eliminates policy conflict through standardized categories across SaaS, IaaS and web. Save your security team's time by avoiding redundant DLP and threat protection configuration steps and having to switch from one tool to the next. Built in the cloud from day one, Netskope scales automatically to meet your needs.

# Netskope Security Cloud Features

| SAAS, IAAS, WEB DISCOVERY AND RISK ASSESSMENT | |
|---|---|
| Customizable Dashboard | A customizable view of all SaaS, IaaS, and web, activities, users, and devices. Granular enough to differentiate between instances of the same SaaS or IaaS service. |
| Netskope Cloud Confidence Index (CCI) | The enterprise-readiness of SaaS and IaaS services based on 50+ criteria like security, auditability, and business continuity. Serves as a guidepost to mitigate risk, influence usage and reduce costs. |
| Forensic analysis | Deep visibility to understand user activities in SaaS, IaaS, and web. 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 SAAS, IAAS, AND WEB** | |
| Netskope Cloud XD™ | Netskope Cloud XD understands all inputs in extreme definition (XD) and performs big data analytics to eliminate blind spots and make policy enforcement simple across all SaaS, IaaS, and web. |
| Real-time policies for all SaaS, IaaS, and web | Security and access policies in context (e.g., service, activity, device). Policies can block, alert, bypass, encrypt, quarantine, and coach. Works with web and managed and unmanaged SaaS and IaaS services. |
| Unified policies for SaaS, IaaS, and web security | Simplify deployment and ongoing management by orchestrating all SaaS, IaaS, and web policies from one interface. |
| Web classification and content filtering | Govern web use with comprehensive web classification and content filtering. Best-in-class URL database covers 99.9% of the web, intelligence that comes from a dedicated in-house web and cloud application research team, and machine learning-based content analysis for classification of uncategorized URLs. |
| 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 managed services through native format-preserving encryption w/ AES-256 encryption and a FIPS 140-2 Level 3-certified KMS and the option of using your on-prem HSM. |
| Encrypt structured data via BYOK | Leverage pre-built integrations with CSP's bring your own key (BYOK) capabilities with AES-256 encryption and a FIPS 140-2 Level 3-certified KMS and the option of using your on-premises HSM. |
| Encrypt unstructured data | Encrypt unstructured data at rest in managed services or in real-time activities with AES-256 encryption and a FIPS 140-2 Level 3-certified KMS and the option of using your on-premises HSM. |

| | |
|---|---|
| **Reduce false positives** | Prevent data leakage from SaaS, IaaS, and web with accuracy and precision. Supports more than 1,000 file types, more than 3,000 data identifiers, proximity analysis, fingerprinting, exact match, OCR, and more, instrumented using a flexible and intuitive wizard-style interface. |
| **Find and control sensitive data at rest** | Find sensitive data resident in managed services such as AWS, 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 policy violations, with workflows to facilitate end-to-end incident management process, detailed forensics, and event-by-event incident history. |
| **Compliance templates** | Use 40 predefined 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. |

## THREAT PROTECTION

| | |
|---|---|
| **Threat intelligence for malicious sites** | Use 40 threat intelligence feeds to 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 near real-time and real time modes. Industry's only visibility and control for web as well as managed and unmanaged SaaS and IaaS. Modes are often deployed simultaneously 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, built upon the NewEdge network infrastructure, provides virtually infinite resources combined with high-performance and scalability. |

## INTEGRATIONS

**Productivity Suites**
Microsoft, Google, Box

**Single Sign-on (SSO)**
Ping Identity, Centrify,
Okta, OneLogin, Microsoft, SecureAuth

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

**Enterprise Mobility  Management**
AirWatch by VMware, Citrix, IBM, Microsoft,
MobileIron

**Data Classification and IRM**
Boldon James, Box, Microsoft, TITUS, Vera

**Security and Threat**
Carbon Black, Cylance, Cyphort, FireEye,
Juniper. 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**
Utilize 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, Demisto, Exabeam,
Google Cloud Platform, Microsoft Azure,
ServiceNow, Slack, Salesforce, Splunk, Sumo
Logic, Workplace by Facebook

**netskope**

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.