SOLUTION BRIEF

Netskope for Google Cloud

Gain visibility and security of your Google Cloud estate including IaaS deployments and Google Workspace SaaS applications as well as cloud services from other vendors. Receive alerts and real-time insights into vulnerabilities and threats from a single console so you can take immediate action to protect your applications, data, and operations.

KEY USE CASES

- **Protect data at rest:** Discover and protect sensitive data at rest in Google Cloud Storage and Google Workspace applications. Ensure sensitive data is encrypted and not publicly exposed.
- **Control user collaboration in real-time:** Enforce granular zero-trust access to Google Cloud accounts and Google Workspace applications. Prevent sharing of sensitive data with unauthorized parties, non-IT-led accounts, and non-compliant devices.
- **Detect and prevent cloud threats:** Scan Google Cloud Storage to discover malware and threats. Surface and block malware and cloud-enabled threats such as insider threats, compromised accounts, and anomalous user behavior and share findings with Google Security products.
- **Visibility into non-IT-led accounts:** Discover and gain visibility into non-IT-led accounts and suspicious activities.
- **Cloud security posture management:** Continuous security posture assessment of Google Cloud deployments to reduce risk and maintain compliance.
- **Continuous conditional access:** Use Netskope visibility into user risk to control access to applications from BeyondCorp Enterprise enrolled devices.
- **Scan, monitor, investigate, and audit:** Push rich, contextualized log data to Google Security Command Center, Chronicle, Siemplify, and Google Cloud Storage.

THE CHALLENGE

Enterprises are rapidly moving workloads and sensitive data into public and shared cloud infrastructure, increasing the attack surface, risk of data loss, and exposure to threats and malware. Netskope for Google Cloud provides organizations with the visibility, compliance, and protection for critical workloads needed to combat these challenges. Netskope enables you to understand your risk exposure, inventory assets, detect misconfigurations, enforce compliance standards, prevent malware attacks, and block data exfiltration attempts.

NETSKOPE FOR GOOGLE CLOUD

Understand the risk to your enterprise and strengthen your security posture across Google Cloud solutions. Netskope and Google security tools leverage Netskope Security Cloud findings for user and data behavior across public cloud and SaaS applications. Netskope provides controls over risky activities and sensitive data, enabling the safe use of Google Cloud. Through complementary solutions, Netskope and Google Cloud deliver continuous zero trust access to cloud services.

CAPABILITIES

COMPLETE VIEW OF GOOGLE CLOUD SOLUTIONS AND APPS

Netskope provides deep visibility into Google Cloud instances, resources, and services, Google Workspace application usage, and all apps in use within your organization. Security teams can view consolidated usage or drill down through each application and instance for granular details. Netskope instance awareness separates real-time interactions between IT-led services from non-IT-led, and malicious actor resources.

Using this information, analysts can discover hidden risks in user activity, data movement, and data usage in services such as Google Storage, BigQuery, Gmail, Google Drive, and other Google Workspace apps. They can also drill down into events from Google Cloud services, such as BigQuery or Google Storage, via stackdriver log integrations, and investigate activity-level audit trails to determine unusual usage by individuals or objects.

Netskope for Google Cloud gives you granular visibility into Google Cloud and Google Workspace activities including the movement of sensitive data both inside and outside of your organization.

GRANULAR SECURITY ACCESS POLICIES

Today's hybrid employees demand the freedom to use their own personal devices while working. Allowing these devices to access sensitive cloud-based corporate resources and data can increase organizational risk. Netskope enables organizations to apply granular access policies across Google Cloud deployments, Google Workspace applications, employee devices, and sensitive data. This prevents sensitive data from going where it shouldn't, and constrains access and changes to critical resources. Netskope provides and compares both API-based and inline inspection into cloud traffic, discovering contextual information that can be utilized by security teams to define granular security and compliance controls that are purpose built for Google Cloud. When users behave in a risky manner, Netskope can work with Google BeyondCorp enterprise to constrain cloud access from users' enrolled devices.

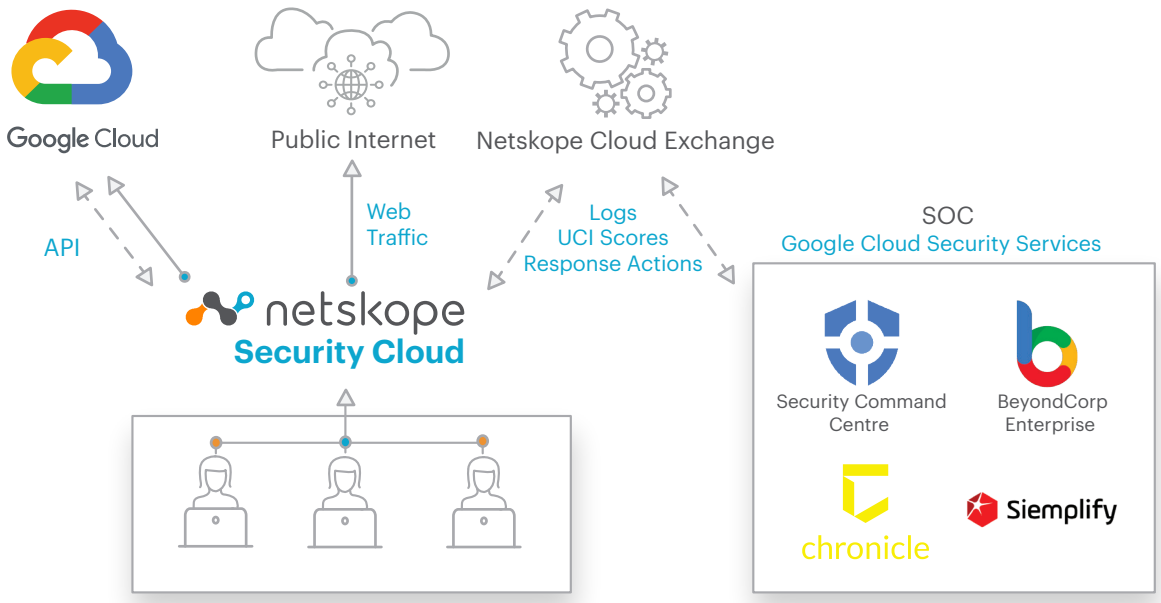
Netskope for Google Cloud enables creation of granular security policies for deep contextual control of your Google Cloud environment.

Teams can continuously remediate security gaps and actively enforce compliance standards using CIS benchmarks and best practices. Security and data protection controls can be modified on-the-fly with information from real-time interactions with Google Cloud resources. Resource access policies can also be extended to constrain data movement between IT-led and non-IT led instances, or within IT-led deployments.

ADVANCED DATA LOSS PREVENTION

Data is increasingly at risk as applications and users move beyond traditional enterprise security perimeters. As employees collaborate, they can inadvertently share or expose sensitive data outside of protected data stores. Born in the cloud, Netskope provides cloud-native data loss prevention (DLP) that protects sensitive data wherever it travels—out to any SaaS application, IaaS service, or website. Netskope empowers security admins to define granular DLP rules that ensure employees using Google Cloud services and resources don't violate corporate security policies.

Netskope has the most advanced DLP capability in the industry, designed for high accuracy and low false positives. With over 3,000 data identifiers, Netskope DLP supports more than 1,500 file types, custom regular expressions, proximity analysis, finger-printing, exact match, and optical character recognition (OCR). Netskope helps customers automate complex and manual policy configuration by providing more than 40 pre-built policy templates (PCI, HIPAA, GDPR, etc). Organizations can quickly customize pre-built templates to fit their unique requirements.



CLOUD THREAT AND MALWARE PROTECTION

Driven by the work from anywhere revolution, enterprises are rapidly moving their critical applications and data to the cloud, attracting unwanted attention from cloud-savvy cybercriminals. Legacy security tools are unable to function properly in the cloud, exposing companies to increasing cloud risk.

Netskope's cloud-native security solutions provide detailed visibility and threat detection for cloud-based deployments and applications. Netskope's Threat Labs specialize in analyzing the latest cloud threats to fortify layered protections against malware and persistent attacks. Netskope also leverages threat indicators from Google Cloud security services to further enhance protection for data flowing to, from, or between cloud services.

SHARE ACTIONABLE TELEMETRY

Netskope for Google Cloud prevents advanced threats, malware, and data leakage, filters URLs by category, and controls app usage by user, location, and device. Use Netskope Cloud Log Shipper to push rich, contextualized inline and security posture findings and alerts to Google Cloud security solutions including Google Chronicle, Security Command Center, Siemplify, and Google Cloud Storage.

DLP and threat-related incidents can be further investigated by analysts, and Google Cloud security administrators can create commands that will work with Netskope to address misconfigurations, reduce the attack surface, and enhance threat protection. Google Cloud products take advantage of the deep visibility into web and cloud activities and data provided by Netskope, and learnings from the entire security ecosystem can then be used inside the Netskope Security Cloud.

DRIVE ZERO TRUST - CONTINUOUSLY

Netskope's AI/ML engines discover risky behavior and identify risky users. Netskope Cloud Risk Exchange (CRE) can push users' raw Netskope risk scores, or an aggregate score across CRE integrated solutions, to the Google BeyondCorp Enterprise (BCE) framework to continuously refine conditional access by those users to applications from BCE enrolled devices.

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.