Netskope for Amazon Web Services

As enterprises move workloads and sensitive data into public cloud infrastructure at a rapid pace, the risk of exposure, sensitive data loss, and threats like malware remain significant challenges. Netskope for Amazon Web Services gives organizations the visibility, compliance, and protection for critical workloads needed to combat these challenges. With Netskope, get an understanding of your risk exposure, detect misconfigurations, inventory assets, enforce compliance standards, and protect against insider threats and malware.

QUICK GLANCE

- Perform an ongoing security audit and ensure compliance tied to security configurations
- Manage compliance for standards like PCI DSS and CIS benchmarks from assessment to remediation and reporting
- View inventory and manage the risk of your cloud resources across AWS and other CSPs
- Detect malware and protect sensitive data stored in Amazon S3 with advanced DLP and threat protection capabilities
- Protect organizations from insider threats with controls for corporate/other owned Amazon S3

NETSKOPE AND AMAZON WEB SERVICES

DevOps teams are designed to deliver with agility and scale. While AWS provides a secure cloud infrastructure, the security of workloads *in* the cloud is the customer's responsibility according to Amazon's Shared Responsibility Model[1]. Traditional CMDB tools or compliance tools with periodic audit ability can present blind spots in your security and risk management checks when operated in the public cloud. With Netskope, you can confidently deploy critical workloads in the cloud knowing that the cloud is configured to meet security requirements, simplify your overall security operations and continuously validate compliance. Built on the Netskope Security Cloud, Netskope for AWS is part of a comprehensive cloud security solution that gives you full control of SaaS, IaaS, and web, from one cloud-native platform that scales automatically.

[1] https://aws.amazon.com/compliance/shared-responsibility-model/

With Netskope, enable key use cases and answer questions like:

- What are the new resources in my environment today?
- Do they pose a compliance/security risk due to their configuration or content?
- Can I continuously monitor for security and compliance across all my AWS accounts?
- Can I quickly focus on the critical compliance and security findings to address them?
- How can I identify unauthorized account usage and stop data exfiltration?
- Can I prevent insider threats, especially with data movement from/to non-corporate Amazon S3?
- How do I moved beyond coarse grained policy control (like upload/download) and create intelligent policies around corporate bucket awareness? For example, prevent copy/sync from corporate-owned source code bucket to personal Amazon S3.

KEY CAPABILITIES

Continuous security assessment

Managing compliance against security standards and industry benchmarks for workloads in your cloud environment requires tools and controls to monitor configurations, enable remediation and continuous enforcement. With Netskope, data is brought into a unified view that will trigger alerts if misconfigurations are detected. You have a unified view of inventory, configuration, and compliance which streamlines the view of your resources on the AWS cloud.

See your current security state and actively enforce standards for PCI DSS and CIS benchmarks. Get back into compliance as quickly as possible with insights for each control and benchmark identified. Detected misconfigurations are flagged according to criticality. With an easy way to monitor and report on the security of the environment, run a report for auditors and quickly remediate and address gaps that were found using recommended guidance.

Continuous compliance reporting

As compliance requirements increase security leaders and industry regulators need validation of compliance status. Netskope delivers continuous compliance audits and provides customizable compliance reports that can be exported to PDF and sent to an auditor to report compliance status. Administrators can also quickly drill down to track activity level audit trails to determine unusual usage by individuals and run ad hoc queries and dynamic reports for compliance reporting purposes. Reports have granular filtering capabilities so organizations can control who gets access on a need-to-know basis. For example, you can make sure the network team responsible for Application A gets the Network Category alerts for the Account that hosts that application.

Cloud inventory

Gain insight into dynamic asset distribution within and across cloud service providers to see a holistic view of your cloud resources, including which resources have alerts associated with them. Compliance results can be summarized based on the resources affected and also by the compliance control. For example, when you have visibility into a new resources that are deployed, you gain insight into the security groups and NACLs that have external access or only internal access. You may decide to tag them in a way to watch for any potential vulnerabilities or activities to ensure the workload is operating within the defined security guardrails.

You can identify resources with similar configurations that end up with different compliance states to investigate root cause analysis for correction.

Real-time activity control

Get real-time visibility and control of activities and create policies to prohibit data exfiltration from managed to unmanaged storage buckets protecting you from accidental or malicious insider behavior. With Netskope, you get increased visibility into Amazon S3 bucket activity using a combination of both real-time and API approaches. This activity level control allows you to apply granular control policies to allow copy/sync to buckets that are "corporate owned" but block copy/sync to buckets that are not. Using patented Cloud XD technology, you can decode activities in real time and place activity-level restrictions for users, groups, and OUs across a wide range of services within your cloud infrastructure.

Using Adaptive Access Control extends granular visibility and control to blind spots such as unmanaged devices that are off network. Enforce IAM access from only managed corporate devices and block access from unmanaged devices. Perform activities like preventing users from deleting Amazon S3 buckets and EC2 instances via the admin console or AWS CLI or preventing them from allowing an S3 bucket containing sensitive information to be configured as public facing. This provides an extra layer of protection that complements existing IAM restrictions.

As custom apps and services are deployed in the public cloud, admins need visibility and granular control regardless of whether the app is public or private. With Netskope, admins define the custom services to protect. Netskope uses heuristics to automatically identify the service and understand which users are logging in, logging out, uploading, or downloading files with no admin intervention to manually map all possible user activities required. Used in conjunction with DLP, organizations can protect sensitive data loss from the custom apps and services.

Cloud storage data protection

Discover sensitive data and prevent unauthorized regulated data from being stored in Amazon S3 using award-winning Netskope DLP. Block or restrict access to data based on risk, users, groups, locations, or device. Use predefined DLP profiles to detect content such as personally identifiable information (PII), payment card industry (PCI) data, protected health information (PHI), source code, profanity, and more stored in your cloud environment. Additionally, build custom DLP profiles using Netskope's robust set of advanced cloud DLP features, including more than 3,000 data identifiers, more than 1,000 file types, support for language-agnostic double-byte characters, custom regular expressions, pattern matching, proximity analysis, fingerprinting, and exact match. These policies can be applied to real-time activities, such as uploads to and downloads from Amazon S3. Select Amazon S3 buckets in any region and have those files scanned for DLP violations. Block users from downloading or uploading sensitive files stored in Amazon S3.

Cloud storage threat protection

Only Netskope Advanced Threat Protection stops illusive attacks across SaaS, IaaS, and web. Comprehensive threat defense for AWS includes real-time, multi-layered threat detection and remediation. Block various strains of malware like ransomware going to and from Amazon S3. Detect malicious insiders and outsiders by identifying compromised credentials or potential account takeover situations and other anomalies by tracking login attempts, login failures, and more. Customize anomaly detection based on specific rules or use machine-learned intelligence to identify cloud anomalies.

CAPABILITIES	DESCRIPTION
Continuous security assessment	• Continuously monitor environment for misconfigurations across multiple clouds • Role-based access controls dedicated to public cloud use cases • Actively enforce standards for PCI DSS and CIS benchmarks • Find and address security gaps quickly with expert recommendations • Run compliance reports for auditors and internal teams
Cloud inventory	• Gain visibility into resources across multiple clouds • Identify the new/existing resources that pose a critical threat to your security posture • Get an inventory of resources that identify changes and risk • Create a compliance program that targets accounts with high valued accounts
Real-time activity control	• Create and enforce policies prohibiting data exfiltration from managed to unmanaged Amazon S3 • Visibility and Control of actions performed via AWS Management Console and AWS CLI
Cloud storage data protection	• Real-time protection against sensitive data loss • More than 1,000 file types and 3,000 data identifiers • Maintain compliance for regulations like PCI and HIPAA • Advanced DLP features include fingerprinting, proximity analysis, exact match, and more
Cloud storage threat protection	• Find and protect against malware to and from cloud infrastructure • Detect threats through AV, threat intelligence, malicious site databases, and deep detection intelligence engines • Get deep protection through cloud sandboxing, heuristic analysis, and anomaly detection • Leverage proactive threat intelligence from Netskope Threat Research Labs

THE NETSKOPE DIFFERENCE

Continuous security and compliance for a multi-cloud environment
Netskope offers a unified view of security, inventory, and compliance for your entire multi-cloud environment. Apply and manage security policy for AWS consistently with other cloud service providers.

Real-time access and activity control
With Netskope, we follow your data outside of your AWS environment applying policies applicable to how people work today. Get real-time activity and access control protecting you from malicious or accidental insider behavior.

Guard data everywhere
Netskope's 360º data protection uses the data inspection techniques like exact match, fingerprinting, and similarity hashes to identify your sensitive data in the cloud. Apply the same policies across SaaS, IaaS, PaaS, and web. Advanced threat protection capabilities stop elusive attacks that traverse SaaS, IaaS, and web to inflict damage.

netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.