Netskope - Public Cloud Security


Key benefits

- Perform an ongoing security audit and ensure compliance tied to security configurations.
- Manage compliance for standards like (Payment Card Industry Data Security Standard) PCI DSS and Center for Internet Security (CIS) benchmarks from assessment to remediation and reporting.
- View inventory and manage the risk of your cloud resources across AWS and other cloud service providers.
- Detect malware and protect sensitive data stored in Amazon Simple Storage Service (S3) with advanced data loss prevention (DLP) and threat protection capabilities.
- Protect organizations from insider threats with controls for corporate/other owned Amazon S3.

Product overview

Netskope delivers comprehensive threat protection for cloud and web services with a unique cloud-native vantage point unifying cloud access security broker (CASB), zero trust private access, and next generation secure web gateway (SWG). Netskope mitigates your risk by giving you control over that access, enabling you to set conditional, granular policies around employee access to both managed and unmanaged cloud services.

Product features

Continuous security assessment
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.

Continuous compliance reporting
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.

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.

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.
How it works

Continuous Security Assessment (CSA) by Netskope monitors your cloud infrastructure for risky misconfigurations such as data exposure and simplifies the remediation of these vulnerabilities. Netskope has multiple options to scan your data-at-rest, detecting DLP violations and malware in Cloud Storage. Netskope can also inspect data in motion, providing visibility into unsanctioned infrastructure-as-a-service (IaaS) accounts and preventing data exfiltration to unmanaged cloud infrastructure.

Differentiators

- **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 360° 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 your infrastructure and web.
What our customers are saying

"At Cloudrise, we deliver seamless and integrated data protection services around AWS cloud services by leveraging Netskope's security cloud solutions to provide unrivalled visibility and real-time data and threat protection. We understand the importance of securing data in the cloud and our customers realize it too."

Rob Eggebrecht, CEO, Cloudrise

Solution available in AWS Marketplace