Use Case-Driven Cloud Security Evaluator Guide

Netskope ONECloud is a unified cloud security platform that provides advanced data protection and comprehensive threat prevention across SaaS, IaaS and web services to help Security Operations (SecOps) administrators protect their cloud data and assets. This document covers six of the most common use cases, the functional requirements to deliver each use case, deployments configurations needed, and how to test Netskope or any cloud security product's ability to cover each use case.

netskope

01

Find and stop sensitive data from being exposed in the cloud

Cloud applications like Office 365 OneDrive, Box, and Google Drive makes it easy to share data with anyone. This streamlines collaboration but also presents risk with regards to sensitive data being exposed externally or publicly.

Netskope enables you to find and control sensitive data from being exposed in the cloud, enabling you to mitigate risk and safely use cloud applications to collaborate.

01

Functional Requirements

- Alert on sensitive data being exposed externally or publicly
- Policy actions such as remove public shares of sensitive data or restrict to view-only
- Comprehensive Cloud Data Loss Prevention (DLP) with features like Optical Character Recognition (OCR) for inspecting images

Deployment Requirements

- API controls for cloud apps such as OneDrive, Box, Google, and more

TIP:

Exercise the strength of the cloud security vendor's DLP by choosing sensitive data embedded in an image (e.g. a screen capture of PII data) and bring in other advanced DLP features such as using fingerprinting to identify sensitive data in a form.

How to Test with Cloud Security Products

- Configure the cloud security product you are testing to connect to target cloud app via API
- Configure the cloud security product to alert when public shares of certain sensitive data are discovered
- Share sensitive data publicly in the target cloud app
- Verify how the cloud security vendor presents the alert and/or dashboard
- Verify the cloud security vendor's ability to facilitate the investigation of the alert
- Verify the cloud security vendor's policy workflow to remove the offending public share
- Verify that the offending public share was removed

02

Granular control for unmanaged cloud apps

Enterprise adoption of SaaS is robust with nearly 1,200 cloud apps on average being used in a given organization. While IT-managed apps like Office 365, Box, and Salesforce are important, they only make up about 2% of the cloud apps being adopted by the enterprise.

It turns out that the cloud apps adopted by lines of business and users are fueling a majority of the growth in the cloud. These cloud apps range from the more than 100 HR apps like the ones used to recruit new employees to developer apps like GitHub and extend to personal cloud storage apps like Dropbox and collaboration apps like Slack and Evernote.

While cloud apps not managed by IT may be important for business productivity, there is an inherent risk with sensitive data leaking in these environments. Since IT does not have access to these apps, they lose visibility and control and are forced to deal with the situation using legacy security tactics like blocking at the perimeter or the endpoint. This presents not only technical challenges but also business challenges given how the adoption of these apps helps the business.

Unlike other security products, Netskope was architected from the beginning to provide real-time, granular visibility and control of thousands of cloud apps led by lines of business and users. This enables you to optionally block the use of high risk cloud apps, but more importantly, safely enable the majority of apps that the business relies on.

02

Functional Requirements

- Steer all cloud traffic (thousands of cloud services) and decode in real-time dozens of activities such as login, logout, upload, download, share, post, view, edit, etc.
- Differentiate between corporate-managed instances of apps and personal instances and reflect the difference in policy
- Support the selection of app categories as part of policies
- Provide “allow” actions as part of a layered policy

Deployment Requirements

- Support for various forward proxy deployment modes for steering thousands of unmanaged apps for real-time visibility and control

TIP:

Instead of specifying single apps not managed by IT, choose category-level policies so you can cover thousands of cloud apps in a single policy. Verify the cloud security vendor supports this. Also, try enforcing a policy that restricts what activities can be performed based on contextual details such as AD group, geographic location, or network location.

How to Test with Cloud Security Products

- Select 5-6 cloud apps such as Slack, Dropbox, Evernote, etc. that may be used by lines of business and not managed by IT
- Select at least two cloud apps that are managed by IT and may have personal instances in use. Examples are IT-sanctioned Google Drive and Slack and personal unsanctioned Google Drive and Slack.
- Configure the cloud security product for instance-awareness, identifying IT-managed versions of the apps you selected in the previous step
- With the cloud security product configured for real-time visibility and control, upload sensitive data to each of the identified cloud apps and verify that the activities are captured by the product
- Configure policies in the cloud security product to block PII data going to any of the selected apps in previous steps, while allowing PII to go to the versions of the apps managed by IT
- Attempt to upload PII to an unmanaged app and verify the block
- Attempt to upload PII to the app instance managed by IT and verify that the activity is allowed

03

Ensure social media compliance

Social media's ability to give organizations direct access to their audience makes it a useful tool for generating new business, attracting talent, and staying connected with customers.

At the same time, social media presents a significant risk for sensitive data exposure and compliance violations tied to insider trading, privacy laws, and more. This presents a challenge for CISOs that are faced with the decision to completely block social media to be compliant or allow social media so the business can benefit and hope that employees do the right thing.

Netskope provides granular control of social media, ensuring compliance and safely enabling the use of social media in the enterprise so CISO's don't have to make the difficult decision to block or allow its use.

03

Functional Requirements

- Steer social media traffic and decode in real-time activities such as login, logout, upload, download, share, post, and dozens more
- Custom Cloud DLP rules along with features like custom keyword dictionaries and boolean operators to focus inspection scope
- Real-time policies with the ability to focus on user groups, specific app categories including social media and apply granular DLP rules covered in the previous step
- Coaching workflows to help curb the user's non-compliant behavior

Deployment Requirements

- Support for various forward proxy deployment modes for steering hundreds of social media apps for real-time visibility and control

How to Test with Cloud Security Products

- Configure the cloud security product's DLP to look for content with the words, "guarantee" or "recommend" combined with a public company name or stock symbol
- Expand the configuration to bring in the user group' "finance"
- Implement a real-time policy to block the offending content when seen in the social media category
- Attempt to post the following to Twitter and verify block-"guarantee AAPL will do well in Q4"
- Verify event and alert in sequence in the cloud security product's incident management system

TIP:

Test the cloud security product's custom coaching page facility

04

Continuously assess your IaaS security posture

Netskope's Continuous Security Assessment for IaaS helps address the risks tied to misconfigurations that may lead to resources in AWS, Azure, and Google Cloud Platform being inadvertently exposed to the internet.

Netskope achieves this by continuously monitoring and auditing your public cloud configurations, using benchmarks such as CIS to identify misconfigurations and help you remediate so you improve your security posture and ensure compliance.

04

Functional Requirements

- Continuous security scan and audit for AWS, Azure, and GCP
- Single dashboard presenting summarized assessment results across your multi-cloud environment
- Remediation steps
- Compliance templates including CIS Foundation, PCI-DSS, and AWS and GCP Best Practices
- Asset inventory view across your multi-cloud
- Creation of custom rules

Deployment Requirements

- API integration with AWS, Azure, and GCP

How to Test with Cloud Security Products

- Configure the cloud security product to connect to your multi-cloud environment with AWS + Azure and/or GCP
- Verify visibility of inventory across your multi-cloud environment
- Configure the continuous policy audit for these environments and apply all available benchmarks
- Verify results of a scan
- Perform recommended remediation steps on the failed rule and verify rule passes after the next scan

TIP:

Create a custom rule to be used as part of a scan

05

Protect against cloud and web-based malware and ransomware

Netskope provides advanced protection against cloud and web-based malware and ransomware, enabling you to protect against threats in real-time in addition to the threats that exist with data at rest in the cloud.

05

Functional Requirements

- Inspect and apply threat protection for content-at-rest in dozens of cloud apps managed by IT
- Perform real-time threat protection for all cloud and web traffic for users on-premises
- Perform real-time threat protection for users on personal devices accessing corporate-managed cloud apps
- Perform real-time threat protection for all cloud and web traffic for users off-network
- Inspect TLS/SSL traffic at cloud-scale
- Leverage 3rd party intelligence feeds as part of the inspection

Deployment Requirements

- API integration with corporate-managed cloud services
- Real-time deployment modes including forward and reverse proxy

TIP:

Test the cloud security product's custom coaching page facility

How to Test with Cloud Security Products

- Enable and configure the cloud security product's threat protection capabilities
- Configure API and real-time deployments for SaaS and IaaS
- Attempt to visit a known malicious website and verify that the product blocks the user
- Attempt to sync a malware test file from a shared folder to a local Box or OneDrive sync client and verify that product blocks the sync activity
- Attempt to open an email link that goes to a malware test file hosted in the cloud and a malware test file hosted on a website and verify the product blocks the activity
- Verify sandbox capabilities provided by the cloud security product by detonating a malware test file and observing the associated report
- Verify ransomware detection and remediation capabilities by a ransomware test file to infect test files and verify that ransomware has been detected and that you can recover files via a UI workflow
- Verify integration capabilities with the cloud security vendor by configuring and walking through a workflow to use intelligence for malware scanning and sharing intelligence with Endpoint Detection and Response (EDR) solution like CrowdStrike and Carbon Black and have the EDR product automatically isolate the infected endpoint

06

Adaptive access control for cloud and web

Netskope's adaptive access control uses context-awareness to help balance the level of trust against access-related risk while improving the user experience.

There are two primary areas of adaptive access control. The first is corporate-managed devices accessing the cloud and web and the second is personal devices accessing cloud services managed by IT. In both cases, applying context will help address risk while improving the user experience.

06

Functional Requirements

- Classify devices as managed or unmanaged and reflect posture in policy
- Contextual policies for unmanaged devices, reflecting details about the user, location, device, app, and content
- URL filtering for managed devices on and off-network and bring in context such as user groups into policy

Deployment Requirements

- Support for a reverse proxy deployment to access unmanaged devices that are off-network
- Support for real-time proxy modes to steer cloud and web traffic in real-time for users on and off-network

TIP:

Verify how many products and consoles were required to administer and configure the adaptive access control use cases that span cloud and web

How to Test with Cloud Security Products

- Create a policy to block gambling sites except for users in the marketing group that are using a managed device with encryption enabled on the device
- Configure device classification in the cloud security vendor's product
- Verify that users outside of marketing and are not using a managed device with encryption enabled get blocked when trying to access a gambling site
- Verify that users in marketing are using a managed device with encryption get access to gambling sites
- Create a policy that blocks users on unmanaged devices from downloading PII data from Box, OneDrive, or your target IT-managed cloud app
- Configure a custom coaching message that tells the user about the non-compliant behavior
- Attempt to download PII from the target app from an unmanaged device and show custom coaching message

Test Results

Given guidance on how to test a cloud security vendor's ability to cover each use case, here is where you can tally your test results. Use a scoring system of 0-5 with 5 being the highest and most comprehensive coverage of the use case. Giving a vendor a 0 would obviously reflect the vendor's inability to cover the use case. Some vendors may cover some of the requirements, but come up short, resulting in a lower score.

It is also worth documenting how many separate products and administrator consoles the cloud security vendor requires to cover all use cases. This could impact your ability to deploy, manage, and operationalize the vendor's products.

USE CASE	VENDOR A Score (0-5): Product(s) required:	VENDOR B Score (0-5): Product(s) required:
Find and stop sensitive data from being exposed in the cloud	S: P:	S: P:
Granular control for unmanaged cloud apps	S: P:	S: P:
Ensure social media compliance	S: P:	S: P:
Continuously assess your IaaS security posture	S: P:	S: P:
Protect against cloud and web-based malware and ransomware	S: P:	S: P:
Adaptive access control for cloud and web	S: P:	S: P:
Number of use cases comprehensively covered by meeting all functional requirements		
Number of products and administrator consoles required to deploy and manage		

About Netskope

Netskope is the leader in cloud security. We help the world's largest organizations take full advantage of the cloud and web without sacrificing security. Our patented Cloud XD technology eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud services and millions of websites. With full control through one cloud-native interface, our customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection that stops elusive attacks. Netskope — smart cloud security.

netskope.com