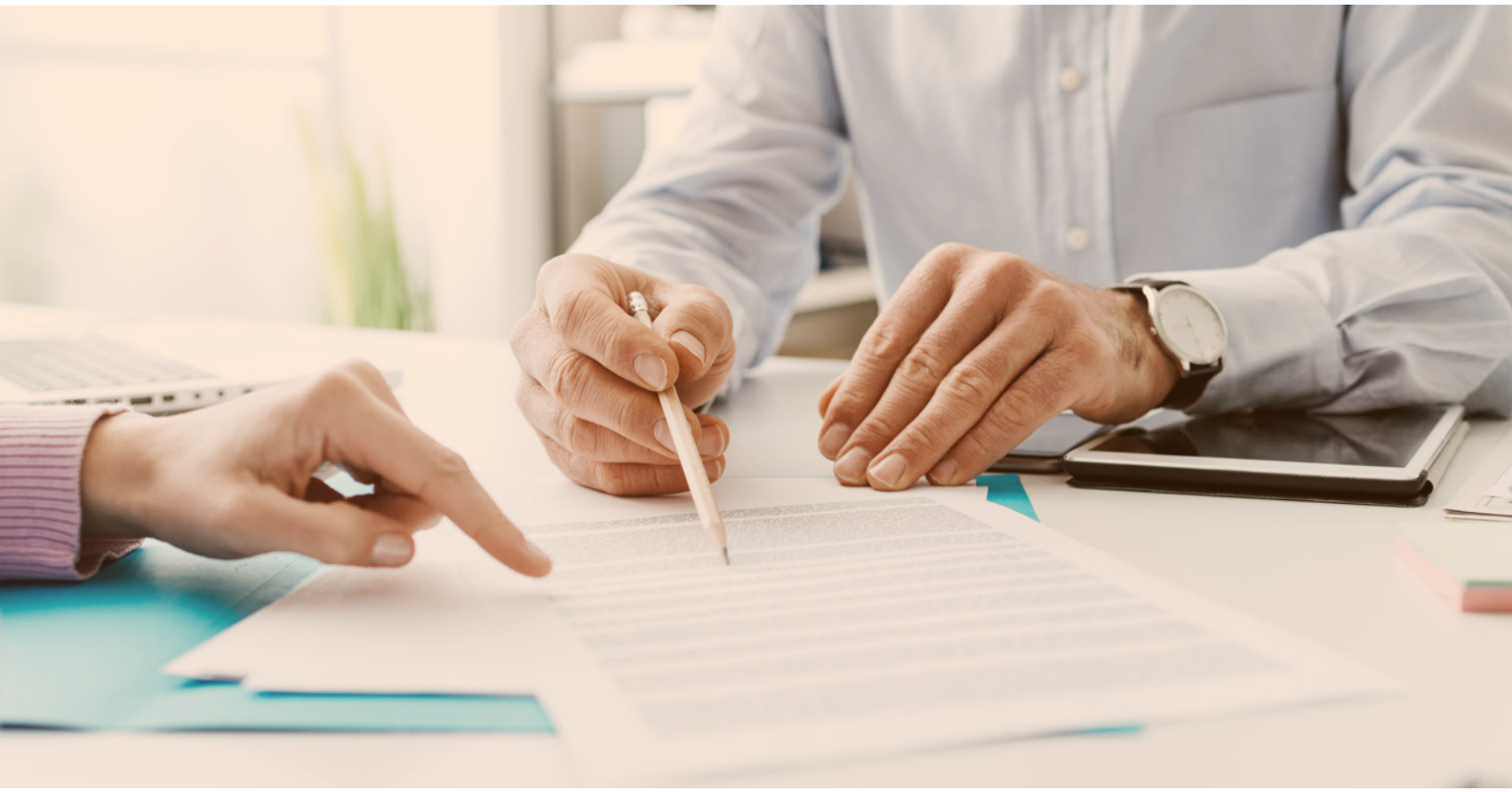
netskope

WHITEPAPER



10 Questions to Ask Your Cloud Access Security Broker

INTRODUCTION

According to Gartner, by 2020, 60 percent of large enterprises will use a cloud access security broker. Organizations are increasingly turning to CASB vendors to address cloud service risks, enforce security policies, and comply with regulations, even when cloud services are beyond their perimeter and out of their direct control.

Attempting to maneuver the CASB vendor landscape and determine how each vendor is different can be a daunting task. Most CASBs support core functionality such as discovery and risk assessment, DLP, and threat protection for SaaS, others may also support security controls for IaaS. When evaluating CASB vendors, it is recommended that you focus on use cases that are important to you. Here are ten use case centric questions that you should consider as you start the process of evaluating CASB vendors.

QUESTION #1:

Rather than simply blocking or allowing the apps discovered in my organization, how do you help safely enable the hundreds or potentially thousands of cloud services that our lines of business and users are adopting?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
Securing cloud services that are unsanctioned (shadow IT), but permitted is a challenging use case for a number of reasons. First, in order to secure a large number of apps, you need to understand what risky activities are taking place so you can agree appropriate controls. These apps often do not have published APIs so your CASB vendor needs to be able to decode what is happening without relying on assistance from the app vendor. Second, to cover unsanctioned apps the CASB vendor needs to be able to steer thousands of these apps and decode the risky activities in real-time. If a CASB vendor requires a per-app configuration then this is simply not scalable when you have so many apps that need to be secured. Third, the CASB vendor needs to support category-level policies so you can triage a large number of apps with a small set of policies. Creating 1,000 policies for 1,000 cloud apps is not an effective approach.	Netskope is the only CASB vendor that safely enables the thousands of unsanctioned, but permitted, apps that your lines of business and users are adopting. Powered by our patented Cloud XD, Netskope is the only CASB vendor that is able to decode risky activities in real-time covering thousands of apps that do not have published APIs. Only Netskope enables you to provide granular controls for these apps in context of user, device, location, activity, and content. For example, stop data exfiltration of sensitive data going to unsanctioned cloud services. Finally, only Netskope enables you to effectively triage thousands of cloud services by providing category-level policies. Netskope allows you to apply security controls like DLP and activity restrictions for all apps in app categories such as cloud storage, HR, finance, etc.	After getting an understanding of what apps are running in your environment, set up activity restriction policies and DLP for categories of apps that are prone to data loss. For example, create a policy to prevent uploads of sensitive data to cloud storage, or HR categories. Once your policies are in place, test them against dozens or more of the unsanctioned applications discovered in your environment. Compare the process and the results for each CASB vendor and their ability to achieve this key use case.

QUESTION #2:

How do you enforce separate policies across multiple instances of a cloud app?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
It is very common to see personal instances of sanctioned cloud apps like Microsoft OneDrive, Google Drive, Box, and Dropbox. One of your use cases may be to apply additional restrictions on the personal version, while relaxing restrictions on the corporate-sanctioned version. For example you might want to block PII data to a personal Dropbox instance, but allow PII data to the corporate-sanctioned Dropbox instance. The challenge here is that most CASBs do not have any ability to differentiate between instances of cloud services. For those that do, the capability may be limited to only one popular app like Microsoft OneDrive.	Powered by our patented Cloud XD, Netskope differentiates between instances of dozens of cloud apps. This coverage enables you to craft different policies for a sanctioned vs an unsanctioned instance, or a marketing vs an R&D instance and so forth.	Craft a policy for a few of your sanctioned cloud applications, allowing an activity such as PII data uploads. Next, craft another policy that blocks uploads of PII to unsanctioned instances of the same cloud apps. Compare which CASBs support this key functionality and for how many cloud apps they can identify different instances.

QUESTION #3:

How do you see and stop data exfiltration taking place from a sanctioned to an unsanctioned cloud app?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
A common scenario is when an employee, downloads sensitive data from a sanctioned cloud app like Microsoft OneDrive and then uploads that data to a personal cloud app like Gmail or Dropbox. The challenge is getting visibility the employee's activities once the data leaves the sanctioned cloud app. Controls need to be implemented that stop the exfiltration without disrupting any legitimate use of either the sanctioned or the personal cloud app.	Powered by our patented Cloud XD technology, Netskope is the only CASB that sees and controls activities and data movement across sanctioned and unsanctioned cloud services.	Download sensitive data from a some of your sanctioned cloud services and then upload that data to an unsanctioned cloud service. See how the CASB reports on the activity. Next, implement a policy that blocks the upload of the sensitive data to unsanctioned cloud apps. Do this without blocking access to the unsanctioned cloud app.

QUESTION #4:

Can you give examples of how well your DLP performs when it comes to detecting sensitive data in hard-to-find places?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
Managing risk tied to data loss in the cloud is a big challenge. There are many scenarios where sensitive data movement across cloud apps, or exposure from within cloud apps, evades basic content inspection techniques. Consider for example, text embedded in images or text stored within hidden areas of documents. Look for a CASB that can find and secure sensitive data wherever it goes.	Netskope's award-winning cloud DLP provides robust content inspection supporting the ability to scan for data embedded in images (Optical Character Recognition) or residing within hidden tabs in Excel workbooks.	Create a policy to alert when PCI data is discovered within a sanctioned cloud storage app such as Google drive. Next, upload PCI data embedded in an image to Google Drive Next, create and upload an Excel document that has PCI data, but use a VB Script to hide the tab with the PCI data Compare each CASB vendor's ability to find this data.

QUESTION #5:

Can you share details about how accurate your DLP is and what you can do to reduce false positives?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
It is critical to have an accurate DLP system or your security team will spend too much time sifting through meaningless alerts and false positives. Look for a CASB that supports advanced features such as exact data matching (EDM), fingerprinting, and contextual policies to help improve accuracy.	Netskope's award-winning cloud DLP supports advanced features such as exact data matching, fingerprinting, and contextual policies to greatly improve accuracy and reduce false positives.	Test exact data matching functionality by providing a structured data source that contains specific data values which can be tokenized by the DLP engine.. Then, instead of looking for any PII data in any combination (such as first name, last name, SSN, and home address), the DLP engine should look specifically for your source data in the combination you specify (e.g last name, SSN, and home address).. Test with data that includes values for fields that aren't from your dataset, also test with data that includes PII identifiers outside of those you have asked the DLP engine to look for. For fingerprinting, use the CASB to fingerprint a document . Create a DLP policy that triggers on the fingerprint you created. Optionally adjust the threshold of the fingerprint matching to trigger on excerpts from the document. For example, block the fingerprinted data from being uploaded to Dropbox. For the last test, create a contextual DLP policy, that incorporates a user group, network location, device type, activity, and data content. For example, block users in the finance group, outside of HQ, on a Windows device, from downloading documents from Microsoft OneDrive that are tagged as confidential. Test and compare each CASB vendor's ability to enhance the accuracy of DLP policies with exact data match, fingerprinting, and contextual details.

QUESTION #6:

How do you secure users that are on managed devices, but are outside the office and accessing any of the thousands of unsanctioned cloud services directly?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
A common blind spot for CASBs is the scenario where users are off the network and accessing unsanctioned cloud services from their corporate-managed device. This blind spot presents risk tied to data loss and threats.	Netskope supports an optional client deployment for Mac, PC, and iOS that provides access to this traffic. Once the traffic is steered by the client from the corporate-managed device, Netskope provides real-time visibility, control, and protection for thousands of unsanctioned cloud services.	Setup the CASB to block sensitive data to unsanctioned cloud apps like Trello or WeTransfer. Test by posting sensitive data to Trello, or uploading it to WeTransfer, from a managed device that is off the network. Repeat for other unsanctioned cloud apps to verify breadth of support.

QUESTION #7:

How do you protect against various strains of malware and ransomware from using cloud apps to hide, spread, and infect?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
Cloud apps present a perfect place for threats such as malware and ransomware to hide and spread rapidly. t go beyond basic anomaly detection and scan sanctioned cloud apps to find and quarantine malware. There is also a need for real-time protection to protect against malware coming in via desktop file sync apps, or other non-browser agents accessing cloud applications. Whether from , phishing via webmail, or malicious payload delivery from collaboration apps, threat protection needs to cover all of the thousands of cloud services in use within your organisation.	Netskope's Threat Protection capabilities are backed by Netskope Threat Research Labs, a dedicated team focused on the discovery and analysis of new cloud threats. Netskope consumes over 40 threat intelligence sources, and uses advanced machine learning technology to provide multiple layers of threat detection. Netskope's malware detection and analysis capabilities include static and dynamic anti-virus inspection, user behavior anomaly detection, heuristic analysis, sandbox analysis, and next-gen AV integrations.. Netskope's threat protection inspects sanctioned cloud services and quarantines malware that's discovered. In addition, Netskope blocks malware in real-time coming from any of the thousands of sanctioned and unsanctioned cloud services. Netskope's threat protection extends to cover desktop file sync apps, and other non-browser agents accessing cloud applications from your corporate-managed devices.	Setup the CASB to protect against malware and ransomware. Place a malware test file in a sanctioned cloud service like Microsoft OneDrive and verify the CASB detects and quarantines it. Place a malware test file in a shared cloud storage folder and verify the CASB blocks it from downloading via the desktop sync app (e.g. Microsoft OneDrive App.) Create a public link to the malware test file verify the CASB blocks it when a download is attempted from a corporate-managed device. Verify the CASB vendor's threat intelligence capability by configuring the CASB to automatically fetch and apply MD5 and SHA256 hash lists for known malware files from sources such as Carbon Black.

QUESTION #8:

How do you help me prevent employees using IaaS from exfiltrating data from one Amazon S3 bucket to another?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
Amazon Web Services provide a robust set of security controls ensuring only authorized users have access to resources like S3 buckets. The challenge once they have been granted access, is that they can easily copy or sync data from a corporate-managed S3 bucket to a personal S3 bucket or an S3 bucket outside of your organisation's control. Look for a CASB that can address this use case with the ability to block activities such as upload and sync from a managed to an unmanaged S3 bucket.	Netskope is the only CASB vendor to support the ability to block activities such as upload and sync taking place from a managed to an unmanaged S3 bucket	Configure the CASB for this use case and then perform the following activity: From the AWS CLI perform a cp or sync command from a corporate-managed S3 bucket to a personal S3 bucket. The CASB supporting this use case should be able to block this activity.

QUESTION #9:

How does your solution provide visibility into sensitive data stored in Amazon S3 buckets and Azure Blob storage?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
Managing risk tied to the exposure of sensitive data in cloud infrastructure environments like AWS and Azure is a big challenge. Addressing security misconfigurations that lead to exposure of resources to the internet is the first step and most CASB vendor's support this functionality. A further key step is to get visibility into what data has made its way into cloud infrastructure and what the sensitive nature of the data is.	Netskope provides the ability to scan S3 buckets and Azure Blob storage and apply award-winning cloud DLP to alert you to what sensitive data is in these environments.	Setup the CASB to look for and alert on sensitive data in S3 buckets and Azure Blob storage. Compare the results of the findings and the ability to create compliance-centric reports.

QUESTION #10:

What is your approach to securing SaaS, IaaS, and web as part of your offering that also includes CASB?

EXPLANATION	NETSKOPE ADVANTAGE	TEST FOR IT
Gartner's CASB definition encompasses visibility, data security, compliance and threat protection for SaaS and IaaS. There are many advantages to taking a more holistic approach and expanding your security coverage to the general web as well. You may currently be addressing web security separately with a traditional secure web gateway product, with a focus on use cases such as threat protection and acceptable use policies. Combining best-of-breed CASB functionality covering SaaS and IaaS with innovative web security from a unified platform that is delivered from one cloud and one console delivers value never seen before with the current crop of cloud security vendors. Some of the larger security vendors have attempted to bundle together disparate tools, but the result is increased complexity, multiple consoles, and disjointed incident management workflows; and they still lack best-of-breed functionality. With a "one cloud" approach, deployment is simplified, policy conflicts are minimized, and incident management workflows are streamlined. You can achieve visibility, compliance, data security, and threat protection across SaaS, IaaS, and Web from one console and one cloud.	Netskope is the only cloud security vendor that combines best-of-breed CASB for SaaS and IaaS with innovative web security, all from one cloud and one console. For web security specifically, Netskope leverages its patented Cloud XD technology to provide a more intelligent, user-focused view of cloud and web use. Unlike legacy secure web gateway solutions that generate high volumes of log data with every HTTP transaction, Cloud XD synthesizes and distills web activity into the specific user, site and page visits on which security teams want to focus.	Apply an advanced DLP policy incorporating features like exact data matching and fingerprinting to block sensitive data going to SaaS (unsanctioned apps), IaaS (unsanctioned environments) and websites such as social media, and discussion forums. Try to upload and post sensitive data matching the DLP policy to these destinations and manage the incidents from initial creation, through investigation, to closing out the incidents. Compare the complexity of each vendor to configure, manage, and support this use case. Configure each vendor to protect against malware in SaaS, IaaS, and Web. This includes inspecting data already in the environments and blocking malware from these environments in real-time. Use a malware test file and compare the complexity of each vendor's capability to configure, manage, and support this use case. The last test is to compare each vendor's ability to provide visibility into web usage. Start by visiting a series of websites and perform actions such as downloading of content. Incorporate DLP and threat protection as part of the activity if possible. Compare each vendor's ability to provide a clear picture of the user's activity.

SUMMARY

The answers you get to the preceding ten questions along with test validation will help you get clarity around how each CASB vendor is different when it comes to the features and capabilities that will best enable you to address your specific cloud security use cases.

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.

To learn more visit, https://www.netskope.com.