netskope

TOP 6 QUESTIONS TO ASK YOUR CLOUD DLP VENDOR

As you evaluate cloud access security brokers (CASBs) to safely enable sanctioned and unsanctioned (shadow IT) cloud services, cloud DLP is an important component of the solution. This 6-question checklist will give you specific, use case-based examples to help you differentiate between CASBs and choose the right one for your organization.

QUESTION:

CAN I COVER ALL THE WAYS SENSITIVE DATA CAN LEAK?

EXPLANATION:

Over 50% of all cloud traffic comes from mobile devices. Your workforce is also distributed and access cloud services from various locations and networks. You need to be able to enforce your policies wherever your users are and whatever their device or method of access.

NETSKOPE ADVANTAGE:

The Netskope Security Cloud facilitates the most comprehensive monitoring and control at the activity and content level, whether users are on-premises or remote, on a mobile device or even using mobile apps or sync clients. Moreover, Netskope lets you differentiate your policy enforcement between managed (corporate) and unmanaged (personally-owned) devices. Netskope is the only CASB that covers all possible cloud traffic regardless of location, device, or network.

TEST FOR IT:

Test for it in your CASB by triggering a DLP policy in a native sync client. Confirm the policy enforcement and look for a coaching message to the user offering an alternative to the violated policy. Also verify two policies that have the same triggers but different actions based on device ownership.

QUESTION:

WILL I BE ABLE TO SECURE DATA IN ALL CLOUD SERVICES, SANCTIONED AND UNSANCTIONED (SHADOW IT)?

EXPLANATION:

Many CASBs only allow for DLP policy enforcement for sanctioned cloud services like Microsoft Office 365, Google G Suite, Salesforce, Box, and the like. For unsanctioned, shadow IT services, most CASB solutions either cover a limited amount of services (<20) or not at all.

NETSKOPE ADVANTAGE:

Netskope can cover all sanctioned cloud services as well as thousands of unsanctioned ones, unlike other CASBs. With sanctioned services like Microsoft Office 365, the Netskope Security Cloud allows for DLP policies to be set across the entire suite, not just SharePoint, OneDrive, and Outlook, but also services like Dynamics, Power BI, and more. For shadow IT, with comprehensive deployment options and a granular policy engine, Netskope covers thousands of unsanctioned cloud services as opposed to a handful.

TEST FOR IT:

Test for it by setting a granular DLP policy like restricting upload of PII to top shadow IT cloud services used in your organization, especially from off-premises employees.

QUESTION:

WHAT ABOUT DATA PROTECTION IN PUBLIC CLOUDS OR IAAS/PAAS?

EXPLANATION:

Use of IaaS solutions like Amazon Web Services, Google Cloud Platform, Microsoft Azure, and more are exploding as devops teams are creating applications and resources to support strategic goals. Many of the applications deployed on IaaS access and use sensitive data – much of which needs to be visible to IT and secured.

NETSKOPE ADVANTAGE:

Netskope is the only CASB with a platform that allows for DLP policies to be set across resources like Amazon S3 buckets or Microsoft Azure Blob storage both in real time (with uploads and downloads) and in data already residing in those datastores.

TEST FOR IT:

Test for it by setting a policy to restrict upload of sensitive content to an S3 bucket to only a set AD group for compliance and auditing.

QUESTION:

CAN I SECURE SENSITIVE DATA IN UNSANCTIONED, SHADOW IT CLOUD SERVICES INSTEAD OF HAVING TO BLOCK USEFUL SERVICES ALTOGETHER?

EXPLANATION:

Rather than take a sledgehammer to a useful cloud service by blocking it, get visibility and control over it when it comes to data. For example, take a scalpel to an activity such as "sharing" of sensitive content. You can even do so at a category level, such as "block sharing of sensitive data in any cloud storage service if the recipient is outside of the company." This lets you allow, rather than block, useful cloud services while also mitigating risk. While having adequate data security for sanctioned services, many CASBs can only enforce block policies on unsanctioned, shadow IT cloud services at the perimeter or only cover less than 20 unsanctioned services in real time – leading employees to find ways around it like accessing from off-premises or finding cloud services that haven't been blocked and were missed by IT.

NETSKOPE ADVANTAGE:

The average enterprise has more than 1000 cloud services in use. While some of these are not appropriate for your business, many are useful or even critical. The Netskope Security Cloud lets you understand and secure sensitive data granularly at an activity-level (and based on other factors like AD group, geo- location of app or user, device type or ownership status, and content type or classification), enabling you to restrict flow of sensitive data while still allowing the cloud service, even if it's shadow IT.

TEST FOR IT:

Test for it by setting a DLP policy on an unsanctioned cloud service like CubbyShare and restricting upload of sensitive data into that service while showing a coaching message to use a corporate-sanctioned cloud service instead.

QUESTION:

HOW ROBUST ARE THE DLP CAPABILITIES TO MEET ORGANIZATION'S UNIQUE REQUIREMENTS AROUND SENSITIVE DATA AND REDUCE OF FALSE POSITIVES?

EXPLANATION:

Finding and securing sensitive content across cloud services is critical. Many organizations, including highly-regulated ones, have sensitive data that goes beyond those that can be found with pre-defined DLP profiles. To reduce the number of false positives, CASBs need to have advanced DLP features like exact match, fingerprinting of documents, support for custom keywords with weighted dictionaries, and more to meet the needs of these organizations and reduce the complexity of rules and number of false positives.

NETSKOPE ADVANTAGE:

Supporting 3,000+ language-independent data identifiers, 1000+ file types, proximity analysis, volume thresholds, international double-byte characters, document fingerprinting, content exact match, "and" and "or" rules, optical character recognition (OCR) and validation mechanisms such as Luhn check for credit cards, Netskope has the most robust cloud DLP in the market. Finally, Netskope features the most elegant integration with on-premises DLP solutions. With Netskope, you can perform a first pass of detection and protection in the cloud, and then backhaul suspected violations to your highly-tuned systems on-premises via secure ICAP for further inspection.

TEST FOR IT:

Test for it by using OCR to find sensitive data in images or fingerprinting a document being uploaded in cloud services and confirming the coaching message that appears. Perform actions on that content like encryption, quarantine, or legal hold.

QUESTION:

CAN I REDUCE COMPLEXITY AND MANAGEMENT OVERHEAD BY APPLYING ONE DLP POLICY THAT COVERS SAAS, IAAS, AND WEB?

EXPLANATION:

Many self-proclaimed security platform vendors require one DLP system to cover cloud and a separate DLP system to cover web. This is not only challenging operationally, but also impacts your ability to effectively implement incident management workflows that track DLP policy hits across all inspection targets.

NETSKOPE ADVANTAGE:

The Netskope Security Cloud is a unified platform that supports the same cloud DLP for SaaS, IaaS, and Web and requires no special aggregation or connectors, since the DLP engine and associated policies are unified from the start. This dramatically simplifies and streamlines DLP policy administration and incident management.

TEST FOR IT:

Set up a single DLP policy that inspects sanctioned and unsanctioned SaaS (e.g. OneDrive corporate vs. OneDrive personal), IaaS (S3 buckets and Azure blob storage), and web (discussion forums, social media, etc.).

THE NETSKOPE DIFFERENCE

Eliminate blind spots

Netskope Cloud XD™ understands SaaS, IaaS, and web in extreme definition to eliminate blind spots.

Guard data everywhere

360º data protection guards data everywhere through award-winning cloud DLP and encryption.

Stop elusive attacks

Advanced threat protection stops elusive attacks that traverse SaaS, IaaS, and web to inflict damage.

Full control, one cloud

Full control of SaaS, IaaS, and web, from one cloud-native platform that scales automatically.

Netskope is a leader in cloud security. We enable organizations to place robust DLP controls across all SaaS, IaaS, and web.

To learn more about the Netskope Security Cloud, visit **www.netskope.com/platform/DLP.**

netskope.com