netskope

# TOP 6 QUESTIONS TO ASK YOUR CLOUD DLP VENDOR


Whether your organization has already successfully adopted Microsoft 365, or is considering a move to Microsoft 365, you'll want to make sure your sensitive data is protected in Microsoft's environment. Data Leakage Prevention (DLP) for cloud environments is a key Cloud Access Security Broker (CASB) capability and this 6-question checklist provides use case-based examples to help you differentiate between CASB solutions and choose the right one for your Microsoft 365 deployment.

## QUESTION:

### CAN I COVER ALL THE WAYS THAT SENSITIVE DATA COULD LEAK FROM MICROSOFT 365?

**EXPLANATION:**

If you operate a BYOD policy and users are potentially accessing Microsoft 365 from their personal devices then you'll want to stop sensitive data being downloaded to those devices. If you're storing sensitive data in OneDrive for Business or SharePoint sites then you'll want to prohibit users from creating public shares to that data. And finally, if you have data that should simply not be stored in the Microsoft 365 environment at all then you'll need to prevent it being uploaded.

## NETSKOPE ADVANTAGE:

The Netskope Security Cloud provides the most comprehensive CASB functionality by monitoring and controlling data at the user activity and content level, regardless of whether users are on-premises or remote, on a mobile device, or even using mobile apps or sync clients. Real-time inspection and control of users' access to Microsoft 365 differentiates between managed (corporate) and unmanaged (personally-owned) devices. In addition to real-time protection policies, Netskope Security Cloud can integrate directly with OneDrive for Business and SharePoint sites to examine data at rest within the Microsoft 365 environment. Netskope policies to protect data at rest in Microsoft 365 can discover sensitive data and take actions to protect that data; actions can include raising an alert, apply encryption using integration with Microsoft Information Protection, removing any public sharing, or deleting the data.

## TEST FOR IT:

Test that a CASB can inspect, in real-time, sensitive data being uploaded to OneDrive for Business by the OneDrive for Business sync client. Confirm the policy enforcement and customize 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 (personal vs company owned).

## QUESTION:

## WILL I BE ABLE TO PROTECT DATA ACROSS MICROSOFT 365? CAN I GO BEYOND MICROSOFT 365 WITH MY DATA PROTECTION?

**EXPLANATION:**

Many CASBs only provide DLP policy enforcement for managed cloud services like Microsoft 365. And even within Microsoft 365, coverage of the suite may be limited to only the most common services—like Outlook, OneDrive for Business, and SharePoint Sites. Microsoft 365 includes a variety of other apps and services like Power BI, Dynamics, and more, that can contain sensitive data which needs protecting. Also consider the consequences of a user downloading sensitive data from Microsoft 365 and then uploading it to either an Microsoft 365 account that doesn't belong to the organization, or some other shadow IT service. Most CASB solutions either cover only a limited amount of shadow IT cloud applications (fewer than 20) or none at all.

## NETSKOPE ADVANTAGE:

Netskope can protect data in business owned (managed) cloud services, as well as thousands of unmanaged ones—unlike other CASBs. With managed services like Microsoft 365, the Netskope Security Cloud platform allows for DLP policies to be set across the entire suite, not just SharePoint Sites, OneDrive for Business, and Outlook, but also services like Dynamics, Power BI, and more. To control access to unmanaged Microsoft 365 accounts and shadow IT, Netskope supports comprehensive deployment options and a granular real-time policy engine. Netskope allows you to govern the use of thousands of unmanaged cloud services as opposed to a handful, and prevent your sensitive data going where it shouldn't.

## TEST FOR IT:

Test that a CASB can inspect all Microsoft 365 apps by setting a DLP policy to restrict the upload of Personally Identifiable Information (PII), or similarly sensitive data, to unmanaged Microsoft 365 accounts or shadow IT cloud services. Consider focusing testing on off-premises users where the problem is more challenging to solve.

## QUESTION:

### WHAT ABOUT DATA PROTECTION IN OTHER MICROSOFT CLOUD SERVICES SUCH AS MICROSOFT AZURE?

**EXPLANATION:**

Adoption of Microsoft Azure, and similar IaaS services, is exploding as Development Operations (DevOps) teams are creating applications and resources in IaaS platforms to support strategic projects and business goals. Many apps deployed within IaaS environments access and use sensitive data—which, just like the data in Microsoft 365, needs to be visible to IT and protected appropriately.

## NETSKOPE ADVANTAGE:

Netskope is the only cloud security platform with CASB capabilities that allows for DLP policies to be set across resources like Microsoft Azure Blob storage accounts both in real time (inspecting uploads and downloads) and for data at rest within those data stores. For organizations with multi-cloud environments, Netskope DLP can be easily and consistently extended to protect data and resources across other cloud providers such as Amazon Web Services (AWS) or Google Cloud Platform (GCP).

## TEST FOR IT:

Test that a CASB can extend granular data protection policies across Microsoft Azure by setting a policy to restrict the upload of sensitive data to Azure Blob storage accounts to a specific set of users defined by a Microsoft Active Directory group.

## QUESTION:

## CAN I SECURE SENSITIVE DATA IN MICROSOFT 365 THIRD PARTY ECOSYSTEM APPS AND TOOLS?

**EXPLANATION:**

Microsoft provides a supportive ecosystem for developers and there are many third party apps and tools that integrate with the Microsoft 365 environment. To enhance productivity, users may find ecosystem apps to use, such as document signing services like DocuSign or Adobe Sign that connect to Microsoft 365 and have access to sensitive data. Integrations can work in the reverse direction too, with Microsoft 365 apps like Word or Excel being able to open or save files stored in Box or Dropbox cloud storage environments. So many of the third party cloud applications that are able to integrate with Microsoft 365 are genuinely useful to the business, and, therefore, can't simply be blocked by the IT team. Your data protection solution for Microsoft 365 needs to cover these third party ecosystem apps too.

## NETSKOPE ADVANTAGE:

The average large enterprise has more than 1,000 cloud services in use. While some of these applications are not appropriate for your business, a large number will be useful or even critical. Some of those cloud services can be connected to the Microsoft 365 ecosystem, and users may do this without approval from the IT team. Netskope Security Cloud and its market-leading CASB capabilities provide you with visibility and control of, not only the Microsoft 365 apps, but also the Microsoft 365 ecosystem apps and tools, not to mention 1,000s of other unmanaged cloud applications. Netskope Security Cloud lets you control cloud application usage granularly at the activity-level. It can also protect your sensitive data from being shared with, or used by, unmanaged cloud applications.

## TEST FOR IT:

Cloud applications like Box or Dropbox are often integrated with Microsoft 365 applications, and files can be saved directly from Microsoft 365 applications such as Word or Excel. With a CASB DLP policy set: Create a new Word document in Microsoft 365, add some sensitive data such as PII, and verify that a save to Box or Dropbox is prevented. Customize the end-user notification to coach the user saves to Microsoft 365 OneDrive instead.

## QUESTION:

### HOW ROBUST ARE THE DLP CAPABILITIES IN MEETING AN ORGANIZATION'S UNIQUE REQUIREMENTS OF DETECTING SENSITIVE DATA IN MICROSOFT 365?

**EXPLANATION:**

Finding and securing sensitive content across Microsoft 365 is critical. Many organizations, especially highly-regulated ones, have sensitive data that goes beyond data that can be found with pre-defined DLP profiles and traditional DLP capabilities. To reduce the number of false positives, CASB solutions must have AI/ML technology, advanced DLP features like Exact Data Match (EDM), fingerprinting of files, support for custom keywords and RegEx with weighted dictionaries, Optical Character Recognition (OCR), and more to meet the needs of these organizations and reduce the number of false positives.

## NETSKOPE ADVANTAGE:

Supporting 3,000+ language-independent data identifiers, 1000+ file types, AI/ML proximity analysis, volume thresholds, international double-byte characters, document fingerprinting, Exact Data Match, "and"/"or" rules, OCR and validation mechanisms for credit cards, Netskope provides the most enterprise-ready cloud DLP in the market for securing sensitive data across your Microsoft 365 environment. Additionally, in order to manage DLP incidents efficiently, the Netskope Security Cloud platform provides built-in DLP incident management workflows and forensic capture of trigger data.

## TEST FOR IT:

Test that a CASB can discover sensitive data at rest within Microsoft 365 apps using advanced DLP techniques like OCR. Upload a screenshot (image file) of sensitive data to Microsoft 365 OneDrive for Business and verify that it triggers a DLP policy for that data. Upload a jpg or other format image of a driver's license or passport, also try tax and financial document to Microsoft 365 OneDrive for Business and verify it also triggers a DLP policy for sensitive data. Ensure that the policy can perform automatic remediation—delete the file, quarantine the file, etc.—when sensitive data is discovered.

## QUESTION:

### CAN I IMPROVE DATA SECURITY ACROSS MY CLOUD ENVIRONMENTS WHILE STILL REDUCING COMPLEXITY AND MANAGEMENT OVERHEAD?

**EXPLANATION:**

Many vendors implement DLP in a fragmented manner, with different policy controls to manage across cloud and web environments. This is not only challenging operationally, but also impacts your ability to effectively implement incident management workflows that track DLP policy hits across all the internet services—SaaS, IaaS, email, and web—used by your organization.

## NETSKOPE ADVANTAGE:

Netskope Security Cloud uniquely supports the same DLP capabilities for SaaS, IaaS, email, and web access and requires no special aggregation or connectors, since the DLP engine and associated policies are unified from the start. Safely enable Microsoft 365 services and then extend protection to Microsoft Exchange, Teams, Microsoft Azure (IaaS) and general web browsing as well. This unified approach dramatically simplifies and streamlines DLP policy administration and incident management.

## TEST FOR IT:

Set up a single DLP policy that inspects managed and unmanaged SaaS (e.g. Microsoft 365 OneDrive for Business and OneDrive personal), IaaS (Azure Blob storage), email, and web (discussion forums, social media etc.).

# THE NETSKOPE DIFFERENCE

## Eliminate blind spots

Netskope Security Cloud 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 **https://www.netskope.com/products/netskope-for-office-365.**


netskope.com