Top 6 Office 365 Security Use Case Guide

Microsoft Office 365 has become the de facto-standard productivity suite for organizations large and small. Enabled through a cloud platform of software apps, enterprises can increase collaboration and communication throughout their organization. As a cloud-based collaboration platform, Office 365 can enable organizations to deliver Word, Excel, PowerPoint, and Outlook across to their employees regardless of their location. Productivity applications such as SharePoint, OneDrive, Yammer can be seamlessly integrated in this delivery to increase workplace productivity and collaboration.

However, as enterprises move to the cloud-based applications, such as Office 365, they require a different approach to security and compliance of corporate data. The following are the top six use cases that customers should look for when evaluating a CASB (Cloud Access Security Broker) to protect their mission-critical Office 365 deployments.

netskope

01

Remove public shares of sensitive data from OneDrive and SharePoint

OneDrive and SharePoint are cloud-based collaboration tools that make it easier for enterprise users to work together. Deployed across thousands of enterprises, the ease by which employees can create, upload, and share documents can make it harder for security teams to manage the sheer number of documents that are shared within and between organizations.

It's not uncommon to have organizations share links to sensitive data that are still accessible to third-party business partners or even remain publicly accessible on the Internet, long after a project or partnership has ended. Simply forgotten, these links are often discovered when a critical exposure is discovered, forcing security teams to always play catchup. Over time, Office 365 can become a mess of public-facing links, unfettered access to sensitive data, and a permissions nightmare that require a time-exhausting step-by-step evaluation for security risks. Netskope can analyze Microsoft Office 365 environments including OneDrive and SharePoint enterprise deployments, detecting policy violations of shares for enterprise data that violate corporate security policy. Enterprises can store thousands upon thousands of files that can range into the Terabits of storage. Netskope can rapidly scale comprehensive DLP analysis across stored corporate data, looking for shares that contain sensitive data that doesn't conform with corporate security policy as defined by security teams. All violations are immediately removed, helping to trim shared links that no longer provide any useful function for the organization.

01

Functional Requirements

- Ability to find and report sensitive data shared externally or publicly.
- Comprehensive DLP applied to data-at-rest in managed cloud services.
- Ongoing and retroactive policies that support actions such as remove public or external shares, or restrict access to view only.

Deployment Requirements

- API (Out-of-Band)

TIP:

Ask your CASB vendor about how deep they integrate with Microsoft Office 365. Does the level of granular integration allow for discovery of all public data shares that contain sensitive data?

02

Get real-time visibility and control of risky activities across apps in Office 365

Office 365 acts as an IT central nervous system, allowing disparate global teams to work together better. These same systems that enable enormous positive productivity, can be commandeered for risky behavior that can result in sensitive data permanently slipping outside of an enterprise perimeter. Security teams require tools that enable them to monitor and control risk behavior without impacting day-to-day legitimate business activities. Legacy security tools do not have visibility, nor control into user activities across cloud-based applications such as Office 365.

Netskope for Office 365 helps security teams to understand granular activity, data, and context as work flows across Office 365 and thousands of cloud services. A granular and detailed view of Office 365 activity and data flows across your organizations can arm security teams with valuable insights on how data is accessed and by what users and groups. This sets the stage to drive prescriptive security policies enabled in real-time across all Office 365 transactions. Through a forward proxy, cloud services traffic including Office 365 is steered to the Netskope Cloud for real-time security analysis. Powered through Cloud XD, Netskope can obtain granular context by decoding cloud apps, inspecting encrypted traffic, separating thousands of cloud apps into managed and unmanaged groups, and then applying specific risk ratings. Upon discovery, security teams can bolt-down all discovered cloud apps that could potentially act as a conduit to exfiltrate sensitive data out of their enterprise perimeter.

02

Functional Requirements

- Ability to understand granular activity, data, and context across Office 365 apps and thousands of cloud services
- Ability to apply real-time policies to restrict risky activities across Office 365 apps
- Perform DLP analysis on O365 apps and thousands of cloud services

Deployment Requirements

- Forward proxy (Inline)

TIP:

Ask your CASB vendor what deployment modes they support to protect Office 365. An API-mode only deployment provides a limited set of supported use cases. Combining API with CASB inline mode provides the broadest set of protections for Office 365.

03

Prevent data exfiltration from Office 365 to unmanaged cloud services

Organizations often invest considerable amount of security to secure and protect Office 365. Security policies often are focused on restricting access to Office 365 corporate resources to non-authorized individuals and devices. However, the greatest blindspot that is often overlooked is unmanaged applications that coexist on managed devices with access to corporate instances of Office 365. A scenario that is repeated across thousands of organizations is an employee who legitimately downloads files from a corporate instance of Office 365. Once the files have been downloaded to a managed device, an employee can then upload that same file up to an unmanaged cloud application such as a personal instance of Office 365– entirely circumventing established Office 365 controls.

Neskope has designed their CASB security platform from the ground up to ensure avenues out from an organization are locked down so sensitive data does not leak outside of your enterprise perimeter. Netskope, in real-time, understands thousands of cloud apps that operate within your organization, allowing you to develop granular security policies that install security guardrails for legitimate use and prevent risky activities. Through Cloud XD, Netskope can identify thousands of cloud applications, managed or unmanaged, even delineating between corporate and personal instances of Office 365. In contrast, coarse-grained security controls either allow or deny access to Office 365, and can indirectly provide the opportunity to upload sensitive data to personal instances of Office 365 or other unmanaged cloud applications, entirely circumventing established Office 365 security protection controls.

03

Functional Requirement

- Ability to understand granular activity, data, and contextual details across Office 365 apps and thousands of cloud services
- Ability to alert or prevent data exfiltration activities taking place from Office 365 to other apps
- Perform DLP analysis on Office 365 apps and thousands of cloud services
- Ability to differentiate between instances of Office 365 (e.g. personal vs corporate)
- Perform policies at the cloud services category level with both allow and block actions based on instance

Deployment Requirements

- Forward Proxy (Inline)

TIP:

Ask your CASB vendor the breadth of security cloud apps they protect. A completely secured Office 365 deployment can be side-stepped by a user on an unmanaged device or through unfettered access to an unmanaged cloud app.

04

Ensure compliance for Office 365

The Office 365 suite of applications serves as a repository of enterprise data. Data is created, uploaded, downloaded, shared, and collaborated across by enterprise users, an opportunity that could be misused by risky insiders. Sensitive data can be easily leaked, placing their entire compliance and data security requirements of an organization at risk. Security teams need to have the visibility and control to ensure that sensitive data is continuously monitored regardless of where it travels, preventing every opportunity to mishandle data. As customers deploy Office 365, they are responsible for regulatory compliance measures that control how regulated data is accessed and by what user or group. New guardrails are required that ensure data is not accessed, viewed, downloaded or other actions that can place the entire organization at risk for non-compliance.

Netskope provides an additional layer of security controls that helps organizations to comply with regulatory compliance mandates. Granular visibility and controls allow security teams to establish comprehensive DLP enforcement, such as immediately blocking the exfiltration of regulated data outside of enterprise perimeter. Pre-built templates accelerate the development of compliance policies and allow security teams to customize them for organizational requirements.

04

Functional Requirements

- Ability to understand granular activity, data, and contextual details across Office 365 apps and thousands of cloud services
- DLP analysis for Office 365 apps and thousands of cloud services
- DLP analysis with regulatory compliance templates and ability to define context via a policy wizard
- Reporting facility to address auditor's needs to verify compliance measures

Deployment Requirements

- Forward proxy (Inline)

TIP:

Ask your CASB vendor how many pre-built compliance templates are provided. Avoid the task of building each compliance policy from scratch that can require hours of manual work and is prone to errors.

05

Protect against advanced threats in Office 365

Office 365 has increasingly become a target, as cybercriminals move their attack vectors to where enterprise users collaborate, communicate and keep sensitive information. With global access from the cloud, Office 365 can potentially open multiple avenues for cybercriminals to breach and access sensitive corporate data. Security teams require advanced Office 365 threat protection that can defend against the latest attack campaigns that target their organization.

Netskope for Office 365, provides a comprehensive security threat platform to defend against advanced cyberthreats, including cloud service enabled threats such as cloud phishing. Netskope Inline protection can prevent in real-time malicious links and malware embedded deep within enterprise cloud traffic–including Office 365 traffic. Furthermore, Netskope can drill-down into Office 365 traffic, analyzing with deobfuscation tools, sandboxing, and machine learning to detect for malicious patterns, behaviors, and indicators that signal cyberthreats. Organizations, through Netskope can prevent, detect, and quarantine malware and malicious links used in phishing attacks. Malware embedded in SharePoint and OneDrive is blocked during downloads to enterprise users end-devices preventing malware from taking a foothold in your organization.

05

Functional Requirements

- Ability to detect and quarantine malicious malware in OneDrive and SharePoint
- Ability to analyze cloud services and web traffic in real-time to prevent malicious malware
- Ability to report on ransomware infections and allow reverting back to a pre-infected data state
- Detection via deobfuscation tools, sandboxing, and machine learning of anomalous behavior to pinpoint unknown cybercriminal activity or malicious insiders.

Deployment Requirements

- API (Out-of-Band)
- Forward Proxy (Inline)

TIP:

Ask your CASB vendor if they can provide real-time malware prevention and detection as traffic moves back and forth between enterprise users and your cloud apps. Ask how they protect against unknown and hidden threats including cloud phishing using rogue or compromised instances. Do they wait until malicious files and links are stored in your cloud app and then provide remediation only via API?

06

Get visibility and control of unmanaged devices accessing Office 365

Office 365 extends a collaboration and productivity platform to employees regardless of where they are located or the devices they are using. This universal access provides enormous flexibility to accommodate different workplace requirements.

However, as employees access Office 365 from personal devices, new risks are emerging to organizations. With access to Office 365, employees can download corporate data onto personal devices. Organizations often lack visibility into this employee activity, raising a shroud of obscurity into potentially critical activities that involve sensitive data downloaded onto personal devices, right under the nose of security teams. Worse, employees who leave organizations can take corporate data within them on their personal devices, with no insight or control by security teams.

Netskope, through Cloud XD can distinguish between corporate (managed) and personal (unmanaged) devices, empowering security teams with fine-grained controls that can be applied to security policies that regulate what devices can access, download or edit corporate data. This ensures that employees can continue to benefit from Office 365 collaboration tools but without increasing organizational risk.

06

Functional Requirements

- Ability to provide real-time access-control for users, devices, activities, data
- Ability to detect malware or advanced threats taking place from unmanaged devices that access O365
- Ability to differentiate between a managed and unmanaged device
- Ability to perform access restriction policies (view-only, block, etc.) based on DLP profile of data

Deployment Requirements

- Reverse Proxy (Inline)

TIP:

Ask your CASB vendor how they account for unmanaged devices accessing managed cloud apps? If they use a reverse-proxy deployment, ask the number of managed cloud apps that are officially supported.

Most common deployment modes

Protect data in Office 365 and other sanctioned cloud services

Deployment Option	What it Covers	Key Advantages	Coverage Limitations
API (out-of-band)	Near real-time data and threat protection for data-at-rest in managed cloud services	• Protects data-at-rest	• Managed apps only • Not real-time
Reverse proxy	Real-time access to activities, data, and malware movement from a browser on managed and unmanaged devices for managed apps	• Visibility and control for unmanaged devices	• Managed apps only • Browser only
Forward proxy–Netskope Client	Real-time access to activities, data, and malware movement from a browser or native app on managed devices	• Users mobile and remote • Native apps • Managed & unmanaged cloud services • Web traffic	• Managed devices only

A combination of these 3 modes provides 100% use case coverage

About Netskope

The network perimeter is dissolving. A new perimeter is needed that can protect data and users everywhere, without introducing friction to the business. The Netskope Security Cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey.

Reimagine your perimeter with Netskope.

netskope.com