netskope
+
Office

Netskope for Microsoft Office 365

Safe Cloud Enablement for Office Productivity and Collaboration

Microsoft Office 365 is experiencing rapid adoption within enterprises. With as many as 25 percent of Microsoft customers, and an array of services such as Exchange, SharePoint, Lync, Office Web Apps, OneDrive, and Yammer, the suite has become increasingly robust and attractive.

Microsoft Office 365: A Robust Productivity and Collaboration Suite

Microsoft Office 365 is experiencing rapid adoption within enterprises. With as many as 25 percent of Microsoft customers, and an array of services such as Exchange, SharePoint, Lync, Office Web Apps, OneDrive, and Yammer, the suite has become increasingly robust and attractive. It is especially so for organizations that wish to adopt cloud while continuing to take advantage of the valuable productivity tools that their business users enjoy. According to the Netskope Cloud Report™, the suite is among the top 10 used apps in enterprises.

For many organizations, migration to Office 365 is a first foray, or at least a key move, in their cloud journey. It is often the seminal event that defines an organization's acknowledgement of cloud as a viable delivery mechanism for IT services, and is often followed by adoption of a wide variety of cloud services across the organization.

Shared Responsibility in the Cloud

Office 365 is inherently enterprise-ready by objective measures. It is rated "high" in the Netskope Cloud Confidence Index™, a yardstick adapted from the Cloud Security Alliance that scores enterprise cloud apps on their security, auditability, and business continuity. The suite boasts key third-party certifications, flexible security settings, and privacy features. Despite these inherent capabilities, IT organizations are concerned about maintaining visibility and control over sensitive business data moving in and out of the suite and across its ecosystem, as well as user activity within the suite. In what's called a "shared responsibility" model, cloud app vendors are expected to build apps that are inherently enterprise-ready while the enterprises themselves need to be responsible for the activities that their users perform within the apps. These can include malicious activity such as theft of confidential documents, inadvertent exposure of sensitive data, and compromise of authentication credentials.

Netskope for Microsoft Office 365

Netskope™ is the leader in safe cloud enablement. We enable you to confidently adopt the Office 365 suite. What does this mean to you? Building on the robust security capabilities inherent in Office 365, and addressing the shared responsibility model between cloud vendors and their enterprise customers, Netskope gives you deep visibility and granular activity- and data-level control across all of the Office 365 apps, the Office 365 ecosystem of integrated apps, and any other cloud app your organization uses, sanctioned or unsanctioned.

> “For organizations standardizing on Office 365, we can provide rich detection of activity-level anomalies such as excessive downloading or sharing from an Office 365 app, unusually heavy uploads to an app other than the Office 365 suite, or logins from multiple locations.”

Visibility Across All Office 365 Apps and the Ecosystem

Netskope gives you rich visibility into activity- and data-level usage details within every app in the Office 365 suite, along with the suite’s ecosystem apps. This allows you to answer questions such as “Who’s sharing sensitive content outside of the company, and with whom?” across SharePoint, OneDrive, Yammer, or any Office 365 app with a single query. Other common questions include, “Do we have PCI data residing in any of our Office 365 apps, irrespective of when content was uploaded?” or “Is anybody downloading personally-identifiable information to a mobile device?” Similarly, if content originally residing in Office 365 has been opened in another app, such as Google Docs, and then shared, Netskope would show that activity with the same query. In cases in which a line of business owns and administers Office 365, but IT needs visibility for data security or compliance purposes, we can provide that visibility with no disruption to the business.

Beyond on-demand queries, this level of visibility makes possible several important use cases for enterprise IT, including forensic analysis following a suspected cloud data exposure, anomaly detection for detecting malicious activity, and e-discovery of sensitive content for compliance purposes.

Cloud Forensic Analysis

Many customers use Netskope to create a granular cloud activity audit trail Many customers use Netskope to create a granular cloud activity audit trail following a suspected event such as the theft of sensitive content upon employee departure. For an organization standardizing on Office 365, this may include an employee logging into SharePoint or OneDrive using corporate credentials, downloading sensitive content, then logging into a totally different app such as Dropbox or Google Drive using personal credentials, uploading that same content, and then sharing it with a competitor. In just a few clicks, IT can reconstruct this activity in the form of a forensic audit trail to understand just what that user did with which content in which app, and if they shared the content, with whom they shared it.

Cloud Usage Anomaly Detection

Customers also use Netskope to detect anomalies. For organizations standardizing on Office 365, we can provide rich detection of activity-level anomalies such as excessive downloading or sharing from an Office 365 app, unusually heavy uploads to an app other than the Office 365 suite, or logins from multiple locations. These usage anomalies can indicate compromised credentials, out-of-compliance behaviors, and even the presence of malware.

One such example, for apps that don't support multi-factor authentication or for which it is not enabled, is the ability to detect hijacking of a user's account based on anomalous attempted logins. Netskope provides protection by alerting on the attempted access, preventing further access to the app, and reporting on any attempted accesses for security and compliance purposes.

e-Discovery of Sensitive Content

Another aspect of deep visibility is introspection, or the discovery of content that is already resident within cloud apps, irrespective of when it was uploaded or created. For Office 365, Netskope enables you to find content that matches your DLP profiles, whether pre-defined or custom. We inspect all of the content you have within Office 365 apps using industry-standard DLP with 3,000+ data identifiers and covering nearly 500 file types, and supporting keyword search, pattern-matching, proximity search, and regular expression. Once we discover content, we classify it and inventory content owners and users, provide sharing status (private, shared, or public), enable you to download files for review, secure content with strong encryption, and notify content owners.

Netskope lets you create, schedule, and share visual reports on all of the above, as well as export events easily via a REST API. This way you can include visibility about your Office 365 suite (as well as other cloud apps) within your current SIEM or other analytics tool.

Granular, Real-time Policy Enforcement and User Coaching

Beyond visibility and analytics, Netskope also provides the ability to enforce granular policies within Office 365, across its ecosystem, and in other cloud apps. This means that rather than take a blunt-force block/allow approach to apps, IT can direct or shape usage by controlling very granular actions or contextual details, for example, "Don't let users in 'insiders' share confidential documents with people outside of the company," "Alert me if users download content from SharePoint or OneDrive while on a mobile or unmanaged device," or "Coach users that upload content to any cloud storage app other than OneDrive."

Beyond visibility and analytics, Netskope also provides the ability to enforce granular policies within Office 365, across its ecosystem, and in other cloud apps.

With Netskope, you can create sophisticated, precise policies in a few clicks on any contextual detail or activity within an app, app instance, or across a category, and enforce those policies in real time. This means you can block, alert, encrypt, and coach across any app in the Office 365 suite (or any app). You can set policies for activities such as create, delete, download, edit, post, export, share, and even login or contextual details such as location, device, browser, etc. Netskope also has integrations with your enterprise Microsoft Active Directory and popular cloud single sign-on solutions. This means that any activity- and data-level policy enforcement will be in the context of users, their roles, and the groups they belong to, and you can use SSO to detect and enforce Netskope in the case of remote access. You can also use Netskope to detect new cloud apps that should be covered by SSO.

By providing granular activity- and data-level controls in context, we enable three important use cases for enterprise IT. These include blocking risky behaviors without blocking apps, protecting sensitive content moving to or discovered in the cloud, and coaching users for standardization and transparency.

Even when your organization standardizes on Office 365, blocking unsanctioned apps may not be your best route. Why not block the risky behavior instead?

Block Risky Behaviors

Up until now, the only way IT could deal with risky or unsanctioned cloud apps was to block them entirely. This caused a great deal of difficulty, with a raft of requested exceptions and users going to great lengths to go around the system, often for legitimate business purposes. Even when your organization standardizes on Office 365, blocking unsanctioned apps may not be your best route. Why not block the risky behavior instead? Say your users have partners that send them contracts, specs, and presentations as a link from a different cloud storage app than OneDrive. Should you block that app so they can't get to those documents? How about blocking them from uploading your content to any app except OneDrive, while still letting them view or download from other apps from which partners share their content? Netskope can let you enforce this policy in a few clicks.

Protect Sensitive Content

Beyond discovering sensitive content as it's being uploaded to, downloaded from, or resident within Office 365, Netskope lets you take action such as prevent the upload of or encrypt content if it matches a predefined or custom DLP profile such as PII, PHI, PCI, or confidential. In the case of content discovered in one of the Office 365 apps through introspection, we let you take action such as download for review, encrypt the content, and notify content owners. For content encryption, Netskope offers 256-bit encryption and cloud-based, fault tolerant FIPS 140-2 Level 3 certified cloud-based key management with an optional hardware security module (HSM). We also integrate with on-premises, KMIP-compliant key management solutions.

Similar to the use case above, for apps that are outside of the Office 365 suite, you can also enforce granular, activity-level content controls. For example, if your policy is to allow upload of confidential documents only to OneDrive, you can detect and block the activity, and then redirect the user to OneDrive.

Coach Users

When you enforce policies with Netskope, it's always a good idea to coach users. That can mean simply letting them know that you've blocked them from an activity because it's against policy. But even more useful is to give them an alternative, such as blocking them from uploading content to an unsanctioned app, and then coaching them with a URL (or simply redirecting them) to sign up for OneDrive. You may also want to give them a little more say in the matter. For example, if you enforce a policy blocking users from sharing content outside of the company, but then give them a rip-cord to do the activity anyway, you can configure Netskope to let them continue and simply enter a short justification so you can report on it for compliance later on. Similarly, you can provide the opportunity for the user to indicate that the detected activity is a false positive, and let them continue. This gives them more control and lets you gather user feedback, making your detection and policy enforcement stronger.

Beyond discovering sensitive content as it's being uploaded to, downloaded from, or resident within Office 365, Netskope lets you take action against your DLP profiles such as PII, PHI, PCI or confidential.

Netskope Enables These Key Use Cases

FEATURE	BENEFIT
Discover all Microsoft Office 365 and ecosystem apps running in your organization; consolidate instances or redundant apps	› Save cost and reduce complexity and risk › Get the most out of your investment by lighting up integrations between Office 365 and ecosystem apps › Get visibility and control consistently across Office 365 and the apps that share or access the same data
Conduct forensic analysis across your Office 365 suite and its ecosystem, including other apps	› Quickly confirm and report on suspicious or non-compliant activity › Don't guess; prove data exposure so you can take action
Detect cloud anomalies	› Be alerted to anomalous behavior that could signal compromised credentials, out-of-compliance behaviors, and even the presence of malware
e-Discover sensitive content and take action based on risk and compliance requirements	› Know what sensitive content is in your cloud through introspection › Triage your remediation
Block risky activities in cloud apps, e.g., sharing outside of the company	› Say yes to cloud apps while mitigating risk through precise, not coarse-grained, control
Protect sensitive content	› Get control over your sensitive data residing in cloud apps › Prevent the loss or exposure of sensitive data
Coach users	› Shape behavior through education › Create transparency about policy and rationale › Give users some control and a say in the process

Summary

As your organization adopts and standardizes on the Office 365 suite, you need granular visibility and activity-and data-level controls across the entire suite, the ecosystem, and even other cloud apps in your environment. You need to coach users in order to shape usage and create transparency, and you need to report on activities and events for compliance purposes. Netskope helps you do that in a consistent, one-stop fashion, enabling you to safely adopt Office 365 and its ecosystem of useful productivity and collaboration apps.

About Netskope

Netskope™ is the leader in safe cloud enablement. The Netskope Active Platform™ gives IT the ability to find, understand, and secure cloud apps. Only Netskope empowers organizations to direct usage, protect sensitive data, and ensure compliance in real-time, on any device, for any cloud app so the business can move fast, with confidence.

Netskope serves a broad customer base including leading healthcare, financial services, high technology, and retail enterprises, and has been named to CIO Magazine's top 10 cloud security startups and a Gartner Cool Vendor.

Share This Paper f t in