netskope + Office 365

Netskope for Office 365

Safely enable cloud productivity

Enterprises of all sizes are standardizing on Microsoft Office 365. With Netskope for Office 365, you can give users the productivity and freedom they desire while you maintain the visibility and security controls you need to protect sensitive data, prevent its loss, and ensure compliance.

At a glance:

- Prevent loss of sensitive data
- Real-time, granular control of Office 365 and its ecosystem
- Understand usage in Office 365 and its ecosystem
- Standardize on Office 365
- Quarantine sensitive content

Understand usage in Office 365 and its ecosystem

Get visibility into activity and data-level usage details within Office 365, along with the cloud apps that are part of the Office 365 ecosystem. This allows you to answer questions like "Who's sharing sensitive content outside of the company, and with whom?" across any app with a single query. IT can get visibility for security or compliance purposes without disrupting the business.

Key features / benefits

FEATURE	BENEFIT
eDiscover, control, and secure sensitive data stored in Office 365 and OneDrive with industry-leading cloud DLP	Mitigate your security risk by protecting sensitive data
Real-time, granular control of risky activities in Office 365 and ecosystem apps	Allow, don't block. By focusing on identifying specific risky activities and blocking them instead of the app, you can allow safe use of Office 365 and ecosystem apps
Cloud Forensic Analysis	Create an audit trail to help in the investigation of risky activities
Anomaly detection	Use powerful machine learning to help streamline excessive downloads or shares, logins from multiple locations, or other activities that could signal a security threat
Risk dashboard	Mitigate your exposure to security risks and potential threats
Data quarantine	Enable a remediation-centric workflow that helps you mitigate risks, while ensuring minimal impact to users
User coaching	Make users a part of the solution and not simply a part of the problem

netskope
+
Office 365

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

Standardize on Office 365

Find and consolidate redundant instances of Office 365 to save cost, reduce complexity, and encourage collaboration. Discover unsanctioned cloud storage apps and migrate those users to Office 365. Use the Netskope Cloud Confidence Index to make data-driven decisions about which apps to promote, which to limit, and which to consolidate.

Prevent loss of sensitive data using industry-leading cloud DLP

Netskope inspects real-time activities in Office 365 such as uploads, downloads, and shares in addition to inspecting content that is already resident in OneDrive, irrespective of when it was uploaded or created. Netskope enables you to find sensitive content using industry-leading DLP with 3,000+ data identifiers and covering nearly 500 file types along with pre-defined profiles such as Personally-Identifiable Information (PII), Protected Health Information (PHI), Payment Card Information (PCI), Profanity, and Source Code. Features such as keyword search, pattern matching, proximity search, and custom regular expression help ensure that you capture more sensitive data with fewer false positives.

Cloud forensic analysis

Create a granular cloud activity audit trail following a suspected event such as the theft of sensitive content upon employee departure. IT can reconstruct this activity in the form of a forensic audit trail to understand what that user did with what content in which app, and if they shared the content, with whom they shared it.

Cloud usage anomaly detection

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

Risk dashboard

Get an at-a-glance view of a variety of factors that contribute to security risks and potential threats. From risky apps to risky users to risky activities, get a handle on what your potential security risk is when it comes to using Office 365 and its ecosystem of apps. Further evaluate your risk by using the 'Password Breach' visualization to see what users might have compromised credentials.

netskope + Office 365

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

Real-time, granular control of Office 365 and its ecosystem

Instead of taking a coarse- grained allow vs. block approach, enforce granular policies in real-time within Office 365 and ecosystem apps. Apply contextual policies that account for: identity, location, activity, and content. For example, "Don't let financial 'insiders' share confidential reports outside of the company." Block risky behavior without blocking apps and protect sensitive content already resident in Office 365 from getting into the wrong hands.

Control access to Office 365

Netskope provides tight integration with a variety of single sign-on (SSO) vendors in addition to providing built in device-level access control policies that enable you to restrict access to Office 365 based on whether or not users are using a corporate device. Device-level access control is granular so you can for example restrict certain Office 365 activities to corporate, managed devices.

Quarantine sensitive content

Quarantine content that meets your specific criteria or matches a DLP profile. Upon detecting the violation, Netskope automatically places the file in a designated folder, whether the content is in process of being uploaded by the user or Netskope e-discovers it. Based on your policy, Netskope can encrypt that content for you in quarantine and notify the user with a customized message.

Place sensitive content on legal hold

Hold a copy of specific content, such as that matching specified content identifiers or created by a certain individual, for examination by a legal or regulatory reviewer. Netskope automatically and quietly places a copy (encrypted or not) of the file in a designated folder or on-premises. In keeping with the requirements of regulatory investigations, once content is designated for legal hold, Netskope will continue to discover and place files that users modify from the original in your designated legal hold folder.

User coaching

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 Office 365.

Support for mobile and remote

Mobile isn't going anywhere (so to speak), and just like you, we understand that Office 365 usage isn't limited to people who are on premises or on their PC. Cloud not only lends itself to, but is optimized for, on-the-go usage. For that reason, we architected Netskope to work on mobile, whether corporate issued or BYOD, or PC or mobile, as well as any app, whether web-based or a native mobile version. Where other vendors have architectural limitations that prevent them from supporting mobile devices and native apps, Netskope delivers the same capabilities regardless of device, app, or network.

Only Netskope

ANY APP, ANY DEVICE, ANY LOCATION
Allow, Don't Block: Only Netskope enables you to block the activity, not the app
360° Data Protection: Only Netskope secures data in sanctioned and unsanctioned apps
Take Action: Only Netskope enables you to enforce policies in real-time

About Netskope

Netskope™ is the leader in safe cloud enablement. Only Netskope gives IT the ability to find, understand, and secure sanctioned and unsanctioned cloud apps. With Netskope, organizations can direct usage, protect sensitive data, and ensure compliance in real-time, on any device, including native apps on mobile devices and whether on-premises or remote, and with the broadest range of deployment options in the market. With Netskope, the business can move fast, with confidence. Serving a broad customer base including leading healthcare, financial services, high technology, and retail enterprises, Netskope has been named to CIO Magazine's top 10 cloud security startups, Gartner's Cool Vendor list, and featured in such business media as CBS News, Wall Street Journal, and Forbes.