SOLUTION BRIEF

Microsoft OneDrive

Netskope for Microsoft OneDrive helps organizations to accelerate productivity, while ensuring robust security that enables granular control over user activity and data.

KEY USE CASES

- **Enforce granular data loss protection policies within Microsoft OneDrive.** Prevent sensitive data from being downloaded or uploaded to Microsoft OneDrive.
- **Build sharing and collaboration controls.** Restrict sharing of sensitive or regulated data in Microsoft OneDrive to unauthorized parties.
- **Manage the download and sync of data to unmanaged devices.** Enforce granular access policies on unmanaged devices by context-specific user policies.
- **Perform investigations with detailed audit trails.** Examine a complete audit trail of all user and application activity.
- **Detect and manage employee threats and malware.** Detect threats from insider threats, compromised accounts, cloud threats, malicious malware and anomalous user behavior.

THE CHALLENGE

Microsoft OneDrive has fast become a popular cloud storage platform used across both enterprises and consumers. It has become an easy and cost-effective way to store documents, spreadsheets and other files in the cloud for collaboration or long-term storage. However, OneDrive's widespread adoption has increased security risks for organizations. Storing sensitive information remotely can mean increasing an organization's "attack surface," allowing easy access to sensitive data from locations other than what was intended. Furthermore, a very thin line stands between enterprise and consumer instances of OneDrive, making it all the more easy to leak sensitive data from corporate instances to personal instances, without security teams ever being aware. Organizations are looking for a more granular approach to installing security guardrails that allow employees fast and easy access to corporate data stored in OneDrive but without the risk of that same data permanently slipping into unmanaged cloud apps or unmanaged devices.

NETSKOPE FOR ONEDRIVE OVERVIEW

Netskope provides organizations a fine-grained approach to security, by enabling granular visibility and control across all OneDrive accounts within an organization. Employees who access corporate resources from their personal devices can be prevented from downloading files but can be permitted to view or edit files.

Security teams can obtain deep insight and context into OneDrive activity across thousands of files, detailed file access, and detect anomalous behavior that might pose a serious threat. Real-time security controls that can block malicious or unauthorized activity as it occurs, installing security protections in between your Microsoft OneDrive deployment and users, regardless of where they are located.

KEY CAPABILITIES

DEEP VISIBILITY INTO MICROSOFT ONEDRIVE

Netskope enables deep visibility into Microsoft OneDrive and related Office 365 suite of apps. Security teams can view critical contextual details around usage that includes users, devices and activities. A security admin can further obtain risk-based insights that identify sensitive files and expose how they are being shared. Netskope can provide insights on employees that shed a 360 degree view into cloud application use across the organization. Security teams can understand the data interaction between Microsoft OneDrive and other cloud applications. By distinguishing between corporate and personal instances of cloud application use, they can block the upload of a sensitive document accessed from OneDrive into an unmanaged cloud app. CASB solutions that only protect managed apps, often leave a wide-open security blind spot into unmanaged apps that often freely operate from both personal and corporate devices. Unbeknownst to security teams, employees can bypass the restrictive security policies imposed on managed applications such as Microsoft OneDrive and freely upload sensitive data to unmanaged cloud applications, all without ever triggering any security alerts. In order to provide a more complete security protection, Netskope provides an umbrella protection across both managed and unmanaged apps that are in active use in an organization, locking down all possible avenues to exfiltrate sensitive data.

GRANULAR SECURITY CONTROL

Netskope security platform can enable security teams to define deep granular control over Microsoft OneDrive deployments. Powered by Cloud XD, Netskope can enforce detailed security policy based on contextual information such as cloud app, user, instance, activities, and device. Cloud XD provides real-time deep-packet inspection into cloud app traffic, discovering contextual information that can be utilized by security teams to define ultra-tight security controls that are purpose-built for each cloud app that are in active use, regardless if they are managed or unmanaged. Empowered with powerful new security controls, security teams can move away from coarse-grained “allow” or “deny” security policies that often provide primitive enforcement that cannot distinguish between personal or corporate instance of the same cloud app. Employees who use their personal devices to access corporate data stored in the managed cloud app, can have conditional access that can be restricted to view-only and prevented from downloading sensitive files onto their personal device. Netskope can prevent employees from copying sensitive corporate data from corporate to their personal instances of OneDrive or other consumer SaaS apps, helping organizations to define very strict guardrails on how and where sensitive data can move within or outside the corporate perimeter.

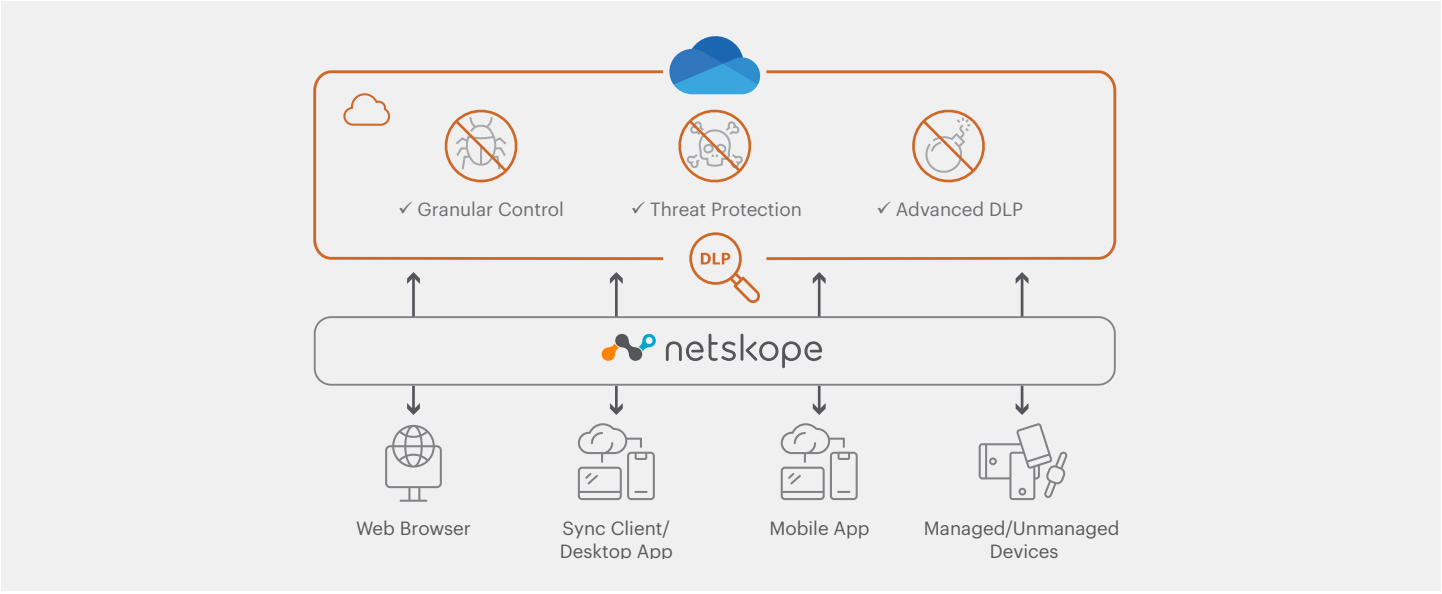

FIGURE 1: Netskope for Microsoft OneDrive

ADVANCED DATA LOSS PROTECTION

Organizations can store significant volume of corporate data on OneDrive, making it harder for security teams to keep sensitive data safe and ensure that the organization remains compliant under strict regulatory mandates. Born in the cloud, Netskope provides native data loss protection (DLP) that protects sensitive data wherever it travels—out to any SaaS application, IaaS Service, or out to the web. Built from the ground up, Netskope has the most advanced DLP capability in the industry, architected for high accuracy and low false positives. With over 3,000 data identifiers, support for more than 1,000 file types, custom regular expressions, proximity analysis, fingerprinting, exact match, and optical character recognition (OCR). Netskope helps customers to automate complex and manual policy configurations by providing over 40+ pre-built policy templates (PCI, HIPAA, GDPR, etc.), who can then speed up implementations by quickly customizing the templates to fit their unique requirements.

Security admins can define granular DLP rules that ensure as employees freely collaborate on files, they don't inadvertently pass along sensitive data that are a clear violation of corporate security policy; protecting your organization while ensuring that employees experience the maximum level of productivity.

CLOUD THREAT AND MALWARE PROTECTION

The Microsoft OneDrive collaboration platform makes it easy for users across an organization to access and work on files. However, this open and easy collaborative environment can make it easy for malicious malware to spread through the organization. Through Netskope, OneDrive traffic is inspected in real-time for malicious malware. Files that contain malware can be quarantined and replaced with tombstone files that are instead propagated through the organization, reducing the risk of further infection. Netskope can see directly into cloud traffic, exposing new cloud threats that often evade legacy security solutions. Netskope Threat Protection provides comprehensive threat defense for cloud services, combining 360° cloud visibility with multi-layered threat detection and flexible remediation capabilities. Security teams can also be alerted through EUBA analytics that leverages machine learning to learn baseline behavior of OneDrive users over 30 to 90 day periods. Anomalous behaviors by employees are automatically flagged to allow security teams to time to investigate, restrict access or provide customized messages in order to coach users on proper use.

BENEFITS	DESCRIPTION	
VISIBILITY AND CONTROL	**OBTAIN DEEP VISIBILITY AND CONTROL INTO MICROSOFT ONEDRIVE:** • What users are accessing Microsoft OneDrive based on role-type, device-type, geographic location, and IP address • What data is being shared, accessed, created, uploaded, downloaded, or deleted • User account creation, deletion, or access-control changes	**SECURITY ADMINS CAN DRILL-DOWN FURTHER INTO USER AND APPLICATION ACTIVITY:** • All activity based on user • All activities generated by specific IP address or geographic location • All access and actions performed on files containing sensitive data (PII, PHI, PCI, intellectual property)
GRANULAR SECURITY ACCESS POLICIES	**CREATE GRANULAR SECURITY POLICIES WITHIN MICROSOFT ONEDRIVE:** • Block specific users from performing OneDrive activities • Enforce policy action: alert, encrypt, restrict access, legal hold, restrict sharing to view. • Restrict sharing policy to predefined policies private, public, shared internally, shared externally • Restrict access by: owner, internal user, specific domain (white/blacklist), view only, disable print/download	**REMEDIATE VIA THE FOLLOWING METHODS:** • Remove or downgrade user access permission to view and edit files • Revoke a shared link • Remove user access permissions • Encrypt a file
ADVANCED DATA LOSS PROTECTION	**DEVELOP GRANULAR DLP POLICIES:** • Define keywords and phrases to detect sensitive or regulated data • Build granular custom regular expression to identify alpha-numeric patterns • 3,000 out-of-the-box data identifiers (Credit Card Number, Personal Names, address, etc.) • 40+ compliance and regulatory templates (PCI-DSS, HIPAA, etc.) • Fingerprint of unstructured files and structured files with exact or partial match • Optical character recognition (OCR)	**DLP REMEDIATION OPTIONS:** • Encrypt file • Quarantine file • Legal hold • Forensic store • Azure RMS enforcement
CLOUD THREATS AND MALWARE PROTECTION	**OBTAIN A 360 DEGREE VIEW INTO ALL CLOUD-BASED THREATS:** • **Insider threats:** Detect anomalous behavior by unusual amounts of data uploaded/data, changes in user behavior, login frequency of cloud service accounts • **Compromised accounts:** Evaluate access attempts by identifying suspicious geographic login-access, brute-force attacks,and unusual login patterns	• **Privileged user threats:** Identify sudden user privilege escalations, dormant accounts, and unusual system access • **Malware:** Block known malware, discover unknown files, and identify command and control behavior signaling data exfiltration

REQUEST A LIVE DEMO OR REQUEST A FREE AUDIT:
https://www.netskope.com/products/casb#content-5dc26b7f4e5d9-3

netskope

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 takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.