SOLUTION BRIEF

Microsoft SharePoint

Netskope for Microsoft SharePoint 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 SharePoint.** Prevent sensitive data from being downloaded or uploaded to Microsoft SharePoint.
- **Build sharing and collaboration controls.** Restrict sharing of sensitive or regulated data in Microsoft SharePoint 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 SharePoint Online is a cloud-based platform that makes it easier for organizations to store, share and manage digital documents. Deployed across organizations of all sizes, large and small, Microsoft SharePoint has become an integral part of enterprise collaboration, enabling the ability to easily share and store internal files. However, the powerful collaboration capabilities that can allow employees to create, edit, share, and store enterprise documents can be misused by employees or worse exploited by cybercriminals. Access from personal devices can further complicate corporate security posture where employees can download corporate data, taking sensitive data with them when they leave an organization. Without fine-grained visibility and control, employees can upload sensitive data up to a personal cloud applications, without security or IT teams ever knowing.

NETSKOPE FOR SHAREPOINT OVERVIEW

Netskope for SharePoint provides an extra layer of security that enables fine-grained visibility and control over SharePoint deployments. Organizations can obtain deep insight on SharePoint activity across thousands of files and documents. A panorama view into the current access permissions, sharing history and downloads across an entire SharePoint deployment can set the stage for security teams to remediate access permissions in order to ensure that they comply with strict corporate security policy.

Netskope can provide real-time security controls that can block malicious or unauthorized activity as its occur—installing security protections in between your Microsoft SharePoint deployment and users, regardless of where they are located.

DEEP VISIBILITY AND CONTROL INTO MICROSOFT SHAREPOINT

Netskope enables deep visibility into Microsoft SharePoint and related Office 365 suite of apps. Security teams can view critical contextual details around usage that includes users, devices, application instance and activities. Netskope can further provide risk-based insights that identify sensitive files and expose how they are being shared. A security admin can make real-time queries that answer specific questions about Microsoft SharePoint use. They can further obtain detailed reports that outline security and compliance reporting. Netskope can provide insights on employees that shed a 360 degree view into cloud application use across the organization. Security teams can understand the interaction between Microsoft SharePoint and other cloud applications. Netskope can distinguish between corporate and personal instances of cloud application use, blocking the upload of a sensitive document accessed from SharePoint into an unmanaged cloud app. CASB solutions that only protect managed apps, often leave a wide-open security blind spot into the unmanaged apps that often freely operate on both personal and corporate devices. Unbeknownst to security teams, employees can by-pass the restrictive security policies imposed on managed applications such as Microsoft SharePoint 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 ACCESS POLICIES

Today's employees demand freedom to actively use their own personal devices within the workplace, while accessing sensitive corporate applications based in the cloud. However, the ability to access and download sensitive data onto personal devices can increase organization risk as employee can without proper security visibility and controls can upload the same sensitive data to personal accounts on cloud-based apps—all under the nose of security teams.

Netskope can apply granular security policies to Microsoft SharePoint deployments, gained through deep contextual information obtained through Cloud XD. Powered by Cloud XD, Netskope security platform injects granular contextual control into your security policies. This provides real-time deep-packet inspection into cloud traffic discovering and organizing contextual information that can be used by security teams to develop ultra-tight security policies that are purpose-built for each unique cloud app, regardless if there are managed or unmanaged—that are in active use in your environment.

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. Powerfully granular security policies can be defined based on cloud app, user, activities and device-type. Automated workflows can quarantine files that have been flagged for review. Violations can be defined that can coach users with customized messages, while restricting unapproved activities.

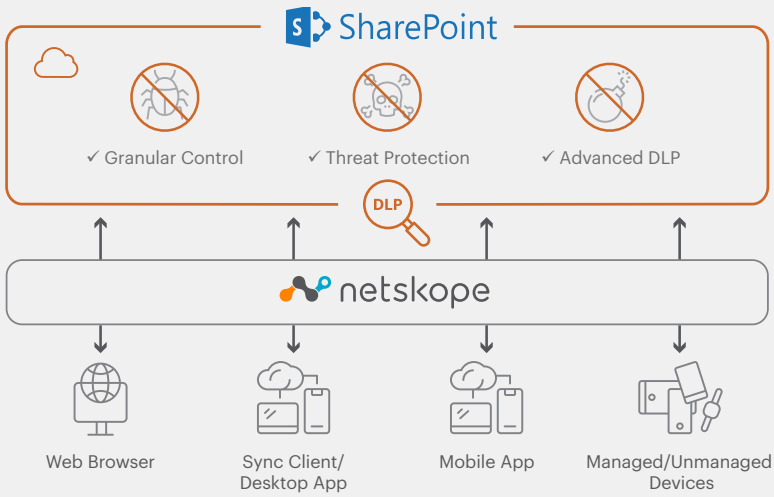

FIGURE 1: Netskope for Microsoft SharePoint

ADVANCED DATA LOSS PROTECTION

Organizations can store significant volume of corporate data on SharePoint, 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) protects sensitive data where ever 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 1000 file types, custom regular expressions, proximity analysis, finger-printing, 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.

Netskope for Microsoft SharePoint enables security admins to define granular DLP rules that ensure that as employee freely collaborate on files, that 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 THREATS AND MALWARE PROTECTION

Microsoft SharePoint 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, SharePoint 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.

Cloud-borne, Netskope can see directly into cloud traffic—exposing new threats that often evade legacy security solutions. Backed by Netskope Threat Research Lab, a dedicated team focused on the discovery and analysis of new cloud threats. 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 SharePoint 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 INSIGHT INTO SHAREPOINT VISIBILITY AND CONTROL: • What users are accessing Microsoft SharePoint 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 • The number of successful and failed login attempts **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
GRANULAR SECURITY ACCESS POLICIES	ENFORCE GRANULAR SECURITY POLICIES WITHIN MICROSOFT SHAREPOINT: • Block specific users from performing SharePoint activities • Prevent file and folder permissions that are accessible from the entire organization or the Internet • Revoke shared links as they are forwarded to non-approved 3rd Party external users • Block file and folder sharing to personal email accounts • Remove excessive edit permissions to external users with access to sensitive data **Remediate via the following methods:** • Remove or downgrade user access permission to view and edit files • Revoke a shared link • Remove user access permissions
ADVANCED DATA LOSS PROTECTION	DEVELOP GRANULAR DLP POLICIES THROUGH EASY TO USE TEMPLATES: • Define keywords and phrases to detect sensitive or regulated data • Build granular custom regular expression to identify alpha-numeric patterns • 3000 out-of-the-box data identifiers (Credit Card Number, Personal Names, address, etc.) • 40+ compliance and regulatory templates (PCI-DSS, HIPPA, etc.) • Fingerprint of unstructured files • Fingerprint of structured files with exact or partial match • Optical Character recognition (OCR) **DLP remediation options:** • Delete file • Quarantine file • Legal hold • Forensic store
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 into account of cloud services • **Compromised Accounts:** Evaluate access attempts by identifying suspicious geographic login-access, brute-force attacks, unusual login patterns • **Privileged user threats:** Identify sudden user privilege escalations, dormant accounts, 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.