netskope

Microsoft 365

SOLUTION BRIEF

Netskope CASB for Microsoft 365

Microsoft 365 is being adopted by organizations of all sizes. As the only CASB with Microsoft Gold Cloud Productivity Partner status, Netskope CASB for Microsoft 365 gives users productivity with the tools they need while maintaining visibility and controls to protect sensitive data, prevents loss, and ensure compliance.

KEY USE CASES

- **Enforce granular data loss protection policies across all Microsoft 365 apps:** Prevent sensitive data from being downloaded or uploaded to all Microsoft 365 apps.
- **Build sharing and collaboration controls:** Restrict sharing of sensitive or regulated data in Microsoft 365 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 insider threats, compromised accounts, cloud threats, malicious malware, and anomalous user behavior.

THE CHALLENGE

Collaboration and communication are key components of productivity in modern organizations. Microsoft 365 provides the necessary environment to facilitate this collaboration and communication, delivering the de facto productivity suite for many organizations of all sizes. Microsoft 365 has been built from the ground-up to accommodate a more mobile workforce, helping to get work done wherever and whenever it happens. However, this flexibility can also facilitate security challenges. Though Microsoft 365 provides native security controls, organizations often find they require a broader approach to security that takes into account enterprise application use and mobile worker mobility.

NETSKOPE CASB FOR MICROSOFT 365

Netskope CASB for Microsoft 365 provides a robust security solution, helping security teams to understand and control risky activities across the Microsoft 365 suite of apps and enable protection of sensitive data and blocking cloud threats. Netskope provides deep visibility into activity and data-level usage within every Microsoft 365 app and any other cloud app your organization uses, managed or unmanaged. Across each app, security teams can observe corporate data violations and potential cyber threats that can endanger the security and compliance of your organization.

CAPABILITIES

A COMPLETE VIEW OF MICROSOFT 365 AND ALL APPS

Netskope can reveal deep visibility across your Microsoft 365 and all apps in use within your organization. Security teams can parse through each individual Microsoft 365 app or obtain a consolidated view of usage. Microsoft 365 apps such as Exchange, SharePoint, and OneDrive can reveal previously unknown critical activity and data usage, insights that security teams were simply unaware before. With Netskope, you can obtain granular visibility into Microsoft 365 activity and the spread of sensitive data within and outside your organization. However, in order to provide a more robust security solution, security teams need to enact granular security controls across both managed and unmanaged cloud apps use. The greatest blindspot for security teams is the unofficial use of unmanaged apps that often proliferate across organizations. The most robust Microsoft 365 security

With Netskope, you can obtain granular visibility into Microsoft 365 activity and the spread of sensitive data within and outside your organization.

can be entirely circumvented by shadow IT or consumer apps that can provide a gateway to exfiltrate sensitive data. Unbeknownst to security teams, an employee could properly download sensitive data from a managed instance of Microsoft 365 and then upload the same sensitive data up to their personal Microsoft 365 instance. Netskope provides a robust cloud security platform that discovers all apps, managed or unmanaged. Through Cloud XD, Netskope can granularly distinguish between corporate and personal instances of any cloud apps, helping locking down all avenues that can allow sensitive data to be exfiltrated outside an organization.

Powered by Cloud XD, Netskope security platform helps to define deep granular contextual control into your security policies.

GRANULAR SECURITY ACCESS POLICIES

Today's employees demand the freedom to actively use their own personal devices within the workplace, while accessing sensitive corporate resources based in the cloud. However, easy access can enable the download of sensitive data onto personal devices that can increase organizational risk, as an employee can upload the same sensitive data back up to their personal cloud-based app—all under the security team's nose.

Netskope can apply granular security policies across Microsoft 365 suite apps, employee devices, and sensitive data, installing guardrails that prevent sensitive data from going where it shouldn't. Powered by Cloud XD, the Netskope security platform helps to define deep granular contextual control into your security policies. 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 in active use, regardless of whether 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 corporate or personal instance of the same cloud app. By safely enabling cloud applications with security guardrails ensures that users and departments can continue to use cloud apps but without impacting the organization's security posture.

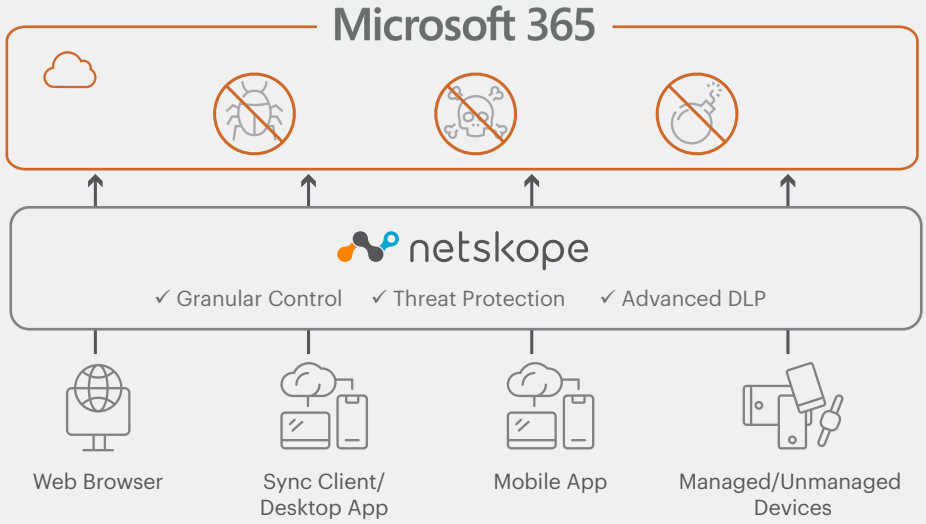

FIGURE 1: Netskope CASB for Microsoft 365

ADVANCED DATA LOSS PROTECTION

Data is at risk as the enterprise perimeter disappears, moving enterprise applications and users beyond their traditional security lines. Born in the cloud, Netskope provides cloud-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, 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 CASB for Microsoft 365, empowers security admins to define granular DLP rules that ensure as employees collaborate, they don't inadvertently pass along sensitive data that is in clear violation of corporate security policy; protecting your organization while ensuring that employees experience the maximum level of productivity.

CLOUD THREAT AND MALWARE PROTECTION

Cybercriminals have moved their attack vectors to the cloud, adjusting to how organizations now deploy their applications and data. They look to circumvent weak security controls. Legacy security solutions that are deployed on-premises often never look into cloud traffic, since the modern enterprise is dispersed across mobile users, who directly access cloud applications from their end-devices.

Born in the cloud, Netskope can protect Microsoft 365 by directly examining cloud traffic,exposing cloud threats that often evade legacy security solutions. Backed by Netskope Threat Labs, a dedicated team focused on the discovery and analysis of new cloud threats, Netskope provides comprehensive threat defense for cloud services, combining 360° cloud visibility with multi-layered threat prevention and flexible remediation capabilities. Netskope can provide deep visibility into cloud traffic that other security solutions simply cannot, stopping new cloud threats that too often evade existing security solutions.

Netskope collects event data from Microsoft 365. Using advanced machine learning, Netskope can flag anomalous behavioral activities in user accounts that can signal data exfiltration attempts by cybercriminals that have bypassed your security defenses.

BENEFITS	DESCRIPTION
DEEP MICROSOFT 365 AND CLOUD APP VISIBILITY AND CONTROL.	**OBTAIN DEEP VISIBILITY AND INSIGHT INTO MICROSOFT 365 APP AND ALL CLOUD APP USE:** • Discover all managed and unmanaged cloud apps (Shadow IT) • Prevent loss of corporate Microsoft 365 data from use of personal Microsoft 365 instances • Prevent loss of corporate Microsoft 365 data from use of unmanaged cloud apps. • Prevent unauthorized data from being shared externally • Prevent regulated, high-value data from being stored in the cloud • Block download of Microsoft 365 data to personal devices • Detect compromised accounts and insider/ privileged user threats • Capture an audit trail of activity for forensic investigations
GRANULAR SECURITY ACCESS POLICIES	**EASILY CREATE GRANULAR ENFORCEMENT POLICIES BASED ON SPECIFIC CONTEXT TO PROTECT SENSITIVE DATA FROM UNAUTHORIZED ACCESS:** **Create granular access control to Microsoft 365 based on:** • Device type (managed, unmanaged) • Activity type (download, upload) • Specific user (John Smith) • User attributes (role, department) • IP address range (e.g. network, proxy) • Geographic location (e.g. Russia) **Enforce granular access policies such as:** • Allow/Deny access to specific apps within Microsoft 365 • Allow/Deny to specific user actions within each Microsoft 365 app • Force step-up authentication.
ADVANCED DATA LOSS PROTECTION	**DEVELOP GRANULAR DLP POLICIES THROUGH EASY-TO-USE TEMPLATES.** • Define keywords and phrases to detect sensitive or regulated data. • Create custom regular expressions to alpha-numeric patterns • File metadata (file name, size and type) • Fingerprint of unstructured files • Fingerprint of structured files with exact or partial match • Keyword dictionaries of industry-specific terms **DLP remediation options:** • Notify the end user • Notify an administrator • Quarantine the file • Delete the file
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, and login frequency into account of cloud services • **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/request-demo

netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

©2021 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 05/20 SB-372-3