netskope

WHITEPAPER

Microsoft Office 365 Security:

Top Use Cases Addressing Customer Concerns in Shared Responsibility Model

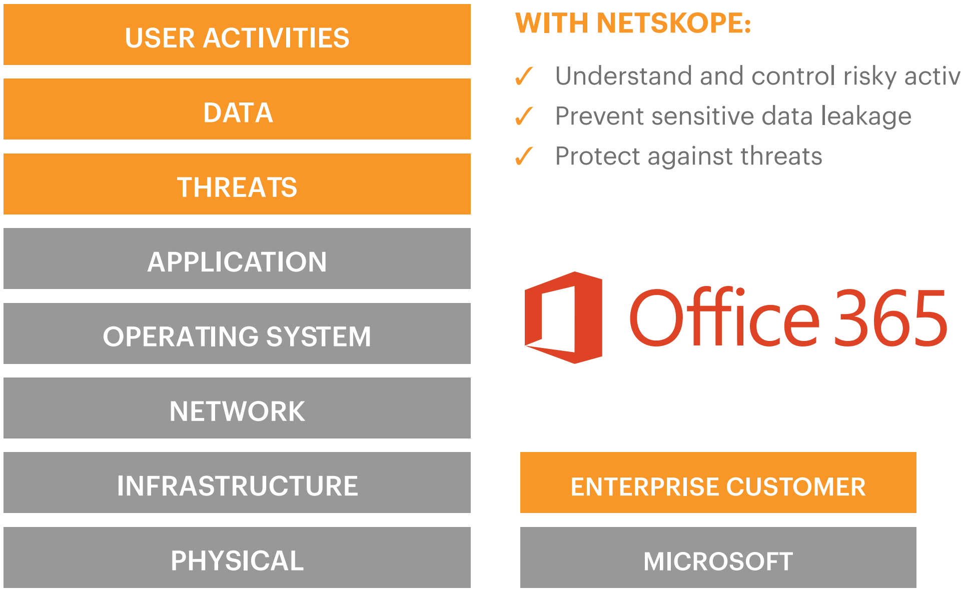
INTRODUCTION

Netskope helps secure some of the largest Office 365 deployments: three of the five largest global retail organizations, five of the largest healthcare organizations in the US, and many large enterprises in other verticals.

Microsoft customers have options when it comes to Office 365 security controls—with varying coverage depending on their license level. But securing the Office 365 suite of cloud services is a shared responsibility between the cloud provider (Microsoft) and the customer. In a shared responsibility model, the cloud provider is in charge of security for the physical layer, infrastructure, network, operating system, and actual application in the data center. The customer, however, is responsible for the activities its users perform, the data stored and processed in the application, and any threats that are targeting the users and organization through the platform.

In addition to fulfilling their requirements in the shared responsibility model, customers also need to consider the security of their data when it is downloaded from Office 365 and potentially transferred to shadow IT applications or other unsanctioned instances of Office 365.

FIGURE 1 | Shared Responsibility Model between customer organization and Microsoft



WITH NETSKOPE:

✓ Understand and control risky activities
✓ Prevent sensitive data leakage
✓ Protect against threats

CLOUD SECURITY PLATFORM NEEDED TO ADDRESS THE SHARED RESPONSIBILITY MODEL

There are three areas of the shared responsibility model that customers are responsible for. These areas all concern the users' interactions with the cloud service or app itself: user activities, data, and threats.

User activities: User activities that organizations are responsible for include risky activities like sharing with external teams, upload and download of data from unmanaged devices, and bulk deletions of data. These cloud activities expose the organizations to various risks as sensitive data may be exposed, threats introduced, or data destroyed.

Data: The data stored in Office 365 are uploaded, download, shared, and collaborated on by users—presenting another responsibility for organizations. Sensitive data could easily be leaked and this creates conflict with the compliance and data security requirements within organizations. Organizations need a way to find sensitive data and take action to remediate anything that's out of compliance or policy.

Threats: Finally, cloud threats such as malware like ransomware, and hybrid threats that use both web and cloud services, are areas of major concerns when they target users of Office 365. Threats and malware may be zero-day variants—necessitating tools and solutions to that are able to protect users against these advanced threats.

HOW NETSKOPE FILLS GAPS AND COMPLEMENTS MICROSOFT SECURITY CONTROLS TO HELP MANAGE RISKS TIED TO DATA LOSS AND THREATS IN OFFICE 365

The Netskope Security Cloud complements the existing security controls of Microsoft, while adding the ability to extend data and threat protection across all SaaS, IaaS, and web use in an organization. Using Netskope, organizations can have a single point of visibility and control across all cloud traffic with consistent policies and protection. Following are the top 5 reasons to secure Office 365 with Netskope.

REASON #1: FULL CLOUD RISK ANALYSIS AND REPORTING

Netskope not only provides detailed information on usage of all Office 365 apps, but also all ecosystem apps connected to Office 365, with full detail on device, user identity, location, activity, and more. Security teams can use this data to inform security policies through the organization and across existing security tools. Netskope also offers information on cloud services beyond those Microsoft reports on so that security professionals can perform vendor assurance and secure (or even sanction) shadow IT cloud services other than Microsoft Office 365. Cloud risk analysis helps address security policy settings across apps interacting with Office 365 services as well as serving as a gauge to help with extending security to cloud services beyond Office 365.

How Netskope fills gaps in Microsoft security controls	
Microsoft	**Netskope**
• Cloud service discovery for 15,000+ cloud services with details like GDPR readiness rating and more • Log upload via cloud tenant admin interface	• Support for 28,000+ cloud services with additional information on pricing, Dunn & Bradstreet business risk rating, and configurable weighting of the importance of attributes • On-premises and inline options for cloud service discovery • Granular activity-level details (user, IP, activities like upload/download/share, sharing destination, etc.) • Dynamic, custom reporting, and ad hoc querying

REASON #2: GRANULAR VISIBILITY AND CONTROL

Restricting risky user activity—from employees, contractors, and others—is part of the responsibility placed on customer organizations. Microsoft provides limited control of these activities across specific apps in the Office 365 suite. Netskope enhances this protection by extending controls across the entire Office 365 suite of apps as well as to dozens of sanctioned cloud services and thousands of unsanctioned, shadow IT services with full detail like location, app activity, content, device, location, network, and more.

How Netskope fills gaps in Microsoft security controls	
Microsoft	**Netskope**
• 11 cloud service APIs supported • Policy actions to remove public shares, restrict sharing, quarantine content • Support for multiple instances of a cloud service (e.g. Box – Marketing, Box – HR) • Policy actions to apply Azure RMS labels to content • Reverse proxy deployment options to access unmanaged device traffic	• Support for 18 sanctioned cloud services via APIs • Ability to differentiate between corporate-sanctioned and personal instances of cloud services • Support for Box classification • Support for thousands of additional cloud services (sanctioned and unsanctioned, shadow IT cloud services included) with inline granular visibility and control (user, location, device, content, app, actions) • Forward proxy deployment options including agent-less remote user support • Ability to see and govern cross-app activity such as Box edit for O365 • Real-time visibility and control for all Office 365 suite of apps • Category-level policies of cloud services (i.e. apply to all cloud storage apps) • Layered policies for granular block and allow actions • All access methods covered: browsers, mobile apps, desktop apps, sync clients

REASON #3: ADAPTIVE ACCESS CONTROLS

Adaptive access controls based on various factors are critical in securing users and protecting against threats. Microsoft has a variety of conditional access controls that Netskope complements to provide granular coverage to control and secure both managed and unmanaged devices accessing cloud services. Many Netskope customers use Microsoft Azure AD conditional access to manage authorization into Office 365 services and then complement that with Netskope's adaptive access control to provide more granular, device-level post-authorization access control. For example, instead of restricting access to Office 365 apps to managed devices only, Netskope enables a more granular policy to allow unmanaged device access to certain content, but restrict access to sensitive content to only managed devices.

How Netskope Complements Microsoft Azure AD Conditional Access	
Microsoft	**Netskope**
• Conditional access controls with Microsoft Azure AD and Intune • Application-, device-, user-, risk- and location-based access policies	• Extension of access controls for more granularity to take into account additional context like specific activity (i.e. only restrict downloads to unmanaged devices instead of blocking all access) • DLP profile • Content type • Cloud service instance or category • Specific cloud activity (download, share, etc.) • OS and browser type • Custom device classification triggers

REASON #4: AWARD-WINNING CLOUD DLP

Data being uploaded, downloaded, and shared in the cloud are the responsibility of the organization using Office 365. Basic controls identifying the data and then taking action (like removing external shares) are important. Finding and protecting sensitive data to prevent data loss and ensure compliance is a top priority among Netskope customers. Netskope fills critical gaps in Microsoft's existing DLP features across the Office 365 suite and beyond to other cloud services.

How Netskope fills gaps in Microsoft DLP

Microsoft	Netskope
• DLP for 9+ cloud services via API and real-time proxy • Support for 60 data identifiers • Ability to scan metadata and hidden fields • Support for keyword matching and regex • Support for exact match	• Extension of DLP to thousands of cloud services via real-time proxy and APIs • Support for 3000+ data identifiers • Visibility into data exfiltration from sanctioned to unsanctioned cloud services • Cloud service instance differentiation • Support for optical character recognition (OCR), custom keyword dictionaries, exact data match, and fingerprinting • Contextual DLP (e.g. sharing with another instance of sanctioned app or with personal instance of same app) • Encryption with support for 3rd party HSMs using KMIP, Salesforce BYOK support, and both API and inline encryption for Office 365

REASON #5: ADVANCED THREAT PROTECTION

Microsoft offers a number of threat protection services, with a major focus on email and endpoint protection. Netskope complements these features with advanced capabilities across multiple layers of threat detection including static and dynamic anti-virus inspection, user behavior anomaly detection, heuristic analysis, sandbox analysis, and more. Detect and remediate compromised credentials and even protect against malware being brought in from unsanctioned cloud services into sanctioned Office 365 ones like OneDrive.

How Netskope Complements Microsoft Threat Protection

Microsoft	Netskope
• Malware, anti-phishing, and cloud threat intelligence and defense across SharePoint, OneDrive, Teams, and Exchange	• Machine learning-based anomaly detection • Malware protection for all sanctioned and unsanctioned cloud services via API and real-time proxies • Dynamic analysis with cloud-based sandbox • Next-generation AV capabilities in partnership with Cylance • Ransomware detection and remediation • Integration with 3rd party EDR solutions

SUMMARY

Netskope—the only CASB to receive Microsoft Gold Cloud Productivity Partner status—enhances Office 365 security by helping security teams understand and control risky activities across the Office 365 suite of services, protect sensitive data, and stop cloud threats. In addition Netskope's security capabilities also extend beyond Office 365 to govern usage of other SaaS, IaaS, and web services. Netskope secures the largest deployments of Microsoft Office 365 and allows organizations to use one platform and one administrative console to secure Office 365 and numerous other SaaS, IaaS, and web services, with full incident management across activity violations, threats, and DLP.