netskope

WHITEPAPER

Microsoft Office 365 Security

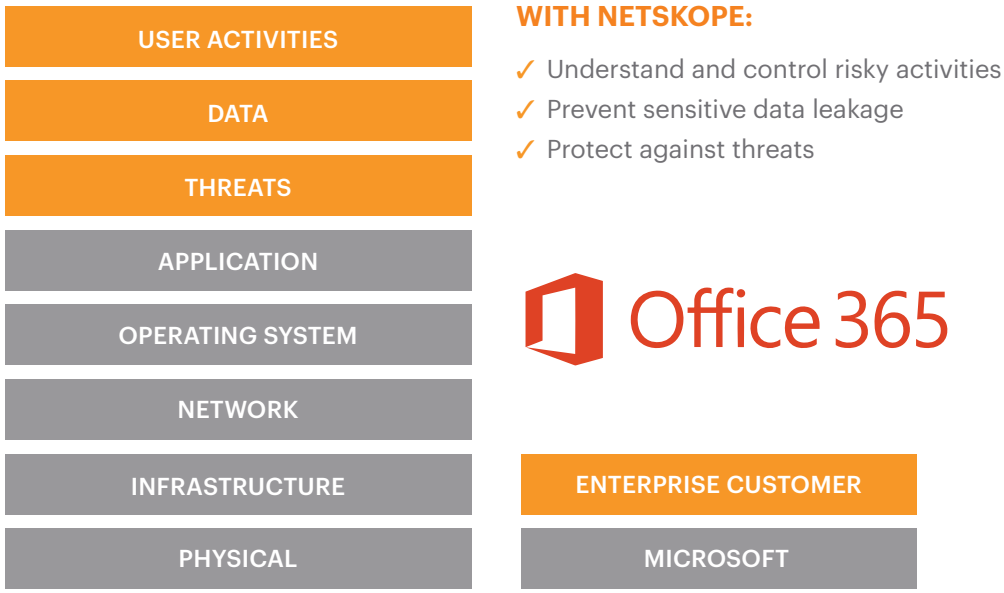
Top Use Cases Addressing Customer Concerns in Shared Responsibility Model

INTRODUCTION

Securing the Office 365 suite of cloud services is a shared responsibility between the cloud provider (Microsoft) and the customer. Under this model, Microsoft is responsible for the security of the underlying infrastructure that supports Office 365 platform, protecting it from cyberattacks. Microsoft is responsible for the security of the software, hardware, and physical facilities that host Office 365 services. However, the customer is responsible for ensuring that their Office 365 deployment is configured securely, accounting for the activities that users perform, ensuring sensitive data is not shared outside their company, preventing threats that target their organizational users, and enforce compliance and data governance policies.

Microsoft customers have options when it comes to Office 365 security controls, with varying coverage depending on their license level. However, critical security gaps can still remain.

FIGURE 1 | Shared responsibility model between customer organization and Microsoft



CLOUD SECURITY PLATFORM NEEDED TO ADDRESS THE SHARED RESPONSIBILITY MODEL

In an Office 365 shared responsibility model, there are three areas where customers are responsible. These areas concern how users interact with Office 365, which may impact an organization's security posture.

User activities: Organizations are responsible for ensuring that users do not engage in risky activities, such as sharing files with external partners, the upload and download of data to unmanaged devices, and bulk deletion of data. These activities, if not monitored or controlled, can expose an entire organization to various risks where sensitive data can be exposed or where external cyber threats can threaten the security posture for the entire organization.

Data: The Office 365 suite of applications serves as a repository of enterprise data. Data is created, uploaded, downloaded, shared, and collaborated by enterprise users, but these are also activities that

could be misused by risky insiders. Sensitive data can be easily leaked, placing the entire compliance and data security requirements of an organization at risk. Security teams need to have the visibility and control to ensure that sensitive data is continuously monitored regardless of where it travels, preventing every opportunity for the mishandling of data that could place the organization out of compliance.

Threats: Office 365 provides a platform that encourages fluid collaboration and communication across an organization. However, this same freedom can be exploited by cybercriminals, impacting the productivity gains offered by Office 365. New cloud threats are emerging that target how enterprises deploy applications and data. A cloud kill chain is used by cybercriminals to target and exploit weakness within the Office 365 suite of applications. New advanced malware and ransomware are targeting Office 365 and exploiting its cloud apps for new command and control and data exfiltration capabilities.

Netskope bridges the gaps with Microsoft security controls to better manage risks in Office 365

The Netskope Security Cloud provides an additional layer of security to Microsoft Office 365's existing security controls, while extending data and threat protection across all SaaS, IaaS, and web use in an organization. Through Netskope, organizations can have a single point of granular visibility and control across all cloud and web traffic with a consistent set of security policies. The following are the top 5 reasons to secure Office 365 with Netskope.

REASON #1: FULL CLOUD RISK ANALYSIS AND REPORTING

Netskope provides granular and detailed information on all usage across all Office 365 apps, including device-type, user identity, location, and activity. Security teams can use this information to develop relevant security policies that conform to how your organization operates. Netskope also provides insights on cloud services that are in active use by enterprise users that include both managed and unmanaged cloud apps, extending coverage beyond existing Microsoft cloud app coverage. Through Cloud XD, customers can obtain granular visibility and control on app instance, activity, and data that can help scenarios where users download sensitive data from a managed instance of Office 365, but then quickly upload that same data up to a personal instance of Office 365, circumventing existing Office 365 controls.

How Netskope fills gaps in Microsoft security controls	
Microsoft	**Netskope**
• Cloud service discovery for 18,000+ cloud services • Log upload via cloud tenant admin interface	• Support for 32,000+ cloud services. Provides information on pricing, Dunn & Bradstreet business risk rating, and configurable importance weighting of attributes. • On-premises and inline options for cloud discovery • Granular activity-level details (user, IP, activities like upload/download/share, sharing destination, etc.) • Custom reporting and ad-hoc querying

REASON #2: GRANULAR VISIBILITY AND CONTROL

Customers, as part of the shared responsibility model, are responsible for restricting users (employees, contractors, external business partners) from performing risky activities. Microsoft does provide native security controls, however they provide limited control of user activities within the Office 365 suite. Netskope provides a more comprehensive security model that includes both real-time and API security coverage. The Netskope Security Platform can ingest real-time enterprise cloud application and web traffic, scaling performance as required. This inline security protection allows enterprises to send their Office 365 traffic to Netskope to provide granular control over user activity as it occurs in real-time. Powered through Cloud XD, enterprises are given a panorama view of all cloud apps, including corporate and personal instances of Office 365, enabling security teams to establish effective security controls that actually lock down all possible avenues for data to leak outside your enterprise perimeter.

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 • Policy actions to apply Azure RM labels to content stored in cloud service • Reverse proxy deployment options to access unmanaged device traffic	• Support for 19 managed cloud services via APIs • Ability to differentiate between corporate (managed) and personal (unmanaged) instances of the same cloud service • Support for thousands of cloud services (managed and unmanaged) within inline granular visibility and control (user, location, device, content, and app actions) • Forward proxy deployment options to steer traffic directly to the Netskope Cloud • Visibility into cross-app activity (e.g. Box edit of Office 365 documents) • Real-time visibility and control for all Office 365 suite of apps • Category-level policies that can be applied across all cloud services (e.g. apply storage security policy for all cloud storage apps) • Granular definition of policies for block, allow, exception actions • All access methods covered: browsers, mobile apps, desktop apps, sync clients

REASON #3: ADAPTIVE ACCESS CONTROLS

Adaptive access controls are critical in securing users, providing proper access to data, and defending against threats. Netskope can enhance Microsoft's existing conditional access controls to provide better granular secure access across all managed and unmanaged devices. Netskope customers use Microsoft Azure AD conditional access to authorize users into Office 365 services, but then utilize Netskope's adaptive access control to provide a much more granular, device-level post-authorization access control.

For example, instead of restricting access to Office 365 cloud apps to only managed devices, Netskope can enable a much more granular policy that allows unmanaged device access to certain content, while restricting access to sensitive content to only managed devices.

How Netskope complements Microsoft Azure AD conditional access	
Microsoft	**Netskope**
• Conditional access control via Microsoft Azure AD • Application, device, user, risk, and location-based access policies • Granular access controls that can take into account additional context such as specific activity (e.g. restrict only downloads to unmanaged devices instead of blocking all access)	• Controls specific cloud activity (download, share, etc.) • Identify end-device by OS and browser types • DLP profile with granular policy definition • Content: Provides over 3000+ data identifiers (e.g. SSN, phone #) for over 1000+ file types • Exact matching and fingerprinting • Context-aware DLP (app instances, instance awareness) • Identify and protect data anywhere, on any device

REASON #4: AWARD-WINNING CLOUD DLP

Data, as part of the shared responsibility model, is managed by organizations using Office 365. Basic security controls that identify sensitive data and take remediating action (like removing external shares) are important. Finding and protecting sensitive data to prevent data loss and ensure compliance has been a top priority of Netskope customers. Netskope fills in the critical gaps in Microsoft's existing DLP features across the Office 365 suite and other critical cloud apps, helping to force a single unified DLP security policy that spans across cloud apps and websites used within the enterprise perimeter.

How Netskope fills gaps in Microsoft DLP	
Microsoft	**Netskope**
• DLP for 28 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	• Full DLP coverage of thousands of cloud services via Inline (forward proxy and reverse proxy) and APIs • Support for 3000+ data identifiers • Visibility into data exfiltration from managed to unmanaged cloud service • Instance identification between personal and corporate instances of the same cloud app • Support for optical character recognition (OCR), custom keyword dictionaries, exact data match and fingerprinting • Contextual DLP (e.g. prevent sharing between instances of a managed app and unmanaged (personal) instance of a same app • Encryption support with 3rd-party HSMs using KMIP, Salesforce BYOK support, API and Inline encryption for Office 365

REASON #5: ADVANCED THREAT PROTECTION

Microsoft offers a number of threat protection services, with a strong emphasis on email and endpoint protection. However, threats are moving to the cloud, where corporate data is increasingly being stored. A new cloud cyberkill chain forms the basis on how cybercriminals are adjusting their attack vectors to target sensitive data stored in the cloud. Security solutions that focused on protecting the endpoint or on-premises IT infrastructure often are unable to decode modern cloud app traffic that consists of API/JSON. Powered by Cloud XD, Netskope is able to decode cloud application traffic to capture user identity, instance, activity and data. Modern cloud-based malware and threats can be recognized through Cloud XD, providing a security forklift upgrade to existing security tools. Once traffic is decoded, Netskope can apply advanced security capabilities which emphasize cloud-based threats. Built in multiple layers, security protection can be progressively raised as traffic goes through a series of security threat detection mechanisms that include static and dynamic malware analysis, user behavior anomaly detection, heuristic analysis, and advanced sandbox analysis.

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 managed and unmanaged cloud instances via inline (real time) and API (near real time) modes • Dynamic and static malware analysis with cloud-based Sandbox • Next-generation AV capabilities with partnership with Cylance • Ransomware detection and remediation • Integration with 3rd-party EDR solutions

SUMMARY

Netskope provides an additional layer of security that can upgrade your Office 365 protection by empowering security teams to understand and control risky activities across Office 365 suite of services that protect sensitive data and stop cloud threats. Furthermore, Netskope Cloud Security platform is able to extend security coverage across both managed and unmanaged cloud apps and web traffic that provide a consistent set of security visibility and enforcement that provides true security for your Office 365 deployment that Microsoft alone can not provide. 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.

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

To learn more visit, https://www.netskope.com.