netskope

WHITEPAPER

Plugging Five Big Security Gaps in Office 365

INTRODUCTION

Many of Netskope's largest customers also happen to be some of the largest Microsoft Office 365 customers. From three of the five largest global retail organizations to five of the largest healthcare organizations in the US, and enterprises across multiple verticals in between, Netskope helps secure their Office 365 deployments.

Microsoft customers have options when it comes to Office 365 security controls and as you can see in the table below, one of the first options might be to look towards Microsoft directly to address your security needs:

TABLE 1 | Microsoft's native security capabilities

	O365			EMS	
Microsoft Security Offerings	E1/G1	E3/G3	E5/G5	E3	E5
Azure AD	✔	✔	✔		
Basic data governance (archiving)	✔	✔	✔		
eDiscovery search	✔	✔	✔		
Exchange Online Protection	✔	✔	✔		
Exchange S/MIME Encryption	✔	✔	✔		
Secure Score	✔	✔	✔		
Security and Compliance Center	✔	✔	✔		
Azure RMS (BYOK option)		✔	✔		
Data Governance (manual retention, deletion policies, manual classification)		✔	✔		
Data Loss Prevention		✔	✔		
eDiscovery hold and export		✔	✔		
Exchange Online messaging encryption		✔	✔		
Advanced Data Governance			✔		
Advanced eDiscovery			✔		
Advanced Security Management			✔		
Advanced Threat Protection			✔		
Customer Lockbox			✔		
Threat Intelligence			✔		
Advanced Threat Analytics				✔	✔
Azure AD Premium 1 (conditional access, multi-factor authentication)				✔	✔
Azure Information Protection Premium P1 (Manual Data Classification)				✔	✔
Intune				✔	✔
Azure AD Premium P2 (risk-based conditional access, PIM)					✔
Azure Information Protection Premium P2 (HYOK, Automatics Data Classification)					✔
Cloud App Security			✔		✔

Microsoft offers 25 security options, each with varying features and functionality that range from threat protection and DLP for Exchange email to Cloud App Security that focuses on visibility and control for SaaS. This paper will focus on the gaps that exist after adding Cloud App Security, Advanced Threat Protection, and Azure AD Premium with conditional access and how Netskope can help fill those gaps by either replacing these Microsoft security services or in some cases, complementing them.

GAP #1 – MICROSOFT DOES NOT PROVIDE REAL-TIME VISIBILTY AND CONTROL

Applicable Microsoft security services: **Cloud App Security**

When it comes to a cloud access security broker, there are two primary deployment methods – API and inline proxy. An API deployment uses an out-of-band connection to sanctioned cloud services to provide visibility and policy control ranging from restricting sharing of certain content to outside of an organization to quarantining sensitive data that has already made its way to sanctioned cloud services such as OneDrive, SharePoint, and other apps supported by the API interface. An inline deployment, on the other hand, provides real-time visibility and control supported by various forward and reverse proxy deployment options. Use cases enabled by inline deployments range from providing visibility and control of unsanctioned cloud services to preventing exfiltration of sensitive data in real time.

Microsoft's CASB offering, Cloud App Security, is API-only and cannot provide real-time visibility and control. The Netskope all-mode CASB architecture supports both inline via forward and reverse proxy options and out-of-band via API. More than 2/3 of Netskope customers deploy in multiple modes to accomplish an expanded set of use cases. Netskope combines inline deployment options with the ability to extract granular, contextual details about cloud usage using patented technology. Check the table below to see what you are missing...

TABLE 2 | Real-time visibility and control features

Real-time Visibility and Control Features	Microsoft Cloud App Security	Netskope Active Platform
Deep visibility (user, location, device, content, app, app instance, 50+ activities)		✔
Differentiate between personal and corporate instances of cloud services		✔
Granular policies across sanctioned and unsanctioned cloud services incorporating user, device, content, app, and app instance		✔
Category-level policies incorporating sanctioned and unsanctioned cloud services		✔
Layered policies with the ability to "allow" specific activities		✔
Real-time coverage for users on-premises, mobile, and remote and access from browser, mobile app, desktop app, and sync client		✔

GAP #2 – MICROSOFT ONLY COVERS A LMIITED NUMBER OF APPS

Applicable Microsoft security services: **Cloud App Security**

Microsoft's API connector is limited to supporting OneDrive for Business and SharePoint Online in the Office 365 suite with third-party app support extended to Box, Dropbox for Business, G Suite, Salesforce, ServiceNow, and Amazon Web Services. Netskope supports 14 different app configurations with an API deployment method, and thousands of cloud services when inline. For Office 365 specifically, Netskope extends visibility and control beyond just OneDrive and SharePoint, supporting apps like Power BI, Skype for Business, Teams, and Delve.

Netskope also supports inline visibility and control for thousands of cloud services, which is key for safely enabling the unsanctioned, yet permitted ones. Netskope also differentiates between personal and sanctioned versions of cloud services like OneDrive and SharePoint. Here is a comparison of app coverage across both API and inline deployment modes.

TABLE 3 | Cloud services Support

Cloud Services Support via API	Microsoft Cloud App Security	Netskope Active Platform
OneDrive for Business	✔	✔
SharePoint Online	✔	✔
Outlook.com	✔	✔
Box	✔	✔
Google Drive	✔	✔
Dropbox for Business	✔	✔
Salesforce	✔	✔
ServiceNow	✔	✔
AWS	✔	✔
Google Cloud Platform		✔
Slack		✔
Slack Enterprise Grid		✔
Egnyte		✔
Jive		✔

Cloud Service Support via Inline	Microsoft Cloud App Security	Netskope Active Platform
Number of SaaS / IaaS / PaaS decoded and granular usage details extracted in real-time	None	Thousands

GAP #3 – MICROSOFT DLP LACKS ADVANCED FEATURES, IMPACTING COVERAGE AND ACCURACY

Applicable Microsoft security services: **Cloud App Security and Microsoft DLP**

Cloud DLP continues to be a key driver for many customers deploying Netskope, including customers looking to protect sensitive data in Office 365 from loss. Microsoft offers two versions of DLP, one that is part of Cloud App Security and a separate one that is focused on Exchange and OneDrive exclusively. Both of Microsoft's DLP offerings are not only based on separate engines and interfaces, but they also lack app coverage and the advanced features required to address cloud DLP use cases precisely and accurately.

On the other hand, Netskope's award-winning Cloud DLP is delivered from a single engine and interface and provides broad coverage and advanced features for unmatched accuracy and precision. Here is a comparison.

TABLE 4 | Data Inspected

Data Inspected (breadth of coverage)	Microsoft DLP	Netskope Active Platform
Number of cloud services that can be inspected with DLP	**9**	**Thousands**
Content to and from mobile apps, desktop apps, and sync clients		✔
Content enroute to and from unsanctioned cloud services		✔
Files exfiltrated from sanctioned to unsanctioned apps		✔
App instances		✔
Metadata		✔
Hidden fields		✔
Password-protected files		✔
Body of webmail, social media, and other apps		✔
True file type inspection		✔
Number of data identifiers	**51**	**3,000+**
Number of file types	**100**	**500+**

TABLE 5 | DLP Accuracy

DLP Accuracy	Microsoft DLP	Netskope Active Platform
Keyword matching	✔	✔
Regex	✔	✔
Proximity		✔
Fingerprinting with similarity hashing		✔
Exact match		✔
Customer keyword dictionaries		✔
Global data identifiers		✔
Boolean logic		✔
Incorporate context in DLP policy		✔

GAP #4 – MICROSOFT ADVANCED THREAT PROTECTION IS LIMITED TO EMAIL AND ENDPOINTS

Applicable Microsoft security services: **ATP for Office 365, Exchange Online ATP, Windows Defender ATP, Cloud App Security**

Microsoft offers a number of threat protection services, but they are primarily centered around email and endpoint protection and not cloud services specifically. Cloud App Security provides basic rules-based anomaly detection, but no cloud-specific malware protection is supported.

Netskope provides advanced, cloud-specific threat protection that uses a combination of rules- and machine-learning-based anomaly detection in addition to malware protection for both sanctioned and unsanctioned cloud services. Netskope can be deployed in a complementary fashion to ATP for Exchange email and Windows Defender endpoint security. Here is a run-down of the threat protection gaps covered by Netskope.

TABLE 6 | Threat Protection Features

Threat Protection Features	Microsoft Cloud App Security	Netskope Active Platform
Rules-based anomaly detection (unusual login activity, high number of uploads/downloads, etc.)	✔	✔
Machine learning-based anomaly detection	✔	✔
Inspect cloud traffic in real-time and prevent malware from being uploaded to or downloaded from cloud services*	✔	✔
Detect users that have had their credentials compromised in a past data breach	✔	✔
Inspect sanctioned apps outside of the O365 suite including Box, Google Drive, Salesforce, and more for malware		✔
Network Intelligence with 40+ feeds combined with proprietary intelligence via dedicated threat researchers		✔
Integration with EDR and sandbox vendors		✔

• Note: Requires Windows Defender ATP for endpoints

GAP #5 – MICROSOFT CONDITIONAL ACCESS CONTROL IS NOT GRANULAR ENOUGH

Applicable Microsoft security services: **Azure AD Premium 1, Intune**

The final gap is focused on the access control use case. A critical CASB use case is the need to control and secure both managed and unmanaged devices accessing cloud services. Microsoft provides conditional access control, which is a service that is part of Azure AD Premium and can be extended to BYOD via Intune. Many Netskope customers use Microsoft conditional access control to manage authorization into Office 365 services and 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 you to get more granular and allow unmanaged device access, but restrict access to managed devices only if the content is sensitive.

Here is a run-down of the capabilities provided by Microsoft conditional access control and how Netskope complements those capabilities by filling in the gaps.

TABLE 7 | Supported Services

Supported Services	Microsoft Conditional Access Control	Netskope Active Platform
Other O365 suite apps such as Skype for Business, Dynamics, Live Calendar, Access, Sway, and Planner		✔
Thousands of sanctioned and unsanctioned cloud services		✔
Applications registered with the Azure Application Proxy	✔	✔
Azure Remote App	✔	✔
Developed line of business and multi-tenant applications registered with Azure AD	✔	✔
Dynamics CRM	✔	✔
Federated applications from the Azure AD application gallery	✔	✔
Microsoft Office 365 Yammer	✔	✔
Microsoft Office 365 Exchange Online	✔	✔
Microsoft Office 365 SharePoint Online (includes OneDrive for Business)	✔	✔
Microsoft Power BI	✔	✔
Password SSO applications from the Azure AD application gallery	✔	✔
Visual Studio Team Services	✔	✔
Microsoft Teams	✔	✔

TABLE 8 | Supported Conditions

Supported Conditions	Microsoft Conditional Access Control	Netskope Active Platform
DLP Profile (GDPR, PCI, PHI, etc.)		✔
Content type (500+ file types)		✔
Cloud service instance		✔
Cloud service category		✔
Activities (50+ activities – edit, post, login, upload, download, etc.)		✔
OS and browser type		✔
Device platform – Mac		✔
Dozens of managed device classification triggers		✔
Device platform – IOS, Android, and PC	✔	✔
Group Membership	✔	✔
Location	✔	✔
Device Enabled	✔	✔
Sign in and user risk	✔	✔

SUMMARY

Microsoft Office 365 offers a range of security capabilities, but still has significant security gaps in real-time visibility and control, app coverage, DLP, threat protection, and access control. Irrespective of where you are in your Office 365 journey, you should consider additional security controls to either replace or complement what Microsoft can offer. Netskope can close the five key gaps in Microsoft's security capabilities:

Key Capabilities	Microsoft	Netskope Active Platform
Real-time visibility and control of cloud services		✔
Cloud services coverage	**9**	**Thousands**
Advanced DLP that is precise and accurate		✔
Advanced cloud threat protection beyond email and endpoints		✔
Adaptive access control with broad services and conditions coverage		✔

Netskope is the leader in cloud security. Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real-time, whether accessed from the corporate network, remote, or from a mobile device. This means that security professionals can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and unmatched breadth of workflows, Netskope is trusted by the largest companies in the world. Netskope — security evolved.

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