Enhance your security to get ready for Copilot for Microsoft 365

Agenda

- Preparing your customer for Copilot for Microsoft 365
- Zero Trust Principles for Copilot for Microsoft 365
- Planning a Security Strategy for Copilot for Microsoft 365
- Next Steps to get started with Copilot

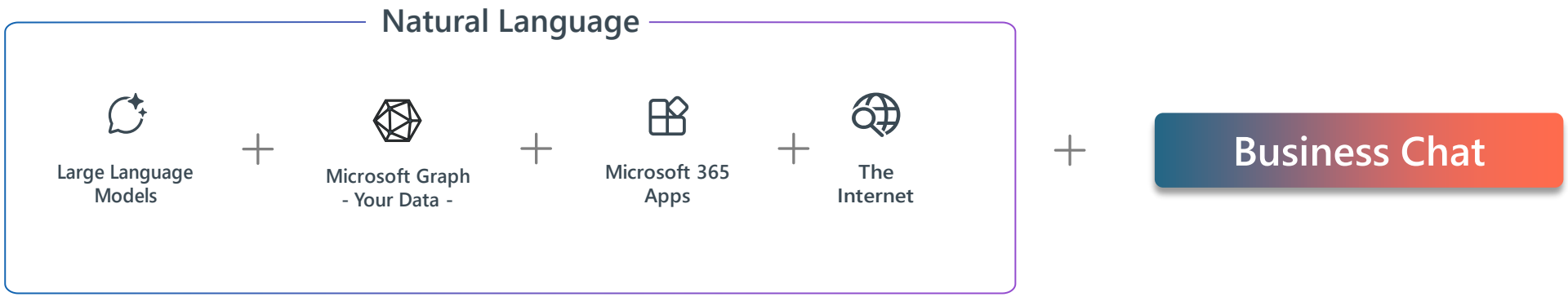
Preparing your customer for Copilot for Microsoft 365

Three layers of Microsoft 365 Copilot

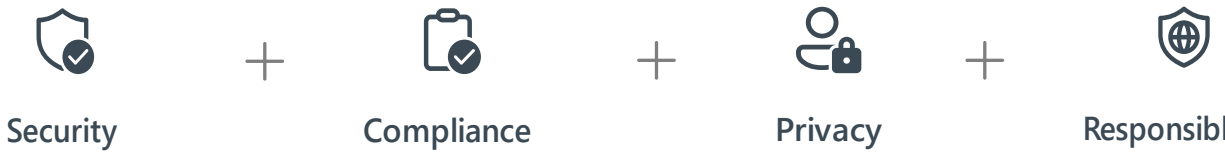
1. Embedded in your customer's Microsoft 365 apps

- Be more analytical in Excel
- Be more productive in Outlook
- Be more creative in Word
- Be more expressive in PowerPoint
- Better meetings in Teams

2. Turns words into a powerful productivity tool

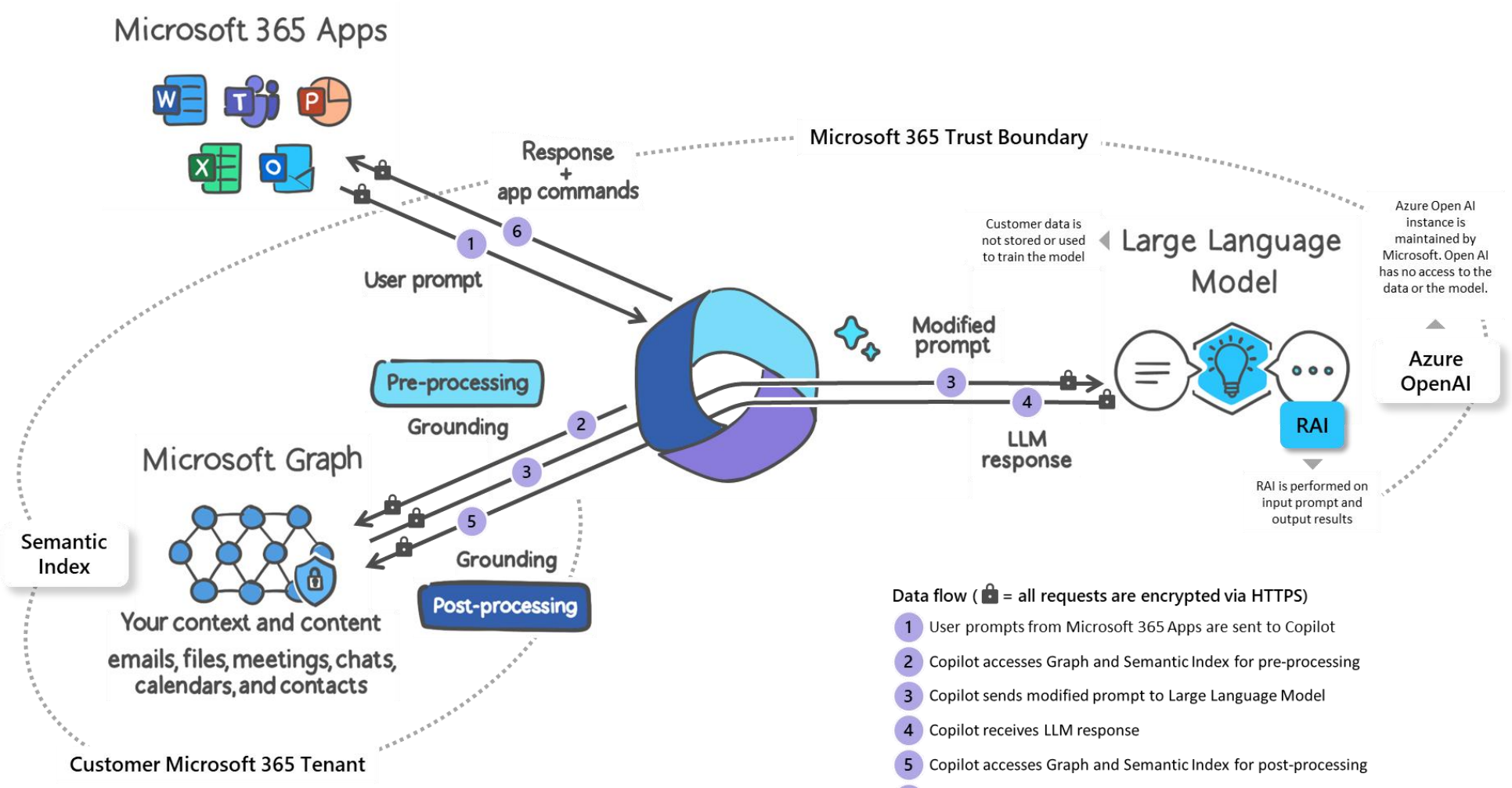


3. Built on Microsoft's comprehensive platform



Crayon

Copilot for Microsoft 365 basic architecture



Data flow (= all requests are encrypted via HTTPS)

1. User prompts from Microsoft 365 Apps are sent to Copilot
2. Copilot accesses Graph and Semantic Index for pre-processing
3. Copilot sends modified prompt to Large Language Model
4. Copilot receives LLM response
5. Copilot accesses Graph and Semantic Index for post-processing
6. Copilot sends the response, and app command back to Microsoft 365 Apps

A Copilot for every Microsoft Cloud experience

Every employee

Copilot for Microsoft 365

Works alongside you in the apps you use every day.

Microsoft Copilot

AI-powered chat with commercial data protection.

Windows Copilot

The first centralized AI assistance on a platform.

Functional business roles

Microsoft Copilot for Sales

Maximize productivity with the AI assistant designed for sellers.

Dynamics 365 Copilot

Turbocharge your workforce with a copilot for every job role.

Security and IT professionals

Microsoft Security Copilot

Defend at machine speed with Microsoft Security Copilot.

Developers and data professionals

GitHub Copilot

Increase developer productivity to accelerate innovation.

Power Platform Copilot

Imagine it, describe it, and Power Platform builds it.

Copilot for Microsoft Fabric

Infusing the power of large language models into Power BI.

Preparing your customer for Microsoft 365 Copilot

Review Licensing

Ensure users are on the appropriate license:

- Office 365 E3
- Office 365 E5
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 A5
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium

Ensure prerequisites for Copilot are in place

- User must have a Entra ID Account
- Some features will require the user to have a OneDrive
- Outlook features require the New Outlook Client (Classic support for Copilot is on the roadmap)
- Set Microsoft 365 App update channel to either Current, Monthly Enterprise or Preview Channels

Validate Microsoft 365 Adoption

- Review tenant adoption report
- Drive usage across the tenant, well adopted environments are ideal

Optimise your environment for Copilot

- Run and review the Copilot Optimisation Assessment
- Review your security policies and access controls
- Review your Information Architecture and Data Governance

Crayon

Zero Trust Principles for Copilot for Microsoft 365

Zero Trust Principles

Verify explicitly

Requirement: Always authenticate and authorize based on all available data points.
Met By: Use Entra to enforce the validation of user credentials, device requirements, and app permissions and behaviours.

Least privileged access

Requirement: Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
Met By: Validate JEA across your organization to eliminate oversharing by ensuring that correct permissions are assigned to files, folders, Teams, and email. Use Purview to create sensitivity labels and data loss prevention policies to protect data.

Assume breach

Requirement: Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.
Met By: Use Exchange Online Protection (EOP) and Microsoft Defender XDR services to automatically prevent common attacks and to detect and respond to security incidents.

Crayon

Security and Compliance controls for Copilot for Microsoft 365

Essential security controls

Copilot + M365 Business Standard

Multi-factor Authentication with security defaults

Device-based access & security controls for M365 resources

Basic content and keyword search for Copilot generated data

Comprehensive security controls

Copilot + Microsoft 365 Business Premium

Everything in M365 Business Standard, plus:

Conditional Access policies based on identity, device, location, & network

Terms of use policies to accept before getting access

Restrict saving business data and files to approved applications only

Protect sensitive M365 data from exfiltration and improper use (files & emails only)

eDiscovery, litigation hold and retention policies

Note: Not all features/products shown.

Security and compliance value for Copilot for M365 in Business Standard and Business Premium

	Scenario	Business Standard	Business Premium
Identity & Access Management	Login to Copilot for Microsoft 365 with a single identity	•	•
	Enforce MFA when accessing Microsoft 365 to use Copilot	Basic MFA	•
	Enable end-user password reset, change, and unlock when accessing Microsoft 365	Cloud only	•
	Implement Conditional Access policies based on identity, device, and location when accessing Microsoft 365 to use Copilot		•
	Enable near real-time access policies enforcement, evaluate critical events, and immediately revoke access to Microsoft 365		•
	Require employees or guests to accept terms of use policy before getting access		•
Endpoint Management	Push/deploy Microsoft 365 apps to devices and grant access to Copilot in those apps		•
	Manage Microsoft 365 app updates		•
	Restrict the use of Microsoft 365 apps and Teams – as well as Copilot in those apps – on personal devices		•
	Prevent saving files – including those generated by Copilot – to unprotected apps		•
	Wipe all work content – including content generated by Copilot – if a device is lost, stolen or compromised	•	•
	Revoke work access on noncompliant devices	Except Windows	•
Data security & compliance	Search for Copilot generated data by content, keyword search, apply legal hold, and export the search results; investigate incidents related to Copilot and respond to litigations	Content, keyword search, and export only	Standard
	Audit logs for Copilot interactions	Standard	Standard
	Apply a retention or deletion policy for Copilot interactions	•	•
	Data Loss Prevention policies to protect sensitive data, generated by Copilot and saved in Microsoft 365 locations, from exfiltration		Files & email
	Prohibit Copilot from summarizing or including data that users have no extract permissions in its response messages for the said users		•
	Exclude sensitive files that users have no view permission from being processed by Copilot for the said users	•	•

Security and Compliance controls for Copilot for Microsoft 365

Baseline security

Copilot +
Office 365 E3

Multi-factor Authentication
with security defaults

Manual sensitivity labels
for Copilot generated content
(Office only)

Core security controls

Copilot +
Microsoft 365 E3

Conditional Access
policies based on identity, device, location, & network

Manual sensitivity labels
for **non-Microsoft** documents
(e.g., pdf)

Endpoint management
capabilities

Best in class security controls

Copilot +
Microsoft 365 E5

User/session risk
and access control

Automatic sensitivity labels
for **non-Microsoft** documents
(e.g., pdf)

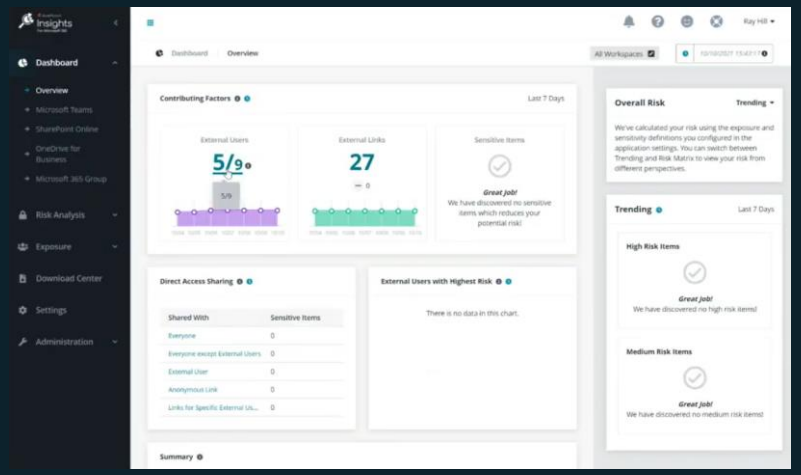
Discover and evaluate the risk of 400+ **AI apps** & implement **controls to for their use** at work

O365 and M365 security value for Copilot

	Scenario	O365 E3	M365 E3	M365 E5
Identity & Access Management	Login to Copilot for Microsoft 365 with a single identity	•	•	•
	Enforce MFA when accessing Microsoft 365 to use Copilot	Basic MFA	•	•
	Enable end-user password reset, change, and unlock when accessing Microsoft 365	Cloud only	•	•
	Implement Conditional Access policies based on identity, device, and location when accessing Microsoft 365 to use Copilot		•	•
	Enable near real-time access policies enforcement, evaluate critical events, and immediately revoke access to Microsoft 365		•	•
	Control access over cloud apps (Microsoft 365 and third party)			•
	Review who has access to content in Microsoft 365 – Copilot – to reduce oversharing			•
	Require just-enough and just-in-time approval for admin roles that can manage Copilot app access			•
Endpoint Management	Push/deploy the Microsoft 365 apps to devices and grant access to Copilot in these apps		•	•
	Manage Microsoft 365 apps updates		•	•
	Restrict the use of the Microsoft 365 apps and Teams – as well as Copilot in these apps – on personal devices		•	•
	Prevent saving files – including those generated by Copilot – to unprotected apps		•	•
	Wipe all work content – including content generated by Copilot – if a device is lost		•	•
	Revoke work access on noncompliant devices		•	•
Data security & compliance	Search for Copilot generated data by content, keyword search, apply legal hold, and export the search results; investigate incidents related to Copilot and respond to litigations	Standard	Standard	Premium
	Audit logs for Copilot interactions	Standard	Standard	Premium
	Apply a retention policy for Copilot interactions	Standard	Standard	Automated
	Data Loss Prevention policies to protect sensitive data, generated by Copilot and saved in Microsoft 365 locations, from exfiltration	Files & email	Files & email	+ Endpoint, Teams
	Inherit sensitivity labels and cite sensitivity label in output and references in Copilot	•	•	•
	Prohibit Copilot from summarizing or including data that users have no extract permissions in its response messages for the said users	•	•	•
	Exclude sensitive files that users have no view permission from being processed by Copilot for the said users	•	•	•
	Label and protect Microsoft 365 content, used by Copilot	Office only	Manual	Automated
	Detect business or code of conduct violations for Copilot prompts and responses			•
	Prevent Copilot access to content encrypted with Double Key Encryption			•
	Use ready-to-use machine learning trainable classifiers to identify sensitive information and create custom classifiers			•
Threat Protect	Discovery and risk evaluation across 400+ AI apps in an organization			•
	Ability to block or sanction the use of any discovered AI app in the organization			•

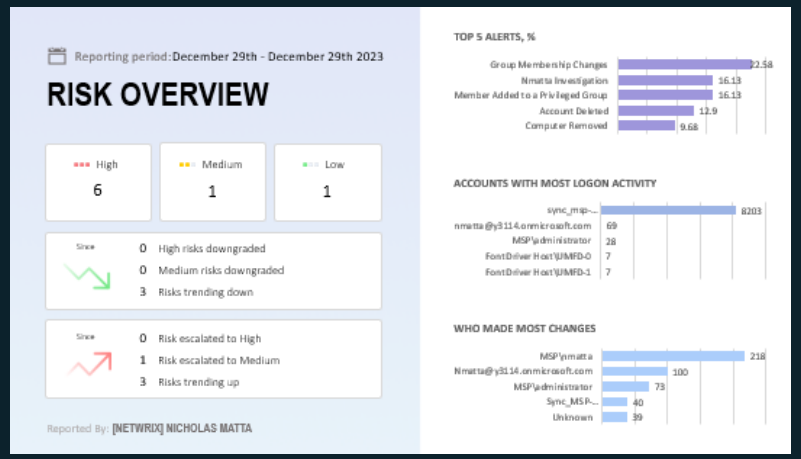
Compliment your Copilot security strategy

AvePoint Insights



AvePoint Insights is a tool that helps you monitor Office 365 permissions by providing tenant-wide security reports across your Microsoft cloud services. It aggregates sensitivity and activity data across your tenant, prioritizing critical permissions issues for action. You can then edit these issues in bulk from actionable reports. This makes securing collaboration in Teams, Groups, Sites, and OneDrive easier.

Netwrix 1Secure



Netwrix 1Secure is a SaaS solution designed to help partners secure and support multiple clients' Microsoft 365 systems, file servers, and data from a single console. This solution is efficient and cost-effective, allowing MSPs to stand out in the market and keep their clients' data safe.

Crayon

Planning a Security Strategy for Copilot for Microsoft 365

Key considerations for security with Copilot for Microsoft 365

Data Protection	User Access	Application Protection	Device Management and Protection
To prevent your organization's data from being at risk of overexposure or oversharing, you must ensure that your data is properly categorized organized and protected.	To prevent bad actors from using Copilot to more quickly discover and access sensitive data, the first step is to prevent them from gaining access through strong access policies and regular access reviews.	Enforce Application Protection policies can prevent the inadvertent or intentional copying of Copilot-generated content to apps on a device that are not managed by the organisation	Ensure that your devices are managed, monitored and protected with the appropriate policies, to prevent bad actors from compromising and using devices to gain access to Copilot and company data.

Discover – Know your data and understand the risks

Knowing your Data

What is sensitive?

- Define what is sensitive to the organization
- Generic & customer specific
  - Company secrets
  - Highly confidential
  - Personal Identifiable Information

Where does data live?

- Created inventory of all data repositories
- Considered as copilot source
  - Microsoft 365
  - 3rd party sources
  - Structured and unstructured

Who has access?

- What content can employee access
- Internal & external to the organization
- Access control and access management
- Oversharing

How is it used?

- Sensitive data overexposure
- Unprotected data
- Is the use of sensitive data managed

What is the risk?

- What if data is exposed
- Which data could harm the organization
- What would be the impact & cost
- Are we at risk
- Are we compliant

Protecting your data

Implement controls to mitigate and reduce risk.

Data Lifecycle controls

- Minimize obsolete data
- Retention policies and automatic deletion
- Records management for business, legal or regulatory record keeping requirements

Data Protection controls

- Protect sensitive information
  - Data encryption
  - Watermarking
- Prevent Data loss
- Protect against Oversharing and external sharing

Data access controls

- Optimize access permissions, remove, block
- Correct oversharing
- Exclude data sources

Data labeling

- Apply sensitivity labels to data
- Manual, user initiated
- Automatic, based on content, location, purpose, etc.

Data classification

- Select and define sensitive info types
  - Generic, out of the box
  - Customer specific, custom defined to specification

Organizational risk tolerance define next steps.

Low risk
Enable copilot

Medium risk
Implement (additional) data security and in parallel enable coplot.

High risk
Implement data security before enabling copilot

Elevate Productivity

Discover – Protect user access to Microsoft Copilot for Microsoft 365

Use strong authentication and real-time, risk-based adaptive access policies without compromising user experience

Can users access?

- Are Entra ID identities being used?
- Are on-premise identities being used and are they synchronized to Entra ID?

Who has access?

- Do different groups of users require different access permissions?
- Do you use strong authentication methods to prevent credentials theft?
- Do you review access?

Is access controlled?

- Do you have adaptive access policies in place based on location, device risk or user risk?
- Do admins have just-enough and just-in-time access to manage access to data and resources?

Is access fast and simple?

- Do users need multiple accounts and passwords to access data and resources?
- Do users need to re-enter their credentials to access different resources?
- Can users reset or change their own password?

What is the risk?

- What if data is exposed outside of the company?
- What if the wrong users access sensitive data?
- What would be the impact & cost?
- Are we at risk?
- Are we compliant?

Protect

Implement controls to mitigate and reduce risk.

Review access

- Review and manage user access using access reviews for group members or application access

Seamless access

- Setup single sign-on to provide an easy and fast sign-in experience
- Setup self-service password reset and change, and account unlock.
- Setup passwordless authentication

Secure adaptive access

- Setup conditional access policies based on device compliance, user and location or real-time risk.
- Enable just-in-time and just-enough access for admin roles

User access

- Create user groups that require different access permissions
- Setup multifactor authentication to verify a user's identity

User identity

- Setup a single identity for users to access data and resources
- Synchronize on-premise identities to the cloud

Organizational risk tolerance define next steps.

Low risk
Enable copilot

Medium risk
Implement (additional) Identity & Access management features and policies, and in parallel enable coplot.

High risk
Implement Identity & Access management before enabling copilot

Elevate Productivity

Discover – Secure apps used to access to Microsoft Copilot for Microsoft 365

Control how data is accessed and shared by apps on mobile devices

On which devices?

- Do users access Microsoft 365 apps from personal devices?
- Do users access Microsoft 365 apps from third-party MDM managed devices?
- Do users access Microsoft 365 apps from unmanaged devices?

Which apps?

- From which Microsoft 365 apps do users need access to Microsoft 365 and Microsoft Copilot?
- Do users need access to Microsoft 365 from third-party apps?
- Are users allowed to use personal apps?

Are apps protected?

- Is a PIN, fingerprint or face ID required to access corporate apps?
- Can certain actions to move or access corporate data be prohibited or monitored within the apps?

How is data shared?

- Can you control how corporate data is shared between corporate and personal apps or storage locations?

What is the risk?

- What if shadow IT is used to access company data?
- What if corporate data is exposed to personal apps or public locations?
- What would be the impact & cost?
- Are we at risk?
- Are we compliant?

Protect

Implement controls to mitigate and reduce risk.

Wipe app data

- Selectively wipe corporate data from the managed apps when a user leaves the company or when an un-managed device is lost or stolen.

Define managed locations

- Setup OneDrive for Business
- Prevent the saving of company app data to a personal storage location

Set approved apps

- Restrict access to Microsoft 365 to only approved apps

Restrict app data usage

- Require a PIN, fingerprint or face ID to access an app in work context
- Control the sharing of data between corporate and personal apps (Restrict cut, copy, and paste)

Protect apps

- Setup app protection policies to protect the core Microsoft apps
- Setup app protection policies to protect supported third-party apps
- Protect in-house built apps

Organizational risk tolerance define next steps.

Low risk
Enable copilot

Medium risk
Implement (additional) mobile application management features and policies, and in parallel enable coplot.

High risk
Implement mobile application management before enabling copilot

Elevate Productivity

Discover – Secure access to Microsoft Copilot for Microsoft 365 from any device

Ensure that only secure, up-to-date and compliant Windows physical or virtual devices and mobile devices have access

Which devices?

- Windows physical devices
- Windows virtual devices (Windows 365 or AVD)
- Android Devices
- iOS/iPadOS devices
- macOS devices

Are devices managed?

- Are users accessing Microsoft 365 from unmanaged devices?
- Are users accessing Microsoft 365 from an MDM managed device?
- Are devices company-owned or personal?

Are apps up to date?

- Are the Microsoft 365 apps deployed remotely to all types of managed devices?
- Are the Microsoft 365 apps up to date for Copilot?

Are devices secure?

- Are security policies in place to protect devices from vulnerabilities and threats and improve compliance?
- Are devices up to date with the latest OS version?

What is the risk?

- What if compromised devices are used to access company data?
- What if corporate data is exposed?
- What would be the impact & cost?
- Are we at risk?
- Are we compliant?

Protect

Implement controls to mitigate and reduce risk.

Wipe devices

- Fully wipe lost or stolen devices
- Wipe all work content on unmanaged devices including content generated by copilot when an employee leaves the company

Revoke access

- Revoke access to non-compliant devices
- Remediate non-compliant devices

Set compliance

- Deploy device compliance policies
- Create conditional access policies based on device compliance for accessing Microsoft 365

Manage apps

- Deploy Microsoft 365 apps
- Deploy app configuration policies
- Deploy app update policies

Manage devices

- Enroll devices into device management
- Deploy device configuration policies
- Deploy device protection policies
- Deploy OS update policies

Organizational risk tolerance define next steps.

Low risk
Enable copilot

Medium risk
Implement (additional) endpoint management features and policies, and in parallel enable coplot.

High risk
Implement endpoint management before enabling copilot

Elevate Productivity

Next Steps

Call to Action

- Review the Copilot Adoption Kit
- Sign up for the Microsoft Solution Assessment
- Attend the Crayon SMB Masters Program
- Watch the Copilot for Microsoft 365 Tech Accelerator (VOD)
- Watch the AvePoint Expand Your MSP Business with Copilot for Microsoft 365 Webinar (VOD)
- Follow us on LinkedIn
- Follow Microsoft, AvePoint and Netwrix on LinkedIn

Crayon

Partner Incentives

Netwrix Copilot Incentive

Crayon MSP partners will be given the security assessment reporting module at no cost with any Netwrix 1Secure subscription.
This module enables our MSP partner to automatically produce a risk report deliverable on credentials and data that also tracks risk growth/improvement over time.
For more details please contact your account manager

Earn up to $2,000 cashback with Microsoft 365 Copilot

Dive into this incredible chance to elevate your M365 Copilot earnings while empowering your customers with the transformative potential of AI.
Simply, the more you sell Copilot, the more you can supercharge your earnings.
https://clicklive.rhipe.com/M365Copilot-IncentiveOffer.html

Useful Links

Manage access to tiles and sites	https://learn.microsoft.com/en-us/microsoftsearch/manage-access-files-sites
Sharing and permissions in the SharePoint modern experience	https://learn.microsoft.com/en-us/sharepoint/modern-experience-sharing-permissions
Learn about Data Loss Prevention	https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
Enable content on a site to be searched	https://learn.Microsoft.com/en-us/sharepoint/make-site-content-searchable
Data access governance reports for SharePoint sites	https://learn.microsoft.com/en-us/SharePoint/data-access-governance-reports
Basic Security Set Up for Microsoft 365	https://learn.microsoft.com/en-us/Microsoft-365/community/basic-security-set-up-for-microsoft-365
Microsoft 365 isolation controls	https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-365-isolation-controls
Configure your Microsoft 365 tenant for increased security	https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-wide-setup-for-increased-security

Crayon

Questions

55 experts across 5 portfolios and 30+ vendors

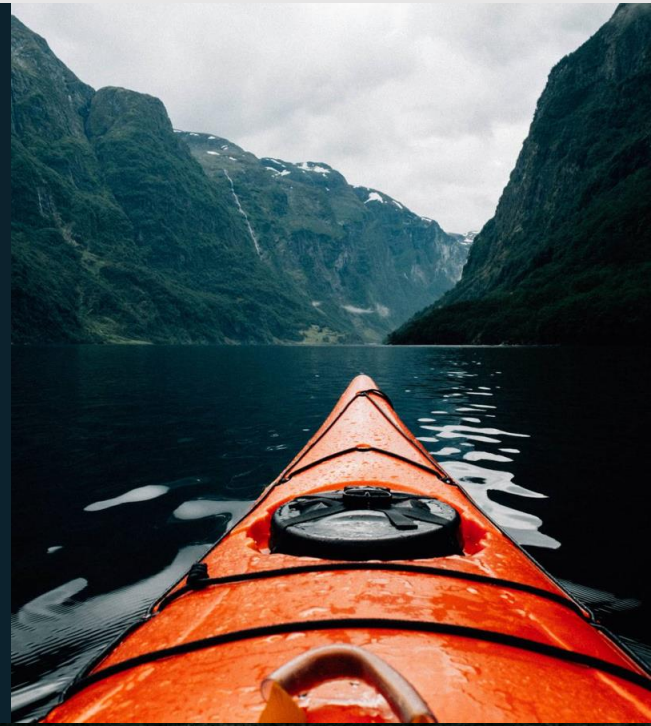
Business Apps	Business Continuity	Cloud	Productivity	Security
6 experts	5 experts	11 experts	8 experts	25 experts
Microsoft Power BI, Power Apps, Power Automate, AI Builder, Power Virtual Agents Dynamics 365 Customer Service, Marketing, Field Service, Sales Business Central, Finance, Project Operations, Supply Chain	veeam AvePoint Acronis skykick BACKUP365 Runecast Crayon Backup As a Service	Microsoft vmware by Broadcom OCTOPUS nerdio wasabi Cloud Ctrl	Microsoft SIGNIFLOW zimbra access4 DocuSign swoosh	AIRLOCK DIGITAL, Delinea netwrix, TREND MICRO eset, usecure SMX, BlackBerry probax, ninjaOne CoreView, HORNETSECURITY DNSFilter, AUTOMOX SMARTENCRYPT by rhype, Invicti

Crayon

Extend your capabilities

Crayon Channel Services

- ERP Implementation
- Azure Migration Services
- Essential 8 Security Assessment
- Cloud Security Assessment
- Backup-as-a-Service
- Cloud Cost Optimisation
- Support-as-a-Service



Crayon Group - Classification: Public