



span

MICROSOFT 365 COPILOT TECHNICAL READINESS

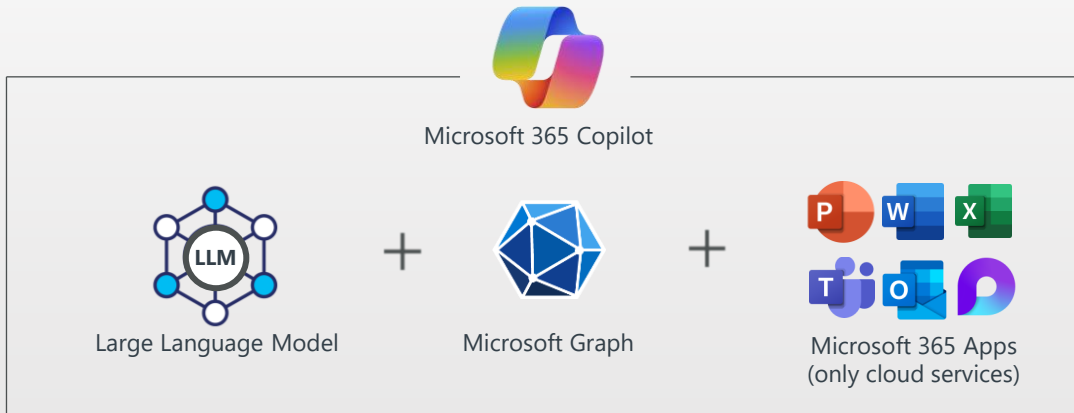
www.span.eu



MICROSOFT 365
COPILOT

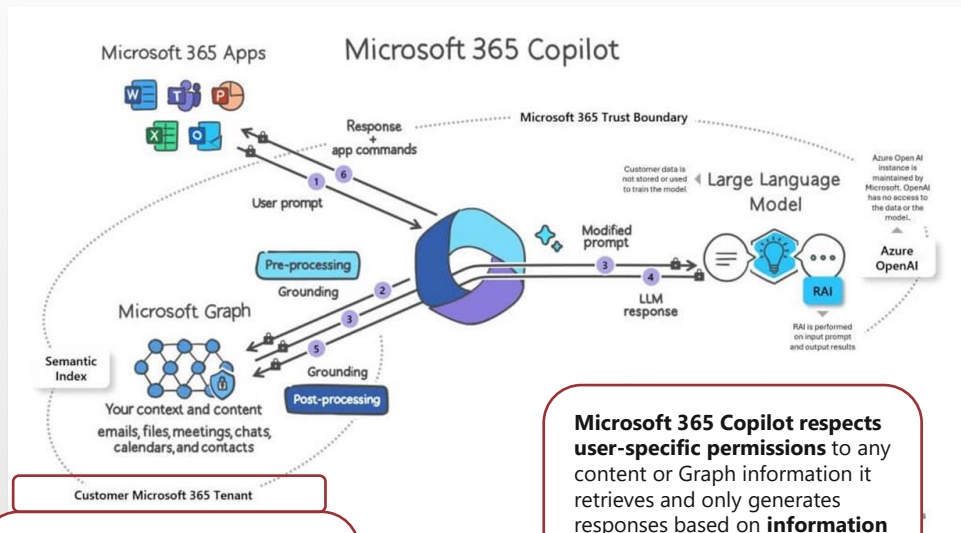
WHAT IS MICROSOFT 365 COPILOT?

Microsoft 365 Copilot is an AI-powered feature integrated into **Microsoft 365 apps**, leveraging the strengths of **Large Language Models (LLMs)** with your **business data within Microsoft Graph** – your calendar, emails, chats, documents, meeting, and more - to boost your productivity in applications like Outlook, Teams, Word, PowerPoint and others.



HOW MICROSOFT 365 COPILOT WORKS ?

- Copilot **receives an input prompt** from a user in an app, e.g., Word, PowerPoint
- Copilot **preprocesses the input prompt through grounding calls in Microsoft Graph**, improving the specificity of the prompt, to provide answers that are relevant and actionable to specific task
- Copilot **sends the prompt to LLM for processing**, accessing the data that individual user has access to (e.g., existing, Microsoft 365 role-based access controls)
- Copilot **takes the response from the LLM and post-process it again** through grounding calls to Microsoft Graph, responsible AI checks, security, compliance and privacy reviews
- Copilot **returns the response to the app**, where user can review and assess the response



Microsoft 365 Copilot is designed to **work within your Microsoft 365 tenant**, i.e., it is available only to users who have access to your organization's Microsoft 365 account.

Microsoft 365 Copilot respects **user-specific permissions** to any content or Graph information it retrieves and only generates responses based on **information that a user has explicitly permissions to access**.

MICROSOFT 365 COPILOT VALUE & BENEFITS

Value

- **Productivity**
 - Increased efficiency
 - Boosted creativity
 - Focused working
- **Workflow**
 - Structured emails
 - Productive meetings
 - Content writing and creation
 - Effective search
 - Data analysis
- **Role**
 - Sales
 - Human resources
 - Finance
 - Marketing
 - IT




Benefits

- **Productivity**
 - Focus is shifted on important work
 - Less time is spent on repetitive tasks
 - Easy to use with no additional installations
- **Workflow**
 - Less time is spent on processing content
 - Faster design of first drafts and ideas
 - Search is customized based on user preferences and needs
- **Role**
 - Tasks are completed faster
 - Insights in needed data is more streamlined
 - Time management is more efficient
 - Enhanced security for business

Results

- **Boost in employee's productivity**
- **Growth in business opportunities**
- **Reduced costs of doing business**
- **Increased employee's wellbeing**
- **Strategic competitiveness**

BING CHAT AND MICROSOFT 365 COPILOT COMPARISON

	 Bing Chat	 Bing Chat Enterprise	 Microsoft 365 Copilot
	Personal	Work	Work
GPT Large Language Model	✓	✓	✓
AI-Powered Web Search	✓	✓	✓
Commercial Data Protection		✓	✓
Enterprise Security, Privacy & Compliance			✓
Microsoft 365 Graph (content & context)			✓
Microsoft 365 Apps			✓

MICROSOFT COPILOTS OVERVIEW



Copilots for Web – available

M365 Copilot – not available in all apps yet

Windows Copilot – due to Europe’s privacy protection laws, it is only available in US, UK, and selected countries in Asia and South America

Dynamics Copilot – partially available (US only, announcement for Sweden, Australia, and UK)

Fabric Copilot – in private preview

Security Copilot – in private preview

GitHub Copilot – available

Power Platform Copilot - partially available (US only, announcement for Sweden, Australia, and UK)

MICROSOFT 365 COPILOT IN **SHORT**



Grounded in
your business data

Microsoft 365 Copilot has real-time access to both your *content and context* in the Microsoft Graph.



Comprehensive
security, compliance, & privacy

Copilot inherits your security, compliance, and privacy policies set up in Microsoft 365, and is compliant with GDPR and EUDB*



Architected to protect
data

Your data never leaves its secure partition, and it is never used for training purposes.



Integrated into the
apps you use every day

Word, Excel, PowerPoint, Outlook, Teams, and more.



Individual user & admin
always in control

User decides what to use, modify, or discard.



Designed to
learn new skills

As Copilot learns about processes, it can perform more sophisticated tasks and queries.

**GET READY FOR
MICROSOFT 365 COPILOT**

WHY DO YOU NEED TO GET **READY?**

Microsoft 365 Copilot searches for **information from your organization's tenant** and can only surface organizational data to which individual users have **at least view permissions**.

Ungoverned data

- 52% of all data within organisations is **unclassified or unlabelled**, indicating that organisations have **limited or no visibility** over vast volumes of potentially business-critical data
- 76% of organizations owns data that is **redundant, obsolete, or trivial** (ROT), and have **no data retention governance** in place
- Only 34% of employees use their organization's **sanctioned cloud storage and file sharing tools**

No formal data processes

- 43% of organizations have **no formal process for creating and managing SharePoint sites**
- 13% of **shared files are visible to the entire organization**, number is even higher without implemented file sharing processes and security policies
- 46% of employees still use **email to share documents** with colleagues or with **'anyone can access'** option.

Low adoption

- Only 29% of employees use their organisation's official content management system to **store and manage documents**
- When using existing organization's tools, users are **not well informed and trained** in governance and processes and are **leaning back** to 'old' ways of working

DATA PROTECTION AND GOVERNANCE ASSESSMENT



SERVICES IN SCOPE OF TECHNICAL ASSESSMENT

• Microsoft Entra ID

- Users
- Roles
- Security groups

• Exchange Online

- Mailbox size
- Activity
- User access

• SharePoint and OneDrive for Business

- Standalone SharePoint sites
- Personal and group-connected sites

• Microsoft Teams

• Viva Engage



TECHNICAL ASSESSMENT **ACTIVITIES**

● **Permission analysis**

- Report user permission
- Role-based access control

● **Governance policies review**

- SharePoint and OneDrive sharing policies
- Retention and archiving policies

● **Usage and activity reports**

- Total number of files stored in SharePoint sites and how many files are actively being used
- Storage consumption report across all multiple services

● **Sites and M365 group membership report**

- Detailed permission matrix report, cross-referencing site members and departments
- Review group privacy restrictions
- Identify 'orphaned' sites and groups. i.e., missing or not having owners

● **Content consumption across the organization**

- Identify on-premise content that is viable for migration to Microsoft 365, to utilize all the additional features and benefits it provides

TECHNICAL ASSESSMENT OUTPUT

RECOMMENDATIONS FOR **SHORT TERM ACTIONS**

● **Implement governance policies best practices**

- Manage users access to your organization's resources
- Establish compliance with your business standards
- Ensure security of your data

● **Implement retention and archiving policies**

- Efficiently manage, retain, and preserve organizational data in compliance with regulatory requirements
- Facilitate easy accessibility and safeguarding against data loss
- Ensure the quality of search results for efficient information retrieval

● **Provide a roadmap to increase security posture**

- Establish a plan outlining measures, priorities, and actions to fortify and enhance organization's overall security framework

● **Validate user access using Search in the context of different roles and departments**

- Improve your overall information access and protection

TECHNICAL ASSESSMENT OUTPUT

RECOMMENDATIONS FOR LONG TERM ACTIONS

● Just Enough Access

- Ensure users have the precise level of permissions necessary to perform their roles or tasks without excess access, thereby reducing potential security risks

● Microsoft Syntex - Advanced management capabilities

- Implement advanced access policies for secure content collaboration:
 - Site access restriction for SharePoint sites
 - Restrict OneDrive access to a security group
 - Data access governance reports for SharePoint sites, used to discover sites that contain potentially overshared or sensitive content
 - Enforce more stringent access conditions using access policy for SharePoint sites and OneDrive
 - Secure SharePoint document libraries using sensitivity labels

● Microsoft Purview Information Protection

- Identify files in SharePoint sites and OneDrive locations (including Microsoft Teams files) containing sensitive information or classified content
- Auto-apply controls to limit and/or block access

● Identity governance and Entitlement Management

- Manage and control user access rights and permissions across Entra ID and related M365 services, ensuring security, compliance, and streamlined access management.

● Privileged Identity Management and Conditional Access

- Govern and regulate access to sensitive resources.
- Define policies that adapt access based on specific conditions and user scenarios, collectively enhancing security and minimizing risks.

● Migrate on-premise content to Microsoft 365

TECHNICAL REQUIREMENTS



TECHNICAL REQUIREMENTS



Licenses

- Microsoft 365 E3 or E5
- Microsoft 365 Copilot
 - Current Microsoft requirement is at least 300 licenses per enterprise



Microsoft 365 Apps for Enterprise version of Office:

- User devices update channel must be *Current Channel* or *Monthly Enterprise*
- Allow the use of *Connected Experiences* in Office



Microsoft Entra ID

- Users must have *Microsoft Entra ID* (formerly Azure Active Directory)



New Outlook client and access to M365 apps

- For full Copilot experience users must be switched to *new Outlook (Monarch) client*
 - Classic Outlook for Windows will be supported in the future (rollout start March 2024)
 - User must be enabled for OneDrive, Teams and Loop to use Copilot features in those apps



Network requirements

- Network traffic towards *Microsoft 365 endpoints* must be allowed



span

THANK YOU!

www.span.eu