Microsoft

Learning Path 1:

Prepare your organization for Microsoft 365 Copilot

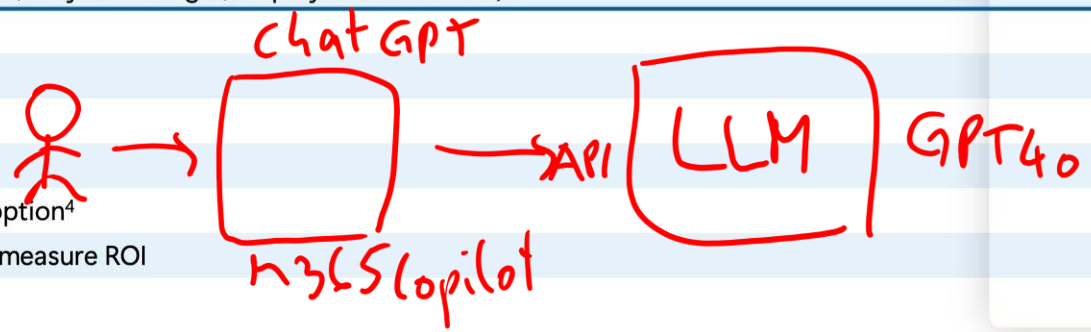
Learning Path agenda

Module 1: Implement Microsoft 365 Copilot

Module 2: Examine data security and compliance in Microsoft 365 Copilot

● Included ▲ Included — Metered

		Microsoft 365 Copilot Chat Free + Consumption	Microsoft 365 Copilot $30 pupm
Chat	Copilot Chat – Web grounded (powered by GPT-4o)	●	●
	Copilot Chat – Work grounded (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)		●
	Copilot Pages	●	●
	File upload[1]	●	●
	Code Interpreter[1]	●	●
	Image generation[1]	●	●
Agents[2]	Create agents using Copilot Studio[3], including SharePoint agents	●	●
	Discover and pin agents	●	●
	Use agents grounded in Web data	●	●
	Use agents grounded in work data (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)	▲	●
	Use agents that act independently using autonomous actions	▲	▲
Personal assistant	Copilot reasons over personal work data (e.g., Outlook, OneDrive, Teams meeting transcripts and chats)		●
	Copilot in Teams		●
	Copilot in Outlook		●
	Copilot in Word		●
	Copilot in Excel		●
	Copilot in PowerPoint		●
	Copilot Actions		In preview
	Pre-built M365 agents (Interpreter, Facilitator, Project Manager, Employee Self-Service)		In preview
Copilot Control System	Enterprise Data Protection (EDP)	●	●
	IT management controls	●	●
	Agent management	●	●
	SharePoint Advanced Management		●
	Copilot Analytics to measure usage and adoption[4]		●
	Pre-built reports and advanced analytics to measure ROI		●

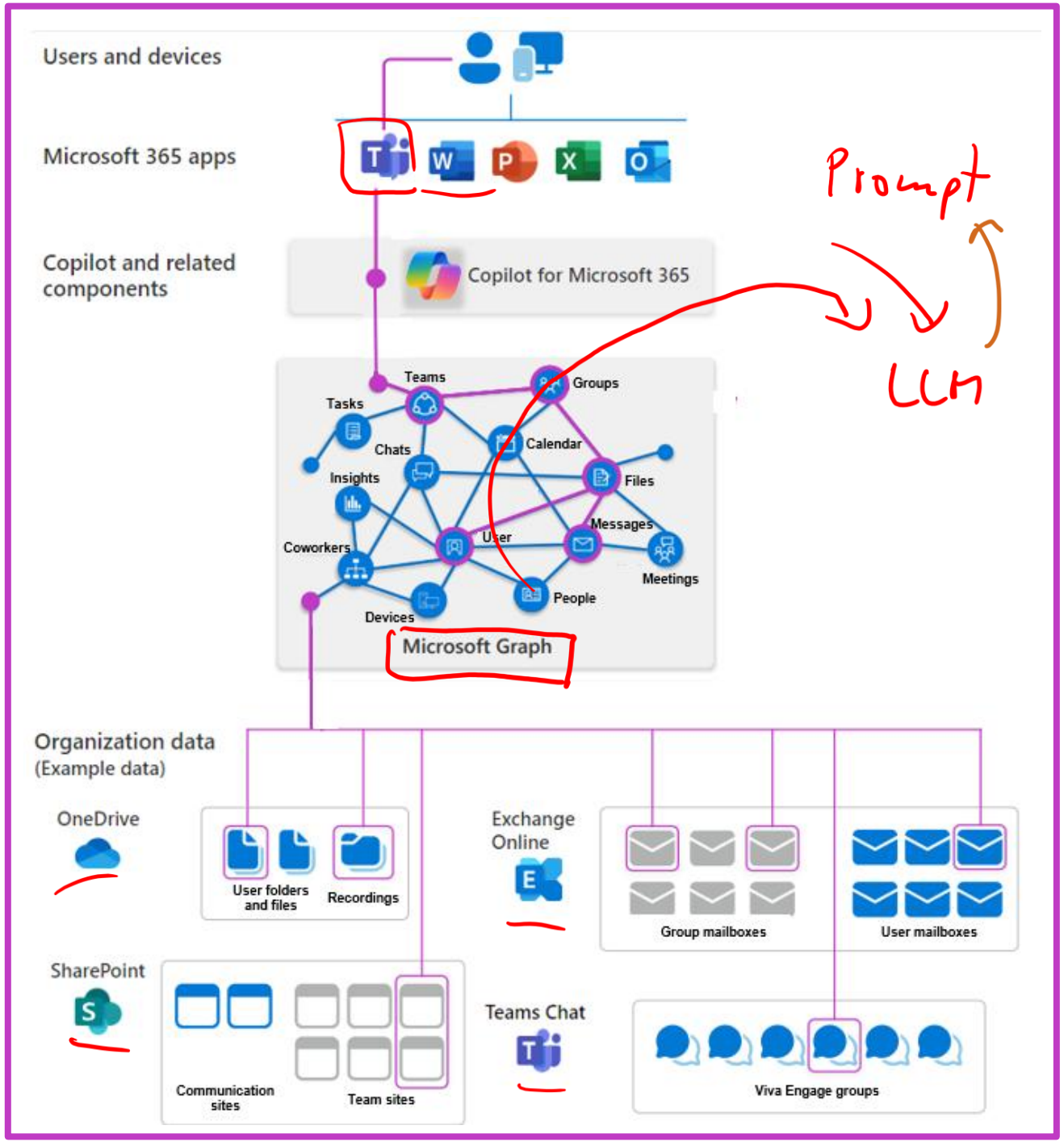


1. Limits apply. 2. Applies to employee-facing agents only. 3. Learn more about the full capabilities of Copilot Studio: aka.ms/CopilotStudioCapabilities 4. Basic reporting in Microsoft Admin Center available for Copilot Chat.

Examine the Copilot for Microsoft 365 logical architecture

Copilot's logical architecture

- Users can initiate Copilot prompts from devices that have Microsoft 365 apps installed.
- Copilot components include:
  - The Copilot service, which orchestrates the responses to user prompts.
  - An instance of the Microsoft Graph for the data of your Microsoft 365 tenant.
  - Your Microsoft 365 tenant that contains your organization data.



Examine the key components of Copilot for Microsoft 365

LLMs

- Specialize in understanding and generating human-like text
- Operate as generative AI, producing new content
- Provide the engine that drives Copilot capabilities
- Privately hosted on the Azure OpenAI Service

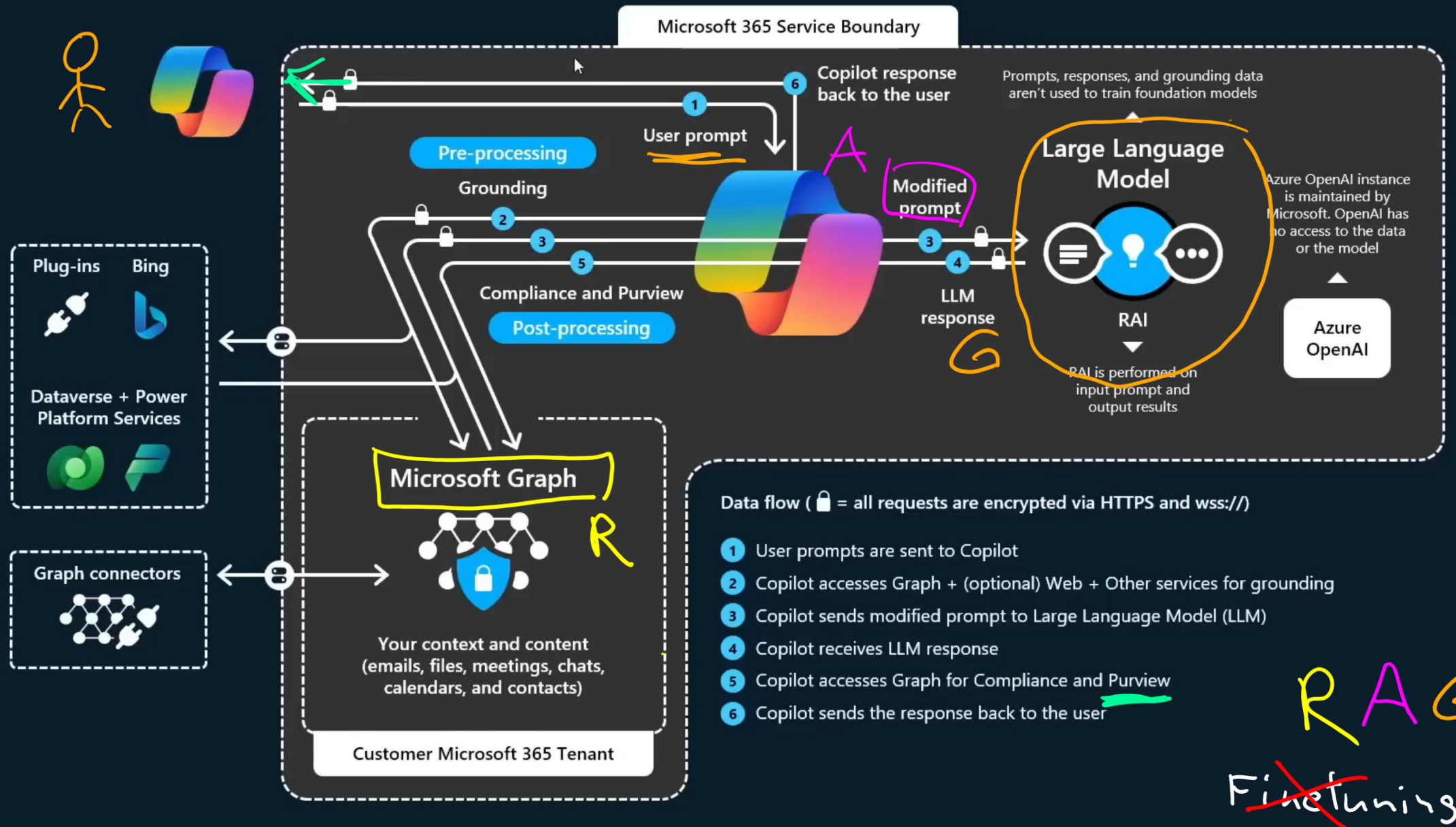
Natural Language Processing (NLP)

- Key AI technology for machines to understand, interpret, and respond to human language
- Components include Tokenization, Semantic Analysis, Sentiment Analysis, and Language Translation

Microsoft 365 Apps

- Collaborate seamlessly with Copilot, enhancing user support across the entire Office Suite
- For example, Copilot in Word specifically assists users in the process of creating, comprehending, and editing documents

Copilot for Microsoft 365 architecture

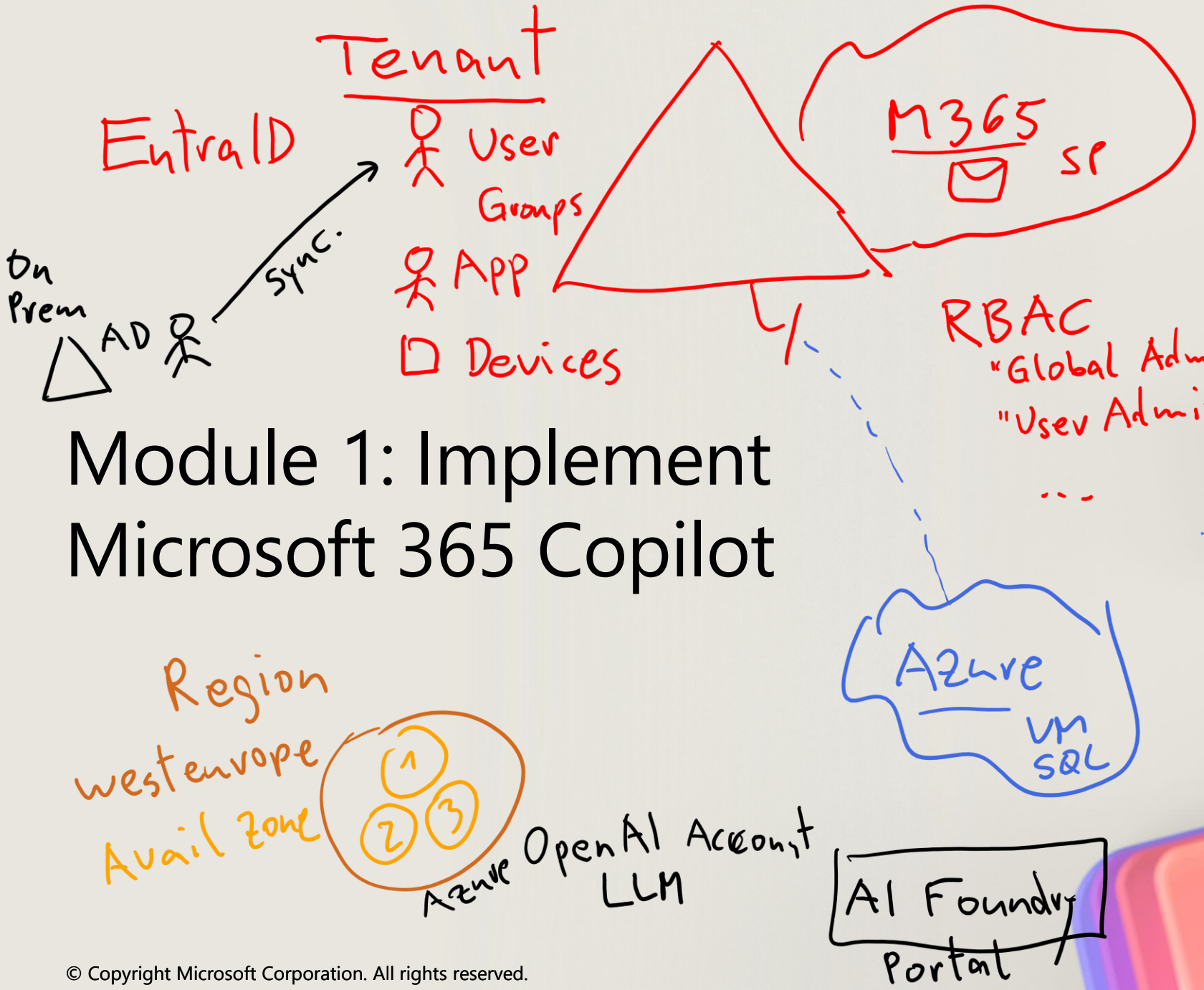


Data flow (🔒 = all requests are encrypted via HTTPS and wss://)

1. User prompts are sent to Copilot
2. Copilot accesses Graph + (optional) Web + Other services for grounding
3. Copilot sends modified prompt to Large Language Model (LLM)
4. Copilot receives LLM response
5. Copilot accesses Graph for Compliance and Purview
6. Copilot sends the response back to the user

RAG

~~Fine~~tuning



Module 1: Implement Microsoft 365 Copilot

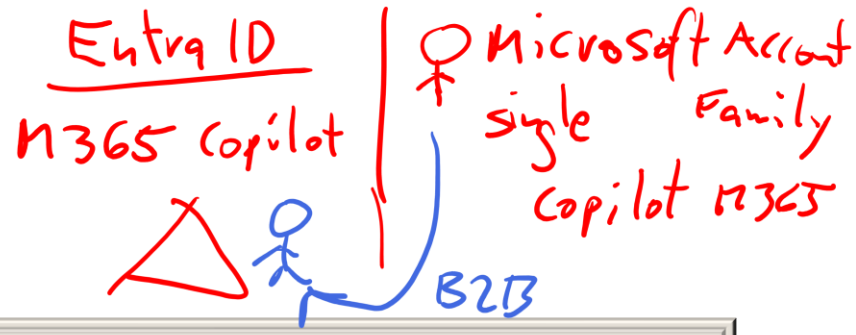
Introduction

Microsoft 365 Copilot is an AI powered productivity tool that integrates with Microsoft Graph and Microsoft 365 to provide real-time intelligent assistance

This module examines the following key tasks that administrators must complete as they prepare for Microsoft 365 Copilot:

1. Complete the prerequisites for Microsoft 365 Copilot
2. Implement SharePoint Advanced Management tools to prepare for Microsoft 365 Copilot
3. Prepare your data for searches in Microsoft 365 Copilot
4. Protect your Microsoft 365 Copilot data with Microsoft 365 security tools
5. Assign your Microsoft 365 Copilot licenses
6. Extend Microsoft 365 Copilot
7. Drive Microsoft 365 Copilot adoption throughout your organization

Get ready for Microsoft 365 Copilot



Prerequisites for Microsoft 365 Copilot:

- Deploy the latest cloud-connected version of Microsoft 365 Apps for enterprise
- Ensure all users have a Microsoft Entra account to authenticate
- Consider provisioning 1-TB OneDrive to every user, since Copilot file handling requires OneDrive
- Install the new Outlook for Windows to enable Copilot integration
- Implement the Microsoft Teams desktop or web app to enable Copilot within Teams chat, meetings, and channels (mobile-only users have limited functionality)
- User devices must be on either Current Channel or Monthly Enterprise Channel to access Microsoft 365 Copilot features
- Ensure all users have cloud-based Microsoft 365 licenses rather than legacy on-premises licenses

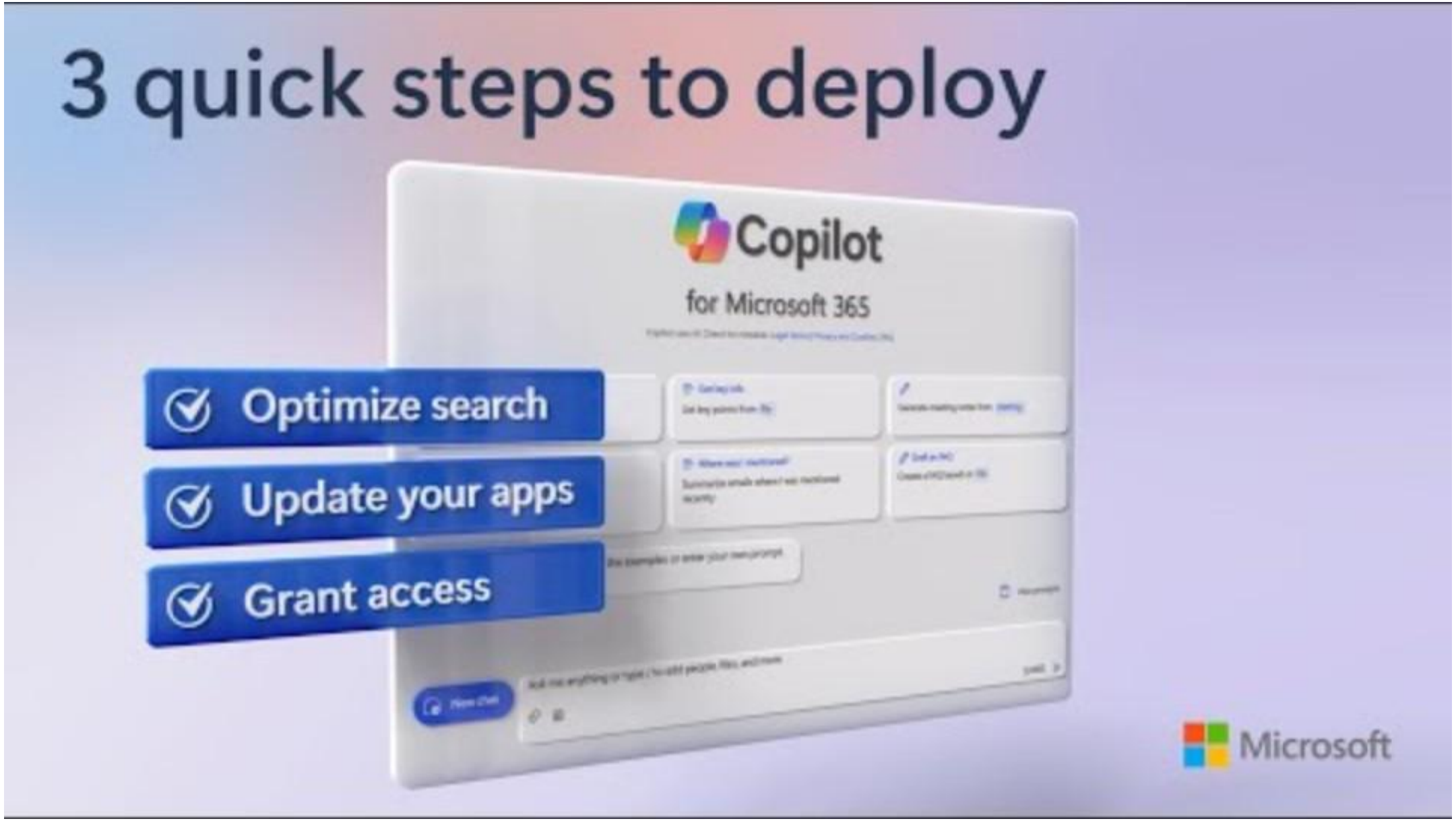
Continued on next slide

Get ready for Microsoft 365 Copilot (continued)

Best practices as you prepare to launch Microsoft 365 Copilot

- Identify early adopter teams or individuals to pilot Microsoft 365 Copilot and provide feedback
- Once Copilot is implemented, monitor usage and feedback to track how extensively users are employing it across your organization
- Use employee feedback to help improve user training
- Use the Microsoft 365 permission model to help ensure the right users or groups have the right access to the right content
- Implement the security and compliance tools within the Microsoft 365 and Azure ecosystems to tighten permissions, implement "just enough access", and prevent data oversharing

Video – How to get ready for Microsoft 365 Copilot faster



Discussion – Video review

- What are your key takeaways from this video, and why?
- What features related to Microsoft 365 Copilot did you find interesting in relation to your own Copilot implementation?

Implement SharePoint Advanced Management tools to prepare for Microsoft 365 Copilot

Microsoft SharePoint Premium - SharePoint Advanced Management (SAM) is a Microsoft 365 add-on that helps organizations address their data governance needs

Perform the following steps **to prepare your SharePoint service for Microsoft 365 Copilot using SAM tools:**

Step 1: Reduce accidental oversharing with SharePoint sharing settings

- Update sharing link defaults
- Consider implementing site-level controls that restrict members from sharing

Step 2: Clean up unused sites to manage content sprawl

- Run the Inactive SharePoint sites policy feature from SAM

Step 3: Identify sites with potentially overshared content

- SAM includes reports that identify the most overshared sites
- SAM also includes tools to help limit access of confidential data by Copilot

Step 4: Control access to content

- SAM includes Restricted Access Control (RAC) policies that you can implement to restrict access to a site or OneDrive account with overshared content

Step 5: Take proactive measures on business-critical sites, such as:

- Block downloads from selected sites through a block download policy
- Apply encryption action with "extract rights" on business-critical documents

Prepare your data for searches in Microsoft 365 Copilot

Data preparation tips

- Clean out redundant, outdated, and trivial (ROT) content to ensure users only work with current and relevant content
- Organize content into logical folders and sites to help Copilot infer relationships and relevance
- Eliminate redundant drafts and outdated versions of files to reduce confusion and contradictions for Copilot
- Tag files with keywords to help Copilot categorize, search, and recommend content
- Standardize file names to enable Copilot to better grasp content

Data governance best practices

- Assign a data steward to oversee preparation and continue maintaining quality
- Document your data policies and practices related to Microsoft 365 and Microsoft 365 Copilot utilization
- Draft a comprehensive data governance policy that codifies rules for:
  - Restricted data
  - Anonymization procedures
  - Stewardship rules
  - Employee training requirements
  - Access authorization procedures
  - Monitoring practices

Protect your Microsoft 365 Copilot data with Microsoft 365 security tools

Microsoft tools for securing data

- Microsoft Purview Information Protection
- Microsoft Purview sensitivity labels
- Microsoft Entra Conditional Access policies
- Microsoft Entra Privileged Identity Management (PIM)
- SharePoint site access reviews
- Microsoft Graph connectors and plugins

Best practices to prevent oversharing

- Conduct an access review for sites, documents, emails, and other content to identify overexposed assets
- Tighten permissions on overexposed assets so that only authorized users have access
- Validate that access restrictions don't impede any user's ability to do their jobs
- Test search functionality to confirm users can only access data relevant to their roles

Video – How your data is protected in Microsoft 365 Copilot

Discussion – Video review

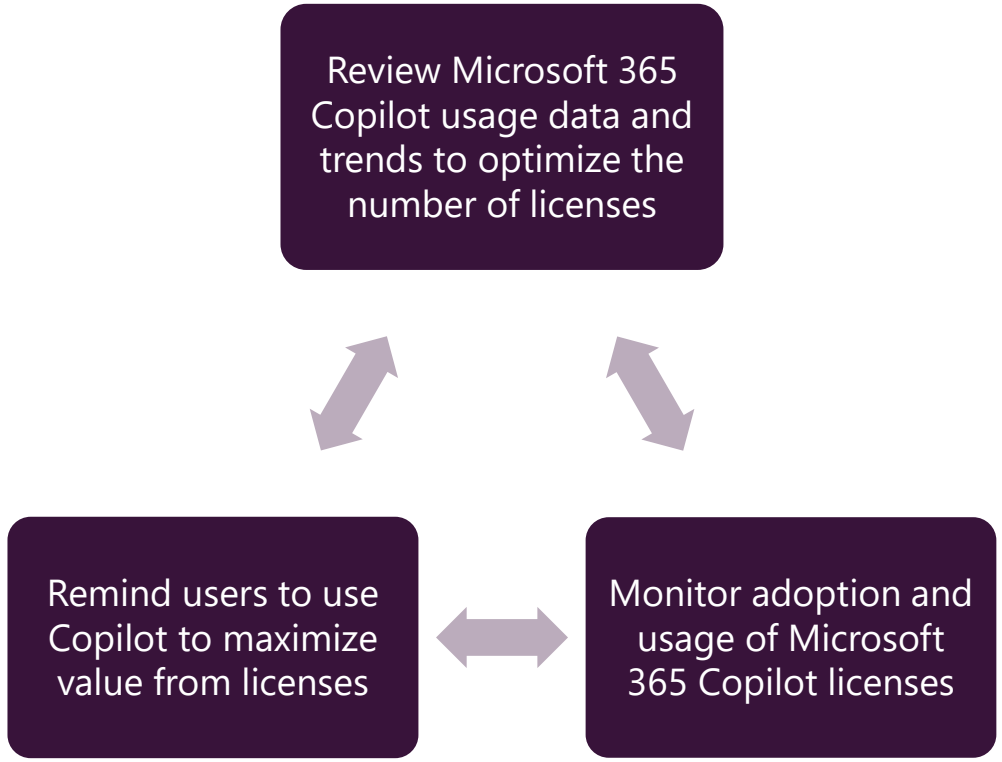
- What are your key takeaways from this video, and why?
- What features related to Microsoft 365 Copilot did you find interesting in relation to your own Copilot implementation?

Assign your Microsoft 365 Copilot licenses

Microsoft 365 Copilot is an add-on product to select Microsoft 365 subscription plans

Enabling Copilot is as easy as assigning licenses to selected users

Users that you assign Microsoft 365 Copilot licenses to must also have an appropriate Microsoft 365 license assigned to them



Users must have one of the following base licenses to be eligible for a Microsoft 365 Copilot license:

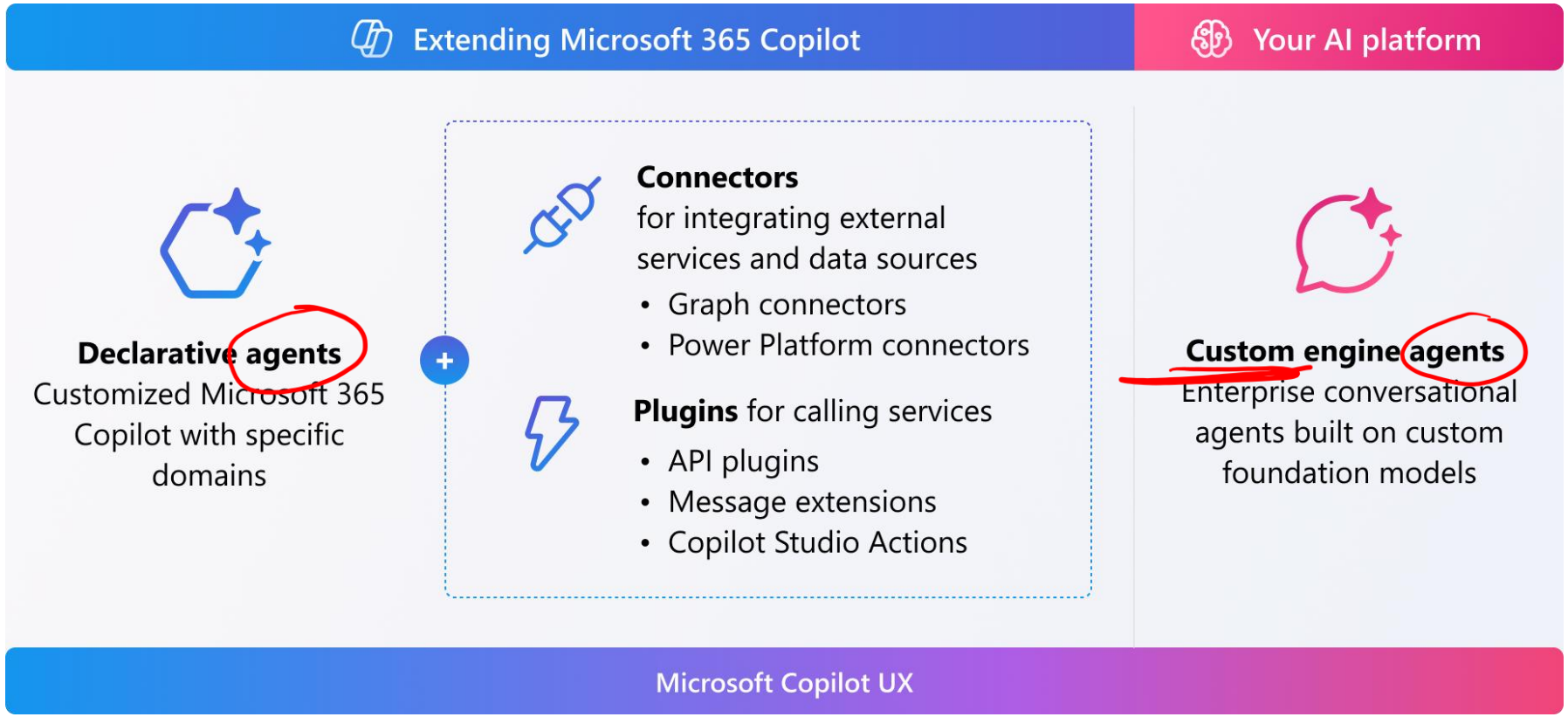
- Microsoft 365 (or Office 365) E3 or E5
- Microsoft 365 Business Standard or Business Premium
- Microsoft 365 (or Office 365) A3 or A5 for faculty

Extend Microsoft 365 Copilot

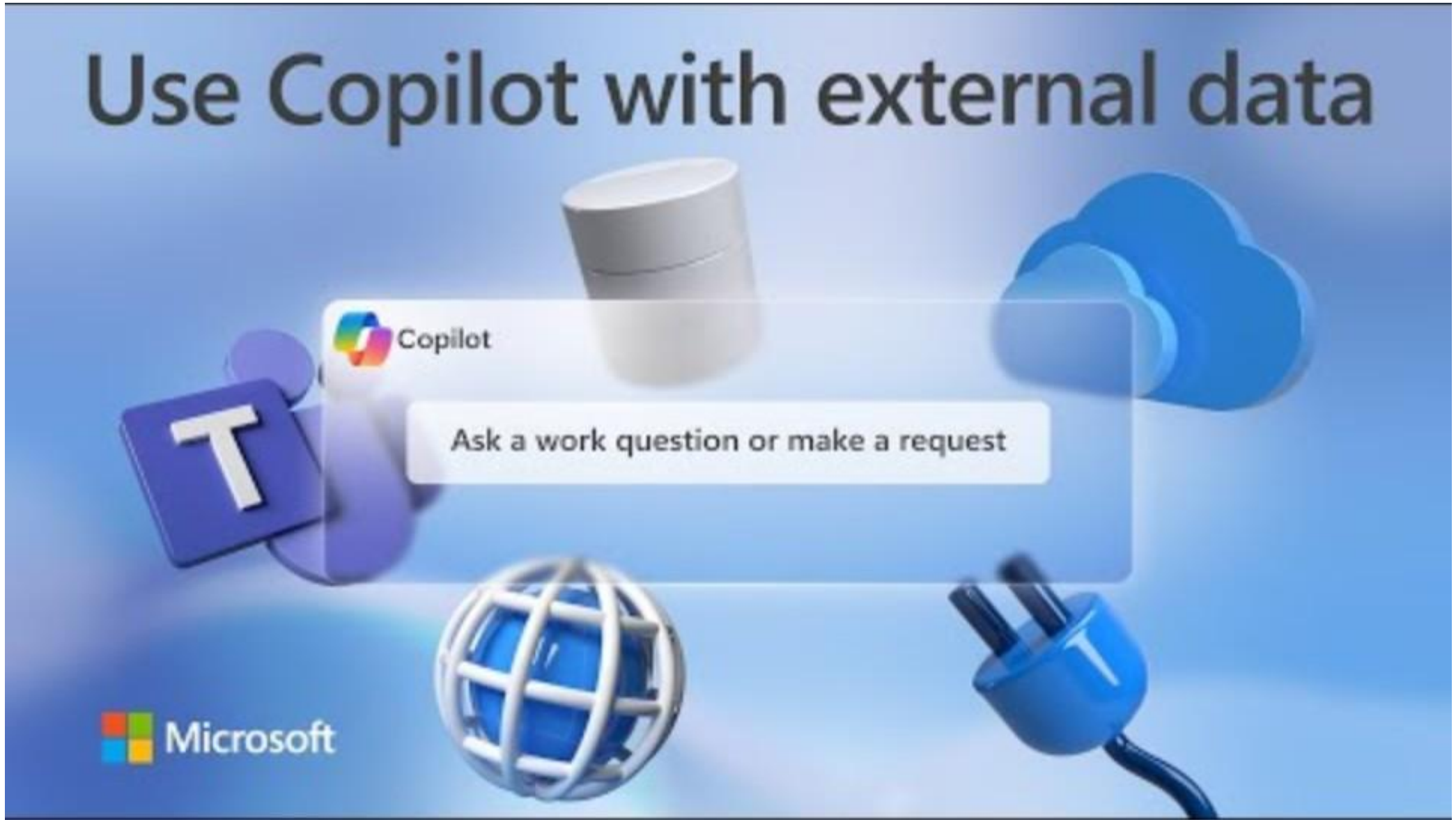
Copilot extensibility is the ability to customize and extend Microsoft 365 Copilot with more knowledge and skills

- Developers can extend Microsoft 365 Copilot by building agents that bring custom knowledge, skills, and process automation into Microsoft 365 Copilot
- IT admins can configure appropriate Copilot connectors to expand knowledge available to all users in their tenant
- Copilot connectors respect the data access limitations from the knowledge source itself

AI Foundry



Video – How Microsoft 365 Copilot can work with external data

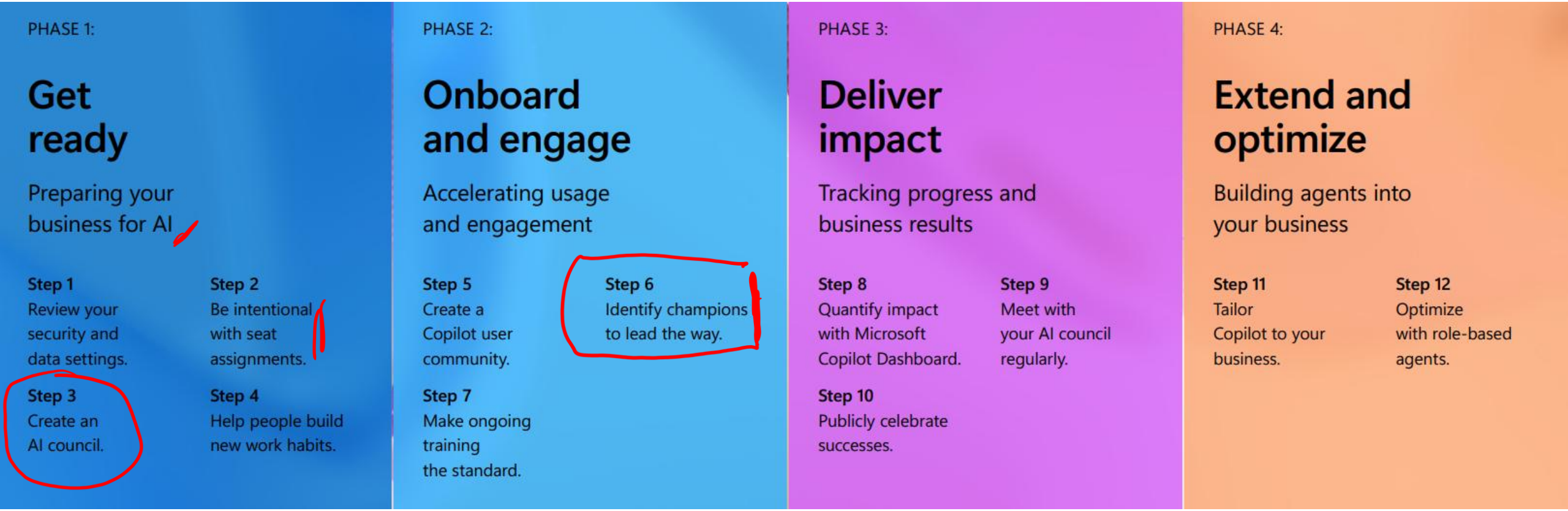


Discussion – Video review

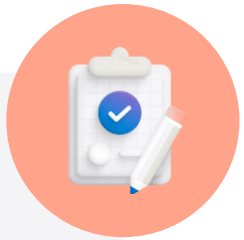
- What are your key takeaways from this video, and why?
- What features related to Microsoft 365 Copilot did you find interesting in relation to your own Copilot implementation?

Drive Microsoft 365 Copilot adoption throughout your organization

The following diagram displays the phases that make up the Microsoft 365 Copilot adoption roadmap



Summary



This module examined the following key tasks that administrators must complete as they prepare for Microsoft 365 Copilot:

- Complete the prerequisites for Microsoft 365 Copilot
- Prepare your data searches in Microsoft 365 Copilot
- Protect your Microsoft 365 Copilot data with Microsoft 365 security tools
- Assign your Microsoft 365 Copilot licenses
- Drive Microsoft 365 Copilot Center of Excellence

Module 2: Examine data security and compliance in Microsoft 365 Copilot

Introduction

Microsoft 365 Copilot applies the security measures used in the Microsoft 365 and Azure ecosystems to protect data privacy and security

This modules examines how Microsoft 365 Copilot:

1. Uses an organization's proprietary business data
2. Protects sensitive business data
3. Uses Microsoft 365 isolation and access controls
4. Meets regulatory compliance mandates

Examine how Microsoft 365 Copilot uses your proprietary business data

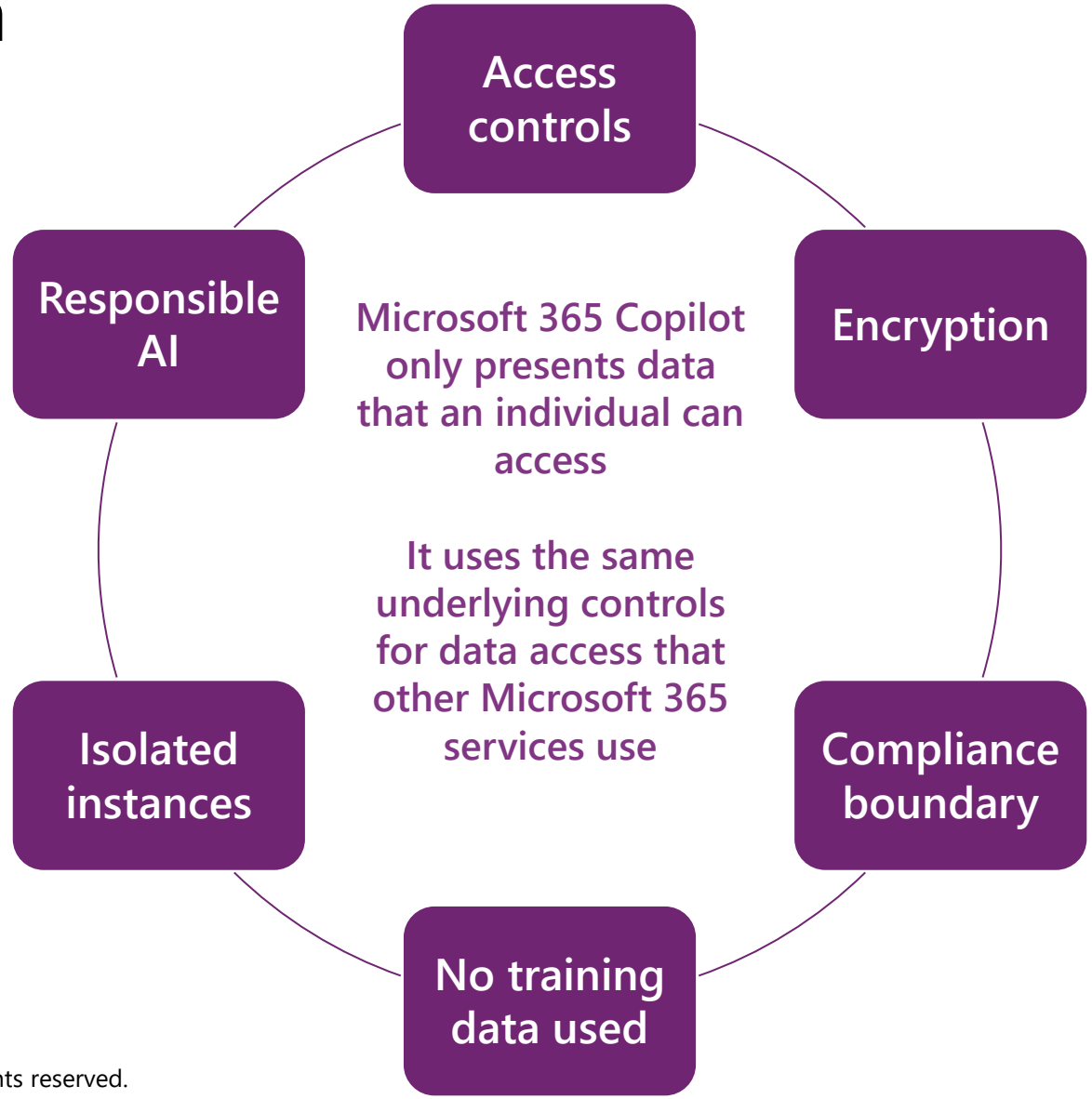
Data access

- Microsoft 365 only surfaces the cloud content for the current user's tenant
- Microsoft 365 Copilot doesn't search other tenants on which the user may also be a B2B guest, or noncurrent user's tenants set up with either cross-tenant access or cross-tenant sync
- Copilot only accesses data the user has permission to view within their tenant
- It then personalizes each response to a user's business context

Security, privacy, and data residency

- Microsoft 365 Copilot follows these foundational principles:
  - Built on Microsoft's comprehensive approach to security, privacy, and individual data
  - Architected to protect tenant, group, and individual data
  - Committed to responsible AI
- Copilot doesn't use OpenAI's publicly available services
- All processing is performed using Azure OpenAI services with its own separate instances of the LLMs

Examine how Microsoft 365 Copilot protects sensitive business data



LLM

Examine how Microsoft 365 Copilot uses Microsoft 365 isolation and access controls

Tenant isolation

Prevents the actions of one tenant from affecting the security or service of another tenant or accessing the content of another tenant

Key aspects of Microsoft 365 tenant isolation include:

- Separate infrastructure
- Data segregation
- Authentication boundaries
- Service customization
- Compliance controls
- Monitoring and diagnostics
- Regular validation

These protections provide threat protection and mitigation equivalent to that provided by physical isolation alone

Data isolation and access control

- Microsoft Entra ID and Microsoft 365 use a highly complex data model that includes tens of services, hundreds of entities, thousands of relationships, and tens of thousands of attributes
- Specific systems own individual pieces of data, but no single system holds all the data
- Microsoft 365 services cooperate with Microsoft Entra ID in this data model
- Microsoft Entra ID is the "system of truth" for shared data, which is typically small and static data used by every service
- Microsoft 365 uses both physical storage and Azure cloud storage (for example, Exchange Online uses its own storage, while SharePoint Online uses both SQL Server storage and Azure cloud storage), hence the need for extra isolation of customer data at the storage level

Examine how Microsoft 365 Copilot uses Microsoft 365 isolation and access controls

Tenant isolation

Prevents the actions of one tenant from affecting the security or service of another tenant or accessing the content of another tenant

Key aspects of Microsoft 365 tenant isolation include:

- Separate infrastructure
- Data segregation
- Authentication boundaries
- Service customization
- Compliance controls
- Monitoring and diagnostics
- Regular validation

These protections provide threat protection and mitigation equivalent to that provided by physical isolation alone

Data isolation and access control

- Microsoft Entra ID and Microsoft 365 use a highly complex data model that includes tens of services, hundreds of entities, thousands of relationships, and tens of thousands of attributes
- Within this model, there's no single source of directory data
- Specific systems own individual pieces of data, but no single system holds all the data
- Microsoft 365 services cooperate with Microsoft Entra ID in this data model
- Microsoft Entra ID is the "system of truth" for shared data, which is typically small and static data used by every service
- Microsoft 365 uses both physical storage and Azure cloud storage (for example, Exchange Online uses its own storage, while SharePoint Online uses both SQL Server storage and Azure cloud storage), hence the need for extra isolation of customer data at the storage level

Examine how Microsoft 365 Copilot meets regulatory compliance mandates

Microsoft ensures that Microsoft 365 Copilot complies with the following key regulatory mandates:

Data privacy

- Microsoft reinforces customer control over its data by complying with privacy laws and standards
- Microsoft uses physical security, background screening, and a multi-layered encryption strategy to protect data
- For content accessed through Copilot plugins, encryption can exclude programmatic access, thus limiting the plugin from accessing the content

Transparency

- Microsoft provides detailed documentation on GitHub that explains:
  - How Copilot is designed
  - What its capabilities are
  - Its limitations in generating responses
- Microsoft enables user control over adopting Copilot suggestions to ensure transparency

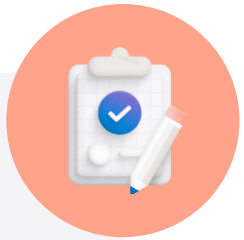
Fairness

- Microsoft continuously evaluates Copilot using tests designed to detect demographic biases, unfair outputs, or harm
- The purpose of this process is to prevent unfair treatment, detect fairness issues, and correct problems
- Users can reject biased or unfair suggestions and report them to Microsoft

Accountability

- Microsoft provides channels like GitHub discussions and Copilot support for giving feedback, lodging complaints, or getting assistance
- Microsoft conducts regular internal reviews with respect to compliance with regulations and ethical AI principles
- Customers can use Copilot services and its output without worrying about copyright claims

Summary



This module explored how Microsoft 365 Copilot applies the security measures used in the Microsoft 365 and Azure ecosystems to protect data privacy and security

It examined how Copilot:

- Uses an organization's proprietary business data
- Protects sensitive business data
- Uses isolation and access controls
- Meets regulatory compliance mandates

Learning Path review

Discussion – Learning Path review

- What are your key takeaways from this learning path, and why?
- What are the key features discussed in this learning path related to Microsoft 365 Copilot that were of special interest to you?