Microsoft

Learning Path 2:

Manage Microsoft 365 Copilot administration

Learning Path agenda

Module 1: Apply principles of Zero Trust to Microsoft 365 Copilot

Module 2: Manage Microsoft Copilot

Module 3: Manage Microsoft 365 Copilot

Module 1: Apply principles of Zero Trust to Microsoft 365 Copilot

Introduction

Organizations should apply the principles of Zero Trust security when preparing to implement Microsoft Copilots

This module explores how to deploy various Zero Trust security measures that are essential for a secure Microsoft Copilot environment

1. Prepare for Microsoft Copilots using Zero Trust security
2. Apply Zero Trust principles to your Microsoft Copilot and Microsoft 365 Copilot deployments
3. Deploy or validate your:
   - Data protection
   - Identity and access
   - App Protection policies
   - Device management protection
   - Threat protection services
   - Secure collaboration for Microsoft Teams
   - Minimum user permissions to data

Prepare for Microsoft Copilot using Zero Trust security

Zero Trust is a security strategy

It isn't a product or a service, but an approach in designing and implementing the following set of security principles:

Verify explicitly	• Always authenticate and authorize based on all available data points. • Enforce the validation of user credentials, device requirements, and app permissions and behaviors.
Use least privilege access	• Limit user access with Just-In-Time (JIT) and Just-Enough-Access (JEA) policies, risk-based adaptive policies, and data protection. • Validate JEA across your organization to eliminate oversharing by ensuring that correct permissions are assigned to files, folders, Teams, and email. • Use sensitivity labels and data loss prevention policies to protect data.
Assume breach	• Validate JEA across your organization to eliminate oversharing by ensuring that correct permissions are assigned to files, folders, Teams, and email. • Use sensitivity labels and data loss prevention policies to protect data. • Use Exchange Online Protection (EOP) and Microsoft Defender XDR services to automatically prevent common attacks and to detect and respond to security incidents.

Apply Zero Trust principles to your Microsoft Copilot deployment

This training focuses on the following Copilot offerings:

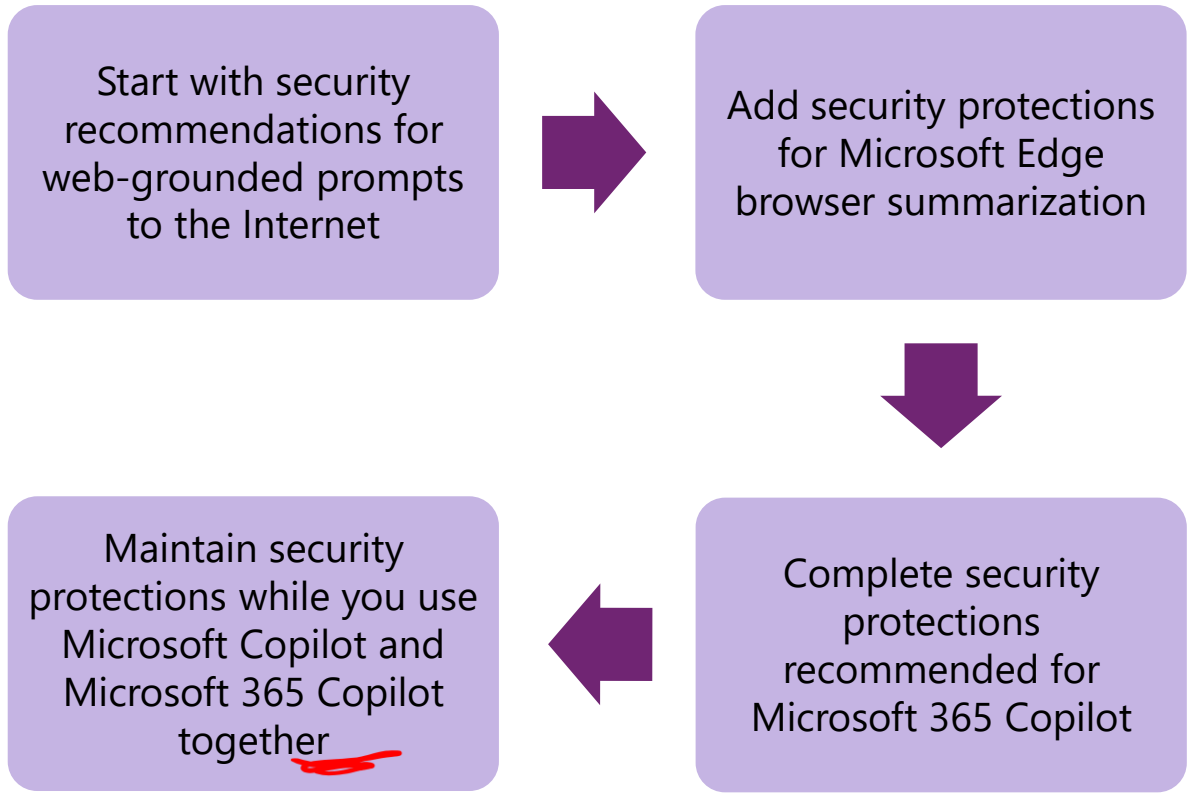
Microsoft Copilot

- Provides assistance based on data from the public web in the Bing search index
- Available for free, although a premium tier called Copilot Pro is available that offers extra perks
- Doesn't have access to organizational resources or content within the Microsoft 365 Graph, such as documents in OneDrive, emails, or other data

Microsoft 365 Copilot

- Integrated into the Microsoft 365 suite of products, including Word, Teams, Outlook, Excel, PowerPoint, and so on
- Designed specifically for business contexts
- Uses an organization's data that's stored in the company's Microsoft 365 ecosystem

You should apply Zero Trust principles to these two Copilot offerings in stages:



Explore Zero Trust recommendations for your Copilot configuration

Configuration	Accessible data	Zero Trust recommendations
Without Microsoft 365 Copilot licenses (Work/Web toggle not available) and with Microsoft Edge browser page summarization disabled	For Web-grounded prompts: - Internet data only	None required, but highly recommended for overall security hygiene.
Without Microsoft 365 Copilot licenses (Work/Web toggle not available) and with Microsoft Edge browser page summarization enabled	For Web-grounded prompts: - Internet data - Organization data on local, intranet, and cloud locations that Copilot in Microsoft Edge can summarize	Apply Zero Trust protections. For organization data on local, intranet, and cloud locations, manage devices with Intune and apply mobile application management (MAM) and mobile device management (MDM) policies. Also apply data loss prevention (DLP) policies.
With Microsoft 365 Copilot licenses (Work/Web toggle available) and with Microsoft Edge browser page summarization disabled	For Graph-grounded prompts: - Microsoft 365 tenant data - Internet data if the web plug-in is enabled - Data for Copilot-enabled plug-ins and connectors For Web-grounded prompts, only internet data	Apply Zero Trust protections.
With Microsoft 365 Copilot licenses (Work/Web toggle available) and with Microsoft Edge browser page summarization enabled	For Graph-grounded prompts: - Microsoft 365 tenant data - Internet data if the web plug-in enabled - Data for Copilot-enabled plug-ins and connectors For Web-grounded prompts: - Internet data - Organization data that can be rendered in a Microsoft Edge browser page, including local, cloud, and intranet resources	Apply Zero Trust protections. For organization data on local, intranet, and cloud locations, apply MAM and MDM policies and DLP policies.

Apply Zero Trust principles to your Microsoft 365 Copilot deployment

To apply Zero Trust principles to Microsoft 365 Copilot, you should complete the following steps and apply the corresponding Zero Trust principles:

Step	Zero Trust principle(s) applied
1. Deploy or validate your data protection	Verify explicitly Use least privileged access
2. Deploy or validate your identity and access	Verify explicitly Use least privileged access
3. Deploy or validate your App Protection policies	Use least privileged access Assume breach
4. Deploy or validate your device management protection	Verify explicitly
5. Deploy or validate your threat protection services	Assume breach
6. Deploy or validate secure collaboration for Microsoft Teams	Verify explicitly Use least privileged access
7. Deploy or validate minimum user permissions to data	Use least privileged access

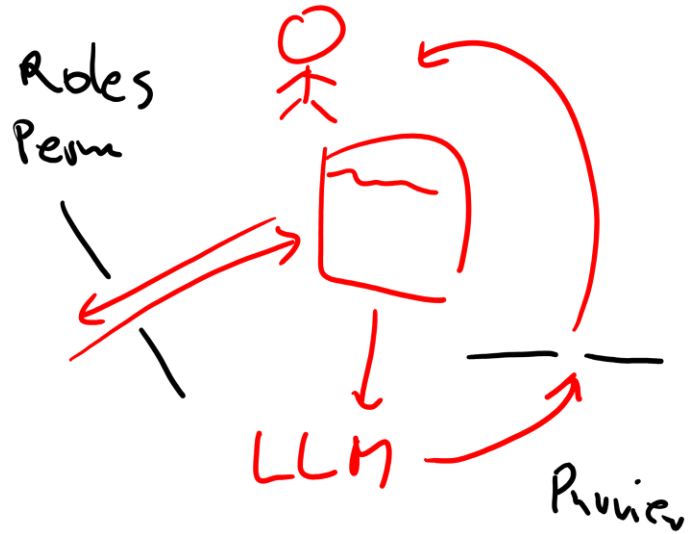
Deploy or validate your data protection

To protect your organization's data in its Microsoft 365 tenant, you must prevent the data from being at risk of over-exposure or oversharing. To do so, you must ensure that:

- Your data is categorized with sensitivity levels that the system automatically applies or that your users manually apply
- You can view how sensitivity labels are being used in your Microsoft 365 tenant

Strengthen your data security and compliance with these Microsoft Purview features:

Microsoft Purview Information Protection	Data classification	Customer key
Communication compliance	Auditing	Content search
eDiscovery	Retention and deletion	Customer Lockbox

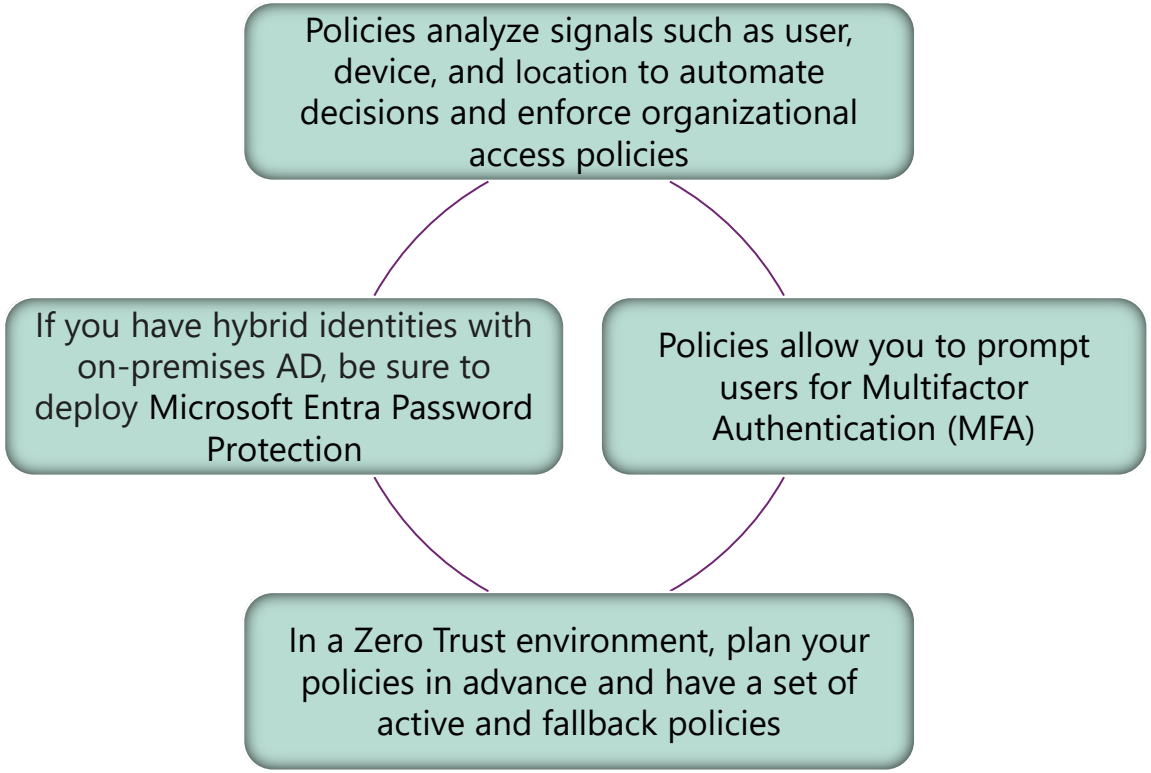


Deploy or validate your identity and access

Prevent bad actors from gaining access to Copilot and sensitive data by:

- Requiring the use of strong authentication that can't be compromised by simply guessing user passwords
- Viewing how sensitivity labels are being used in your Microsoft 365 tenant
- Reviewing access granted to user accounts to prevent oversharing

Create Microsoft Entra Conditional Access policies from policy templates



Deploy or validate your App Protection policies

App Protection policies are Intune's solution for protecting against data leakage:

- They provide rules that ensure an organization's data remains safe or contained within a managed app
- They allow you to control how apps on mobile devices access and share data, even when a device isn't managed (such as personal devices)
- They ensure corporate data in the apps you specify can't be copied and pasted to other apps on the device

Apply Microsoft's data protection framework for App Protection policies, which consists of the following levels:

- **Level 1: Enterprise basic data protection**
  Minimum protection for an enterprise device
- **Level 2: Enterprise enhanced data protection**
  For devices where users access sensitive or confidential information
- **Level 3: Enterprise high data protection**
  For devices accessed by high-risk users or groups, or for devices run by an organization with a larger or more sophisticated security team

Core App Protection policy settings:

- A managed app in Intune is a protected app that Intune manages and has Intune App Protection policies applied to it
- Examples of policy settings include:
  - Protecting company data while leaving personal data untouched
  - Restricting data transfer and copy-and-paste functions
  - Encrypting company data
  - Enabling App Protection without requiring enrollment
  - Enforce access requirements to access company data

Deploy or validate your device management protection

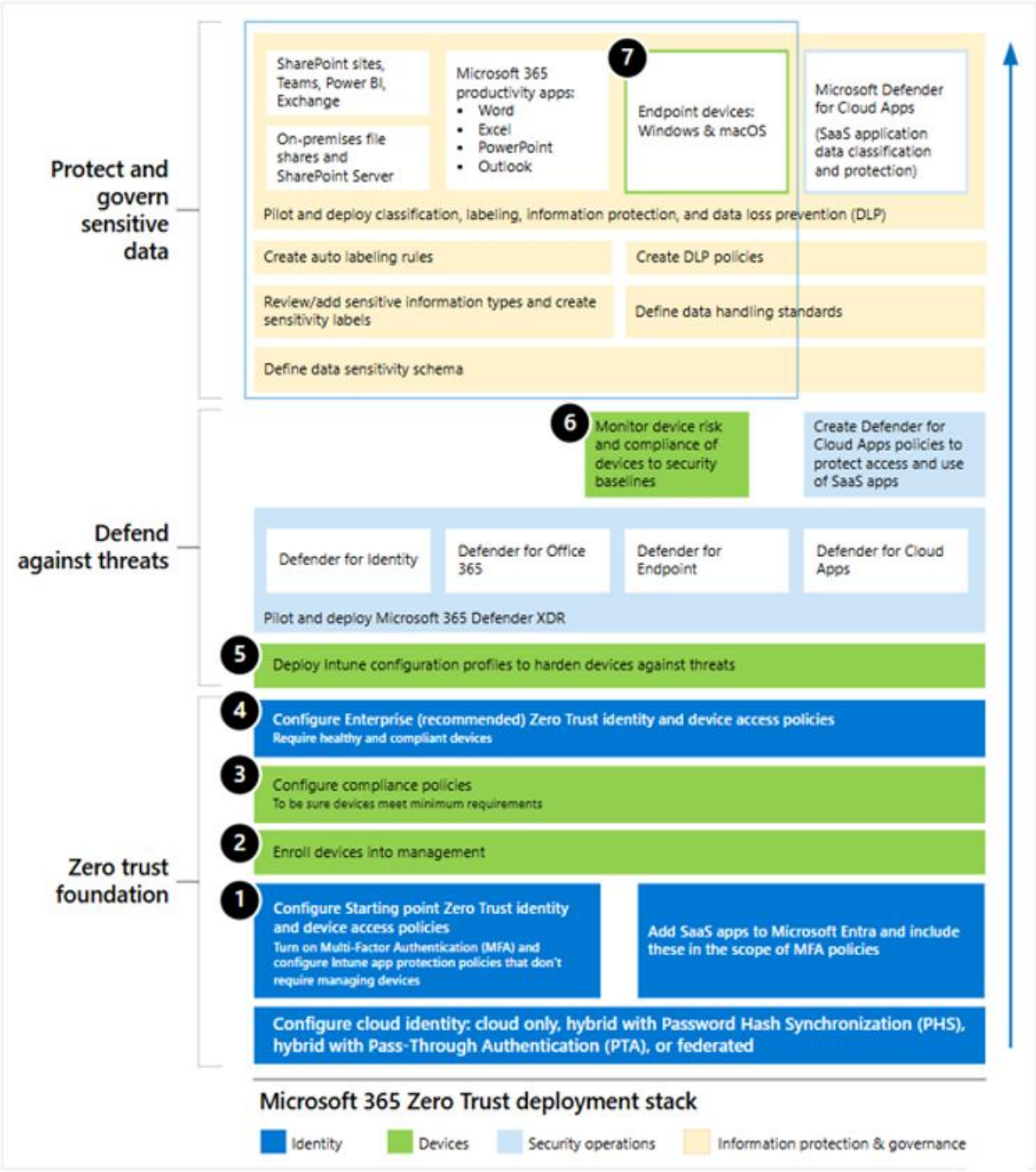
A core component of enterprise-level security includes managing and protecting devices with Microsoft Intune

- Since organizations have an incredible diversity of endpoints accessing their data, endpoints can become the weakest link in your Zero Trust security strategy
- To ensure you're not exposing your data to risk, you must monitor every endpoint for risks and employ granular access controls

The diagram shows the 7 steps to achieve a Zero Trust security posture

In this illustration:

- **Devices are enrolled into management with Intune**
- **Intune onboards devices to Microsoft Defender for Endpoint**
- **Devices that are onboarded to Defender for Endpoint are also onboarded for Microsoft Purview features, such as DLP**



Deploy or validate your threat protection services

The following Microsoft 365 threat protection services provide advanced security features to protect users, devices, data, and organizations from various threats and attacks:

Microsoft Entra ID Protection

- Protects user identities and credentials

Microsoft Defender for Office 365

- Protects email and collaboration platforms from phishing, malware, ransomware, and other threats

Microsoft Defender for Endpoint

- Protects endpoints from malware, exploits, and other attacks

Microsoft Defender for Identity

- Protects on-premises Active Directory from identity-based attacks

Microsoft Defender for Cloud Apps

- Protects cloud apps and data from unauthorized access and data loss

Deploy or validate secure collaboration for Microsoft Teams

Configure secure collaboration for Microsoft Teams using these Microsoft products and features:

Microsoft Defender for Office 365

- Safe Attachments for SharePoint, OneDrive, and Teams. Safe Links for Teams

Microsoft SharePoint

- Site and file sharing policies, Site sharing permissions, Sharing links, Access requests, Site guest sharing settings

Microsoft Teams

- Guest access, private teams, private channels, shared channels

Microsoft Purview

- Sensitivity labels

Microsoft SharePoint Advanced Management

- Site access restrictions, conditional access policies for sites, default sensibility labels for libraries

Continued on next slide

Deploy or validate secure collaboration for Microsoft Teams (continued)

Microsoft provides guidance for protecting Microsoft Teams data at three different levels – Baseline, Sensitive, and Highly sensitive

- These tiers gradually increase the protections that help prevent oversharing and potential information leakage, as shown in this table

	Baseline	Sensitive	Highly sensitive
Public or private team	Either	Private	Private
Unauthenticated sharing	Allowed	Blocked	Blocked
File sharing	Allowed	Allowed	Limited to people in the team
Team membership	Anyone can join public teams. Team owner approval required for private teams.	Team owner approval required to join.	Team owner approval required to join.
Document encryption			Available with sensitivity labels
Guest sharing	Allowed	Can be allowed or blocked	Can be allowed or blocked
Unmanaged devices	No restriction	Web-only access	Blocked

Deploy or validate minimum user permissions to data

Deploying or validating minimum user permissions to data is a critical step in adhering to the Zero Trust principles within your Microsoft 365 environment

- To prevent your organization's data from being at risk of overexposure or oversharing, ensure that all users have Just Enough Access (JEA) to perform their jobs and no more
- Users shouldn't discover data they aren't supposed to be able to view, or share data that they shouldn't be sharing

What is Just Enough Access (JEA)?

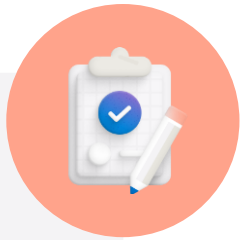
- JEA provides users with the least permissions necessary to perform their jobs, which limits the chance of data breaches and unauthorized access
- Key concepts of JEA include:
  - Users should only access data necessary for their job functions
  - Permissions should be regularly reviewed and updated based on changing roles and responsibilities
  - Implement granular access controls to minimize the spread of sensitive information

Detect oversharing

To maintain a secure environment, it's essential for organizations to detect and rectify instances of oversharing at the file level, and at the site, team, and container level

- At the file level:
  - Use Microsoft Purview Information Protection to identify and manage sensitive data
- At the site, team, and container level:
  - Audit and enforce access restrictions
  - Utilize SharePoint Advanced Management to identify potential oversharing

Summary



This module examined the following items related to applying principles of Zero Trust to Microsoft Copilots:

- Prepare for Microsoft Copilot using Zero Trust principles
- Apply Zero Trust principles to your Microsoft Copilot and Microsoft 365 Copilot deployments
- Zero Trust recommendations for your Copilot configuration
- Deploy or validate:
  - Your data protection
  - Your identity and access
  - Your App Protection policies
  - Your device management protection
  - Your threat protection services
  - Secure collaboration for Microsoft Teams
  - Minimum user permissions to data

Module 2:
Manage Microsoft Copilot

Introduction

This module examines the following topics that provide a comprehensive understanding of how to effectively manage Microsoft Copilot:

1. Compare Microsoft Copilot and Microsoft 365 Copilot
2. Explore Microsoft Copilot with enterprise data protection
3. Manage Microsoft Copilot in Microsoft Edge
4. Manage Microsoft Copilot on mobile devices

Compare Microsoft Copilot and Microsoft 365 Copilot

Microsoft Copilot and Microsoft Copilot 365 use advanced AI technologies, but they serve different purposes and have distinct features

- **Microsoft Copilot is a generative AI service grounded in data from the public web in the Bing search index only**
- **Microsoft 365 Copilot builds upon the base Microsoft Copilot functionality by adding the following features:**
  - Access to data within your tenant's Microsoft 365 Graph
  - Prompts and responses are processed entirely within your Microsoft 365 service boundary, along with other Microsoft 365-specific security, compliance, and privacy features.
  - Access to this generative AI capability from Microsoft 365 applications
  - Advanced document generation, enhanced collaboration, and integration of data across the Microsoft 365 suite

Explore Microsoft Copilot with enterprise data protection

In Microsoft Copilot, enterprise data protection (EDP) is designed to safeguard both user and organizational data

- **Users can only access Copilot with EDP using their Microsoft Entra ID work or school account**
  - This information is removed from chat data at the start of a chat session
  - Search queries triggered by prompts from a Microsoft Entra ID user aren't linked to users or organizations by Bing
- **Microsoft doesn't retain prompts or responses from Microsoft Entra ID users when using Copilot**
  - Prompts and responses are maintained for a short caching period for runtime purposes
  - After the browser is closed, the chat topic is reset, or if the session times out, Microsoft discards prompts and responses
  - Because prompts and responses are discarded, they can't be used as part of a training set for the underlying LLM
- **Chat data sent to and from Copilot with EDP is encrypted in transit and at rest**
  - Even if the data is intercepted or accessed by unauthorized parties, it remains unreadable and secure
  - Microsoft has no 'eyes-on' access to it
- **Advertising shown to Microsoft Entra ID users isn't targeted based on workplace identity or chat history**
  - This ensures that users' personal and professional data remain private
  - It also helps in maintaining the confidentiality of sensitive work-related information

Video – Enterprise data protection overview

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?

Manage Microsoft Copilot in Microsoft Edge

Microsoft Copilot can be accessed in the Microsoft Edge sidebar

- You can ask complex questions, find comprehensive answers, summarize information, and find inspiration just like when you use Microsoft Copilot in Bing
- With Microsoft Copilot in Edge, you can also ask questions based on the page content or a PDF that's open in the browser

Access Copilot in Microsoft Edge

- The organization's Copilot service plan must be turned on, and the user must have an eligible license
- The user must sign in to bing.com/chat with their Microsoft Entra ID

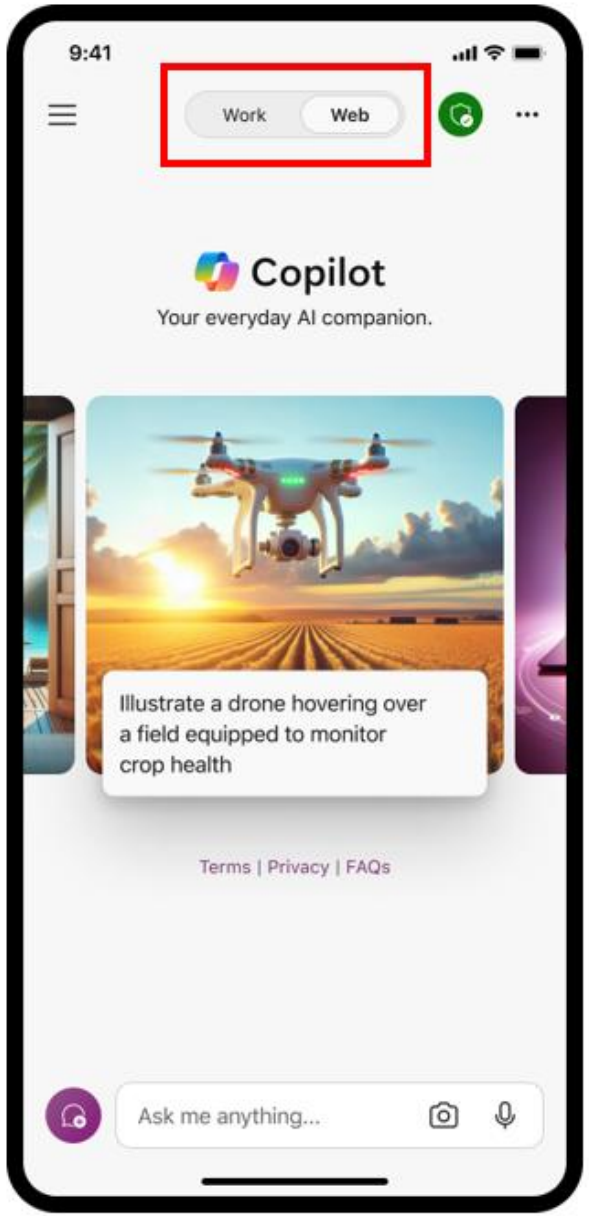
Manage Copilot in Microsoft Edge

- Administrators can use group policy settings to manage the behavior of the Copilot in Microsoft Edge sidebar.
- **DiscoverPageContextEnabled policy** - Prevents Copilot from using webpage or PDF content from being used to respond to prompts
- **HubSidebarEnabled policy** - Automatically blocks Copilot and all Microsoft Edge sidebar apps from being enabled

Manage Microsoft Copilot on mobile devices

Microsoft Copilot is accessible on mobile devices to help you be more productive and creative on the go with AI-powered chat for the web

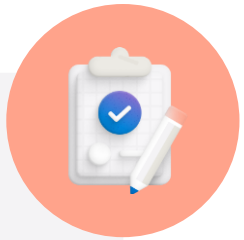
- Copilot can also be accessed by visiting copilot.microsoft.com using a mobile web browser or in the Microsoft Edge mobile app through a native Copilot button
- Enterprise data protection in Copilot is currently available through the following iOS/Android mobile applications when eligible users are signed in with their Microsoft Entra ID accounts:
  - Microsoft Copilot mobile app
  - Microsoft 365 mobile app
  - Microsoft Start mobile app
  - Bing mobile app



For a dedicated Copilot experience on mobile, Microsoft recommends the Copilot mobile application, which is available for iOS and Android

- If users have access to both Microsoft Copilot and Microsoft 365 Copilot, they're able to switch between Work and Web scopes using a toggle at the top of the UI
- Microsoft Copilot with enterprise data protection is also available in the Microsoft 365 mobile app
- To manage Copilot in the Microsoft 365 mobile app, admins can enable or disable Copilot in the Microsoft 365 mobile app by using an app configuration policy in Intune

Summary



This module examined the following topics that provide a comprehensive understanding of how to effectively manage Microsoft Copilot:

- Compare Microsoft Copilot and Microsoft 365 Copilot
- Explore Microsoft Copilot with enterprise data protection
- Manage Microsoft Copilot in Microsoft Edge
- Manage Microsoft Copilot on mobile devices

Module 3:
Manage Microsoft 365 Copilot

Introduction

This module examines how to effectively manage Microsoft 365 Copilot administration

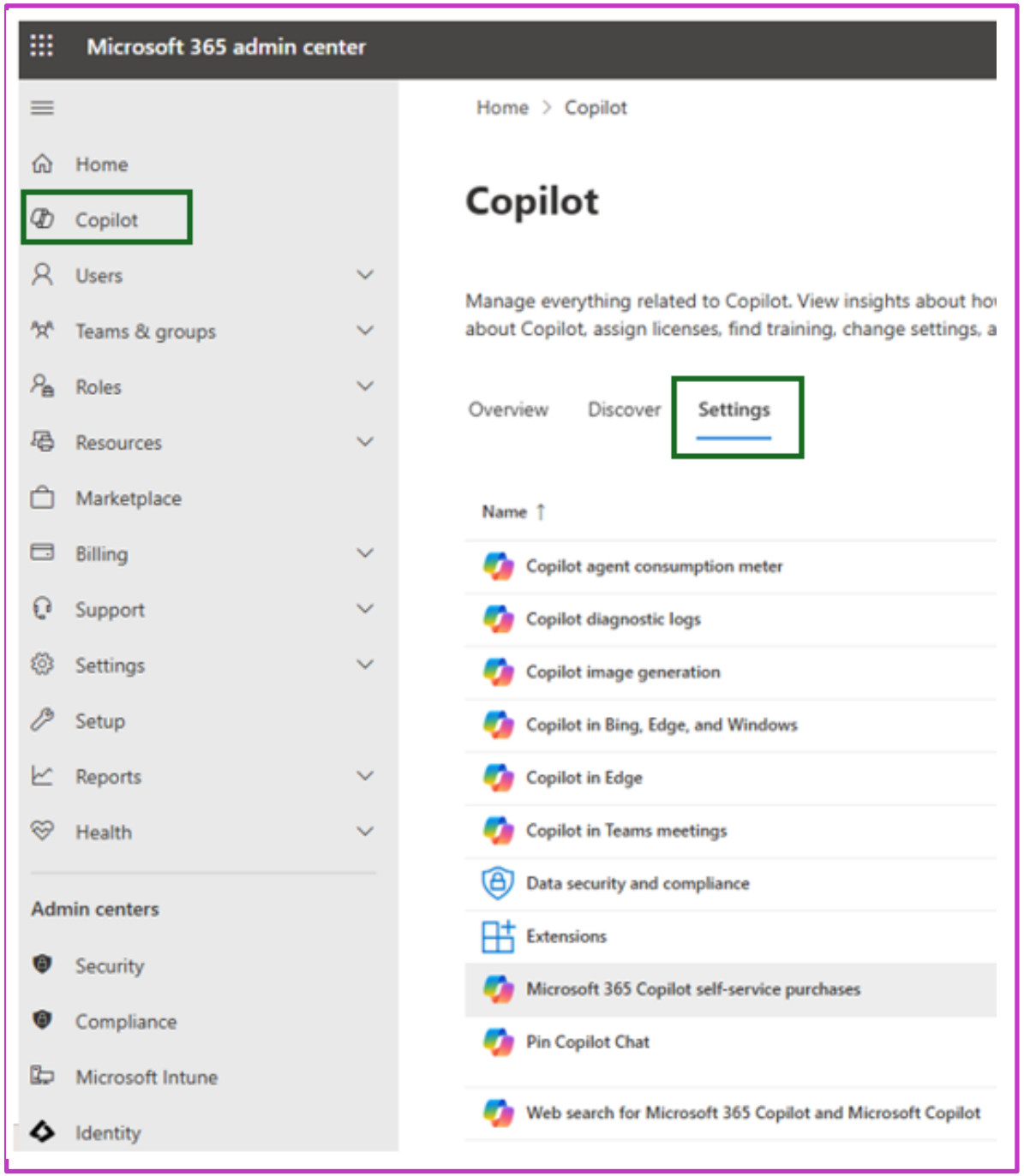
1. Manage Microsoft 365 Copilot settings
2. Manage web access for Microsoft 365 Copilot
3. Manage Copilot for Microsoft Teams meetings and events
4. Explore Microsoft Purview data protections for AI apps
5. Secure data for AI apps using the Microsoft Purview AI Hub
6. Monitor the value of Microsoft 365 Copilot through the Copilot Dashboard
7. Track Microsoft 365 Copilot readiness and usage across your organization
8. Monitor Microsoft 365 Copilot interactions using a communication compliance policy
9. Delete your Microsoft Copilot interaction history

Manage Microsoft 365 Copilot settings

You can manage how users in your organization interact with Microsoft 365 Copilot by going to the Settings tab on the Copilot page in the Microsoft 365 admin center

Some of the key features that are available on the **Settings** tab include:

- Copilot agent consumption meter
- Copilot diagnostic logs
- Copilot image generation
- Copilot in Bing, Edge, and Windows
- Copilot in Edge
- Copilot in Teams meetings
- Data security and compliance
- Extensions
- Microsoft 365 Copilot self-service purchases
- Pin Copilot Chat
- Web search for Microsoft 365 Copilot and Microsoft Copilot



Simulated lab exercise

Simulation: Review the Microsoft 365 Copilot settings

Simulation instructions

To access the link to the simulation and the instructions for each task, navigate to this Learn training module and unit

Manage web access for Microsoft 365 Copilot

Microsoft 365 Copilot and Microsoft Copilot have an optional chat feature known as web grounding that allows Copilot to reference web content when responding to user prompts

- Referencing web content improves the quality of Copilot responses by grounding them in the latest information from the web
- Two distinct controls are available to manage web grounding - one for IT Administrators and another for end users

IT admin control for web grounding

A privacy setting for "**optional connected experiences**" allows IT admins to enable or disable web grounding for users or groups across their tenant

- **Enabled.** Web grounding is enabled in both Copilot experiences. However, in Microsoft 365 Copilot, users can choose for themselves whether to enable or disable web grounding using the web content plugin toggle. This toggle is NOT available to users in Microsoft Copilot
- **Disabled.** Web grounding is disabled in both Copilot experiences. This setting overrides a Microsoft 365 Copilot user's selection with the web content plugin toggle

End user control for web grounding

The web content plugin toggle offers individual control over whether the user wants real-time web content in Microsoft 365 Copilot responses based on their personal preference

The end user toggle is only available as part of Work chat in Microsoft 365 Copilot

- If the "optional connected experiences" setting is enabled by an admin, a Microsoft 365 Copilot user can disable or re-enable the web content plugin in work chat
- To do so, users can select the plugin menu in the chat input box to enable or the web content plugin

Simulated lab exercise

Simulation: Manage web access for Microsoft 365 Copilot

Task 1

Enable this setting for the entire organization

Task 2

Enable this setting for an individual user account

Simulation instructions

To access the link to the simulation and the instructions for each task, navigate to this Learn training module and unit

Manage Copilot for Microsoft Teams meetings and events

Microsoft 365 Copilot in Teams meetings and events is an AI tool that captures important conversation points

- Each meeting and webinar participant with a Microsoft 365 Copilot license can ask prompts that are only visible to them
- Administrators can manage how users in your organization use Copilot in Teams meetings and events

Manage your transcription policy

You can use the **Recording & Transcription** section in the Teams admin center or PowerShell to manage your transcription policy. Options include:

- **On, Only during the meeting.** Transcription is enabled only while the meeting is in progress.
- **Off, Only during the meeting.** Transcription is disabled for the entire meeting unless another user with permission enables transcription.
- **On, During and after the meeting.** Transcription is enabled during the meeting and the transcript is saved for later use.
- **Off, During and after the meeting.** Users can't interact with Copilot unless another participant with permission to transcribe turns on transcription for this meeting.
- **Any, Off.** Transcription is disabled regardless of the meeting's status.

Manage Copilot for your Teams' users

You can use the Teams admin center or PowerShell to manage how your users use Copilot in Teams meetings and events. Options include:

- **On**. When organizers with this policy create meetings and events, Copilot's default value in their meeting options is **Only during the meeting**. Organizers can change this value to **During and after the meeting**.
- **On with saved transcript required**. This setting is the default value. When organizers with this policy create meetings and events, Copilot's default value in their meeting options is **During and after the meeting**. This option is enforced; organizers can't change this value.
- **On with transcript saved by default**. When organizers with this policy create meetings and events, Copilot's default value in their meeting options is **During and after the meeting**. Organizers can change this value to **Only during the meeting**.

Simulated lab exercise

Simulation: Manage Copilot in the Teams admin center

Simulation instructions

To access the link to the simulation and the instructions for each task, navigate to this Learn training module and unit

Explore Microsoft Purview data protections for AI apps

Administrators should use Microsoft Purview to mitigate and manage the risks associated with AI usage and implement corresponding protection and governance controls

- Microsoft 365 Copilot uses existing Microsoft Purview controls to ensure that data stored in your tenant is never returned to the user or used by a large language model (LLM) if the user doesn't have access to that data

- **Microsoft 365 provides an extra layer of protection when you apply sensitivity labels created in Microsoft Purview to the content**
  - When a file is open in an Office app, or an email or calendar event is open in Outlook, the sensitivity of the data is displayed to users in the app with the label name and content markings (such as header or footer text) that are configured for the label.
  - When the sensitivity label applies encryption, Copilot only returns the data if the user is assigned the Extract and View usage rights.
- **Besides sensitivity labels, other Microsoft Purview capabilities that can strengthen your data security and compliance for Microsoft 365 Copilot and Microsoft Copilot include:**
  - Data classification
  - Customer Key
  - Communication compliance
  - Auditing
  - Content search
  - eDiscovery
  - Retention and deletion
  - Customer Lockbox

Secure data for AI apps using the Microsoft Purview AI Hub

The Microsoft Purview AI Hub is a centralized platform designed to efficiently manage and govern AI models and applications across an organization

- It ensures that AI deployments aren't only effective but also secure and compliant with industry standards and regulations
- It provides easy-to-use graphical tools and reports to quickly gain insights into AI use within an organization

AI Hub – A central AI management location

The AI Hub offers the following capabilities that enable your organization to safely adopt AI without having to choose between productivity and protection:

- Insights and analytics into AI activity in your organization
- Ready-to-use policies to protect data and prevent data loss in AI prompts
- Compliance controls to apply optimal data handling and storing policies

How to use the AI Hub

You need an account that has appropriate permissions for compliance management

- For example, an account that's a member of the Microsoft Entra Compliance Administrator group role

To help you quickly gain insights into AI usage and protect your data, the AI Hub provides preconfigured policies that you can activate with a single selection

- Allow at least 24 hours for these new policies to collect data to display the results in the AI Hub or reflect any changes that you make to the default settings

Simulated lab exercise

Simulation: Using the AI Hub

Simulation instructions

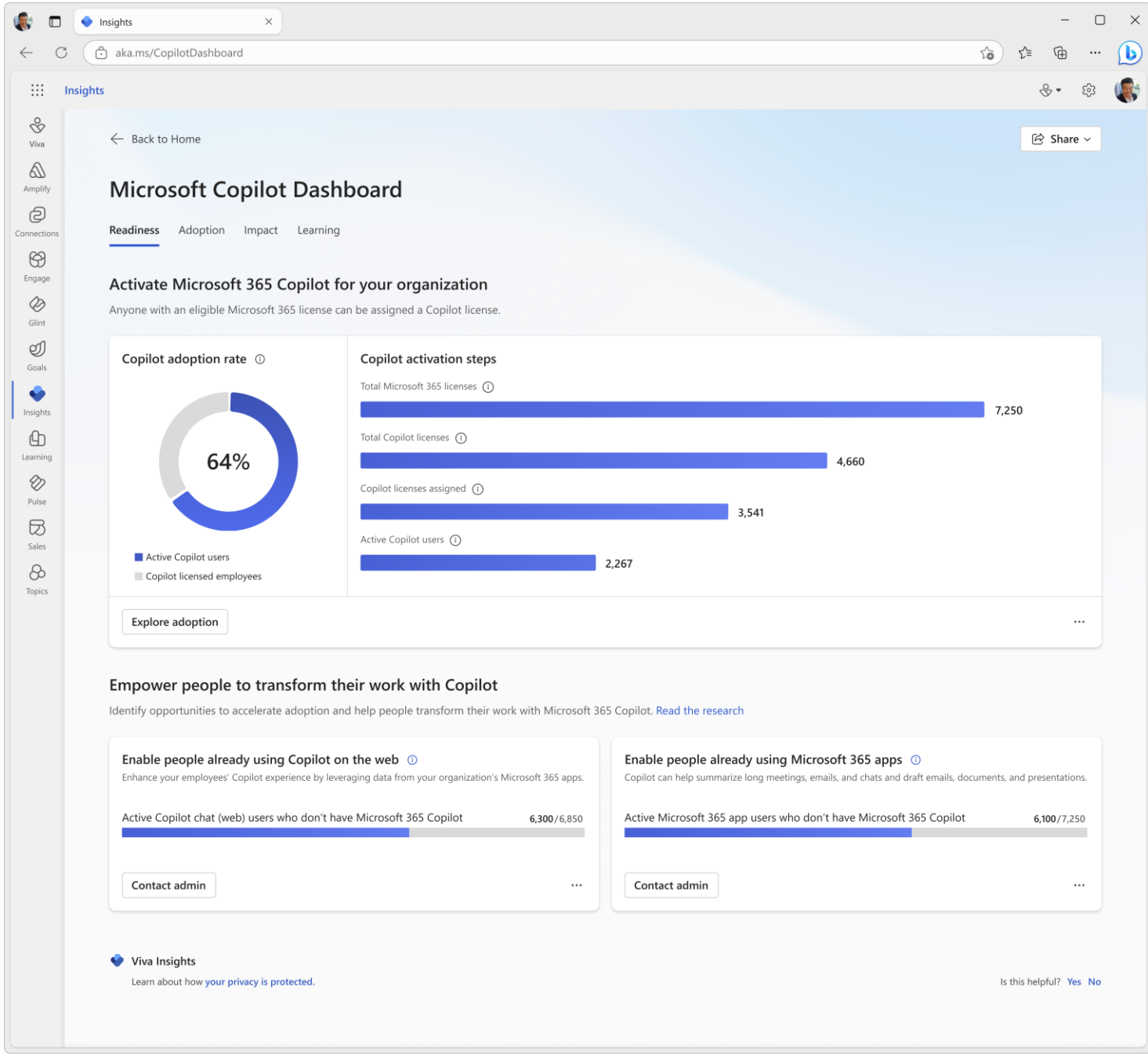
To access the link to the simulation and the instructions for each task, navigate to this Learn training module and unit

Monitor the value of Microsoft 365 Copilot through Copilot dashboard

The dashboard provides actionable insights to help your organization get ready to deploy AI, drive adoption based on how AI is transforming workplace behavior, and measure the impact of Copilot

The dashboard offers specific metrics related to the following aspects of Copilot usage:

- **Readiness**. Focuses on the preparedness of your organization to effectively use Copilot.
- **Adoption**. Tracks how well your organization is adopting Copilot.
- **Impact**. Measures the effectiveness and value that Copilot brings to the organization.
- **Learning**. Provides insights into the learning and development aspects related to Copilot.



Track Microsoft 365 Copilot readiness and usage across your organization

It's important for administrators to explore the readiness and usage of Microsoft 365 Copilot across their organizations

- You can use the Microsoft 365 Usage dashboard to display the activity overview across the Microsoft 365 apps in your organization
- The following two key reports in the Microsoft 365 Usage dashboard enable you to see how people in your business are using Microsoft 365 Copilot services.

Microsoft 365 Copilot readiness report

With this report, you can:

- View which users are technically eligible for Copilot
- Track and assign your organization's available Copilot licenses
- Monitor usage of Microsoft 365 apps that Copilot integrates best with
- Review the system's recommendations that your business can take to prepare for Copilot
- Export into an Excel .csv file the Copilot readiness report data of all users with any engagement on Teams meetings, Teams chat, and Outlook email for Office docs in the past 30 days

Microsoft 365 Copilot usage report

With this report, you can:

- View a summary of how users' adoption, retention, and engagement are with Microsoft 365 Copilot
- View several charts of Microsoft 365 Copilot usage, including specific metrics for:
    - Number of enabled users with Copilot licenses, number of active users, and active users rate
    - Number of enabled and active users of Microsoft 365 Copilot apps
    - Daily time trend of Microsoft 365 Copilot among Microsoft 365 productivity apps

Monitor your Copilot interactions using a communication compliance policy

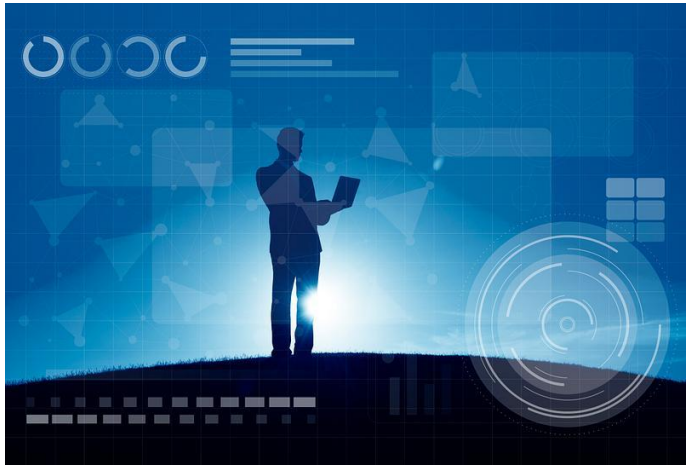
Administrators can use communication compliance policies to analyze prompts and responses entered into Microsoft Copilot and Microsoft 365 Copilot to detect inappropriate or risky prompts or the sharing of confidential information

Communication compliance policies can:

- Define which communications and users are subject to review in your organization
- Define which custom conditions the communications must meet
- Specify who should do reviews

Create a policy to review all Copilot interactions

- When you're first working with Copilot interactions, you may want to review all Copilot interactions to see how your users are using Copilot



Administrators can create a communication compliance policy based on various policy templates

- The focus of this training is on the Detect Microsoft 365 Copilot and Microsoft Copilot interactions template
- With this template, you can create a policy that scans Microsoft 365 Copilot and Microsoft Copilot interactions for:
  - Sensitive information types
  - Keywords
  - Trainable classifiers
  - Conditions

Simulated lab exercise

Simulation: Create a compliance policy that detects Microsoft 365 Copilot interactions

Simulation instructions

To access the link to the simulation and the instructions for each task, navigate to this Learn training module and unit

Delete your Microsoft 365 Copilot interaction history

Copilot interaction history is the record of the prompts and responses that your organization's users have with Microsoft 365 Copilot

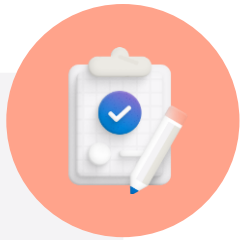
Managing your Microsoft 365 Copilot interaction history is crucial for maintaining:

- **Data privacy**
  - Ensuring that sensitive information isn't retained longer than necessary, which helps protect customer privacy
- **Compliance**
  - Meeting organizational and legal requirements for data retention and deletion
  - For companies that must adhere to strict data retention policies due to industry regulations, managing Copilot interaction history allows them to avoid potential fines and legal issues
- **Security**
  - Minimizing the risk of data breaches by regularly purging unnecessary data, which can protect the organization from potential security threats

When you select the administrative setting to delete Microsoft 365 Copilot interaction history, a deletion request is sent to Microsoft

- It might take some time before your Microsoft 365 Copilot interaction history is fully deleted
- If an app is open when you select the **Delete** option, you might continue to see your previous interaction history until you close the app
- The next time you reopen that app and start using Copilot again, your interaction history will be cleared
- That means you’re starting over again with Copilot
- Copilot doesn’t show any previous interactions you had with it

Summary



This module examined the following topics that provide a comprehensive understanding of how to effectively manage Microsoft 365 Copilot:

- Manage Microsoft 365 Copilot settings
- Manage web access for Microsoft 365 Copilot
- Manage Copilot for Microsoft Teams meetings and events
- Explore Microsoft Purview data protections for AI apps
- Secure data for AI apps using the Microsoft Purview AI Hub
- Monitor the value of Microsoft 365 Copilot through the Copilot Dashboard
- Track Microsoft 365 Copilot readiness and usage across your organization
- Monitor Microsoft 365 Copilot interactions using a communication compliance policy
- Delete your Microsoft Copilot interaction history

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 that you foresee implementing at your organization?