



Level Up CSP Microsoft 365 and Copilot

In person series

Modern Work & Business Applications

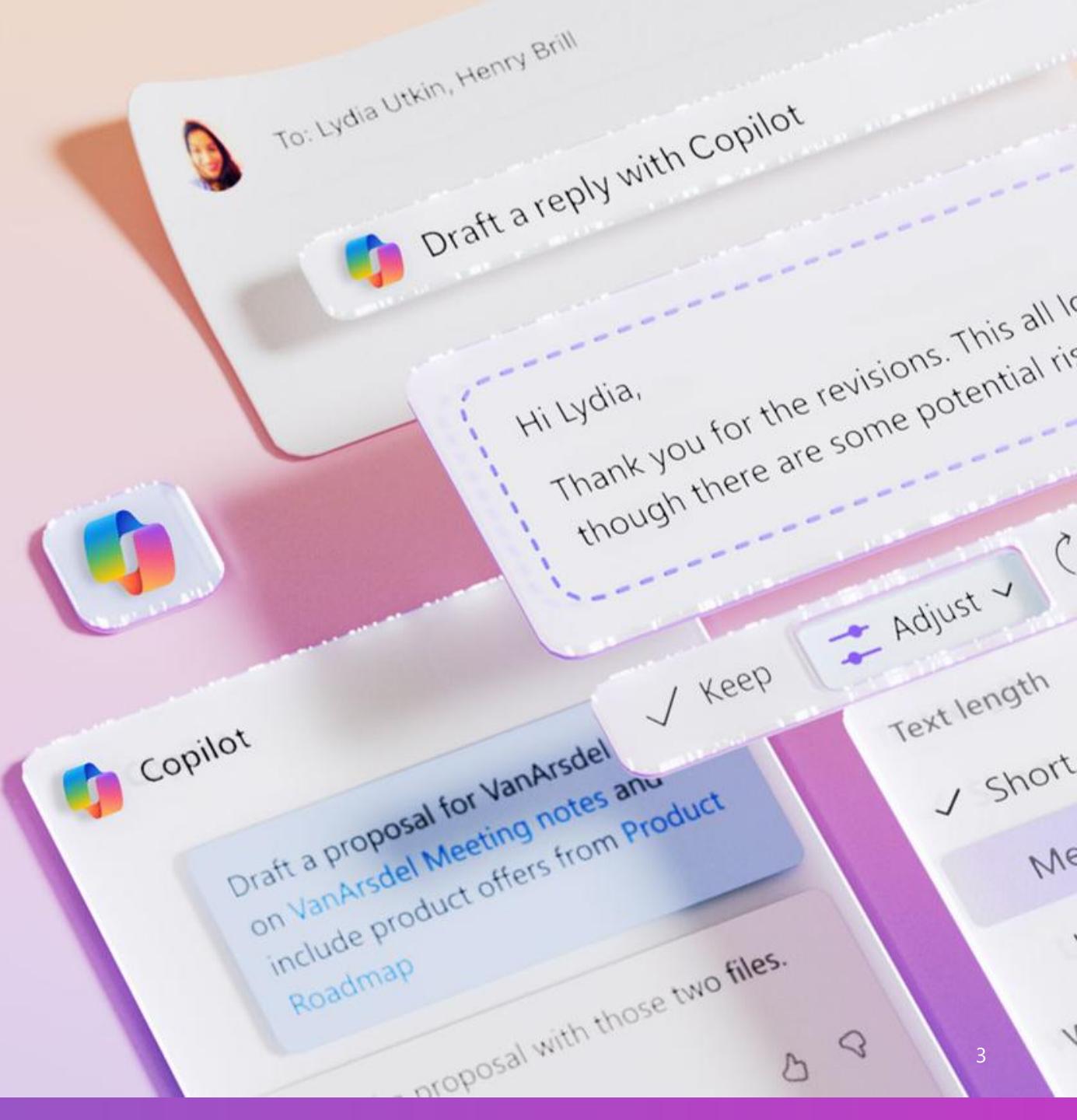




Before

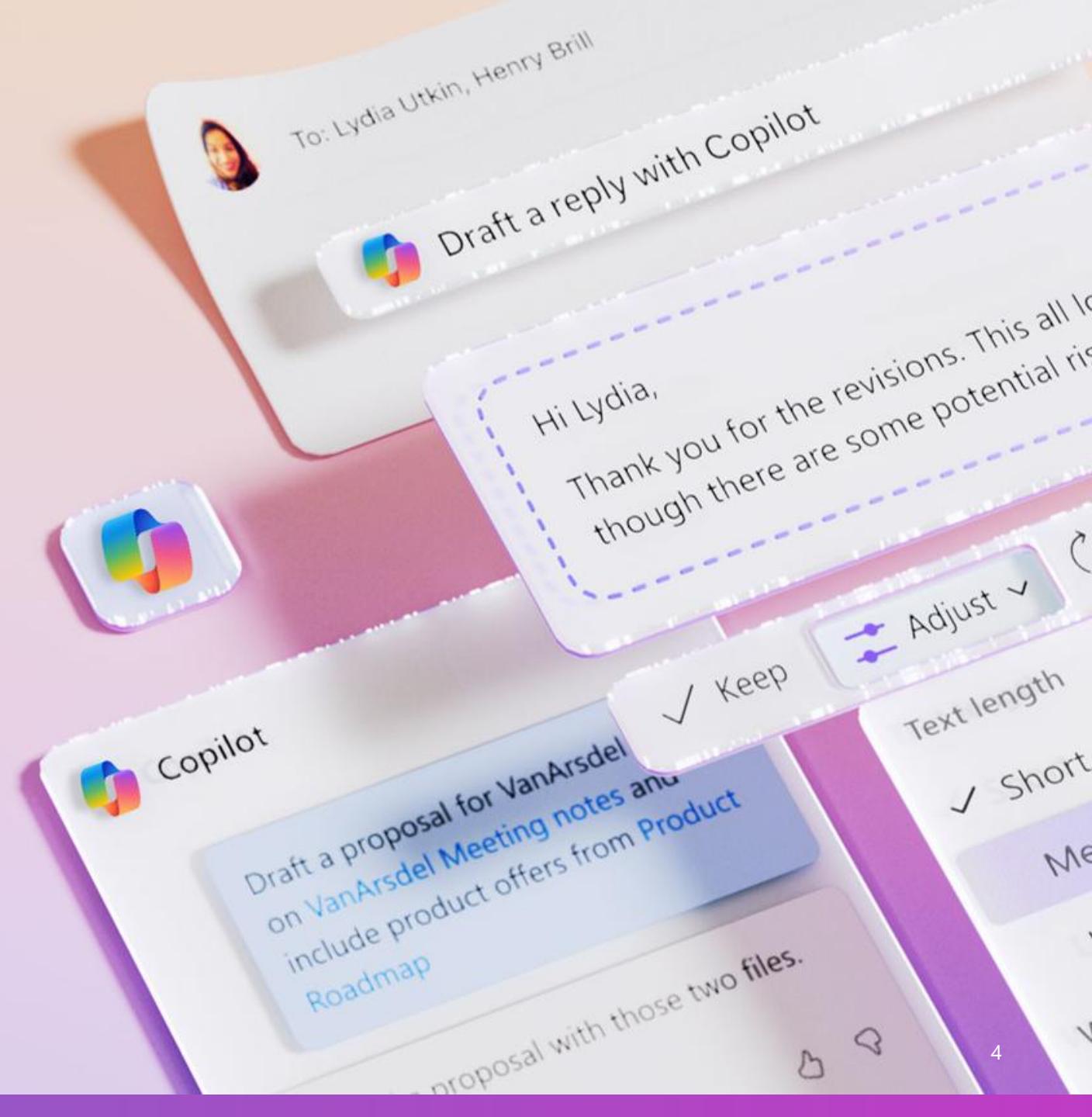


Things to consider



Things to consider

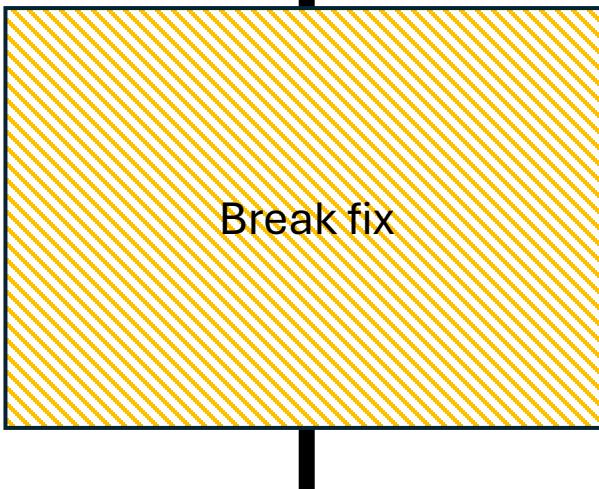
1. Changing role of the Technology advisor



V1

Reseller

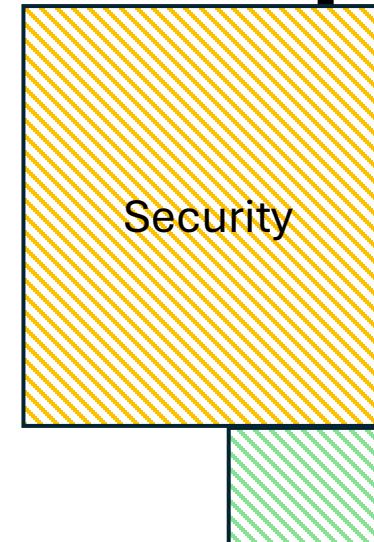
- Hardware = High
- Consult = Low
- Recurring = Low
- Tools = Low
- Dev = Low



V2

MSP

- Hardware = Medium
- Consult = Medium
- Recurring = High
- Tools = High
- Dev = Low



V3

Consultant

- Hardware = Low
- Consult = High
- Recurring = ?
- Tools = Low
- Dev = High



V1

Reseller

- Hardware = High
- Consult = Low
- Recurring = Low
- Tools = Low
- Dev = Low

V2

MSP

- Hardware = Medium
- Consult = Medium
- Recurring = High
- Tools = High
- Dev = Low

V3

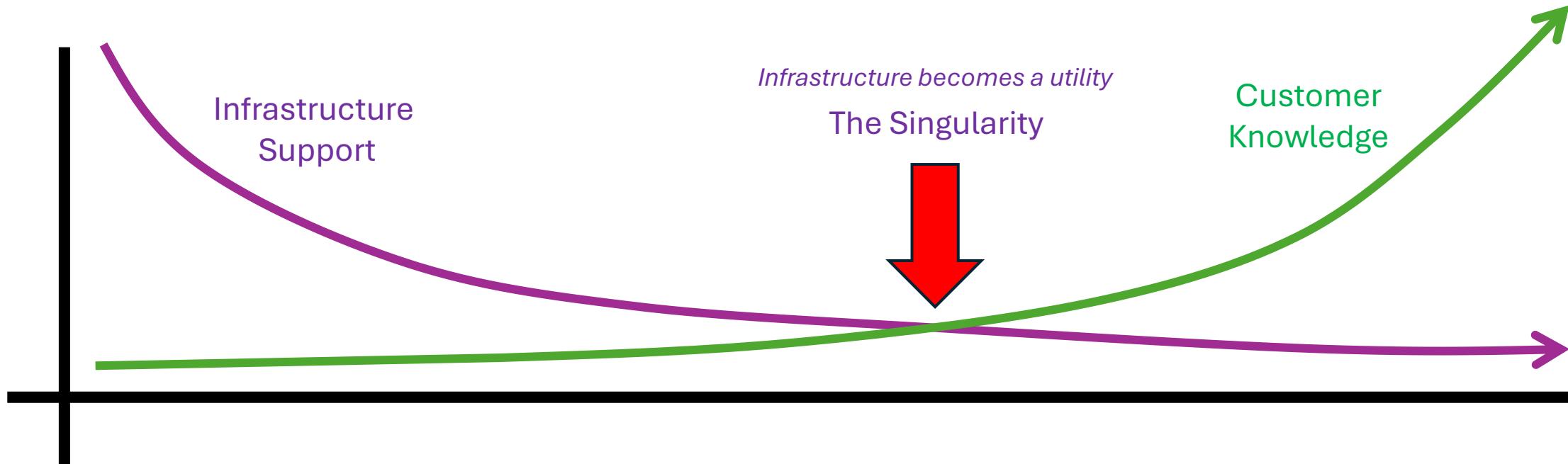
Consultant

- Hardware = Low
- Consult = High
- Recurring = ?
- Tools = Low
- Dev = High

Infrastructure
Support

Infrastructure becomes a utility
The Singularity

Customer
Knowledge



V1

Reseller

- Hardware = High
- Consult = Low
- Recurring = Low
- Tools = Low
- Dev = Low

V2

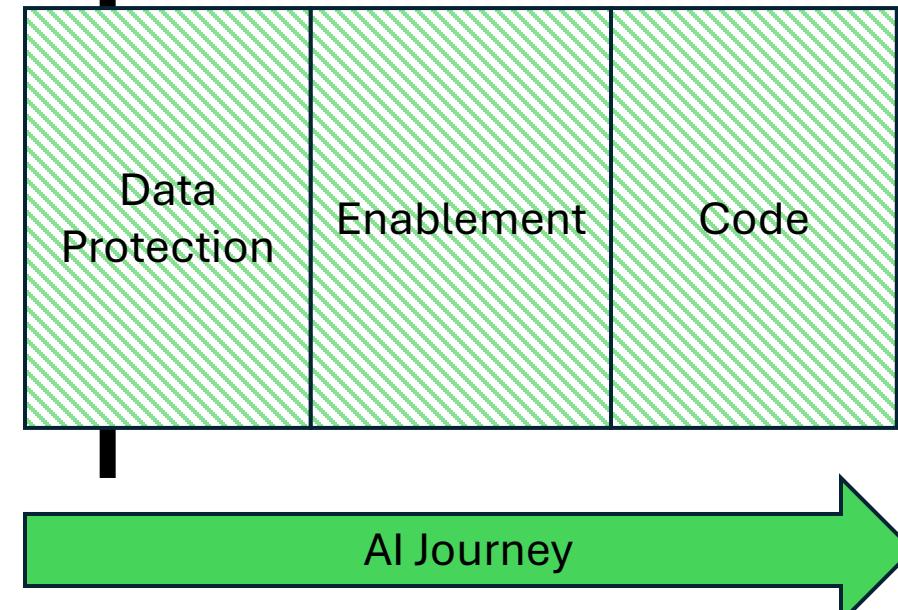
MSP

- Hardware = Medium
- Consult = Medium
- Recurring = High
- Tools = High
- Dev = Low

V3

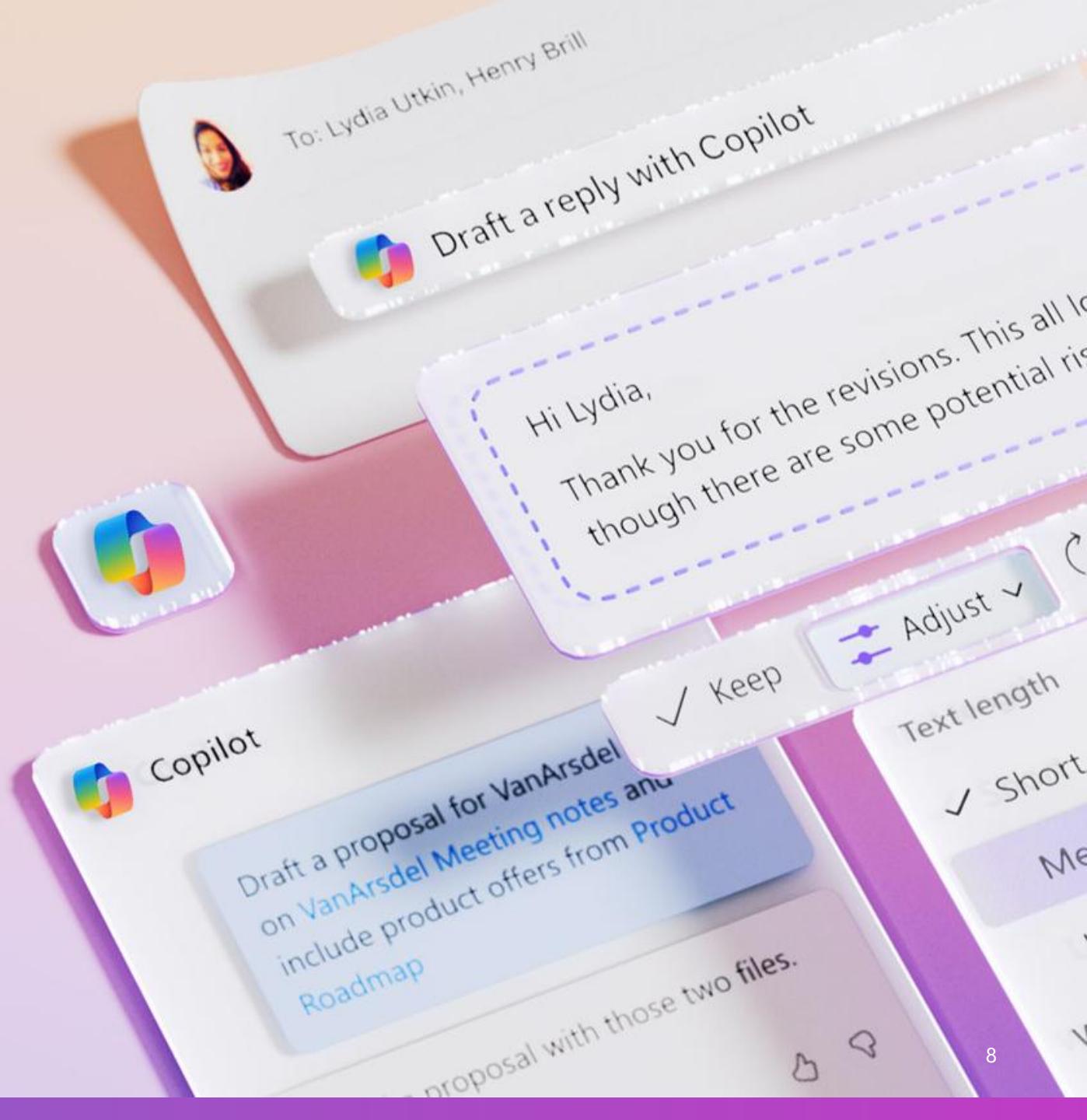
Consultant

- Hardware = Low
- Consult = High
- Recurring = ?
- Tools = Low
- Dev = High

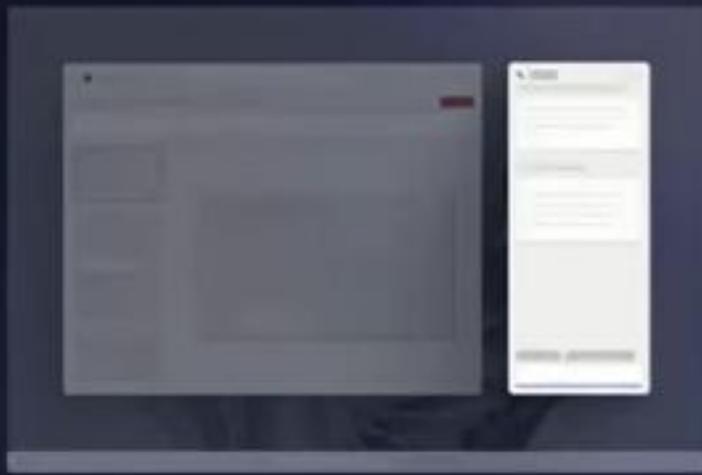


Things to consider

2. Changing role of the delivery of AI to users

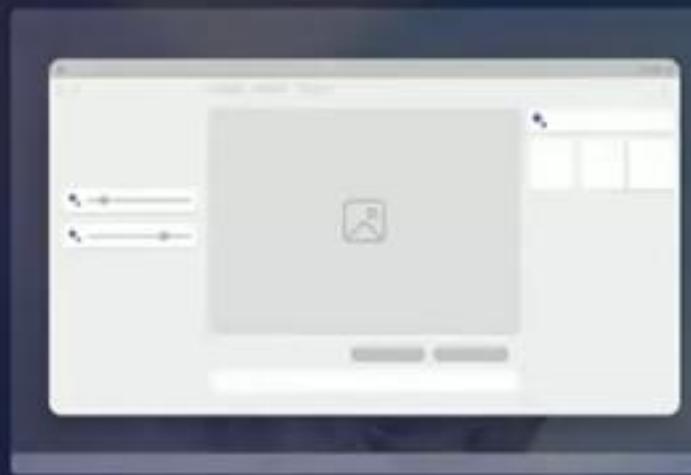


Beside



Add Copilots to be a helper
to your application

Inside

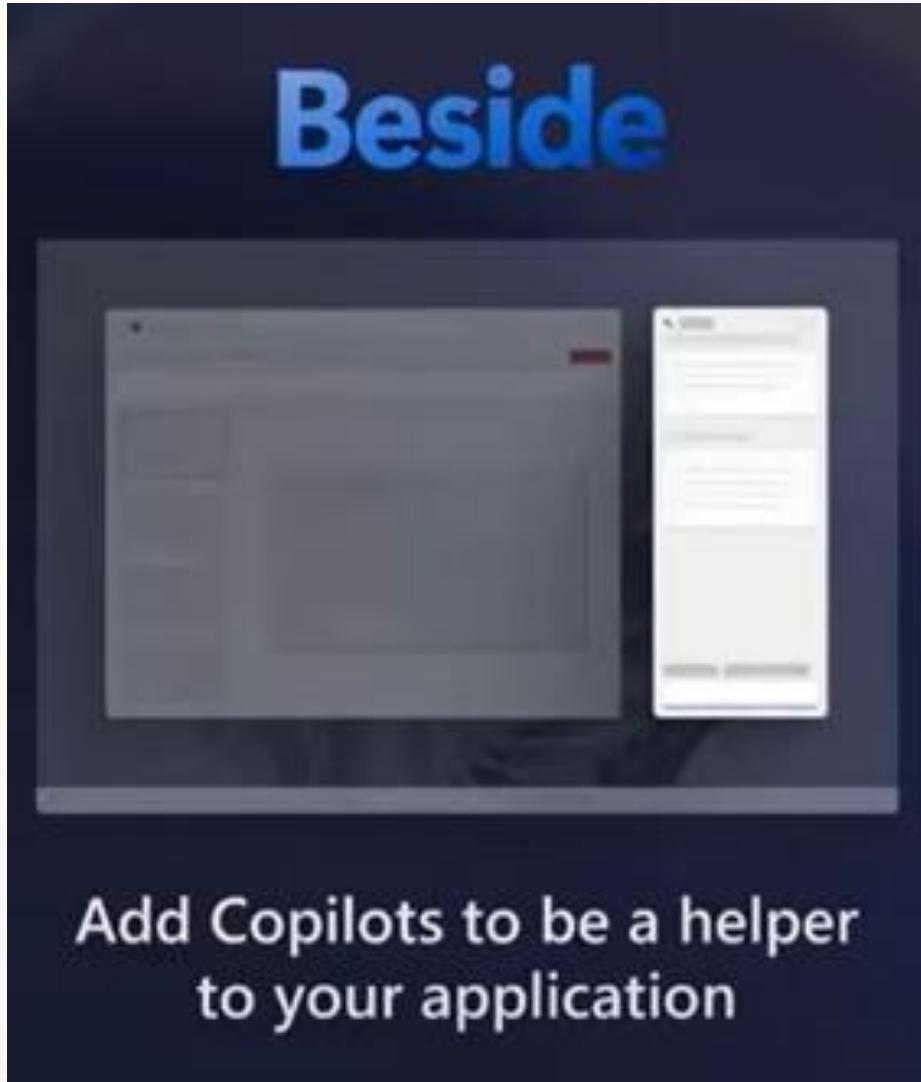


Create applications with AI
at the center of the experience

Outside



Agents help orchestrate
across apps and tasks



- Keeps original application architecture
- Keeps customer familiarity with application

Inside



Create applications with AI
at the center of the experience

- New interaction model
- More automatic
- Less explicit
- More implicit

Outside



Agents help orchestrate
across apps and tasks

- AI becomes the orchestrator
- Becomes more like an agent
- Tailored to suit the individual
- Works across applications, devices, time, etc

At the end of day



It's a tool

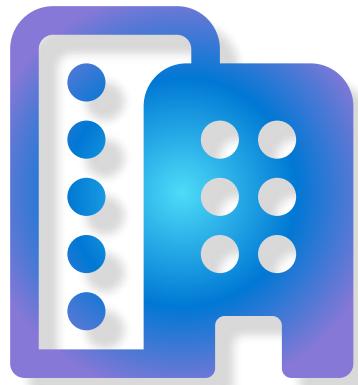
Putting both tools to work for you

Copilot



Current web data

Copilot for Microsoft 365



Your company data

Microsoft Work Trend Index

AI Productivity Research



Copilot Early Access
Program users



18,000+ people
across 12 markets



7 observational
studies

SPEED

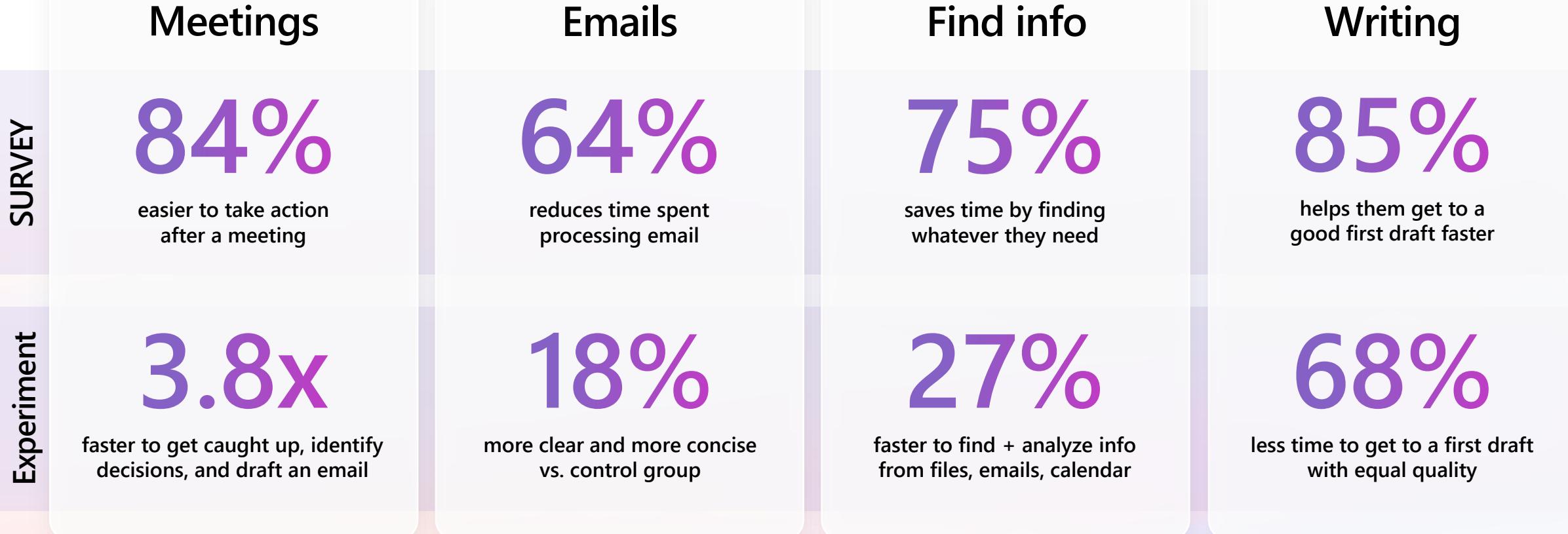
QUALITY

EFFORT



Source: [Work Trend Index Special Report: What Can Copilot's Earliest Users Teach Us About Generative AI at Work? November 2023](#)

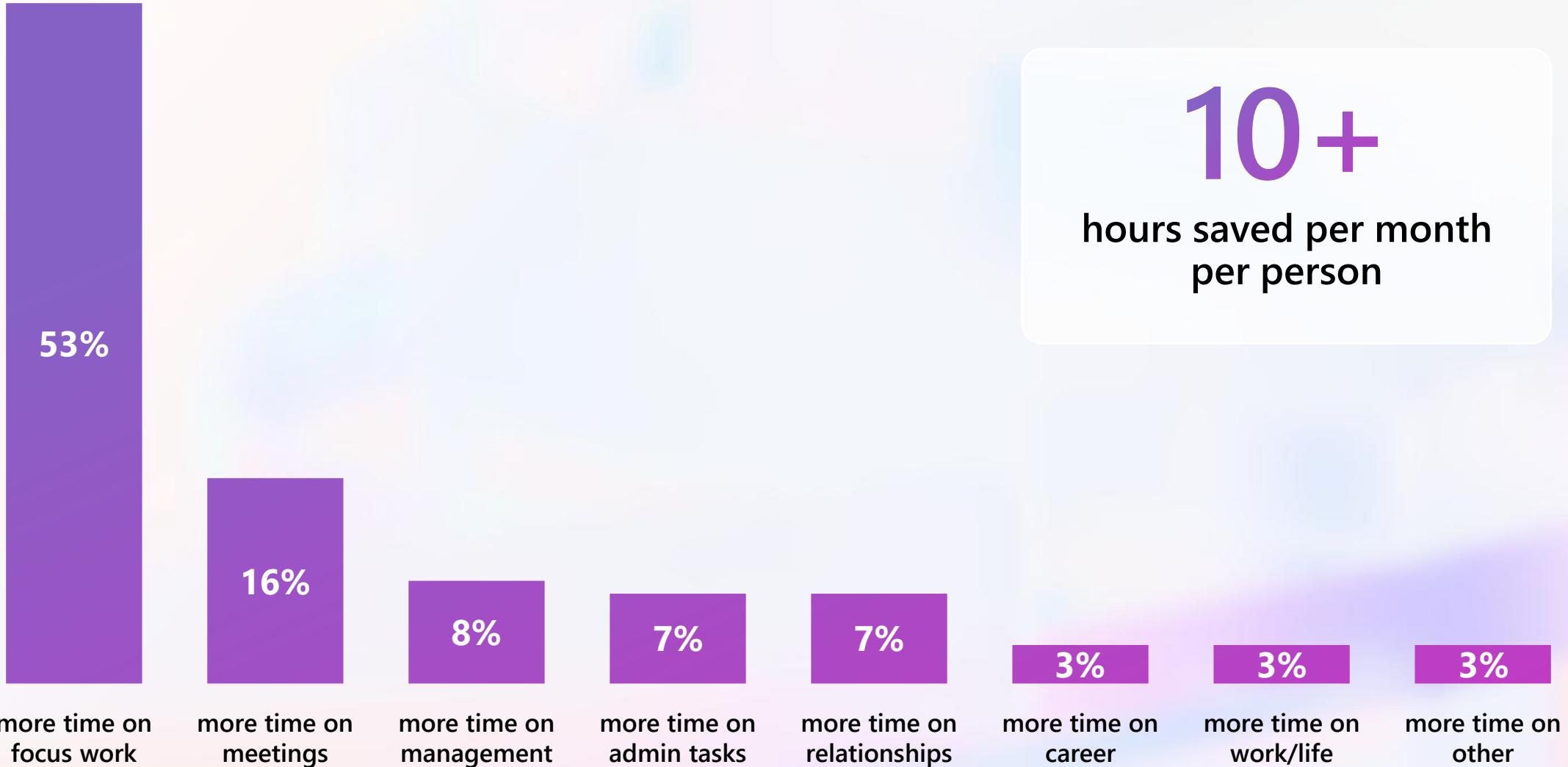
Emerging work patterns



Qualitative source: Survey of Copilot for Microsoft 365 Early Access Program users, October 2023.

Quantitative source: Microsoft Office of the Chief Economist, October 2023, "A Day in the Life Study." Microsoft Internal Research Team, October 2023, "The Missed Meeting: Evaluating Copilot's Effectiveness in Teams."

Microsoft Office of the Chief Economist, October 2023, "The Strain of Searching Study."



10+

hours saved per month
per person

Preparing your customers for the era of AI



What are your organization's **goals** for using AI?



What are your organization's **pain points** that AI can address?



What are your organization's **current capabilities** in terms of AI?



Does your organization have a **data strategy** in place?



Does your organization have the necessary **infrastructure and resources** to support AI initiatives?



Does your organization have a plan to **measure AI impact and upskill** its workforce in AI?

Copilot productivity gains



said they were more productive with Copilot



said Copilot improved the quality of their work

Source: Microsoft Office of the Chief Economist, October 2023, "A Day in the Life Study."; Microsoft Internal Research Team, October 2023, "The Missed Meeting: Evaluating Copilot's Effectiveness in Teams." Microsoft Office of the Chief Economist, October 2023, "The Strain of Searching Study."

Email processing

64% Spent less time processing email

Information search

75%

Spent less time searching for information in their files

Copilot's impact on meetings, searching, writing, and summarizing

3.8x

faster

getting caught up on
a missed meeting

29%

faster

in a series of tasks
(searching, writing, and
summarizing)

Copilot's best users saved



10+ hours per month

Source: Survey of Copilot for Microsoft 365 Early Access Program users, October 2023. Note: this figure relates to 22% of respondents and is not an average.

Get Ready for Copilot for Microsoft 365

Empower employees with secure, AI-powered tools

Standardize on M365

Organize sensitive business data

Start using Gen AI with Copilot

Migrate Data to Cloud

Optimize your data management and security practices

Immediate Customer Value

Microsoft Copilot with commercial data protection for users signed in with Entra ID at no additional cost

Migrate/upgrade to cloud – Exchange Online, Teams, SharePoint online, Microsoft 365 apps

Protect business data from external threats with Identity & Endpoint

Long Term Value

Train users on using AI in the workplace for faster ROI realization

Create and build your graph for a more relevant experience with Copilot for Microsoft 365

Manage data retention and labeling for safer AI use internally

Partner Opportunity

- Inoculate your customer base against competitor solutions
- User adoption & change management

- Acquire new customers
- Data Migration Services

- Upsell to M365 Business Premium
- Security Managed Services

Partner opportunities

AI + Copilot
Advisory

Readiness
Assessment

Deployment

Adoption &
Change
Management

Extensibility

Practice development resources aka.ms/AIFutureOfWorkPartner

Understand the partner services opportunity



Advisory



Readiness



Deployment



Adoption &
Change
Management



Extensibility

Partner opportunities

AI + Copilot Advisory

- Lead business transformation conversations.
- Provide guidance for the responsible use of AI.
- Identify personas and scenarios that would deliver the most value if reimagined with AI.

Readiness Assessment

- Assess licensing and technical readiness.
- Assess customer data protection and governance.
- Showcase the benefits of Copilot.
- Identify high-value scenarios.

Deployment

- Close readiness gaps.
- Assign licenses and configure with Setup Guide.
- Address optimization opportunities:
 - Remediate overprivileged and risky users.
 - Mitigate device risk.
 - Prevent over-exposure of data.

Adoption & Change Management

- Build and execute an adoption plan that includes:
 - Creation of a Copilot Center of Excellence.
 - Awareness strategy.
 - Learning plan.
 - Success measures and reporting.
- Deliver extended training and adoption support.

Extensibility

- Conduct line-of-business app assessments.
- Extend value with Copilot plugins and connectors.
- Connect data to Microsoft Graph and Dataverse.
- Deliver integration, customization, and configuration services.
- Build unique experiences with Copilot Studio.

Actions and investments in the customer journey

Sales Journey

Listen and Consult

Inspire and Design

Empower and Achieve

Realize Value

Manage and Optimize

Partner Services

AI + Copilot Advisory

Readiness Assessment

Deployment

Adoption & Change Management

Extensibility

Action and Investment

Leverage pitch decks, demos and other content at aka.ms/AIFutureOfWorkPartner

Deliver the [Copilot for Microsoft 365 Optimization Assessment](#) and [Copilot for Microsoft 365 Pre-Sales Workshop](#)

Share the [Copilot for Microsoft 365 Onboarding Kit](#)

Leverage the [Copilot for Microsoft 365 Adoption materials](#) and [Deliver Adoption Accelerator workshop engagement](#)

Deliver [Microsoft Copilot Studio content](#) and use the [Copilot for Microsoft 365 Adoption guidance](#)

Accelerate customer AI readiness before deploying Copilot

Proactively get customers ready to embrace the AI-powered future of work:

1. Move customers to **AI-ready licenses** within the Microsoft 365 suite
2. Prepare customers to meet Copilot **technical requirements**
3. Reassure customer **data privacy** concerns and ensure comprehensive **compliance and security** controls

Microsoft 365 Copilot | Winning Customers

Customer on
Microsoft 365
E3/ME5
/Biz Premium

Yes?

Lead with Copilot

Address technical readiness gap

Copilot uses information available to users within the MS Graph. To retrieve their business data, users will need to deploy and adopt Microsoft 365 first.

Enable Copilot Center of Excellence

Leverage [deployment and adoption resources](#)

Copilot ready

No?

Lead with Secure Productivity + Copilot

Deploy Microsoft 365 E3/BP

Drive usage & pitch Copilot

Microsoft 365 is foundational to being AI ready. Although Copilot will be a different license, customers will need to be on Microsoft 365 E3/E5 as a base license.

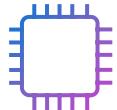
Leverage the [Microsoft 365 E3 offers and promos](#)

Unify a complex, disconnected IT ecosystem into a single secure foundation



Devices

that meet specific job requirements



Operating system

that's secure, easy to manage, update, and use



Security

that defends against cyberattacks across multiple platforms



Management

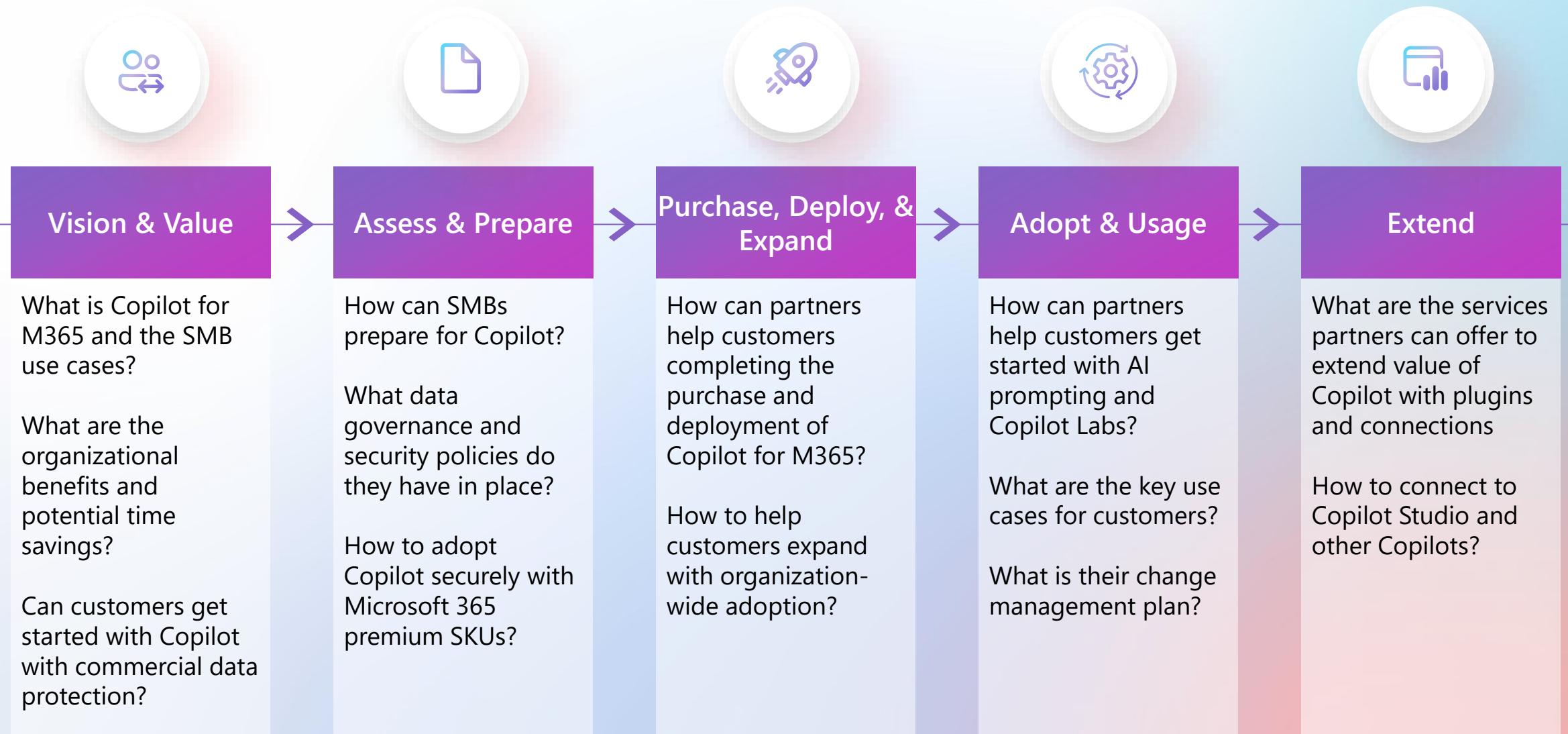
that is built for a heterogenous device estate, including personal devices



Collaboration

that connects every employee across all devices

The customer journey with Copilot for Microsoft 365



Target customers



Customer Profile	Microsoft 365 Copilot licensed customers	Microsoft 365 E3/E5 Customers	On-Premises Customers
Customer Needs	<ul style="list-style-type: none">Customers have 300 seats or more, and looking to expand the number of seats in the same tenant or in a new oneIdentify high-value scenarios and start planning for pilot launch	<ul style="list-style-type: none">New to Microsoft 365 CopilotLooking to adopt generative AI quickly	<ul style="list-style-type: none">Not on Microsoft 365 E3/E5 licensesLooking to move to an Enterprise suite and bring SharePoint, OneDrive, etc. to the cloud
Sales Play	<ul style="list-style-type: none">Conduct envisioning sessions, readiness assessments, and art of the possible workshopsConfigure Microsoft 365 Copilot for high-impact scenariosSupport deployment of pilotDrive adoption across the organization and set up a champ community for 2 – 3 scenariosContinue to improve, train, and support	<ul style="list-style-type: none">Lead with the value proposition of Microsoft 365 CopilotEmbed generative AI into the productivity apps your customer uses every day to unleash creativity, unlock productivity, and uplevel skillsDrive adoption of Microsoft 365 (Copilot uses information available to users within MS Graph to retrieve their business data)Leverage deployment and adoption resources	<ul style="list-style-type: none">Lead with secure productivity and Microsoft 365 CopilotCopilot inherits your customer's security, compliance, and privacy policies in Microsoft 365Set up a strong Zero Trust foundation, streamline endpoint management, and elevate productivityMicrosoft 365 is foundational to being AI-readyLeverage the ME3 offers and promos

Engagement Plan

Tap into 190M seats opportunity with Microsoft 365 Copilot



Listen and Consult

1. Target customers for M365 Copilot upsell:
 - Upsell copilot to +300 ME3/ME5 seats in a tenant with healthy usage
 - Uplevel usage of Microsoft 365 to be ready for M365 Copilot
 - Upsell to ME3 + AI – Lead with Bing Chat Enterprise
2. Engage with BDMs on [driving AI transformation with copilot](#)
3. Assess & document customer motivation & business imperatives

Inspire and Design

4. Deliver the Microsoft 365 Copilot pitch demos based on customer scenarios
5. Nominate and deliver [Microsoft 365 Copilot workshops](#) for [readiness assessment](#) and identify technical, data, and security gaps
6. Build customer success roadmap

Empower and Achieve

7. Secure customer agreement on deployment, remediation, and adoption plan
8. Address [Data security, access, and compliance](#) gaps
9. For eligible customers, connect with Microsoft Commercial Executive to finalize the Microsoft 365 Copilot proposal
10. Close the deal with deployment and management services and product proposal

Realize Value

11. Deliver services to configure Microsoft 365 Copilot and drive adoption for high-impact scenarios

Manage and Optimize

12. [Leverage Microsoft 365 Copilot adoption guidance](#)
 - Deliver Adoption Accelerator
 - Train and support end users
13. Deliver ongoing and proactive engagements to drive higher usage of Microsoft 365 Copilot and expand opportunities



Share opportunity with Microsoft sellers for co-selling



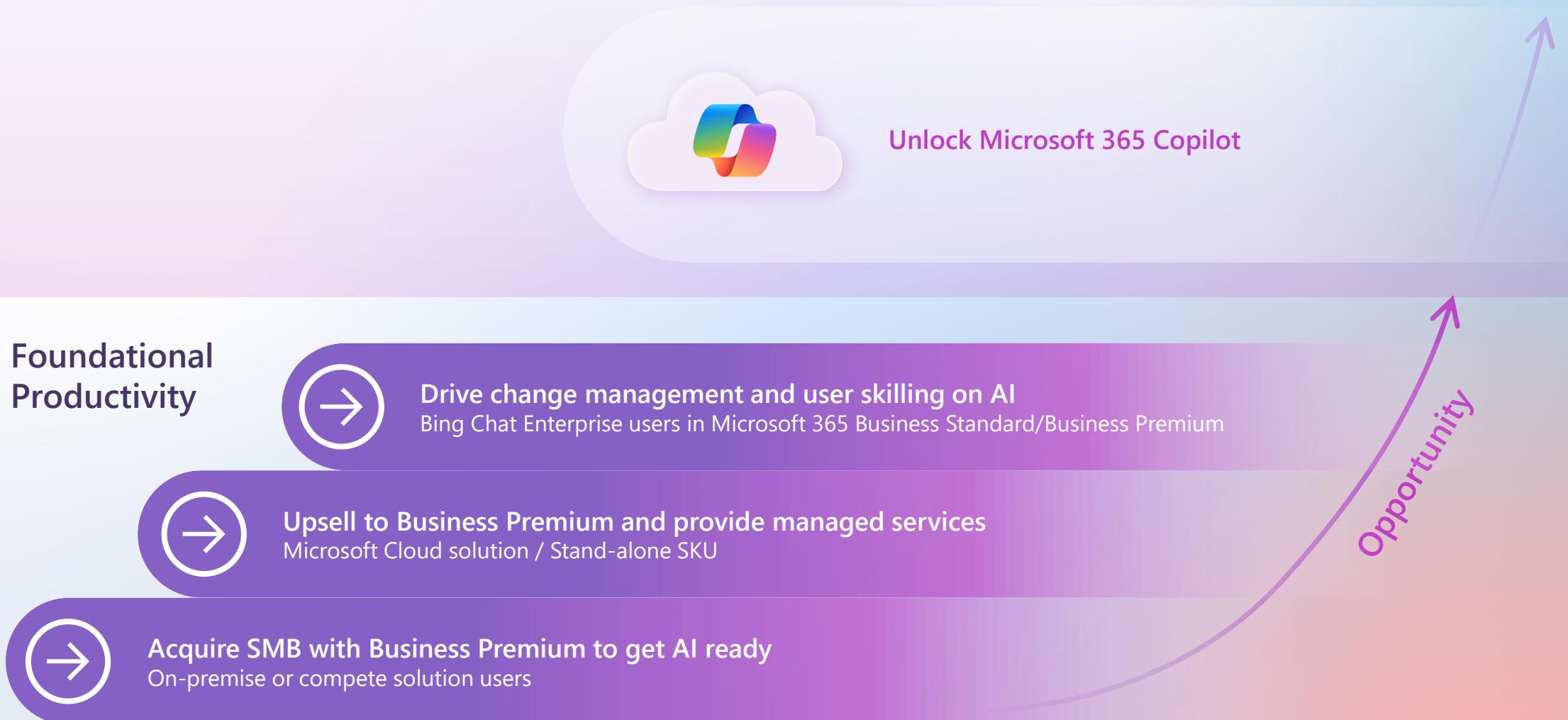
Connect with Microsoft Commercial Executive early for proposal

Packaged partner engagements for M365 Copilot

Inspire & Design		Realize Value
Description	[1] M365 Copilot Workshop	
	[1a] Readiness Assessment	[1b] Art of Possible + Value Discovery
Description	Assess the customer's environment to verify that M365 Copilot prerequisites are met and what steps are needed to ensure data is protected from accidental exposure	Showcase M365 Copilot capabilities, help the customer identify the high value use cases that M365 can enable, and build the plan to implement them
Components	<ul style="list-style-type: none">▪ Assessment delivery guide▪ Technical deck▪ Data protection/governance assessment	<ul style="list-style-type: none">▪ Workshop delivery guides▪ Copilot pitch deck and demos▪ Scenario discovery guide▪ Business value calculator
Outcomes	<ul style="list-style-type: none">▪ Customer readiness scorecard▪ Recommendations to address gaps	<ul style="list-style-type: none">▪ High value use cases▪ Implementation plan
Duration	1 day	2 days
Target customers	High propensity customers for M365 Copilot (focus on customers with +300 E3/E5 licenses and healthy usage)	3 days (non-continuous) Customers with M365 Copilot licenses

Note: Workshops are partner-led, however please engage with Microsoft sellers when executing the workshop for your customer. Share Copilot Referrals through Partner Center

Help SMBs on their AI journey every step of the way



Copilot for Microsoft 365 implementation



Copilot for Microsoft 365

Training and documentation by phase

USER
ENABLEMENT

Get ready

- ✓ **Docs:** User Experience Strategy template (coming soon)
- ✓ **Video:** [Copilot Experiences Explained](#)

TECHNICAL
READINESS

- ✓ **Course:** [Get started with Copilot for Microsoft 365](#) (2 hrs)
- ✓ **Video:** [How Microsoft 365 Copilot works](#) (10 min)
- ✓ **Video:** [How to get ready for Microsoft 365 Copilot](#) (9 min)
- ✓ **Docs:** [Data, Privacy, and security for Microsoft Copilot for Microsoft 365](#)
- ✓ **Docs:** [Microsoft Copilot for Microsoft 365 requirements](#)

Onboard & engage

- ✓ **Course:** Copilot for Microsoft 365 User Enablement Specialist (coming soon)
- ✓ **Tool:** [Copilot Lab](#) (including app specific guidance)
- ✓ **Video:** Creating a User Experience Strategy (coming soon)
- ✓ **Docs:** User Experience Strategy template (coming soon)

Deliver impact

- ✓ **Course:** [Empower your workforce with Copilot for Microsoft 365 Use Cases](#) (7 business group use cases)
- ✓ **Course:** [Craft effective prompts for Copilot for M365](#) (2 hrs)
- ✓ **Article:** [Learn about Copilot prompts](#)
- ✓ **Article:** [Get better results with Copilot Prompts](#)
- ✓ **Article:** [Edit a Copilot prompt to make it your own](#)
- ✓ **Article:** [Share your best prompts](#)

Extend & optimize

- ✓ **Docs:** [Modern Collaboration Architecture](#) people-centric scenario guidance
- ✓ **Course:** [Craft effective prompts for Copilot for Microsoft 365](#) (2 hrs)
- ✓ **Docs:** [Extend Microsoft Copilot for Microsoft 365](#)
- ✓ **Course:** [Optimize and extend Copilot for Microsoft 365](#) (1 hr)
- ✓ **Course:** [Create copilots with Microsoft Copilot Studio](#) (4 hrs)
- ✓ **Course:** [Extend and manage Microsoft Copilot Studio copilots](#) (2 hrs)

Copilot for Microsoft 365

Implementation activities

USER
ENABLEMENT

Get ready

User Enablement Workstream

- ✓ Secure sponsorship and define engagement principles
- ✓ Identify pilot group, high value scenarios and personas
- ✓ Define success criteria, KPIs, and success measurement plan

TECHNICAL
READINESS

Technical Readiness Workstream

- ✓ Perform the Copilot for Microsoft 365 Optimization Assessment
- ✓ Address data security, governance, and data access requirements
- ✓ Build Copilot for Microsoft 365 implementation plan

Onboard & engage

- ✓ Prepare and plan for end-user training
- ✓ Deliver employee communications
- ✓ Onboard executives and user cohorts
- ✓ Deliver user training

Deliver impact

- ✓ Review success measures and collect feedback
- ✓ Identify additional optimization scenarios
- ✓ Collect & share success stories

Extend & optimize

- ✓ Identify high value scenarios
- ✓ Identify opportunities for business process transformation with Copilot Studio, plugins, and connectors
- ✓ Run monthly/quarterly service health reviews
- ✓ Enable and publish plugins to unlock new scenarios and value
- ✓ Optional: design, build and publish your own plugins and copilots

Copilot for Microsoft 365

Implementation activities

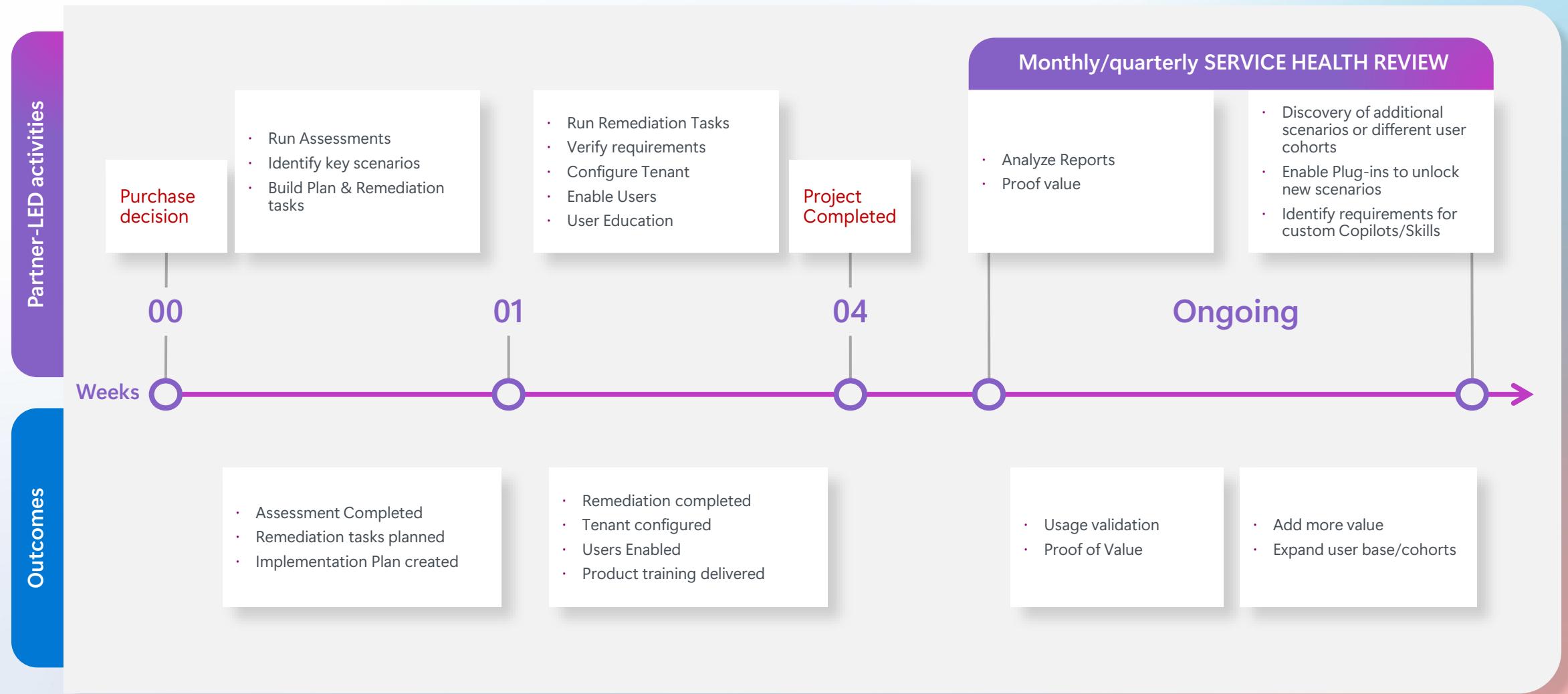
	Get ready	Onboard & engage	Deliver impact	Extend & optimize
USER ENABLEMENT	User Enablement Workstream <ul style="list-style-type: none">✓ Secure sponsorship and define engagement principles✓ Identify pilot group, high value scenarios and personas✓ Define success criteria, KPIs, and success measurement plan	<ul style="list-style-type: none">✓ Prepare and plan for end-user training✓ Deliver employee communications✓ Onboard executives and user cohorts✓ Deliver user training	<ul style="list-style-type: none">✓ Review success measures and collect feedback✓ Identify additional optimization scenarios✓ Collect & share success stories	<ul style="list-style-type: none">✓ Identify high value scenarios✓ Identify opportunities for business process transformation with Copilot Studio, plugins, and connectors
TECHNICAL READINESS	Technical Readiness Workstream <ul style="list-style-type: none">✓ Perform the Copilot for Microsoft 365 Optimization Assessment✓ Address data security, governance, and data access requirements✓ Build Copilot for Microsoft 365 implementation plan	<ul style="list-style-type: none">✓ Ensure appropriate Information protection and data governance controls are in place✓ Prepare customer tenant for Copilot for Microsoft 365	<ul style="list-style-type: none">✓ Activate managed services✓ Analyze reports to observe user adoption, retention, and engagement	<ul style="list-style-type: none">✓ Run monthly/quarterly service health reviews✓ Enable and publish plugins to unlock new scenarios and value✓ Optional: design, build and publish your own plugins and copilots

You
are here



Sample implementation project timeline

Shared milestone view





Prepare customers for Copilot for Microsoft 365 with an AI Evaluation

Execute a Copilot AI assessment with Contoso Life to define their journey to Copilot for Microsoft 365, including the 3 key steps:

Assess the customer's readiness for Copilot for Microsoft 365

- ✓ Foundational productivity readiness
- ✓ Data readiness
- ✓ Security readiness

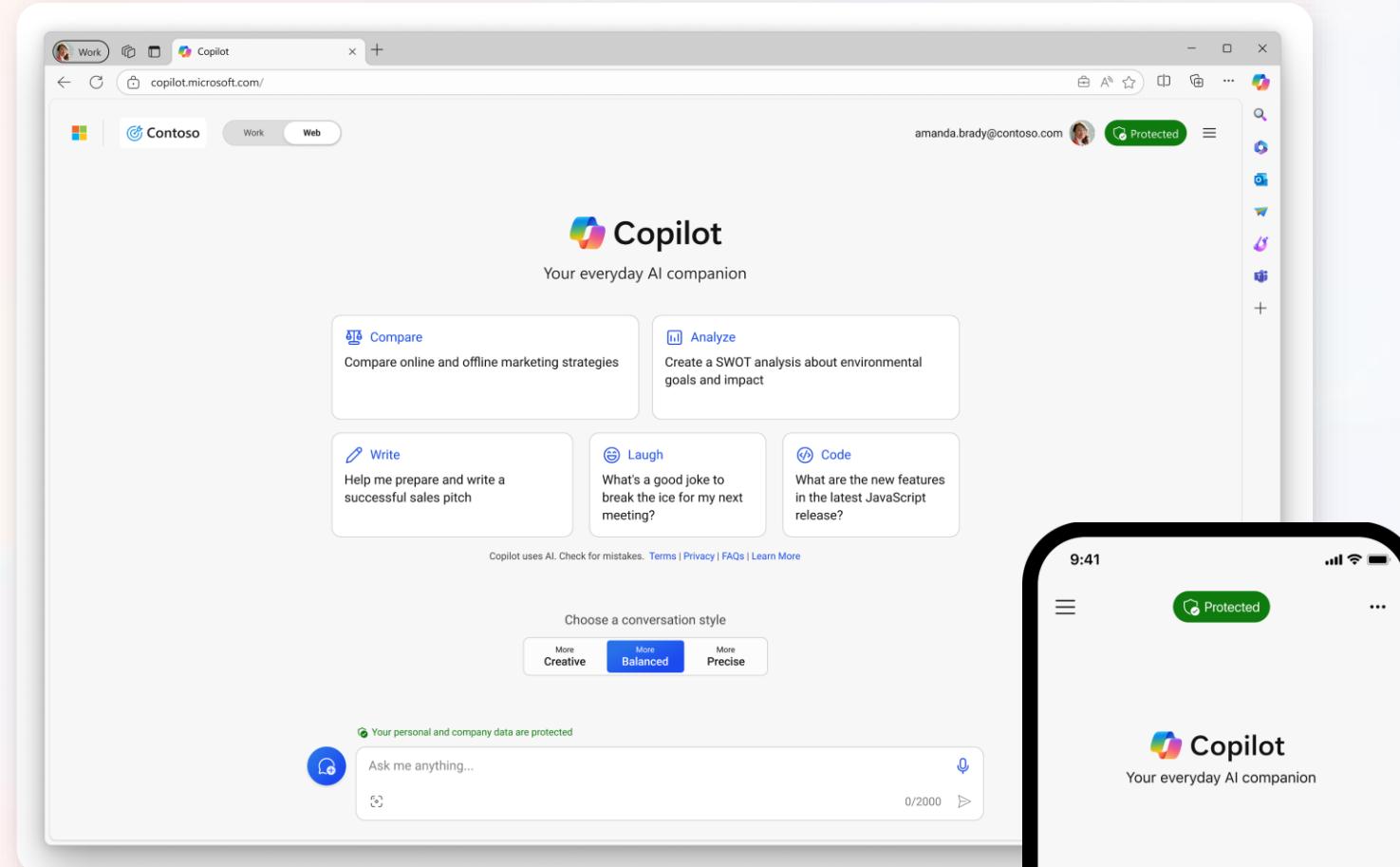
aka.ms/CopilotM365Assessment

The background of the slide features a dynamic, abstract design composed of several overlapping, translucent bands. These bands are primarily colored in shades of blue, orange, and pink, creating a sense of depth and motion. The bands curve and overlap in various ways, with some appearing more solid and others more transparent. The overall effect is reminiscent of a digital interface or a futuristic landscape.

Get ready

**Address security, governance, and
data access requirements**

Commercial data protection is available anywhere Copilot is accessed



Copilot.Microsoft.com on desktop and mobile

Available on desktop via:

- Copilot.Microsoft.com
- Windows
- Microsoft Edge
- Microsoft Bing

Available on mobile via:

- Copilot app: Microsoft Entra ID sign-in support is coming soon
- Edge app
- Bing app
- Microsoft 365 app

Microsoft's AI principles



Fairness



Reliability
& safety



Privacy &
security



Inclusiveness



Transparency



Accountability

Microsoft Cloud — AI you can trust

Your data is **your** data.

Your data is **not** used to train the OpenAI foundation models without permission.

Your data is **protected** by the most comprehensive enterprise compliance and security controls.



Copilot for Microsoft 365

Built on Microsoft's **comprehensive** approach



Security

+



Compliance

+



Privacy

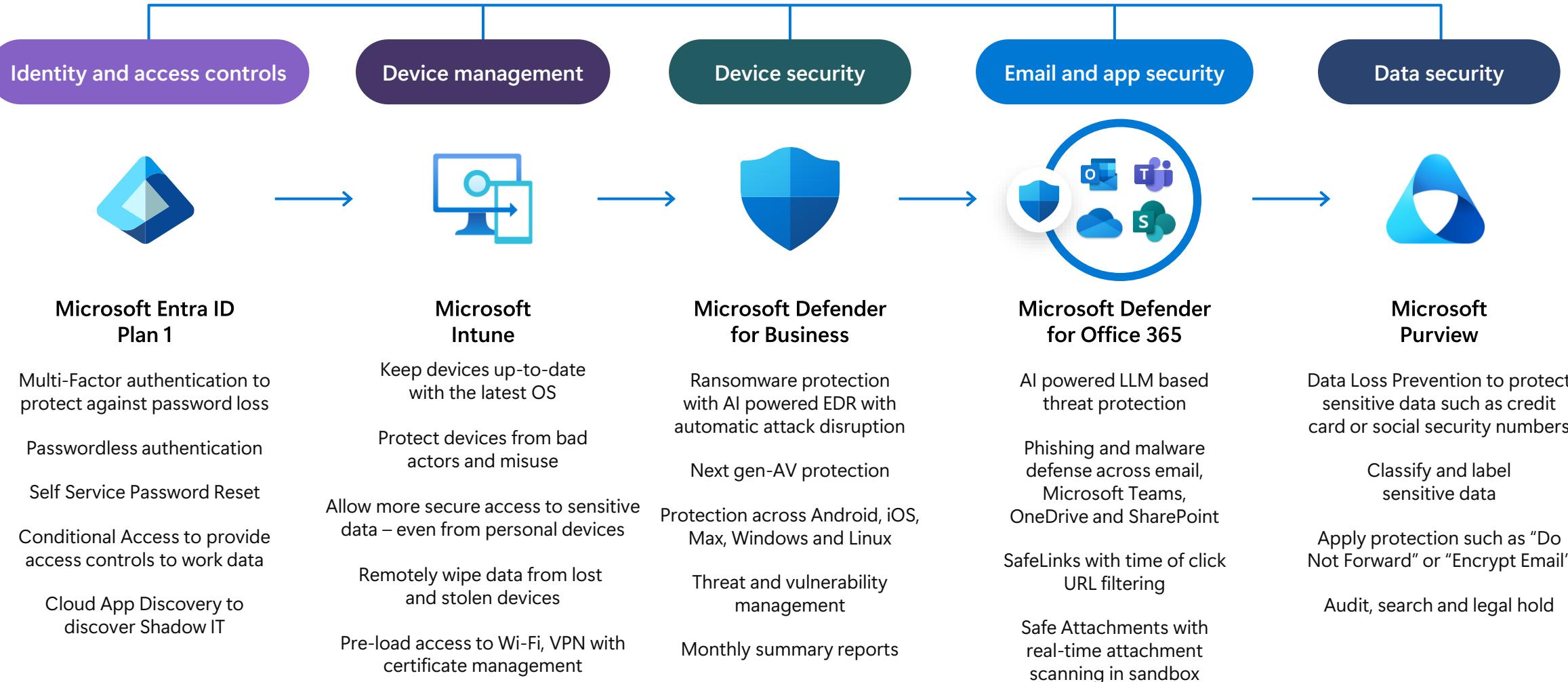
+



Responsible AI

Layered security that improves your security posture

Microsoft 365 Business Premium



Security and compliance for Microsoft 365 Copilot in SMB



Foundational security controls

Microsoft 365 Business Basic or Business Standard
+ Microsoft Copilot for M365

- Multi-factor authentication (MFA) for secure access to M365 applications with Copilot
- Search and export Copilot prompts and interactions
- Audit logs for Copilot interactions
- Retention or deletion policies for Copilot interactions and generated content
- Restricted SharePoint Search for Copilot interactions and generated content



Comprehensive security controls

Microsoft 365 Business Premium
+ Microsoft Copilot for M365

- Multi-factor authentication (MFA) with conditional access based on identity, device, location, and network
- Search, export, eDiscovery case management, and legal hold for Copilot prompts and interactions
- Audit logs for Copilot interactions
- Retention or deletion policies for Copilot interactions and generated content
- Manual sensitivity and retention labels for content processed by Copilot in files and emails
- Data loss prevention policies to help protect sensitive data from Copilot in files and emails

Copilot top questions asked



Security/Compliance

How do we manage authentication and authorization of AI calls to the LLM to ensure data is safe?

How can I be aware when Copilot uses/returns sensitive information?

When and how will we be able to audit Copilot usage; see what content is being accessed?

Privacy/data residency

How and where are prompts stored and are they discoverable?

Where is my data processed?

How do we know our data is secure: how is our data encrypted?

Adoption/Readiness/Impact

What do we need to do to get ready?

What types of admin controls are available?

What type of success criteria / measures should I use to gauge the benefit and impact of giving users Copilot?

Microsoft is built on trust

1

Your data **is**
your data

2

Your data **is**
not used to
train or enrich
foundation
AI models

3

Your data and
AI models **are**
protected at
every step

4

Our Customer
Copyright
Commitment

Microsoft 365 Copilot is the AI assistant you can trust



Security

Honors your existing permissions

Persistent label inheritance
and DLP policies

Risk-based conditional access and
endpoint management



Governance & Compliance

Ramp your data preparedness for AI

Detect and investigate non-
compliant usage

Guided assistance to remain
compliant with AI regulations



Privacy

You control your data

You control your data location

Your data isn't used to train
foundation models

Your Microsoft 365 security, governance, compliance, and privacy policies

Concerns we've heard from you...



Shadow AI use

78%

of AI users use BYOAI

75% of employees are using AI, which means ~58% of employees are bringing their own AI to work¹.



Lack of protection

97%

of organizations

have concerns about implementing AI due to the lack of controls to mitigate risks of data leakage².



Increased AI regulations

By
2027

at least one global company will see its AI deployment banned by a regulator for noncompliance with data protection or AI governance legislation².

1. [2024 Work Trend Index Annual Report from Microsoft and LinkedIn: AI at Work Is Here. Now Comes the Hard Part](#)

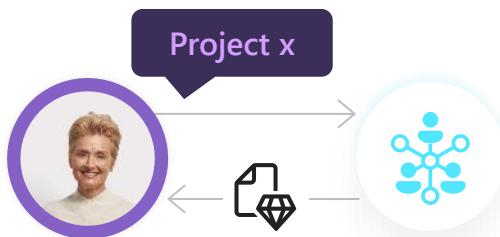
2. [Securing data in an AI-first world with Microsoft Purview, Nov 15, 2023](#)

Security and compliance challenges

1

Data oversharing

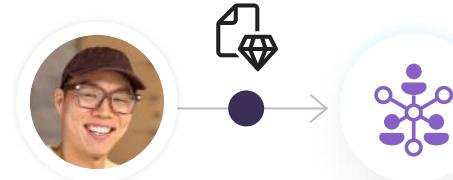
Users may access sensitive data via AI apps they're not authorized to view or edit



2

Data leak

Users may inadvertently leak sensitive data to AI apps



3

Non-compliance usage

Users use AI apps to generate unethical or other high-risk content



Secure and govern Copilot with Microsoft Security



Baseline

Essential security controls

- Multi-factor Authentication
- Audit logging
- Basic content and keyword search

Microsoft 365 Copilot +
Microsoft 365 Business Standard



Core

Comprehensive security controls

Everything in Microsoft 365 Business Standard, plus:

- Conditional Access
- Sensitivity labels
- Data loss prevention policies
- Unified endpoint management
- eDiscovery, litigation hold and retention policies

Microsoft 365 Copilot +
Microsoft 365 Business Premium

Note: Not all features/products shown.

Secure and govern Copilot with Microsoft Security



Baseline



Multi-factor Authentication

Audit logging

Microsoft 365 Copilot
+ Office 365 E3

Core



Conditional Access

Manual sensitivity labels

Data loss prevention policies

Advanced SharePoint sitewide access controls and reporting

Unified endpoint management

Microsoft 365 Copilot
+ Microsoft 365 E3

+ SharePoint Advanced Management

Best-in-class



Conditional Access based on identity risk

Automatically apply sensitivity labels

Automatically remove inactive content

Prevent data leak on endpoint devices

Detect non-compliant usage

Microsoft 365 Copilot
+ Microsoft 365 E5
+ SharePoint Advanced Management

Restricted SharePoint Search

This is intended as a temporary solution to give you time to review and audit site permissions while implementing robust data security solutions from Microsoft Purview and content management with SharePoint Advanced Management

- **Restricted SharePoint Search** is designed for organizations particularly concerned about unintentional oversharing of content.
- When enabled, Copilot experiences and organization-wide search are limited to a select set of SharePoint sites, as well as the individual user's files and content.



PRE-REQUISITES

- Available to tenants with Microsoft 365 Copilot subscriptions.
- Activation requires Global/Tenant/SharePoint admin rights.

IMPACT

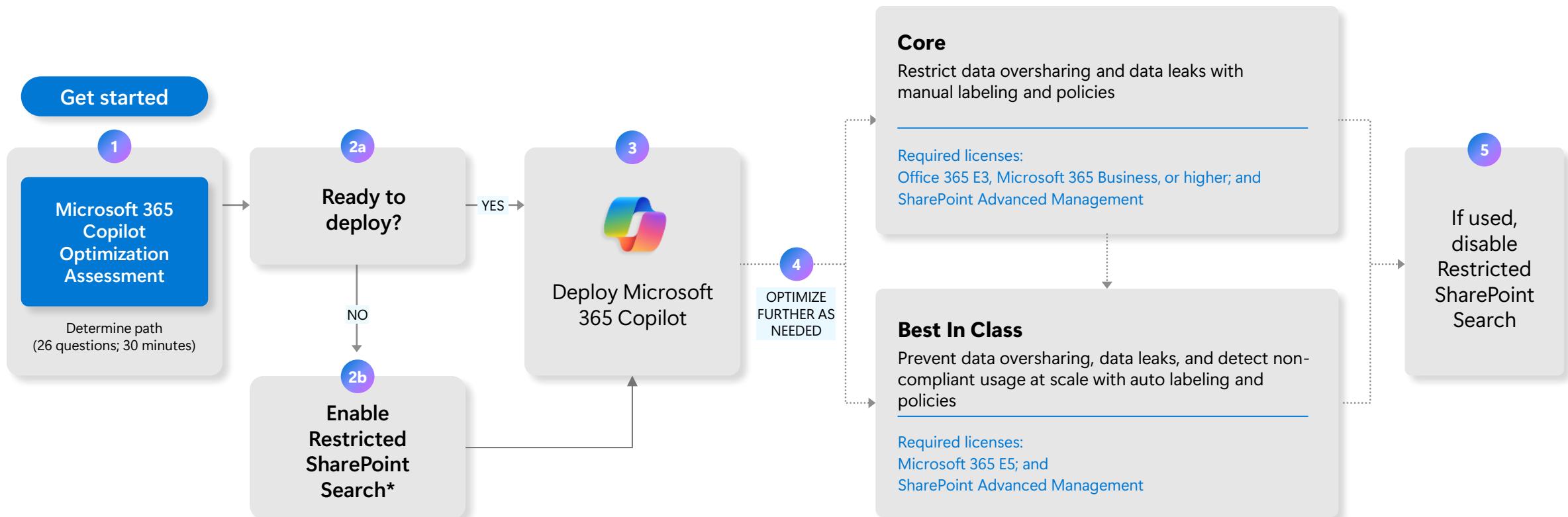
Restricted SharePoint Search disables organization-wide search, while allowing you to select sites that you trust. This means users in your organization can use Copilot to reason over:

- An allowed list of curated SharePoint sites set up by admins (up to 100 SharePoint sites), honoring existing permissions on a site.
- Users' OneDrive, chats they are part of, emails they send and receive, calendars they have access to, etc.
- Files that are shared with and accessed by users.
- Content from users' frequently visited sites.

Access this [blog](#) for more info

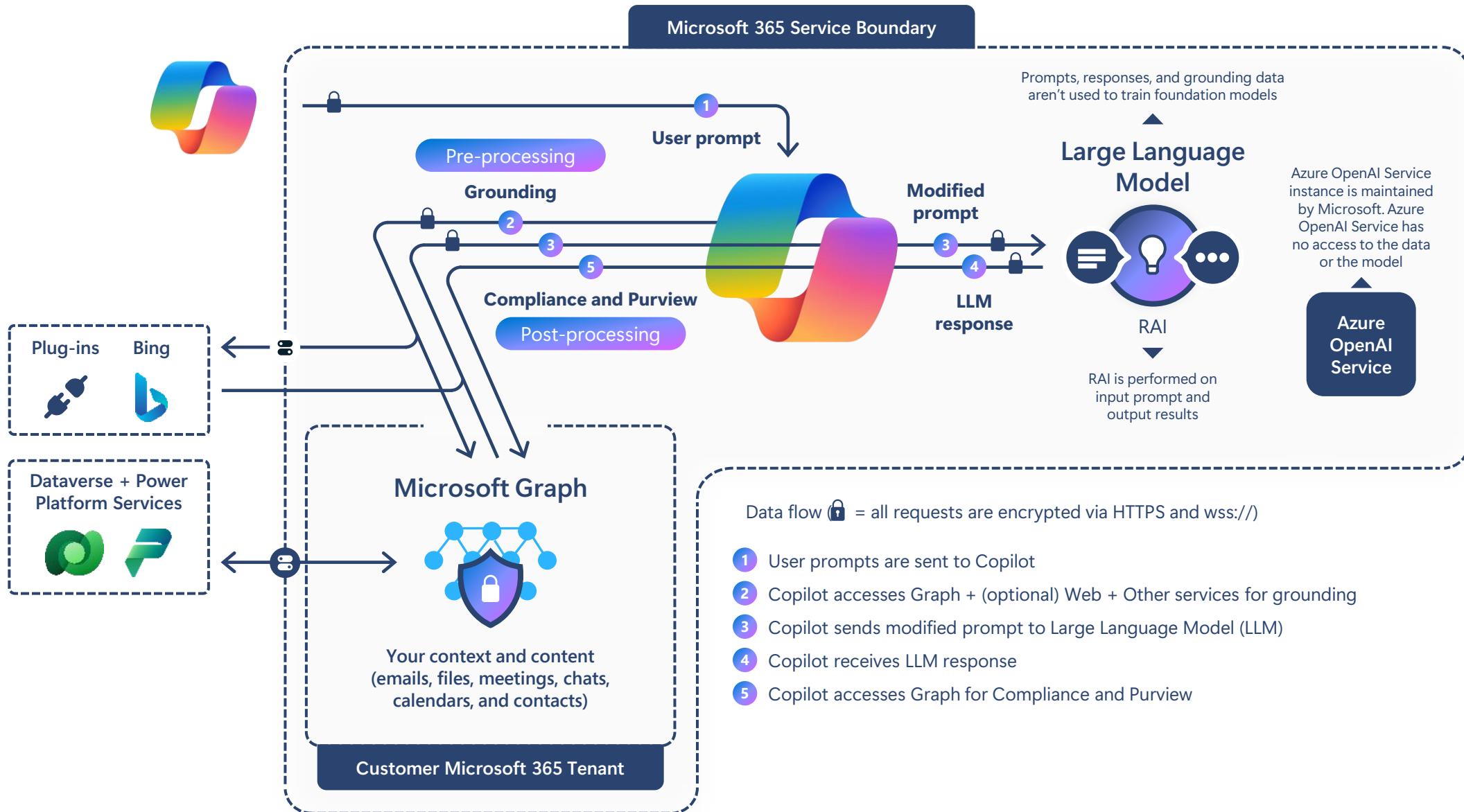
Apply appropriate Data Security controls

Get started quickly and continue to optimize along the way



* Restricted SharePoint Search will limit Microsoft 365 Copilot experiences and organization-wide search. It is a temporary option which gives you time to address oversharing concerns while getting started on your Copilot journey.

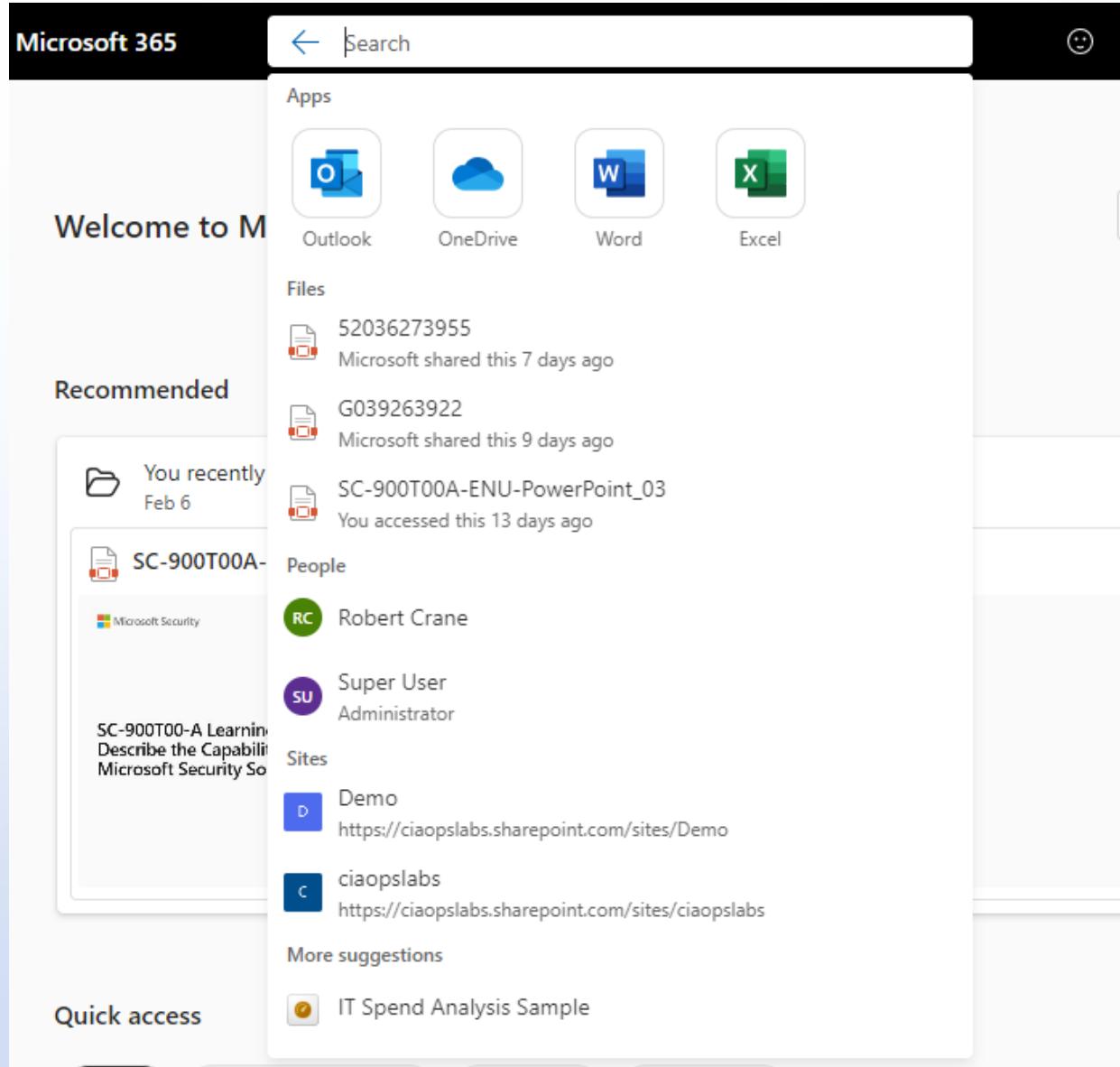
Microsoft 365 Copilot architecture





Getting customers AI ready

What is the number one end user benefit of Microsoft 365?



[+ Add new](#)[Copilot](#) [Delete](#) [Favorite](#) [Download](#) [Move to](#) [...](#)[Sort](#)

Robert Crane

[Home](#)[My files](#)[Shared](#)[Favorites](#)[Recycle bin](#)

Browse files by

[People](#)[Meetings](#)[Media New](#)

Quick access

[Patrons](#)[Presentations](#)[Demo](#)[Patrons - Policies](#)[Team](#)[Work @ Contoso](#)[Summarize](#)[Compare files](#)[Ask a question](#)

		Modified	Modified By	File size
	91254.webm	7 July	Robert Crane	25.0 MB
	03951.webm	6 July	Robert Crane	8.68 MB
✓	Document15.docx	26 June	Robert Crane	13.9 KB
✓	Document14.docx	18 June	Robert Crane	14.6 KB
✓	Document13.docx	14 June	Robert Crane	40.5 KB
✓	Document12.docx	12 June	Robert Crane	13.8 KB
✓	Document11.docx	10 June	Robert Crane	14.7 KB
	Document10.docx	6 June	Robert Crane	14.2 KB
	Document9.docx	29 May	Robert Crane	12.7 KB
	Document.docx	23 May	Robert Crane	13.9 KB
	Secure more with Secure Score in M365 - ...	9 April	Robert Crane	63.0 KB
	Links to Useful Resources.docx	9 April	Robert Crane	11.4 KB



Cloud_App_Security_...

...



pen-holder.snap3dp



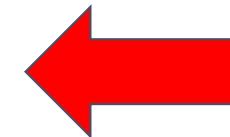
Document6.docx



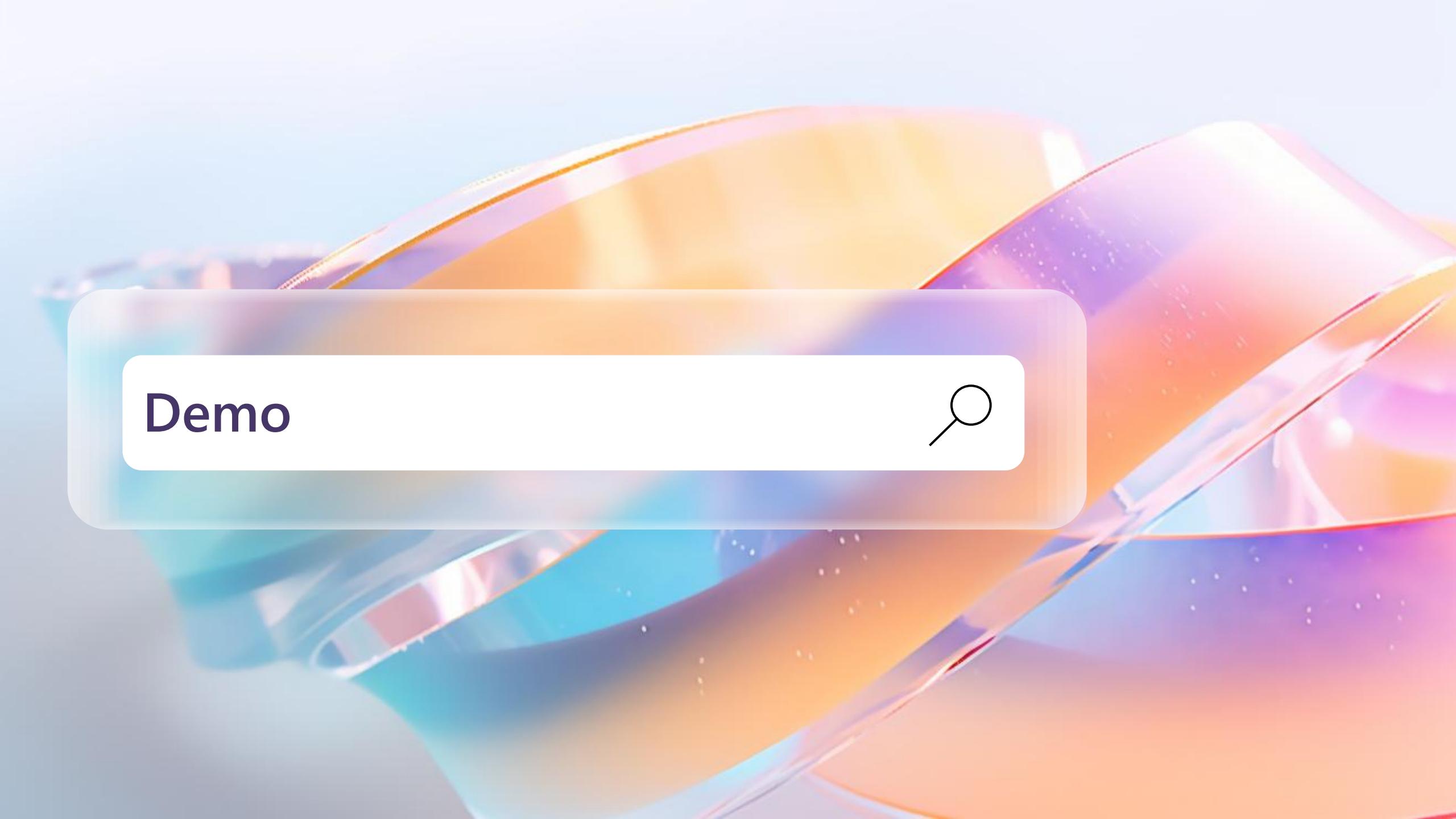
Summarize



Create an FAQ



Ask a question



Demo



Where do I start?



Key processes



Customer service

- Self-help
- Support assignment
- Issue diagnosis
- Problem resolution
- Continuous improvement



Sales

- Customer self-service
- Lead generation
- Customer engagement
- Negotiations and closing
- Post-sale follow-up and upsell
- Sales analysis and forecasting



Marketing

- Customer insights and strategy
- Demand generation
- Content creation
- Campaign execution
- Predictive analysis
- Personalization
- Sales enablement and recommendation



HR

- Employee engagement
- Recruiting
- HR admin and payroll
- Compensation and benefits
- Learning and development
- Talent management
- HR strategy and planning

KPIs by function



Customer service

First call resolution (FCR) rate
Calls answered by agents
Issue resolution time
Customer retention
Case volume
Time to first response
Average call time
Customer experience (CSAT)



Sales

Opportunities pursued
Deal size
Win rate/close rate
Customer retention
Average discount size
Upsell/cross-sell rate
Cost per lead
Sales cycles length



Marketing

Leads generated
Agency spend
Customer retention
Employee retention
Cost per lead
Brand value
Lead conversion rate
Revenue per lead generated



HR

Employee onboarding time
Calls answered by agents
Issue resolution time
Employee retention
Hiring costs per employee
Admin costs per employee
First call resolution rate
Workforce demographics

Sharing Best Practices

At Microsoft, some of the first groups to get Copilot were Sales and Support.

Microsoft sellers:

90 min of time savings per week

83% say they are more productive

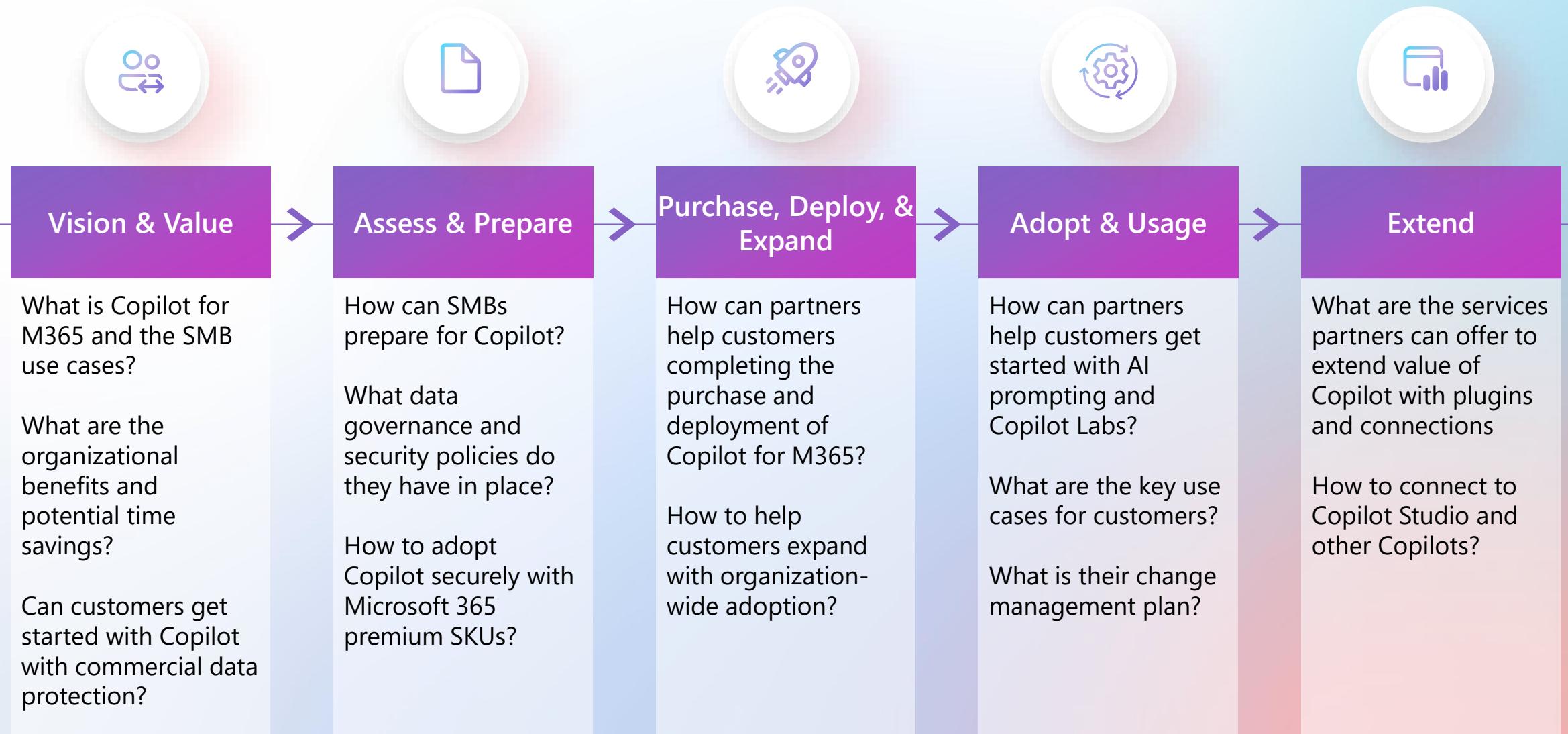
67% spend more time w/ customers

Microsoft support agents:

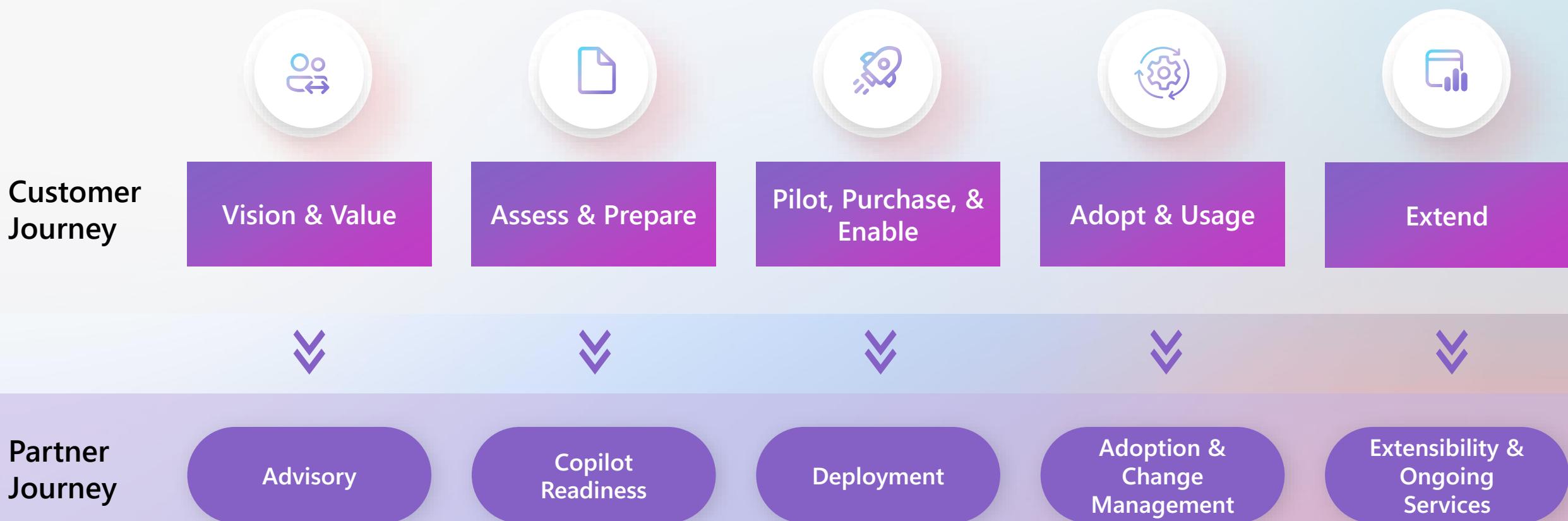
12% reduction in case handling time

10% boost in case resolution

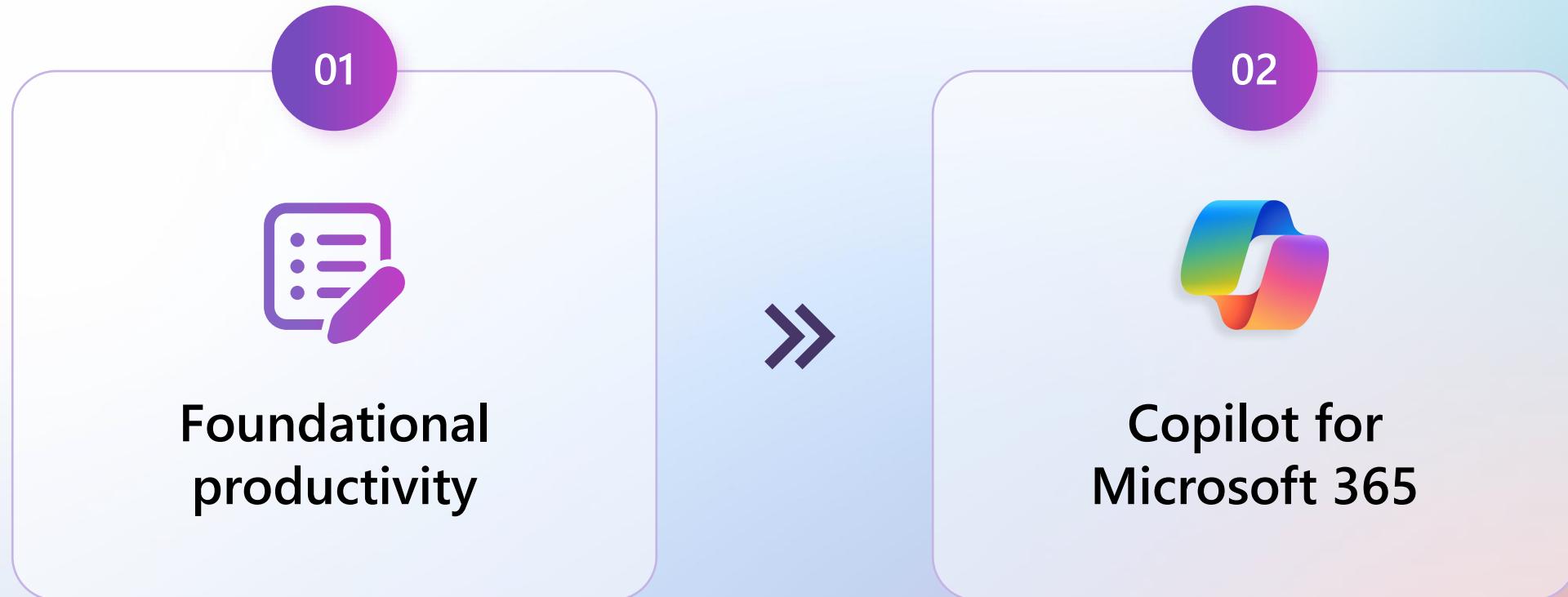
The customer journey with Copilot for Microsoft 365



The customer & partner services journey with Copilot for Microsoft 365



The AI-powered business



The AI-powered business



Foundational productivity

Get AI-ready steps



Empower employees with secure, AI-powered tools

Introduce employees to secure generative AI with Microsoft Copilot with commercial data protection to prepare them for the future workplace.



Standardize onto Microsoft 365

Enrich your Copilot for Microsoft 365 experience by getting your data into the Microsoft 365 Cloud.



Organize sensitive business data

Protect internal data from accidental leakage. Ensure users have the right access to the right internal content.

The AI-powered business



Foundational productivity

Get AI-ready steps



Empower employees with secure, AI-powered tools

Introduce employees to secure generative AI with Microsoft Copilot with commercial data protection to prepare them for the future workplace.



Standardize onto Microsoft 365

Enrich your Copilot for Microsoft 365 experience by getting your data into the Microsoft 365 Cloud.



Organize sensitive business data

Protect internal data from accidental leakage. Ensure users have the right access to the right internal content.

Pre-sales services: Get customers AI Ready

01

Get customers AI ready

Lead with hero SKUs Business Premium and ME3/5

Offer AI evaluation to define customer Copilot journey

Offer AI readiness services

Execute SMB Briefing to drive customer intent

Identify the key customer use cases to prepare for successful adoption



Identify key use cases & initiate adoption plan

Data protection and restriction

Data structuring

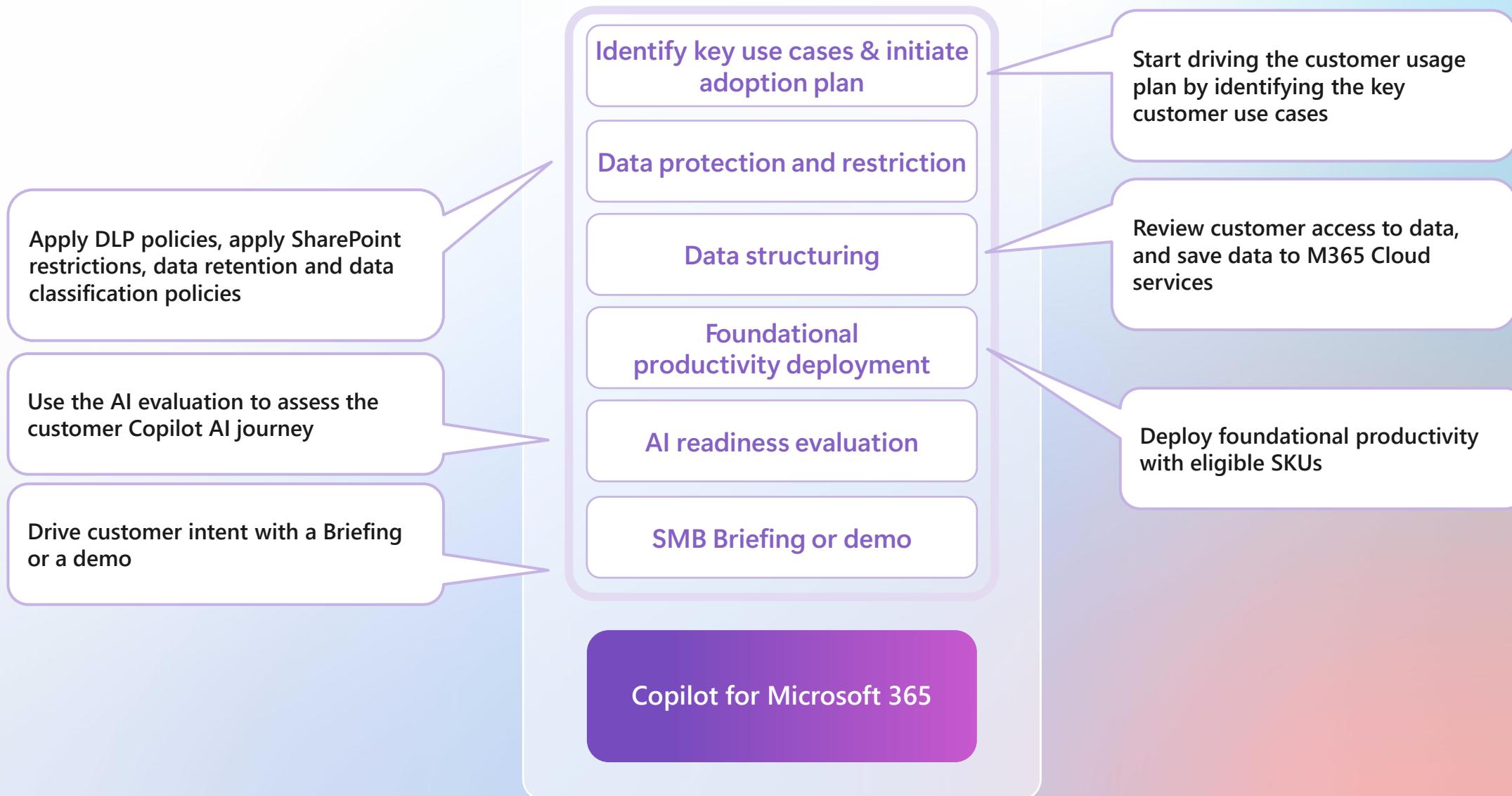
Foundational productivity deployment

AI readiness evaluation

SMB Briefing or demo

Copilot for Microsoft 365

Pre-sales services: Get customers AI Ready





Prepare customers for Copilot for Microsoft 365 with a Copilot Optimization Assessment

Execute a [Copilot Optimization Assessment](#) to help you customers in their AI journey to Copilot for Microsoft 365, including the 3 key steps:

Assess the customer's readiness for Copilot for Microsoft 365

- ✓ Foundational productivity readiness
- ✓ Data readiness
- ✓ Security readiness



<https://aka.ms/CopilotM365Assessment>



Microsoft Copilot

(formerly Bing Chat Enterprise)

Why Microsoft Copilot?

It's powerful and protective

Commercial data protection

Business data is protected



- Included with Entra ID
- Chat data is not saved
- No eyes-on access
- Chat data is not used to train the model

Access to powerful AI models



- Built on the latest AI models (GPT-4 and DALL-E 3)
- No additional cost for Entra ID users¹

Transparent and current



- Citations provided for each response
- Responses sourced with up-to-date information

1. On December 1, Copilot with commercial data protection will be generally available with Microsoft 365 E3, E5, A3, A5 (Faculty only), Business Standard, Business Premium, and eligibility begins for Microsoft 365 F3 for frontline workers. Our intention is to include additional Entra users over time.

Workday efficiencies with Copilot

Summarize a long PDF



Turn a 20-page, jargon-filled PDF into 5 bullets using Copilot in Edge

Draft emails and social content



Use it as your professional writer on call to draft emails, captions, and more

Generate images



Leave behind stock images and text-only reports in favor of custom-generated images for emails, on social, and more

Learn new skills



Ask questions tailored to your needs and interests to get consolidated key points from the internet for you

Get answers for specific, complex questions



Get answers to questions that require multiple data points or a degree of analysis

Extending availability to eligible customers

Users signed into Copilot with their eligible work or school accounts can access Copilot with commercial data protection at no additional cost

Current eligible SKUs*

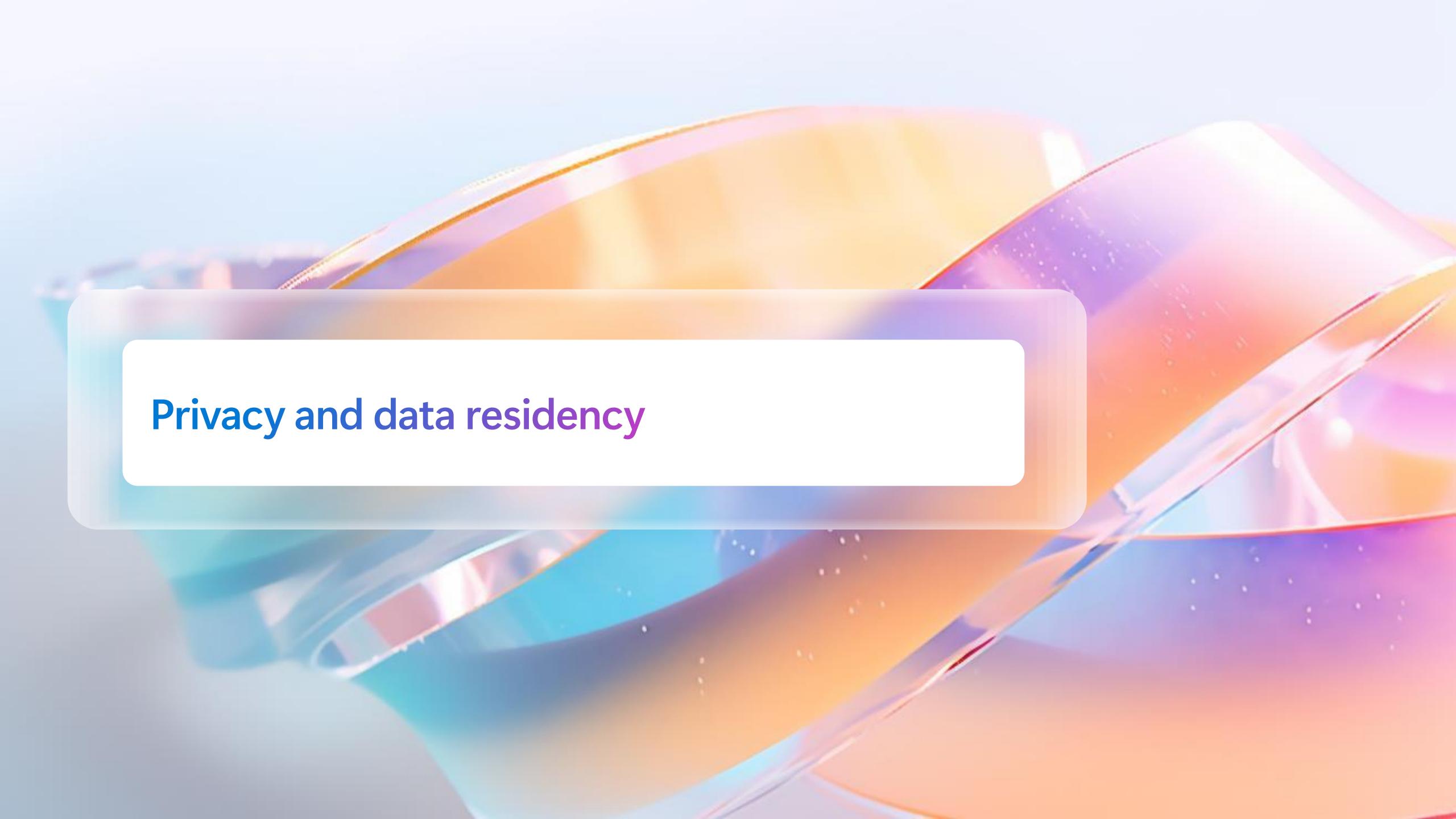
- Microsoft 365 E3, E5, F3
- Microsoft 365 A3, A5 (faculty only)
- Business Standard
- Business Premium

Future eligibility with Entra IDs*

Copilot with commercial data protection will be available to all Entra ID users in the future

Timing to be announced

*Government and student users not included at this time



Privacy and data residency

Microsoft's approach to privacy



You control
your data



You know where
your data is
located



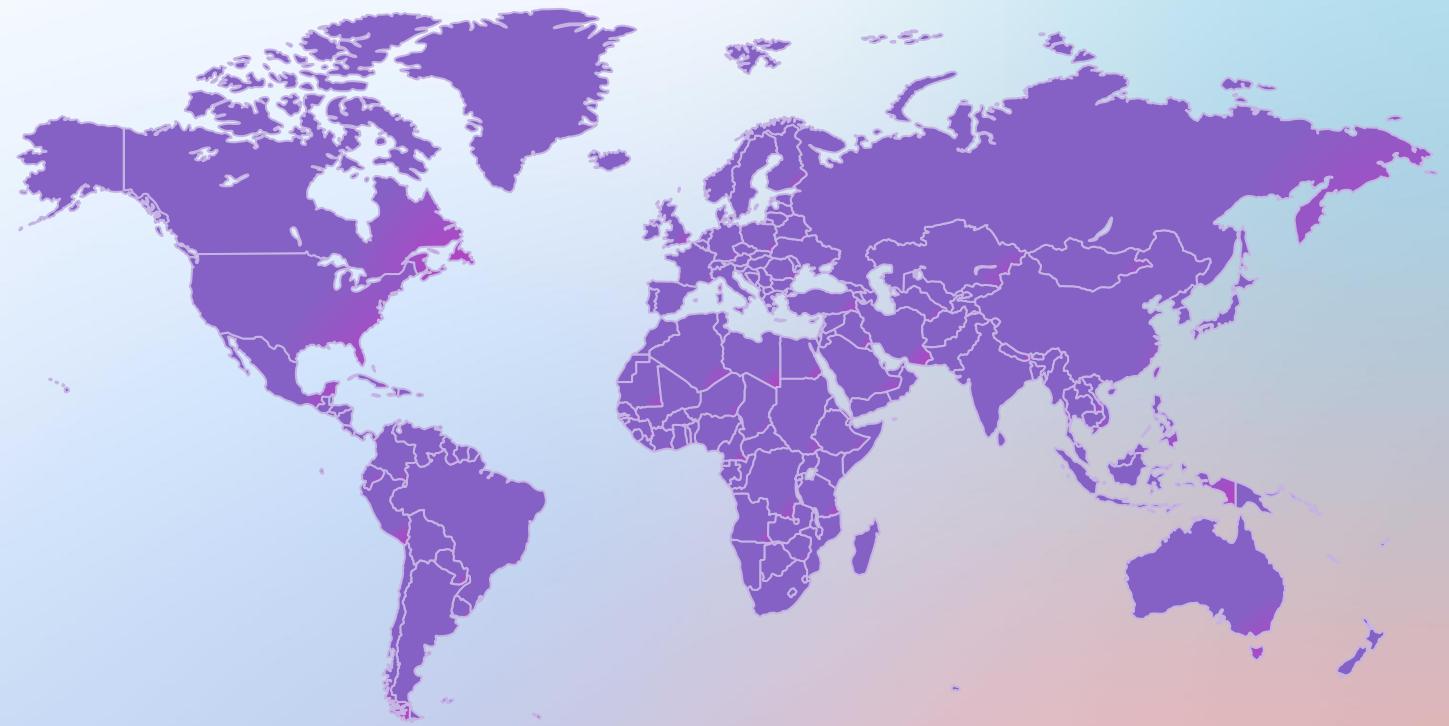
We secure your
data at rest and
in transit



We defend
your data

Where does Microsoft store customer data?

Customers specify a country or region while signing up for a new Microsoft 365 tenant. That selection determines the tenant's default geography. Microsoft makes decisions on where to store customer data by combining that default geography with the available geographies for each service.



Data residency applies to customer data at rest

Data residency commitments provide customers with additional confidence about the location or locations where data is stored at rest.



Microsoft 365 customer data in transit

Data is in transit whenever a user's device is communicating with a Microsoft server, or when a Microsoft server is communicating with another server.



Microsoft encrypts customer data at rest and in transit

Encryption both at rest and in transit helps provide protections against unauthorized access, disclosure, sharing or usage of data.



Microsoft offers several data residency options

Product Terms Data Residency

Advanced Data Residency (ADR)

Add-on

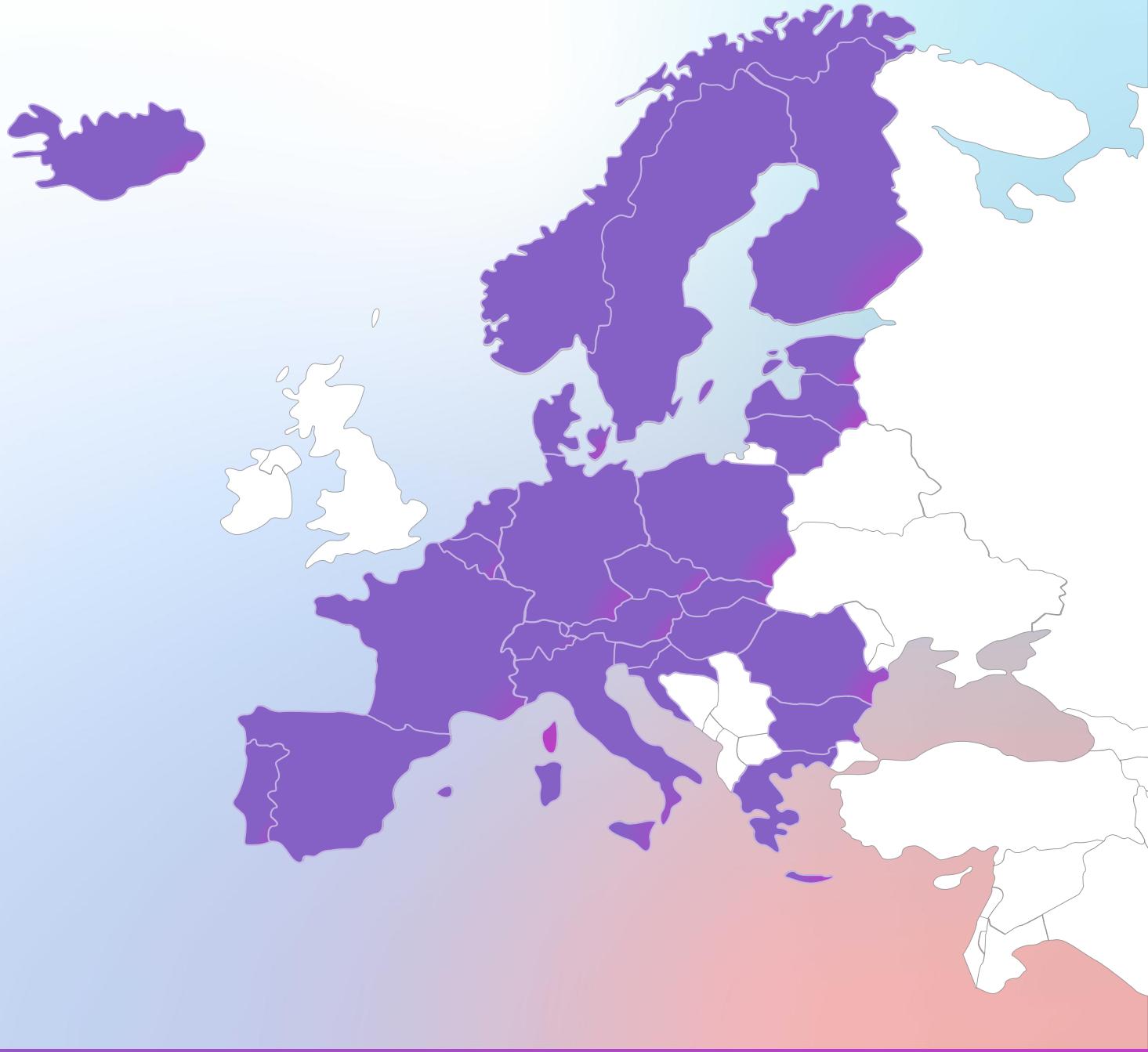
Multi-Geo Capabilities

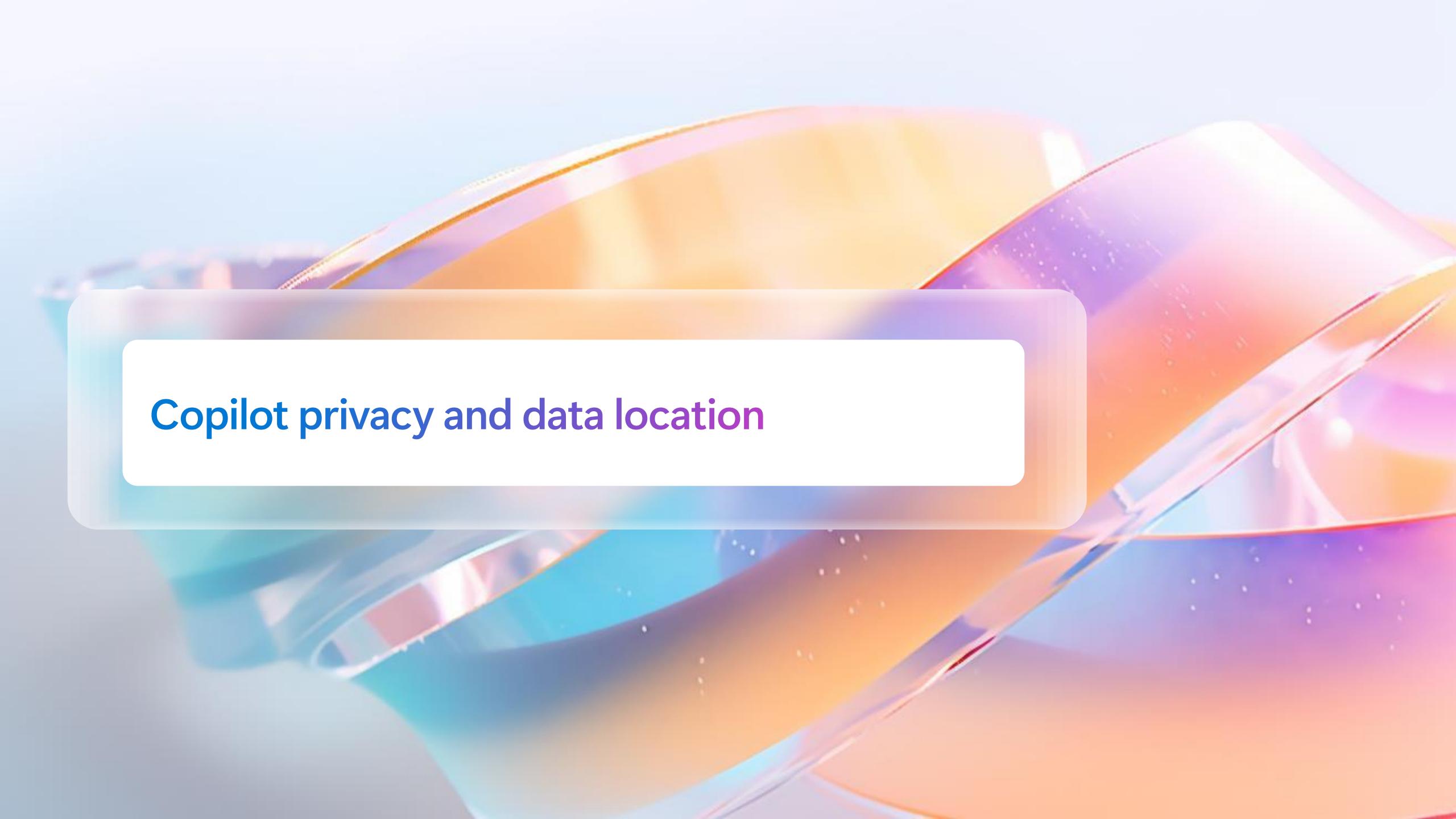
Add-on

European Union Data Boundary (EUDB)

The EU Data Boundary provides more expansive commitments

EUDB terms provide contractual commitments for storing and processing EU + EFTA customer data within the European Union.

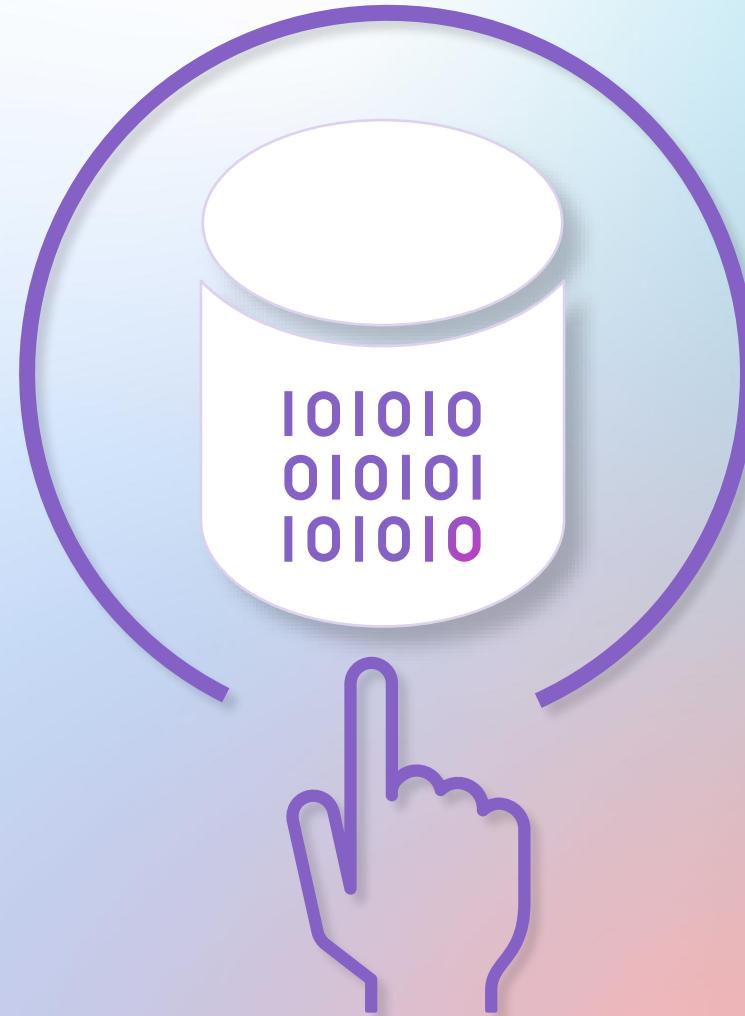




Copilot privacy and data location

You control your data

Microsoft does not use customer data to train foundation LLMs that Copilot uses.



Copilot for Microsoft 365 commitments

Microsoft Product Terms

- Universal License Terms – Microsoft Generative AI services
- Microsoft Copilot copyright commitment
- EU Data Boundary Services
- Core Online Services*

Microsoft Products and Services Data Protection Addendum

Advanced Data Residency (ADR)*

Add-on

Multi-Geo Capabilities*

Add-on

*updates for 2024

Customer scenarios

Customer scenarios

B Contoso is a company based in Brussels, with a sign-up location in Belgium

M Adventure Works is a company based in New York, US, with a sign-up location in the US

Y Fabrikam is a Japanese company based in Tokyo, with a signup location in Japan

Storage of Copilot data

B Contoso Copilot data is stored in the EU

M Adventure Works Copilot data is stored in North America but could be stored anywhere

Y Fabrikam Copilot data is stored in Japan but could be stored anywhere

Processing of Copilot data

B Contoso Copilot data is processed in the EU

M Adventure Work Copilot data is mostly processed in North America but could be processed anywhere

Y All other geographies, including Japan for Fabrikam, Copilot may call into any available region

How do we ensure our customers' data used by Copilot is safe?

- Administrator controls & privacy settings
- SharePoint Online permissions
- OneDrive permissions
- Microsoft 365 Group membership
- Microsoft 365 Group privacy settings (Public/Private)
- Encryption

How do we manage authentication and authorization to ensure data is safe?

Implement Strong Authentication

Manage Vulnerabilities

Microsoft Purview Audit

How does Copilot for Microsoft 365 use proprietary organizational data?

Copilot generates responses anchored in organizational data, such as documents, emails, calendar, chats, meetings, and contacts.

Copilot only surfaces organizational data to which individual users have at least view permissions.

Prompts, responses, and data accessed via Copilot are not used to training foundational LLMs.

How are user interactions with Copilot stored?

Both the user's prompt and Copilot's response are stored, including citations used to ground the response.

All data is processed and stored in alignment with contractual commitments for other content in Microsoft 365.

Features like content search and retention policies apply to Copilot interactions.

Users can delete their Copilot interaction history, including prompts and responses; however, these are soft deleted if a retention policy or legal hold is applied.

Individual Copilot interactions (prompts and responses) are stored in the Non-IPM subtree of the individual users' Exchange Online mailbox, similar to how Teams chat interactions are stored.

How does Copilot handle data residency?

Copilot for Microsoft 365 calls to the LLM are routed to the closest data center.

Calls to the LLM can call into other regions during high utilization periods.

Copilot for Microsoft 365 honors data residency commitments, including Advanced Data Residency (ADR) and Multi-Geo Capabilities.

For European Users (EU), EU traffic stays within the EU Data Boundary.

Shared responsibilities of security for AI usage for Copilot for Microsoft 365



Why Microsoft is uniquely positioned to empower secure AI usage



Integrated

The only security solutions that natively integrate with Microsoft Copilot



Comprehensive

End-to-end security across threat protection, identity & access management, and data security



Intelligent

Industry-leading AI vendor with AI-powered security capabilities

Microsoft Purview with Microsoft 365 Business Premium

Comprehensive solutions to secure and govern your data

Data Security

Secure data across its lifecycle,
wherever it lives

- Data loss prevention
- Information protection

Data governance

Govern data seamlessly to empower your
organization

- Data map
- Data catalog
- Data estate insights

Risk & compliance posture

Manage critical risks and regulatory
requirements

- Compliance manager
- eDiscovery and audit

Office 365 apps

Unstructured & structured data

Across Azure and M365

Shared platform capabilities

Data map, data classification, data labels, audit, data connectors



Action



Security and Compliance controls for Copilot for Microsoft 365

Essential security controls



Copilot + M365 Business Standard

- Multi-factor Authentication
- Audit Logging
- Basic content and keyword search

Comprehensive security controls



Copilot + Microsoft 365 Business Premium

Everything in M365 Business Standard, plus:

- Conditional Access
- Sensitivity labels
- Data loss prevention policies
- Unified endpoint management
- eDiscovery, litigation hold and retention policies

Note: Not all features/products shown.



Security and Compliance controls for Copilot for Microsoft 365

Essential security controls



Copilot + M365 Business Standard

Multi-factor Authentication and security defaults when accessing M365 to use Copilot

Basic security controls for mobile devices accessing M365 resources

Basic content search for Copilot prompts and interactions

Audit logs and retention or deletion policies for Copilot interactions

Prohibit copilot from including sensitive data in responses for users that have no extract permissions

Exclude sensitive files from being processed by Copilot for users that have no view permission

Comprehensive security controls



Copilot + Microsoft 365 Business Premium

Everything in M365 Business Standard, plus:

Conditional Access policies based on identity, device, location, & network to access M365 resources when using copilot

Manage the access and use of M365 apps across devices that use Copilot

Manually label and protect Microsoft 365 content (files and emails only) used by Copilot and inherit and cite sensitivity labels in Copilot outputs

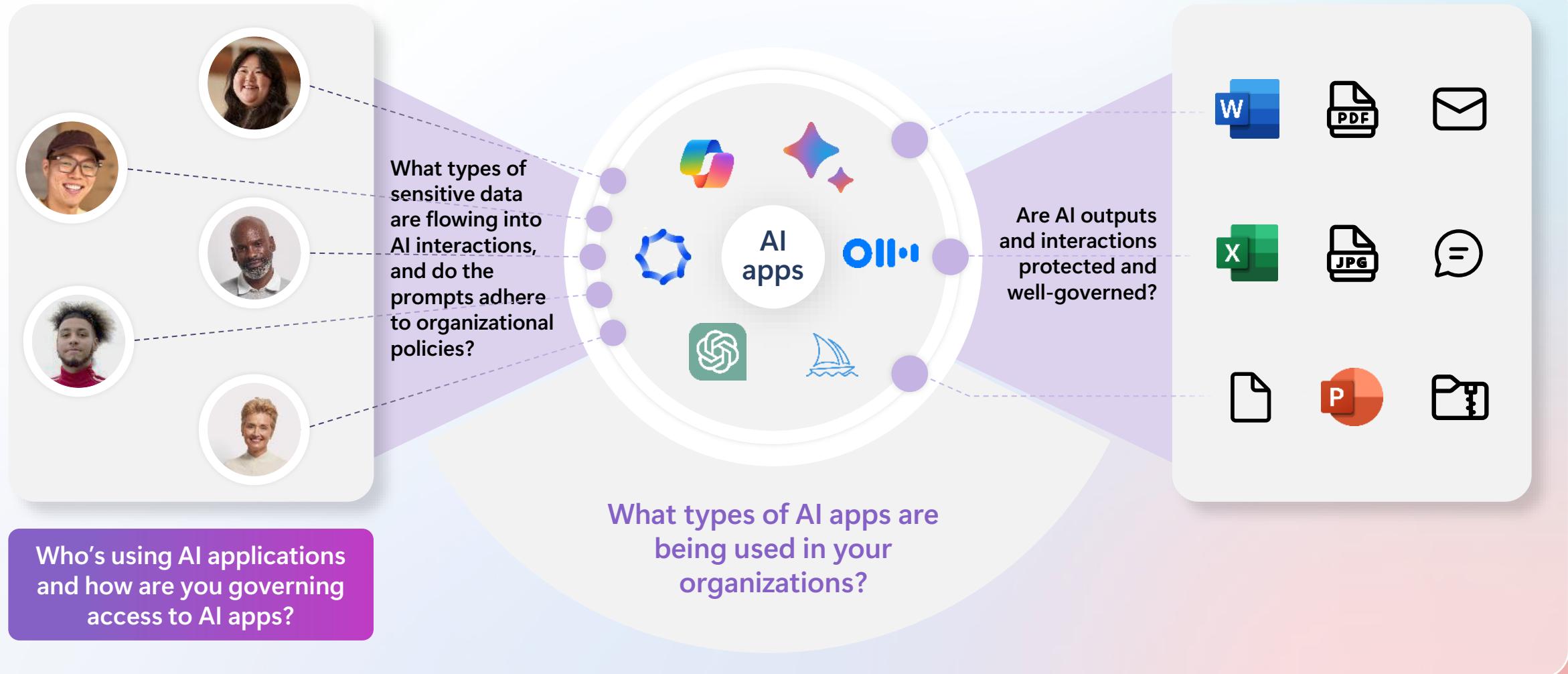
Protect sensitive M365 data generated by Copilot from exfiltration (files & emails only)

eDiscovery, case management and legal hold capabilities for Copilot prompts and interactions

Why is security and data governance important when Deploying Copilot for Microsoft 365?



Information protection & data governance protect against risks





Gather specific information protection and data governance requirements

Decide

Decide who is authorized to conduct investigations (partner, customer, both)

Deploy

Deploy an information protection solution

Know

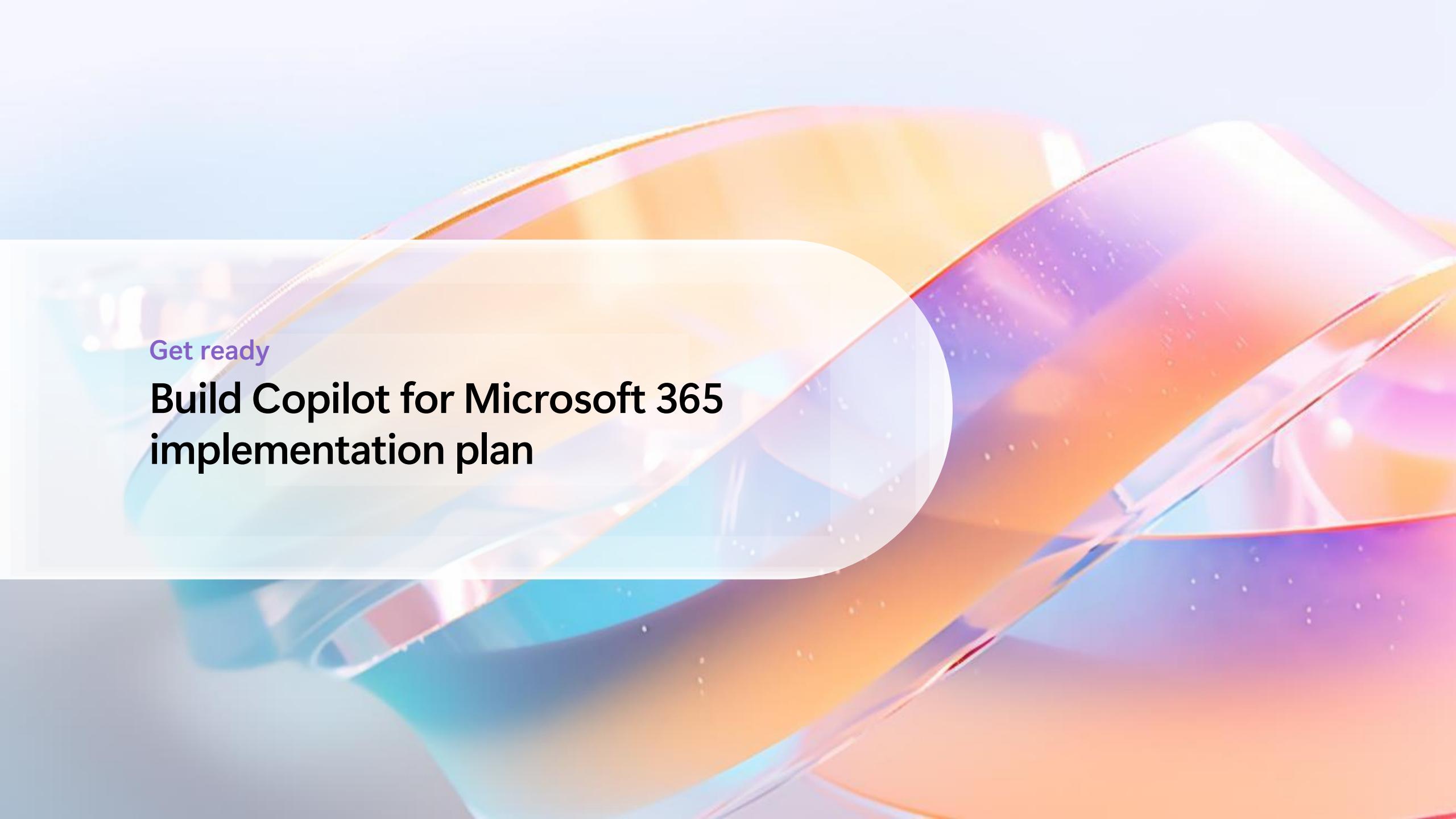
Know your data

Protect

Protect your data

Prevent

Prevent data loss



Get ready

Build Copilot for Microsoft 365 implementation plan

Build an implementation plan

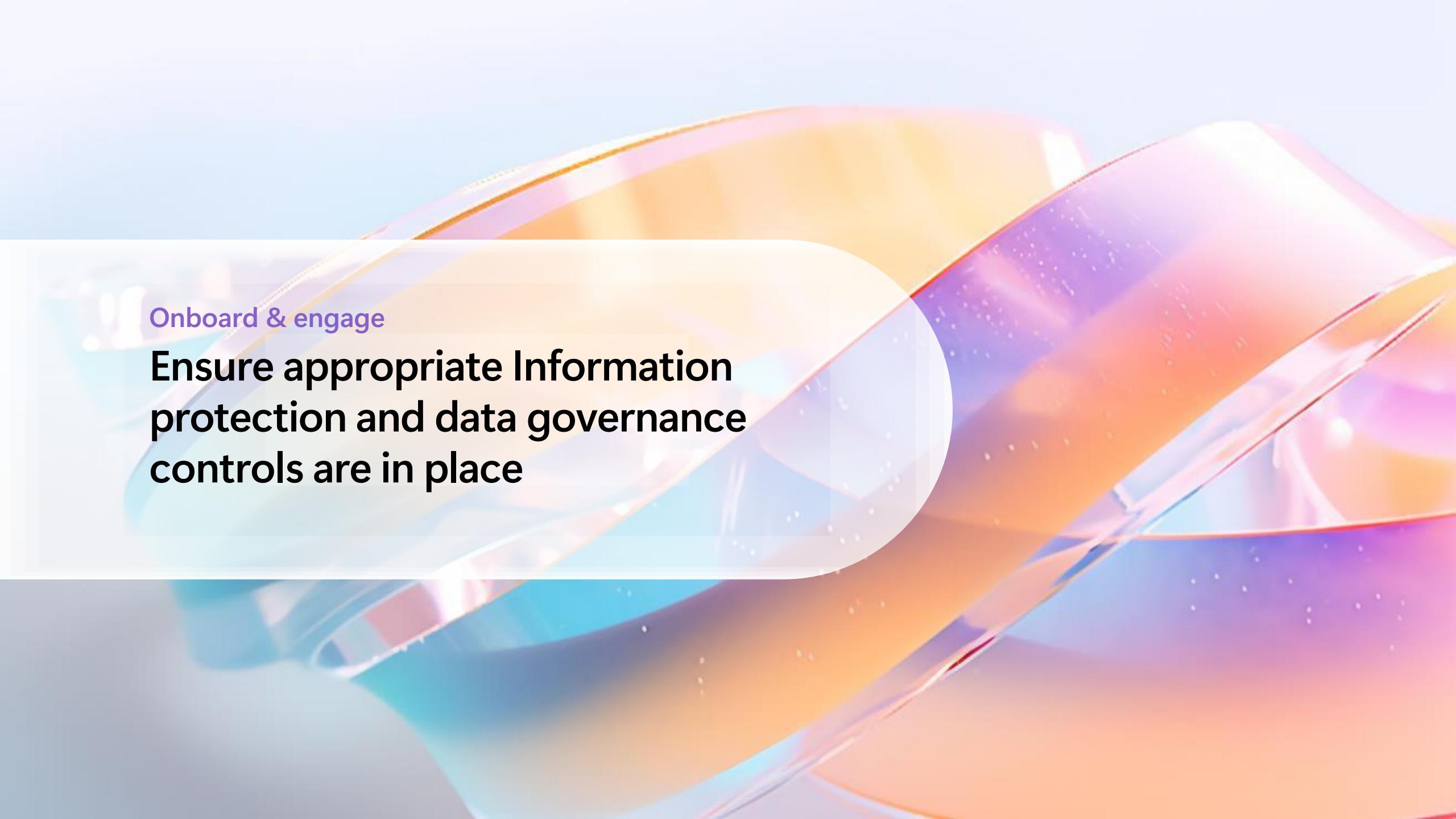
Use the results of the [Optimization Assessment](#) and [scenario discovery](#) to develop a plan for implementation of Copilot for Microsoft 365.

Questions to help develop the plan:

- Are all the gaps in the optimization assessment listed in the plan?
- Have you identified the first set of employees that would get Copilot for Microsoft 365?
- How many licenses would you need to purchase?
- Are there any data security questions that you need to address?
- Do all items have owners and due dates?
- Have you identified key adoption steps for the first set of prioritized scenarios?

Sample plan included in training materials

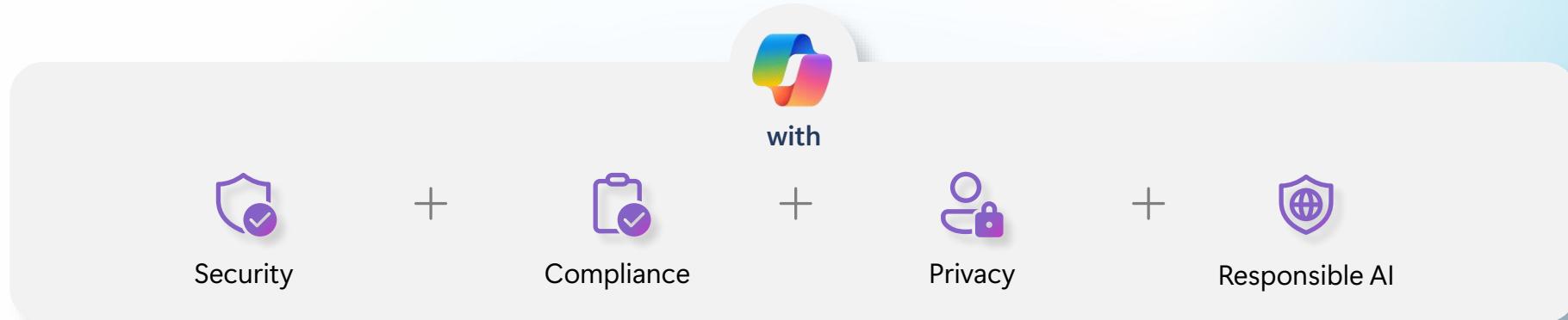
Microsoft 365 - Sample Implementation Plan					
Task	Category	Severity	Status	Comments	
Secure Sponsorship & Setup Team	Kick-Off	Required	Not Started		
Identify Key scenarios and measurement of success	Kick-Off	Required	Not Started		
Perform the Copilot for Microsoft 365 Assessment	Assessment	Required	Not Started		
Finalize requirements for information protection	Assessment	Required	Not Started		
Build Offer	Deal Shaping	Required	Not Started		
Deal Signed	Deal Shaping	Required	Not Started		
Finalize remediation list	Preparation	Required	Not Started	Use the worksheet "Sample Remediation Checklist" in this workbook	A
Build Final Implementation Plan	Preparation	Required	Not Started		P
Acquire Business Premium licenses	Licensing	Required	Not started		A
Acquire Copilot for Microsoft 365 Licenses	Licensing	Required	Not started		A
Configure Microsoft 365 Apps update channels	Pre-requisites	Optional	Not Started	Verify update channel and make adjustments if needed	A
Setup Corporate Templates in PowerPoint	Pre-requisites	Recommended	Not Started	Recommended so Copilot for Microsoft 365 can create branded PowerPoint decks as output	P
Evaluate Outlook versions and potential use of the New Outlook	Pre-requisites	Optional	Not Started	The new Outlook is recommended for integration with Copilot, but Copilot also supports Outlook WebApp	A
Activate Microsoft Loop Components in the tenant	Pre-requisites	Optional	Not Started	Activate Loop in your tenant to bring Copilot into Loop collaborative canvases	A
Configure meeting recording and transcription for post-meeting transcript	Pre-requisites	Optional	Not Started	Enable transcription or meeting recording to allow Copilot in Teams to reference meeting content after a meeting has ended	A
Configure OneDrive and SharePoint default sharing policies	Security, governance, and data access requirements	Required	Not started	Verify and configure OneDrive and SharePoint default sharing policies	A
Configure SharePoint Restricted Search	Security, governance, and data access requirements	Optional	Not Started	Recommend as temporary workaround when assessment revealed that the business has high risk sensitivity and a longer pathway to label and categorize data. Copilot for Microsoft 365 can already be used while in parallel the risks with regards to data access and oversharing can be mitigated	A
Control access to sites and block downloads	Security, governance, and data access requirements	Optional	Not Started	Set up restricted access control and block file download policies on business critical sites	A
Identify and manage inactive sites	Security, governance, and data access requirements	Optional	Not Started	Identify inactive sites, then restrict access or delete	A
Manage sharing controls in SharePoint	Security, governance, and data access requirements	Optional	Not Started	Review site-level sharing controls and remove "Everyone except External users" from people picker	A
Manage oversharing	Security, governance, and data access requirements	Optional	Not Started	Identify potentially overshared content	A
Decide who is authorized to conduct investigations (partner, customer, no)	Security, governance, and data access requirements	Strongly recommended	Not started		A
Enable Purview Audit (Standard) in the tenant	Information protection and data governance controls	Strongly recommended	Not started	Get started with auditing solutions	A
Set up notifications in tenant for privileged role changes (to get notified for information protection and data governance controls)	Information protection and data governance controls	Strongly recommended	Not started		A
Delegate the eDiscovery Manager role	Information protection and data governance controls	Strongly recommended	Not started		P
Enable sensitivity labels on containers & groups	Information protection and data governance controls	Strongly recommended	Not started	Apply a sensitivity label to content automatically	A
Configure sensitivity labels	Information protection and data governance controls	Strongly recommended	Not started	Learn about retention policies and labels	A
Configure retention policies	Information protection and data governance controls	Strongly recommended	Not started	Create and Deploy Data loss prevention policies	A
Configure a DLP policy	Information protection and data governance controls	Strongly recommended	Not started		A
Assign Copilot for Microsoft 365 Licenses	Copilot for Microsoft 365 Service Enablement	Required	Not Started		A
Prepare end-user training materials	User Adoption	Required	Not Started		A
Distribute and deliver end-user training	User Adoption	Required	Not Started		A
Monitor Copilot for Microsoft 365 usage	User Adoption	Required	Not Started	Copilot for Microsoft 365 usage reports in M365 Admin Center	A



Onboard & engage

**Ensure appropriate Information
protection and data governance
controls are in place**

Secure and govern Copilot with Microsoft Security



Discover AI risks

Identify sensitive data in Copilot interactions with [ready-to-use classifiers and labeling](#)

Understand user activities and detect risky access to Copilot with [audit logging](#)

Identify potentially overshared content by reviewing [SharePoint site permissions](#)

Protect sensitive data

Protect access to sensitive data in Copilot interactions with [persistent labeling and DLP policies](#)

Restrict or block risky access with [conditional access and endpoint management](#)

Prevent idle or excessive access with [SharePoint site wide access controls](#)

Govern Copilot usage

Retain and log Copilot interactions, automatically [remove inactive content](#)

Use built-in classifiers to [detect non-compliant use of Copilot](#)

Preserve, review, and analyze prompts and responses to [investigate security and compliance incidents](#)

Let's see how it all works together

Alex worked on a highly confidential project, Project Obsidian

Alex leveraged both Microsoft Copilot and unmanaged consumer AI apps for the project

Her identity was compromised due to the malicious code in the high-risk consumer AI apps

Without knowing the impact of her activities, she continued sharing sensitive data in consumer AI apps.

Project Obsidian's information was leaked before the debut

1



2



3



4



5



Let's see how it all works together

How Microsoft can help

Alex worked on a highly confidential project, Project Obsidian

Alex leveraged both Microsoft Copilot and unmanaged consumer AI apps for the project

Her identity was compromised due to the malicious code in the high-risk consumer AI apps

Without knowing the impact of her activities, she continued sharing sensitive data in consumer AI apps.

Project Obsidian's information was leaked before the debut

1



2



3



4



5



The project owner labeled all documents with the "highly confidential" label to restrict rights to data with **Microsoft Purview**

Discover use of high-risk apps with **Microsoft Defender for Cloud Apps** and **Microsoft Defender for Business**

Detect the compromised identity and take actions (e.g., reset password, restrict access) to protect Microsoft Copilot or other critical resources with **Microsoft Entra Conditional Access**

Early intervention enabled by the **audit trail** in Microsoft Purview. Copilot prompts and response stored and responsive to **content search**.

Gain complete visibility and logs of activities to conduct investigations with **Microsoft Purview**

Govern **access** and secure **data** in Microsoft Copilot for Microsoft 365



Discover overprivileged and risky users and mitigate access risks automatically with **conditional access controls**



Identify and protect sensitive data consistently wherever Copilot interactions occur with **sensitivity labels**

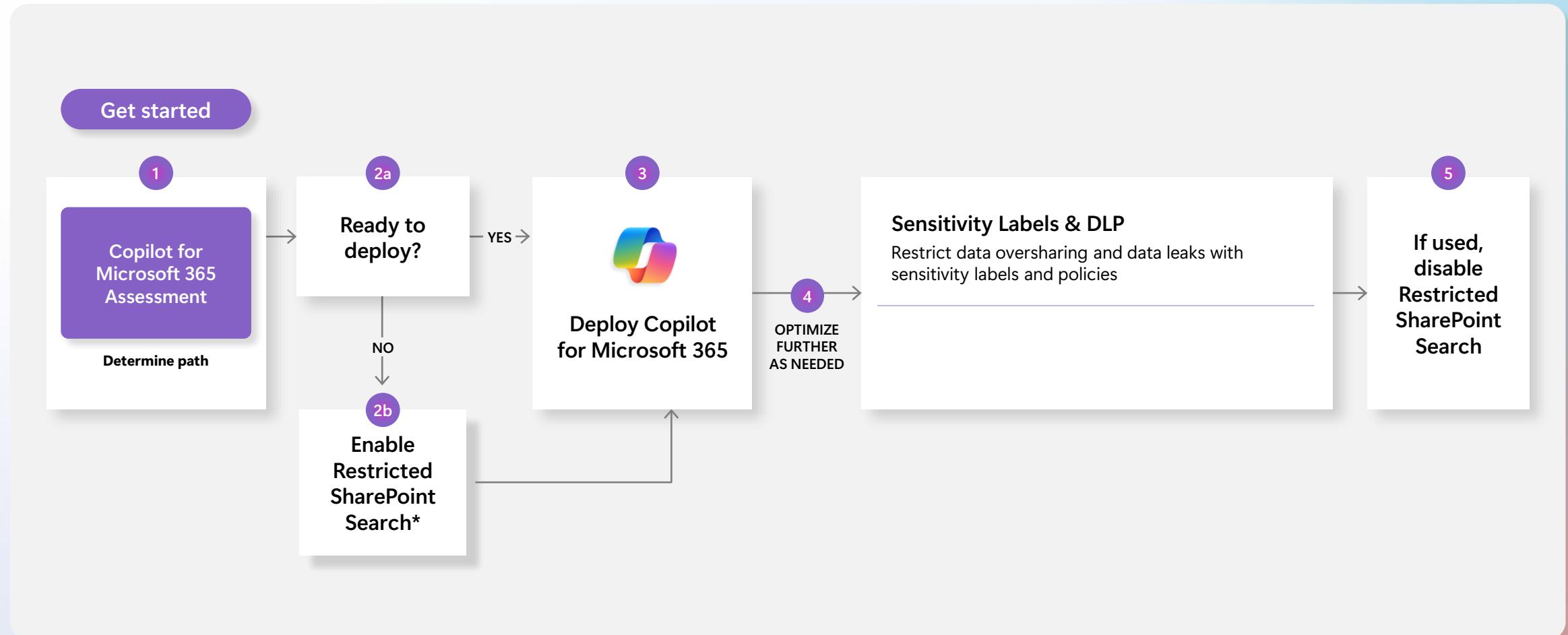


Retain, log, and manage compliance of Copilot interactions to align with organizational policies and regulations



Apply appropriate Data Security controls

Get started quickly and continue to optimize along the way



Demo

Enable Purview Audit (Standard)

Oversharing control: Permission State Report with Actions

Gain Control Over Site Permissions and Overshared Content

Identify Overshared content:

- Customizable and comprehensive permission reports across all sites
- Detect root causes of oversharing (broken inheritance, sharing links, EEEUs, site privacy and more)
- Focus on critical permissions by user count and extended groups
- Integrates with sensitivity labels for enhanced security
- Downloadable, with insights from AI analytics

Scalable Actions:

- Site Access Review with site owner file review dashboard
- Restricted Access Control – limit access to high-risk areas
- Restricted Content Discovery – lock down content from Copilot

Generally available

The screenshot shows a SharePoint site review interface. At the top, there's a summary card titled "Snapshot till March" with a blue "Download detailed report" button. Below it, a navigation bar includes "Initiate site access review", "View all reviews", and "Restrict site access". The main content area is titled "Permissions to many users" under "Site reviews". It lists various items with their names, scopes, user counts, and permission details. A modal window at the bottom right highlights "Broken inheritance, Sharing links, EEEU domain group" with three action buttons: "Manage access" (with dropdowns for "Select", "Retained all permissions", "Modified existing permissions", and "Removed permissions completely"), "Complete review", "Save as draft", and "Cancel".

Name	Scope	Total number of Permisioned users	Total number of groups	Count of Anyone' links	Count of 'People in your org' links	Has EEEU	Has Everyone	Action	Final status
Contoso Finance	SharePoint Site	6804	4	-	-	-	-	Manage access	Select
Finance_projections_FY23.xlsx	File	7142	5	2	2	-	-	Manage access	Select
Vendor Bills	Folder	7524	2	1	2	-	-	Manage access	Select
ProfitabilityPlan.pptx	File	7945	6	1	3	Yes	-	Manage access	Select
Flow map.jpg	File	8580	3	2	1	Yes	-	Manage access	Select
Confidential Q2 CY24 ReOrg	File	9092	4	3	3	Yes	-	Manage access	Select

Data access governance

Reports My review requests

This page provides reports to help you maintain the security and compliance of your data in SharePoint.

[Learn more about data access governance](#)

Sharing links

Identify potential oversharing by monitoring sites where users created new sharing links in SharePoint.

[View reports](#)

Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where sensitive files are stored and the policies applied to these sites.

[View reports](#)

Shared with 'Everyone except external users'

Make sure files, folders, and lists aren't being overshared by reviewing sites that have the most items shared with "Everyone except external users."

[View reports](#)

Content accessible to 'Permissioned users'

[PREVIEW](#)

Review sites with a high number of users across all permission scopes (inherited and broken).

[View reports](#)

Data access governance > Content accessible to 'Permissioned users'

Content accessible to 'Permissioned users' PREVIEW

Review sites with a high number of users across all permission scopes (inherited and broken).



No reports right now

Create a new report using filters.

[Create report](#)

Data access governance > Content accessible to 'Permissioned users'

X

Content accessible to 'Permissioned users' PREVIEW

Review sites with a high number of users across all permission scopes (inherited and broken).



No reports right now

Create a new report using filters.

[Create report](#)

Create a report

Discover sites where the number of users across all permission scopes (inherited and broken) exceeds a threshold

Report name ***Scope *** SharePoint OneDrive For Business**Template *****Privacy (Team sites only)****Sensitivity****Sensitivity Info Type****Report type *** Snapshot till date

Generated based on latest permissions, as of report generation date

 Recent activity for last 28 days**Count of permissioned users**[Create and run](#)[Cancel](#)

Data access governance > Content accessible to 'Permissioned users'

Content accessible to 'Permissioned users' PREVIEW

Review sites with a high number of users across all permission scopes (inherited and broken).

[Learn more about content accessible to 'Permissioned users'](#)

Add a report Run all Refresh status

<input type="checkbox"/>	Report name	Status	Scope	Permissioned users count	Date range	Sites found	Privacy (Team sites only)	Sensitivity	Template
<input type="checkbox"/>	Snapshot till March	Running (this might take a few hours)	SharePoint	Over 1,000	As of Mar 3, 2023	-	Private	All	Communication sites, Team sites
<input type="checkbox"/>	View for Feb	Updated in the last 24 hours	SharePoint	Over 2,500	As of Feb 3, 2023	198	Private	Highly confidential	-

Snapshot till March

As of March 3, 2024

Review sites with a high number of users across all permission scopes (inherited and broken).

Download a detailed .csv report for up to 1M sites.

[Download detailed report](#)[+ Initiate site access review](#) [View all reviews](#) [Restrict site access](#)

100 items

Search

Filters: Site sensitivity: All ▾ External sharing: All ▾

Name	URL	Site access review	Total permissioned users ↓	Files	Sensitive Files ⓘ	Items with unique permissions	EEEU permissions	People in your org links	Anyone links	Site Privacy	Site sensitivity	External sharing
Contoso HR	../teams/contosohr	-	22334	44869	4821	2	2	312	312	Private	Top secret	On
Contoso Marketing	../teams/contosoma	-	15698	41839	4213	1	2	298	298	Private	Confidential	On
Contoso Finance	../sites/contosofin	-	11237	38286	4200	3	2	167	167	Private	-	On
Contoso Team	../sites/contosoteam	-	10134	35310	3189	6	2	124	124	Private	Confidential	On
Contoso Vac	../sites/contosovac	-	8530	31498	3120	2	2	72	72	Public	General	On
Contoso in house	../teams/contosoin	-	6054	30764	3100	1	2	214	214	Public	Confidential	On
Contoso infra	../teams/contosoin	-	3998	28187	2890	5	2	21	21	Public	General	On
Contoso leaders	../teams/contosole	-	2804	22396	2340	8	2	12	12	Public	-	On
Contoso design	../teams/contosoen	-	1890	20189	2310	2	2	9	9	Public	-	On
Contoso BI	../teams/contosoen	-	1890	20189	2231	2	2	9	9	Public	-	On
Contoso HR	../teams/contosoen	-	1890	20189	2213	2	2	9	9	Public	-	On
Contoso Give	../teams/contosoen	-	1890	20189	1313	2	2	9	9	Public	-	On
Contoso Sesh	../teams/contosoen	-	1890	20189	1110	2	2	9	9	Public	-	On
Contoso Sesh	../teams/contosoen	-	1890	20189	989	2	2	9	9	Public	-	On

Snapshot till March

As of March 3, 2024

Review sites with a high number of users across all permission scopes (inherited and broken).

Download a detailed .csv report for up to 1M sites.

[Download detailed report](#)[Initiate site access review](#) [View all reviews](#) [Restrict site access](#)

Filters: Site sensitivity: All External sharing: All

Name	URL	Site access review	Total permissioned users	Files	Sensitive Files ⓘ	Items with unique permissions	EEEU permissions	People in your org links	Anyone links	Site Privacy	Site sensitivity	External sharing
Contoso HR	.../teams/contosohr	-	22334	44869	4821	2	2	312	312	Private	Top secret	On
Contoso Marketing	.../teams/contosoma	-	15698	41839	4213	1	2	298	298	Private	Confidential	On
Contoso Finance	.../sites/contosofin	-	11237	38286	4200	3	2	167	167	Private	-	On
Contoso Team	.../sites/contosoteam	-	10134	35310	3189	6	2	124	124	Private	Confidential	On
Contoso Vac	.../sites/contosovac	-	8530	31498	3120	2	2	72	72	Public	General	On
Contoso in house	.../teams/contosoin	-	6054	30764	3100	1	2	214	214	Public	Confidential	On
Contoso infra	.../teams/contosoin	-	3998	28187	2890	5	2	21	21	Public	General	On
Contoso leaders	.../teams/contosole	-	2804	22396	2340	8	2	12	12	Public	-	On
Contoso design	.../teams/contosoen	-	1890	20189	2310	2	2	9	9	Public	-	On
Contoso BI	.../teams/contosoen	-	1890	20189	2231	2	2	9	9	Public	-	On
Contoso HR	.../teams/contosoen	-	1890	20189	2213	2	2	9	9	Public	-	On
Contoso Give	.../teams/contosoen	-	1890	20189	1313	2	2	9	9	Public	-	On
Contoso Sesh	.../teams/contosoen	-	1890	20189	1110	2	2	9	9	Public	-	On
Contoso Sesh	.../teams/contosoen	-	1890	20189	989	2	2	9	9	Public	-	On

Snapshot till March

This displays list of sites where the number of users across all permission scopes (inherited and broken) exceeds a threshold
Download detailed .csv report for up to 10,000 sites.

[Download detailed report](#)[Initiate site access review](#) [View all reviews](#) [Restrict site access](#)

Filters: Site sensitivity: All External sharing: All

Filters: Site sensitivity: All External sharing: All

These are labelled files and unlabelled files
where a sensitive info type was detected

Name	URL	Site access review status	Files	No. of sensitive files ⓘ	Total permissioned users ↓	Count of EEEU permissions	Count of 'Anyone' lin
Contoso HR	.../teams/contosohr	—	44869	4814	22334	2	312
Contoso Marketing	.../teams/contosomar	—	41839	4423	15698	1	296
Contoso Finance	.../sites/contosofin	—	38286	4178	11237	3	167
Contoso Giving	.../sites/contosogiv	—	35310	3987	10245	6	145
Contoso team	.../sites/contosoteam	—	31498	3546	8530	2	124
Contoso Vac	.../sites/contosovac	—	30764	3215	6054	1	72
Contoso HRA	.../teams/contosohra	—	28187	2895	3998	5	2416
Contoso Media	.../sites/contosomedia	—	22396	2564	2804	8	38
Contoso in house	.../sites/contosoinh	—	20189	2489	1890	3	32
Contoso infra	.../sites/contosoinfra	—	19374	2341	1487	4	23
Contoso design	.../sites/contosodesign	—	13298	2287	1329	1	21
Contoso leaders	.../teams/contosolead	—	9450	2135	1127	5	21
Contoso data	.../teams/consolidata	—	8800	2039	1038	7	647
Contoso BI	—	—	8126	1983	1024	2	721

Initiate site access review

An email will be sent to all site owners, with a request for them to review the sites for potential oversharing.

[Add a comment for site owners](#)

E.g. Check these sites for number of users or permissions or sharing events etc.

Sites added

Contoso Finance
.../sites/contosofin

Contoso Giving
.../sites/contosogiv

[Send](#)[Cancel](#)



Site reviews > Permissions to many users

The list below details inherited and unique permissions which have the highest number of users and possible contributing factors such as links, groups or Everyone Except External Users (EEEU) claims. Remove permissions where they are no longer required to prevent oversharing.

Name	Scope	Number of Permissioned users	Sensitivity Info Type	Sensitivity Label	Number of groups	Number of 'Anyone' links	Number of 'People in your org' links	Has EEEU	Action	Final status
> Contoso Finance	SharePoint Site	6804	US Passport Number +2	Top secret	4	-	-	-	Manage access	Select
> Finance_projections_FY23.xlsx	File	7142	US SSN Number + 4	Confidential	5	2	2	-	Manage access	Select
> Vendor_bills	Folder	7524	US SSN Number + 1	Highly confidential	7	1	2	-	Manage access	Select
> ProfitabilityPlan.pptx	File	7945	US SSN Number	-	6	1	3	Yes	Manage access	Select
> Flow map.jpg	File	8580	US Passport Number	General	3	2	1	Yes	Manage access	Select
> Confidential Q2 CY24 ReOrg	File	9092	ABA Routing Number	-	4	3	3	Yes	Manage access	Select



Site reviews > Permissions to many users

The list below details inherited and unique permissions which have the highest number of users and possible contributing factors such as links, groups or Everyone Except External Users (EEEU) claims. Remove permissions where they are no longer required to prevent oversharing.

Name	Scope	Number of Permissioned users	Sensitivity Info Type	Sensitivity Label	Number of groups	Number of 'Anyone' links	Number of 'People in your org' links	Has EEEU	Action	Final status
> Contoso Finance	SharePoint Site	6804	US Passport Number +2	Top secret	4	-	-	-	Manage access	Select
> Finance_projections_FY23.xlsx	File	7142	US SSN Number + 4	Confidential	5	2	2	-	Manage access	Select
> Vendor_bills	Folder	7524	US SSN Number + 1	Highly confidential	7	1	2	-	Manage access	Select
> ProfitabilityPlan.pptx	File	7945	US SSN Number	-	6	1	3	Yes	Manage access	Select
> Flow map.jpg	File	8580	US Passport Number	General	3	2	1	Yes	Manage access	Select
> Confidential Q2 CY24 ReOrg	File	9092	ABA Routing Number	-	4	3	3	Yes	Manage access	Select

Broken permission inheritance

Files containing sensitive data

Default sharing option is everyone

Site privacy set to public

Use of "everyone except external users" domain group

Restricted Access Control (RAC)

for SharePoint & OneDrive



RAC (Restricted access control) policy can be set at the site level. Even if individual files/folders have broken inheritance and over-shared, only RAC allowed users can access

Copilot honors RAC policy!

Microsoft 365 group-connected sites,
Non-group SharePoint sites, Teams sites,
Shared channel sites, OneDrive sites

Generally available

The screenshot shows the SharePoint admin center interface under 'Data access governance'. The main area displays a 'Snapshot till March' report with a table of sites and their user counts. A modal window titled 'Restricted site access' is open on the right, containing a description and a checkbox labeled 'Restrict SharePoint site access to only users in specified groups'. Below this is a dropdown menu titled 'Add group' with several security groups listed: Contoso Financial Council, Contoso Tech, Contoso Marketing, and Contoso HR. The 'Contoso Marketing' group is currently selected.

Name	URL	Site access review status	Teams	Total permissioned users	Count of
Contoso HR	/teams/contosohr	—	IP	22334	312
Contoso Marketing	/sites/contosomar	Pending	IP	15698	296
Contoso Finance	/sites/contosofin	Completed	-	11237	167
Contoso Giving	/sites/contosogiv	—	-	10245	145
Contoso team	/sites/contosoteam	—	-	8530	124
Contoso Vac	/sites/contosovac	—	-	6054	72
Contoso HRA	/teams/contosohra	—	IP	3998	2416
Contoso Media	/sites/contosocomedia	—	-	2804	38
Contoso in house	/sites/contosohh	—	-	1890	32
Contoso infra	/sites/contosoinfra	—	-	1487	23
Contoso design	/sites/contosodesign	—	-	1329	21
Contoso leaders	/teams/contosolead	—	IP	1127	647
Contoso data	/teams/contosodata	—	IP	1038	721

Snapshot till March

As of March 3, 2024

Review sites with a high number of users across all permission scopes (inherited and broken).

Download a detailed .csv report for up to 1M sites.

[Download detailed report](#)[+ Initiate site access review](#) [View all reviews](#) [Restrict site access](#)

100 items



Search

Filters: Site sensitivity: All External sharing: All

Name	URL	Site access review	Total permissioned users ↓	Files	Sensitive Files ⓘ	Items with unique permissions	EEEU permissions	People in your org links	Anyone links	Site Privacy	Site sensitivity	External sharing
Contoso HR	.../teams/contosohr	-	22334	44869	4821	2	2	312	312	Private	Top secret	On
Contoso Marketing	.../teams/contosoma	-	15698	41839	4213	1	2	298	298	Private	Confidential	On
Contoso Finance	.../sites/contosofin	-	11237	38286	4200	3	2	167	167	Private	-	On
Contoso Team	.../sites/contosoteam	-	10134	35310	3189	6	2	124	124	Private	Confidential	On
Contoso Vac	.../sites/contosovac	-	8530	31498	3120	2	2	72	72	Public	General	On
Contoso in house	.../teams/contosoin	-	6054	30764	3100	1	2	214	214	Public	Confidential	On
Contoso infra	.../teams/contosoin	-	3998	28187	2890	5	2	21	21	Public	General	On
Contoso leaders	.../teams/contosole	-	2804	22396	2340	8	2	12	12	Public	-	On
Contoso design	.../teams/contosoen	-	1890	20189	2310	2	2	9	9	Public	-	On
Contoso BI	.../teams/contosoen	-	1890	20189	2231	2	2	9	9	Public	-	On
Contoso HR	.../teams/contosoen	-	1890	20189	2213	2	2	9	9	Public	-	On
Contoso Give	.../teams/contosoen	-	1890	20189	1313	2	2	9	9	Public	-	On
Contoso Sesh	.../teams/contosoen	-	1890	20189	1110	2	2	9	9	Public	-	On
Contoso Sesh	.../teams/contosoen	-	1890	20189	989	2	2	9	9	Public	-	On

Snapshot till March

This displays list of sites where the number of users across all permission scopes (inherited and broken) exceeds a threshold
Download detailed .csv report for up to 10,000 sites.

[Download detailed report](#)
[+ Initiate site access review](#) [View all reviews](#) [Restrict site access](#)

Filters: Site sensitivity: All External sharing: All

These are labelled files and unlabelled files where a sensitive info type was detected

Name	URL	Site access review status	Files	No. of sensitive files ⓘ	Total permissioned users ↓	Count of EEEU permissions	Count of users
Contoso HR	.../teams/contosohr	—	44869	4814	22334	2	312
Contoso Marketing	.../teams/contosomar	—	41839	4423	15698	1	296
Contoso Finance	.../sites/contosofin	—	38286	4178	11237	3	167
Contoso Giving	.../sites/contosogiv	—	35310	3987	10245	6	145
Contoso team	.../sites/contosoteam	—	31498	3546	8530	2	124
Contoso Vac	.../sites/contosovac	—	30764	3215	6054	1	72
Contoso HRA	.../teams/contosohra	—	28187	2895	3998	5	2416
Contoso Media	.../sites/contosomedia	—	22396	2564	2804	8	38
Contoso in house	.../sites/contosoinh	—	20189	2489	1890	3	32
Contoso infra	.../sites/contosoinfra	—	19374	2341	1487	4	23
Contoso design	.../sites/contosodesign	—	13298	2287	1329	1	21
Contoso leaders	.../teams/contosolead	—	9450	2135	1127	5	21
Contoso data	.../teams/consolidata	—	8800	2039	1038	7	647
Contoso BI	—	—	8126	1983	1024	2	721

[Save](#)

Restricted site access

Use this setting to allow only users in specific security groups to access this SharePoint site. You can add up to 10 security groups. Users not in these security groups will lose access to all this SharePoint site.

[Learn more about Restricted access control for SharePoint sites](#)
 Restrict SharePoint site access to only users in specified groups

Add group

- CF Contoso Financial Council
- CT Contoso Tech
- CM Contoso Marketing
- CH Contoso HR

Microsoft deployment blueprint to address internal oversharing in Microsoft 365 Copilot

Customers with E3 Foundational

Address internal user oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2-4 days	2-4 weeks	1+ months
Deployment steps	<ol style="list-style-type: none">Identify the most popular sites & assess oversharing<ul style="list-style-type: none">Export the top 100 most used sites from SPO admin centerRun SAM permission state report¹Use Purview Content Explorer to view which sites contain sensitive information types (SITs)²Grant Copilot access to popular, low risk sites<ul style="list-style-type: none">Create custom reports from SAM and Content Explorer with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery³Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identifiedTurn on proactive audit and protection<ul style="list-style-type: none">Turn off EEUU (everyone except external users) at the tenant level⁴Turn on Audit and view Copilot interaction activity reports and charts^{1,2}Turn on audit-mode oversharing SPO DLP policy to detect anyone sharing links for labeled and unlabeled data⁵	<ol style="list-style-type: none">Discover oversharing risks<ul style="list-style-type: none">Use permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEUU, company shared links)¹Identify Copilot agent insights & take actions¹Restrict sensitive info from Copilot access and/or processing<ul style="list-style-type: none">Initiate Access Review for all sites that are overshared¹Apply restricted access control (RAC) on business-critical sites¹Exclude critical sites from Copilot reasoning over them¹Increase site privacy<ul style="list-style-type: none">Publish labels to Office apps, Container/Sites, Outlook for manual data protection by user¹Use site labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members¹Turn on enforce-mode oversharing SPO DLP policy to restrict access to sensitive data exposure & start remediating them²Disable RSS (if enabled) to allow full Copilot experience¹Turn on proactive audit and protection<ul style="list-style-type: none">Reduce risk by remediating alerts for overshared documents from the SPO DLP policy and applying sensitive labels¹Improve Copilot responses<ul style="list-style-type: none">Setup retention/deletion policies for SharePoint to reduce data surface²Identify inactive sites, then restrict access or delete¹	<ol style="list-style-type: none">Further reduce risk and simplify oversight<ul style="list-style-type: none">Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners¹Automate SAM permission state report to maintain permissions hygiene¹Automate permission reports and actions to maintain permission hygiene¹Regularly review oversharing reports and restrict access as needed¹Proactively avoid oversharing by applying RAC at site provisioning¹Periodically review inactive sites and take necessary action¹Control site provisioning by allowing creation for users that complete training¹Use change history to identify site changes that may cause oversharing¹Continuously manage all your oversharing DLP alerts via the Microsoft Purview Portal¹

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

LEGEND 1 – Copilot and SharePoint Adv. Mgt. 2 – OE3/ME3

Customers with E5 Optimized

Address internal oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2-4 days	2-4 weeks	1+ months
Deployment steps	<ol style="list-style-type: none">Identify the most popular sites & assess oversharing<ul style="list-style-type: none">Export DAG permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEUU, company shared links)¹Identify Copilot agent insights & take actions¹Grant Copilot access to popular, low risk sites<ul style="list-style-type: none">Run the Purview DSM Oversharing posture assessment to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types¹Restrict sensitive info from Copilot access and/or processing<ul style="list-style-type: none">Initiate SAM Access Review for all sites that are overshared¹Apply Restricted access control (RAC) on business-critical sites¹Exclude critical sites from Copilot reasoning over them with SAM Restricted Content Discovery (RCD)¹Publish sensitivity labels with Purview Information Protection to Office apps, Container/Sites, Outlook for manual data protection by user¹Exclude Copilot from summarizing sensitive content via sensitivity labels¹Turn on proactive audit and protection<ul style="list-style-type: none">Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members¹Turn on Purview Audit and view Copilot interaction activity reports and charts^{1,2}Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance³Turn on audit-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & start remediating them²Disable RSS (if enabled) to allow full Copilot experience¹Increase site privacy<ul style="list-style-type: none">Automatically label new documents and prevent them from oversharing with run time auto-labeling policy, starting with client-side policies and extend to service-side policies¹Apply default site library sensitivity labels to protect new and modified unlabeled documents¹Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access²Improve Copilot responses<ul style="list-style-type: none">Setup Purview retention/deletion policies for SharePoint to reduce data surface²Identify inactive sites with SAM, then restrict access or delete¹	<ol style="list-style-type: none">Discover oversharing risks<ul style="list-style-type: none">Run the Purview DSM Oversharing posture assessment to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types¹Further reduce risk and simplify oversight<ul style="list-style-type: none">Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners¹Automate SAM permission state report to maintain permissions hygiene¹Automate permission reports and actions to maintain permission hygiene¹Regularly review oversharing reports and restrict access as needed¹Proactively avoid oversharing by applying RAC at site provisioning¹Periodically review ownerless sites and take necessary action¹Control site provisioning by allowing creation for users that complete training¹Use change history to identify site changes that may cause oversharing¹Continuously manage all your oversharing DLP alerts via incidents with Microsoft Defender XDR incident queue²View risky user activity in context of oversharing Purview DLP incidents³Restrict sensitive info from Copilot access and/or processing<ul style="list-style-type: none">Run the Purview DSM Oversharing posture assessments to scale out data security actions, pivoted on labels and sensitive information types¹Grant Copilot access to popular, low risk sites<ul style="list-style-type: none">Cross reference the report results from SAM and review DSM for AI with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery¹Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified¹Turn on proactive audit and protection<ul style="list-style-type: none">Turn on Purview Audit and view Copilot interaction activity reports and charts^{1,2}Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance³Turn on audit-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & start remediating them²Disable RSS (if enabled) to allow full Copilot experience¹Increase site privacy<ul style="list-style-type: none">Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members¹Turn on Purview Audit and view Copilot interaction activity reports and charts^{1,2}Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance³Turn on audit-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & start remediating them²Disable RSS (if enabled) to allow full Copilot experience¹Further secure sensitive data<ul style="list-style-type: none">Automatically label new documents and prevent them from oversharing with run time auto-labeling policy, starting with client-side policies and extend to service-side policies¹Apply default site library sensitivity labels to protect new and modified unlabeled documents¹Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access²Improve Copilot responses<ul style="list-style-type: none">Setup Purview retention/deletion policies for SharePoint to reduce data surface²Identify inactive sites with SAM, then restrict access or delete¹	<ol style="list-style-type: none">Discover oversharing risks<ul style="list-style-type: none">Run the Purview DSM Oversharing posture assessment to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types¹Further reduce risk and simplify oversight<ul style="list-style-type: none">Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners¹Automate SAM permission state report to maintain permissions hygiene¹Automate permission reports and actions to maintain permission hygiene¹Regularly review oversharing reports and restrict access as needed¹Proactively avoid oversharing by applying RAC at site provisioning¹Periodically review ownerless sites and take necessary action¹Control site provisioning by allowing creation for users that complete training¹Use change history to identify site changes that may cause oversharing¹Continuously manage all your oversharing DLP alerts via incidents with Microsoft Defender XDR incident queue²View risky user activity in context of oversharing Purview DLP incidents³Restrict sensitive info from Copilot access and/or processing<ul style="list-style-type: none">Run the Purview DSM Oversharing posture assessments to scale out data security actions, pivoted on labels and sensitive information types¹Grant Copilot access to popular, low risk sites<ul style="list-style-type: none">Cross reference the report results from SAM and review DSM for AI with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery¹Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified¹Turn on proactive audit and protection<ul style="list-style-type: none">Turn on Purview Audit and view Copilot interaction activity reports and charts^{1,2}Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance³Turn on audit-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & start remediating them²Disable RSS (if enabled) to allow full Copilot experience¹Increase site privacy<ul style="list-style-type: none">Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members¹Turn on Purview Audit and view Copilot interaction activity reports and charts^{1,2}Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance³Turn on audit-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & start remediating them²Disable RSS (if enabled) to allow full Copilot experience¹Further secure sensitive data<ul style="list-style-type: none">Automatically label new documents and prevent them from oversharing with run time auto-labeling policy, starting with client-side policies and extend to service-side policies¹Apply default site library sensitivity labels to protect new and modified unlabeled documents¹Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access²Improve Copilot responses<ul style="list-style-type: none">Setup Purview retention/deletion policies for SharePoint to reduce data surface²Identify inactive sites with SAM, then restrict access or delete¹

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

LEGEND 1 – Copilot and SharePoint Adv. Mgt. 2 – OE3/ME3 3 – MES/ES Compliance

Get the blueprint:
<https://aka.ms/Copilot/OversharingBlueprintLearn>

Sensitivity labels span your entire data estate

They are a representation of your information taxonomy.

They describe the priority assigned to your categories of sensitive information.



Content labels



Applied to: Office apps, Power BI reports, Azure Data

Protections: Encryption and visual markings



Container labels

Applied to: SharePoint sites, Teams channels, Microsoft 365 groups

Protections: Access control, privacy settings, conditional access

Powerful controls that ensure labels are applied where needed

Apply labels by default, make them mandatory, prevent label downgrades

Demo

Enable labels

Demo

Enable co-authoring for files encrypted with sensitivity labels

Demo

Create a Sensitivity Label

Demo

Configure a retention policy
Configure a DLP policy

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	•	•

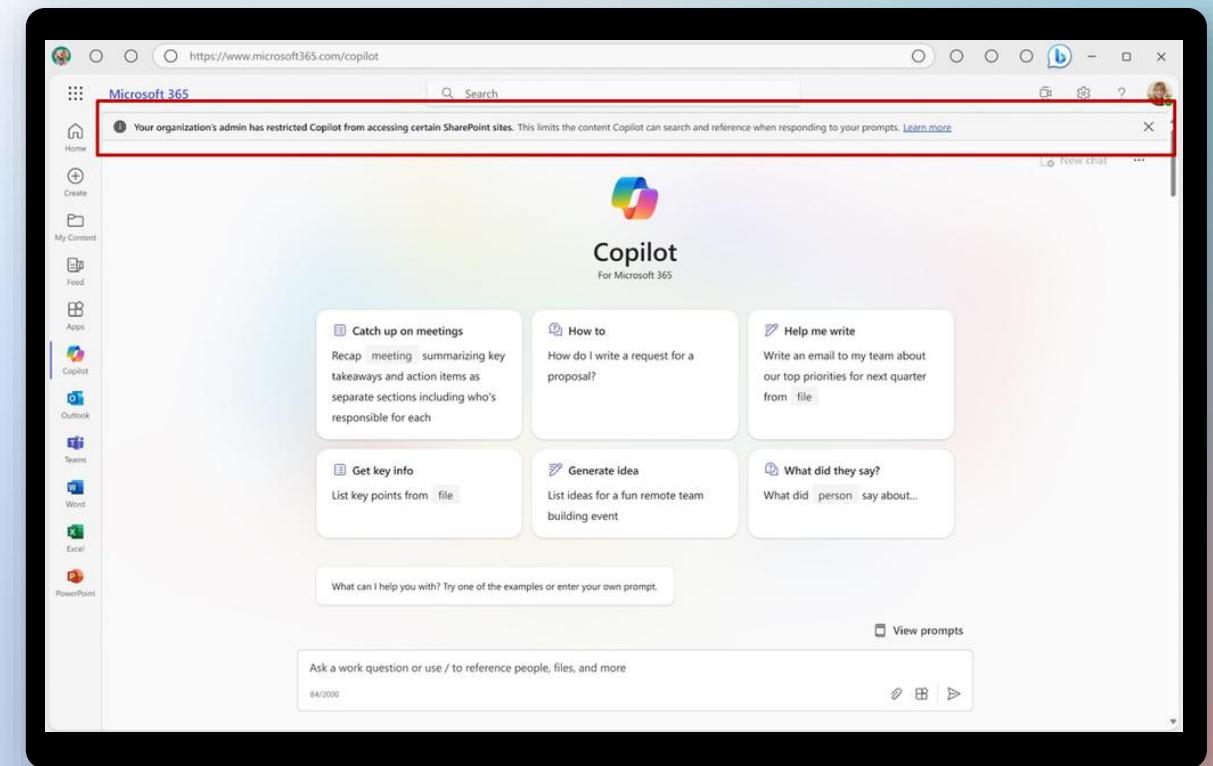
Introducing Restricted SharePoint Search to help you get started with Copilot for Microsoft 365

Restricted SharePoint Search allows you to **disable organization-wide search, and to restrict both Enterprise Search and Copilot experiences** to a curated set of SharePoint sites of your choice.

If you decide to enable it Copilot and non-Copilot users will be able to find and use content from:

- **An allowed list of curated SharePoint sites set** up by admins (with up to 100 SharePoint sites), honoring sites' existing permissions
- **Content from their frequently visited** SharePoint sites
- **Users' OneDrive files, chats, emails, calendars** they have access to
- **Files that were shared directly** with the users
- **Files that the users** viewed, edited, or created

Restricted SharePoint Search is off by default



Restricted SharePoint Search

Expected general availability: H1 CY2024

This is intended as a temporary solution to give you time to review and audit site permissions, while implementing robust data security solutions from Microsoft Purview and content management with SharePoint Advanced Management.

Restricted SharePoint Search is designed for organizations particularly concerned about unintentional oversharing of content

When enabled, Copilot experiences and organization-wide search are limited to a select set of SharePoint sites, as well as the individual user's files and content

PREREQUISITES

- Available to tenants with Copilot for Microsoft 365 subscriptions
- Activation requires Global/Tenant/SharePoint admin rights



IMPACT

Restricted SharePoint Search disables organization-wide search, while allowing you to select sites that you trust. This means users in your organization can use Copilot to reason over:

- An allowed list of curated SharePoint sites set up by admins (up to 100 SharePoint sites), honoring existing permissions on a site
- Users' OneDrive for Business, chats they are part of, emails they send and receive, calendars to which they have access, etc.
- Files that are shared with, and accessed by users
- Content from users' frequently visited sites

Turning on Restricted SharePoint Search does not affect the site's index or associated DLP and labeling policies.

Access this [blog](#) for more info.

File Security

← Link settings
0 - general index.docx ⚡ ⓘ ×

Share the link with

- Anyone Share with anyone, doesn't require sign-in
- People in CIAOPS ⓘ
- People with existing access ⓘ

- People you choose ⓘ

More settings

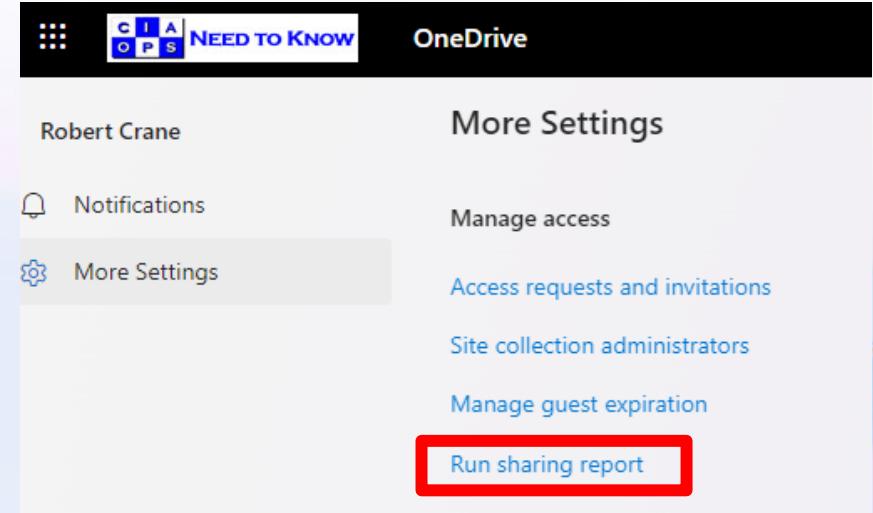
- Can view
- MM/DD/YYYY
- Set password

Apply Cancel

File Security

Shared with external users

 Run report



A	B	C	D	E	F	G	H	I	J	K	L
Resource Path	Item Type	Permission	User Name	User Email	User Or Grp Link ID	Link Type	AccessViaLinkID				
personal/admin_ciaops365_com	Web	Full Control	Robert Crane	admin@cia	Internal						
personal/admin_ciaops365_com	Web	Read	Everyone except extern	SecurityGroup							
personal/admin_ciaops365_com/Blog/Lists/Comments	List	Full Control	Robert Crane	admin@cia	Internal						
personal/admin_ciaops365_com/Blog/Lists/Comments	List	Read	Everyone except extern	SecurityGroup							
personal/admin_ciaops365_com/Blog/Lists/Comments	List	Contribute	Everyone except extern	SecurityGroup							
personal/admin_ciaops365_com/Documents/aip-demo.docx	docx	Contribute	SharingLink	SharePoint:c8c53a73-{Anyone}							
personal/admin_ciaops365_com/Documents/aip-demo.docx	docx	Contribute	Robert Crane	admin@cia	Internal	Anyone	c8c53a73-6c53-4353-bcc3-3db69738d335				
personal/admin_ciaops365_com/Documents/aip-demo.docx	docx	Read	SharingLink	SharePoint:58a04f30-e	Anyone						
personal/admin_ciaops365_com/Documents/Attachments	Folder	Full Control	Robert Crane	admin@cia	Internal						
personal/admin_ciaops365_com/Documents/Attachments/Loop component 1.loop	loop	Full Control	Robert Crane	admin@cia	Internal						
personal/admin_ciaops365_com/Documents/Attachments/Loop component 1.loop	loop	Read	SharingLink	SharePoint:c4025230-{Organization}							
personal/admin_ciaops365_com/Documents/Attachments/Loop component 1.loop	loop	Read	Lewis Collin	lewis.collin	Internal	Organization:c4025230-870c-4643-9fde-5d34d902cb25					
personal/admin_ciaops365_com/Documents/Attachments/Loop component 1.loop	loop	Read	Robert Crane	admin@cia	Internal	Organization:c4025230-870c-4643-9fde-5d34d902cb25					
personal/admin_ciaops365_com/Documents/Attachments/Loop component 1.loop	loop	Contribute	SharingLink	SharePoint:30dc72f6-3	Organization						
personal/admin_ciaops365_com/Documents/Attachments/Loop component 1.loop	loop	Contribute	Lewis Collin	lewis.collin	Internal	Organization:30dc72f6-3de7-439b-8b4f-604e5a036aed					
personal/admin_ciaops365_com/Documents/Attachments/Loop component.loop	loop	Full Control	Robert Crane	admin@cia	Internal						
personal/admin_ciaops365_com/Documents/Attachments/Loop component.loop	loop	Read	SharingLink	SharePoint:0d155769-	Organization						
personal/admin_ciaops365_com/Documents/Attachments/Loop component.loop	loop	Read	Lewis Collin	lewis.collin	Internal	Organization:0d155769-e4d0-48e5-bd85-e8ed12471aa5					
personal/admin_ciaops365_com/Documents/Attachments/Loop component.loop	loop	Read	Robert Crane	admin@cia	Internal	Organization:0d155769-e4d0-48e5-bd85-e8ed12471aa5					
personal/admin_ciaops365_com/Documents/Azure Codex	Folder	Read	Robert Crane	director	cia	External					

File access

The screenshot shows the SharePoint admin center interface. The left sidebar includes navigation items like Home, Sites, Active sites, Deleted sites, Policies, Settings, Content services, Migration, Reports, Content services, Data access governance (which is selected), Advanced, More features, and Advanced management (PRO). The main content area displays a "Welcome to data access governance" message with a sub-section titled "Sharing links". It describes identifying potential oversharing by monitoring sites where users created new sharing links in SharePoint. A "View reports" button is present. At the bottom right of the main area is a "Next" button.

Data access governance > Sharing links

Sharing links

Use these reports to review SharePoint sites where users created the most sharing links for files and folders in the last 30 days. To get the latest data for a report, you must run it, which can take a few hours.

[Learn more about these reports](#)

Run all Refresh status

<input type="checkbox"/>	Report name	Status
<input type="checkbox"/>	"Anyone" links	Not started
<input type="checkbox"/>	"People in your organization" links	Not started
<input type="checkbox"/>	"Specific people" links shared externally	Not started

File activity

Microsoft Defender

NEED TO KNOW

Search

Investigate 6 months back | ?

Advanced filters

Activity log

Queries: Select a query | Save as

App: Microsoft SharePoint Online | User name: Robert Crane (admin@ciaops365.com) | Raw IP address: Enter IP address | Activity type: Select value | Location: Select countries/regions

New policy from search | Export | 1 - 20 of 1,659 activities | Show details | Hide filters | Table settings

Activity	User	App	IP address	Location	Device	Date
ListItemUpdated	Robert Crane	Microsoft SharePoi...	128.94.5.10	Australia	Windows 10	7 May 2024 3:59 PM
PageViewed: SharePoint Page https://ciaops365e1-admin.s...	Robert Crane	Microsoft SharePoi...	128.94.5.10	Australia	Windows 10	7 May 2024 3:59 PM
PageViewed: SharePoint Page https://ciaops365e1-admin.s...	Robert Crane	Microsoft SharePoi...	128.94.5.10	Australia	Windows 10	7 May 2024 3:58 PM
Log on	Robert Crane	Microsoft SharePoi...	128.94.5.10	Australia	Windows 10	7 May 2024 3:58 PM
SignInEvent	Robert Crane	Microsoft SharePoi...	128.94.5.10	Australia	Windows 10	7 May 2024 3:58 PM
FilePreviewed: file https://ciaops365e1.sharepoint.com/s...	Robert Crane	Microsoft SharePoi...	20.190.142.41	Australia	Windows 10	7 May 2024 3:48 PM
Access file: file https://ciaops365e1.sharepoint.com/sites/d...	Robert Crane	Microsoft SharePoi...	128.94.5.44	Australia	Windows 10	7 May 2024 3:01 PM
FileAccessedExtended: file https://ciaops365e1.sharepoint.c...	Robert Crane	Microsoft SharePoi...	128.94.5.44	Australia	Windows 10	7 May 2024 2:59 PM
FileAccessedExtended: file https://ciaops365e1.sharepoint.c...	Robert Crane	Microsoft SharePoi...	128.94.5.44	Australia	Windows 10	7 May 2024 2:59 PM
FileAccessedExtended: file https://ciaops365e1.sharepoint.c...	Robert Crane	Microsoft SharePoi...	2a01:111:f402:f08d:39	United Sta...	—	7 May 2024 2:57 PM
Access file: file https://ciaops365e1.sharepoint.com/sites/D...	Robert Crane	Microsoft SharePoi...	2a01:111:f402:f08d:39	United Sta...	—	7 May 2024 2:57 PM
Access file: file https://ciaops365e1.sharepoint.com/sites/d...	Robert Crane	Microsoft SharePoi...	2a01:111:f402:f08d:39	United Sta...	—	7 May 2024 2:57 PM
Access file: file https://ciaops365e1.sharepoint.com/sites/w...	Robert Crane	Microsoft SharePoi...	2a01:111:f402:f08d:39	United Sta...	—	7 May 2024 2:57 PM

Customize navigation



Onboard & engage

**Prepare customer tenant for
Copilot for Microsoft 365**

Onboard & engage: Deploy apps/configure channel

Deploy Microsoft 365 apps to Business Users

Deploy required apps

To seamlessly integrate with Microsoft Copilot for Microsoft 365, you are required to deploy the following applications for your users:

- Word, Excel, PowerPoint, new Outlook for Windows
- Microsoft Teams, OneDrive, SharePoint, Exchange

Configure Channel

To use Copilot for Microsoft 365, Microsoft 365 apps must run on Current Channel or Monthly Enterprise Channel. Follow this guidance to configure the default update channel. Support options are available to help you make the most of Copilot for Microsoft 365*!

- Develop a list of users who will receive apps
- Map the users to the apps
- Deploy apps using the built-in tool in admin center or customer's preferred method. For additional information, watch these videos on how to deploy Microsoft 365 apps
- For more information on the implementation process, please see Deployment guide for Microsoft 365 apps



Deploy from Microsoft 365

Effort level: Low
Time to complete: 15+ minutes

User impact	Deploy with Intune
Your users will need to schedule to deploy apps in Microsoft 365.	Effort level: Medium Time to complete: 30+ minutes
Description	User impact
When deploying apps in Microsoft 365, users will need to launch the deployment.	The Intune customer experience impacts your productivity. Understanding the customer experience may require time to resolve.
Resources	Deploy Microsoft 365 (cloud) or Office (on-premises) to remote users
Download and deploy or review	Microsoft Intune provides flexible deployment options for Microsoft 365.
Get started	Before you can use Microsoft Intune, one of the first steps is to add Microsoft 365 Apps. By selecting the devices you manage, you can quickly get started.
Go to Apps & devices	Org's use many web apps, and to deploy them.
User impact	Your users will need to schedule to deploy apps in Microsoft 365.
Resources	Deploy with Configuration Manager
Add Microsoft 365 App	Effort level: Medium Time to complete: 30+ minutes
Get started	You can create a customized device. Open the Deployment guide to set up these connected to your internal network.
The app features	Users guide to set up these connected to your internal network.
User impact	Increase IT productivity and efficiency by reducing manual tasks and letting you focus on high-value projects. Maximize hardware and software investments.
Resources	Empower user productivity by providing the right software at the right time.
Deploy Microsoft 365 App	Effort level: Medium Time to complete: 30+ minutes
Get started	If your org plans to deploy apps in Microsoft 365 with Configuration Manager, use the Deploy and update Microsoft 365 (cloud) or Office (on-premises) with Configuration Manager guide to generate a custom script that configures both an apps deployment and updates in Configuration Manager.
Deploy Microsoft 365	After you select your settings, you'll get instructions on how to run the script and add devices to the deployment. The script will:
	<ul style="list-style-type: none">Create security groups and device collections for targeting the deployment and a

*Note: Engage your Microsoft Account Technical Specialist (ATS) or Customer Success Account Manager (CSAM) to discuss the support options available to you.

Onboard & engage: Assign licenses

License your Business Users

Assign licenses

Based on the results of the [Optimization Assessment](#) and [scenario discovery](#), the appropriate licenses need to be assigned to the select set of end users.

Based on the adoption plan, develop a list of users who will receive the licenses first. A few data points to keep in mind:

1. Analyze departments with the highest Microsoft 365 usage data, and based on that analysis start enabling entire teams within Marketing, Sales, or HR
2. Use the Scenario Library to identify top use cases and the key metrics you would like to improve in your functional area

Use the [setup guide](#) to assign required licenses to users or customer's preferred method. You can [assign and unassign licenses](#) for users on the Licenses page under the Active users page.



License your Microsoft Copilot for Microsoft 365 users

Make sure your users have the correct licenses assigned to them. Your users must have a Microsoft 365 E3 or E5 license assigned before you can assign them a license for Microsoft Copilot for Microsoft 365.

Assign licenses to your users or groups:

[Assign group license](#) [Assign user license](#)

Name ↑	Available licenses
<input type="checkbox"/> Microsoft Copilot for Microsoft 365	406154

Onboard & engage: Setup guide

Set up Copilot for Microsoft 365

Use the new Microsoft 365 Copilot setup guide, a wizard-based experience in the Microsoft 365 admin center, to help prepare your organization for Copilot for Microsoft 365:

Review the [list of prerequisites](#) and make sure they are met for your organization

Assign licenses to your users or groups

Promote Microsoft 365 Copilot features to your users with the email announcement template provided in the setup wizard

- Find this wizard in the admin center > Home > Setup page >
- Apps and Email > Get ready for Microsoft 365 Copilot



The image displays two screenshots of the Microsoft 365 Admin Center interface, specifically the 'Set up Microsoft Copilot for Microsoft 365' wizard.

Screenshot 1: Overview Step

This screenshot shows the initial step of the wizard, titled 'Set up Microsoft Copilot for Microsoft 365'. It includes a brief description of Copilot's capabilities, a note that it doesn't need to be installed, and a section titled 'What to expect' with three bullet points: 'Prepare your organization for Copilot.', 'Assign Copilot licenses to your users.', and 'Send an email announcing Copilot and its features to your users.'

Screenshot 2: Readiness Step

This screenshot shows the second step of the wizard, titled 'Prepare your organization for Copilot'. It lists prerequisites such as having Microsoft Entra ID accounts for users and ensuring they have the necessary license. It also includes sections for 'Add or sync your users' and 'Copilot for Microsoft 365 readiness report'. At the bottom, there are 'Back' and 'Next' buttons.

Demo

Setup Guide

Links to learn more (1 of 2)

Copilot Readiness Hub

What is Copilot?

- Introducing Copilot for Microsoft 365
- The Copilot System
- ChatGPT vs. Copilot for Microsoft 365: What's the difference?

How Copilot works

- How Copilot for Microsoft 365 works: Microsoft Mechanics video
- Semantic Index for Copilot
- Microsoft Graph
- Microsoft Graph connectors
- Additional copilot experiences across the Microsoft Cloud
 - Microsoft Dynamics 365 Copilot
 - Copilot in Power Platform
 - Microsoft Security Copilot
 - GitHub Copilot
 - Copilot in Microsoft Stream

Privacy

- Microsoft's privacy policy
- Microsoft Privacy Statement
- Trust Center data protection and privacy
- Data, privacy, and security for Copilot for Microsoft 365
- Data, privacy, and security for Azure OpenAI Service
- Role-based access control
- User permissions and permission levels in SharePoint Server
- Customer Lockbox requests
- Microsoft 365 isolation controls
- Data Protection Addendum

Links to learn more (2 of 2)

Data residency and storage

- EU Data Boundary
 - [Website](#)
 - [Blog](#)
 - [Documentation](#)

How to prepare for Copilot for Microsoft 365

- [Learn about Microsoft feedback for your organization](#)
- [Manage Microsoft feedback for your organization](#)
- [How to manage Microsoft Search](#)
- [Microsoft 365 Product Terms](#)
- [Content management and security in SharePoint, OneDrive, and Teams](#)

Compliance

- [Microsoft Compliance](#)
- [Service Trust Portal](#)
- [Compliance offering definitions](#)
- General Dat Protection Regulation (GDPR)
 - [Full summary](#)
 - [Short summary](#)

Security

- [Configure usage rights for Azure Information Protection \(AIP\)](#)
- [Universal Licensing Terms for Online Services](#)
- [Data Protection Addendum](#)
- [Isolation and Access Control in Microsoft 365](#)

Responsible AI

- Responsible AI core principles
 - [Videos](#)
 - [Documentation](#)
- [Microsoft Responsible AI Standard](#)
- [Governing AI: A Blueprint for the Future](#)



<https://bit.ly/ciacspcopicopilot2025>