INVOKE

We ignite
secure innovation.

Prepare for Microsoft 365 Copilot by Enhancing Data Security and Compliance

Zewei Song, Ph.D.
Cloud Solution Architect – Modern Work
Invoke, LLC
zewei.song@invokellc.com
https://www.linkedin.com/in/zeweis/

AGENDA

- Introduction to Copilot and Purview
- Security and compliance concerns
- Microsoft Purview features and capabilities
- Data security and compliance
- Sensitive data handling with Copilot
- Data lifecycle management
- Monitoring, auditing and discoverability
- AI Hub/demo
- Next steps
- What we can help
- Q & A

MICROSOFT 365 COPILOT

Microsoft 365 Copilot is an AI-powered productivity tool designed to enhance productivity and amplify human creativity across various Microsoft 365 applications. It integrates with apps like Word, Excel, PowerPoint, Outlook, Teams, and others, using large language models (LLMs) and Microsoft Graph to assist users in their daily tasks.

EARLY FINDINGS – MICROSOFT 365 COPILOT

INVOKE

All Up Value

87% agree more **productive**

79% focus on **more important work**

70% able to stay in the **flow**

69% focus on more **satisfying work**

79% spent less time on **mundane tasks**

Value by Workflow

81% allows to spend **less time searching** for information

73% makes **meetings more efficient**

79% allows me to spend **less time processing email**

94% makes all **easier to get started** on a first draft

Value by Role / Function

1 in 3 had >30 min time savings per day (MCAPS)

88% complete **tasks faster** (MCAPS)

63% **simplify** complex tasks (MCAPS)

58% **reclaim time** for more important work (managers)

How much is Copilot **worth** to users?

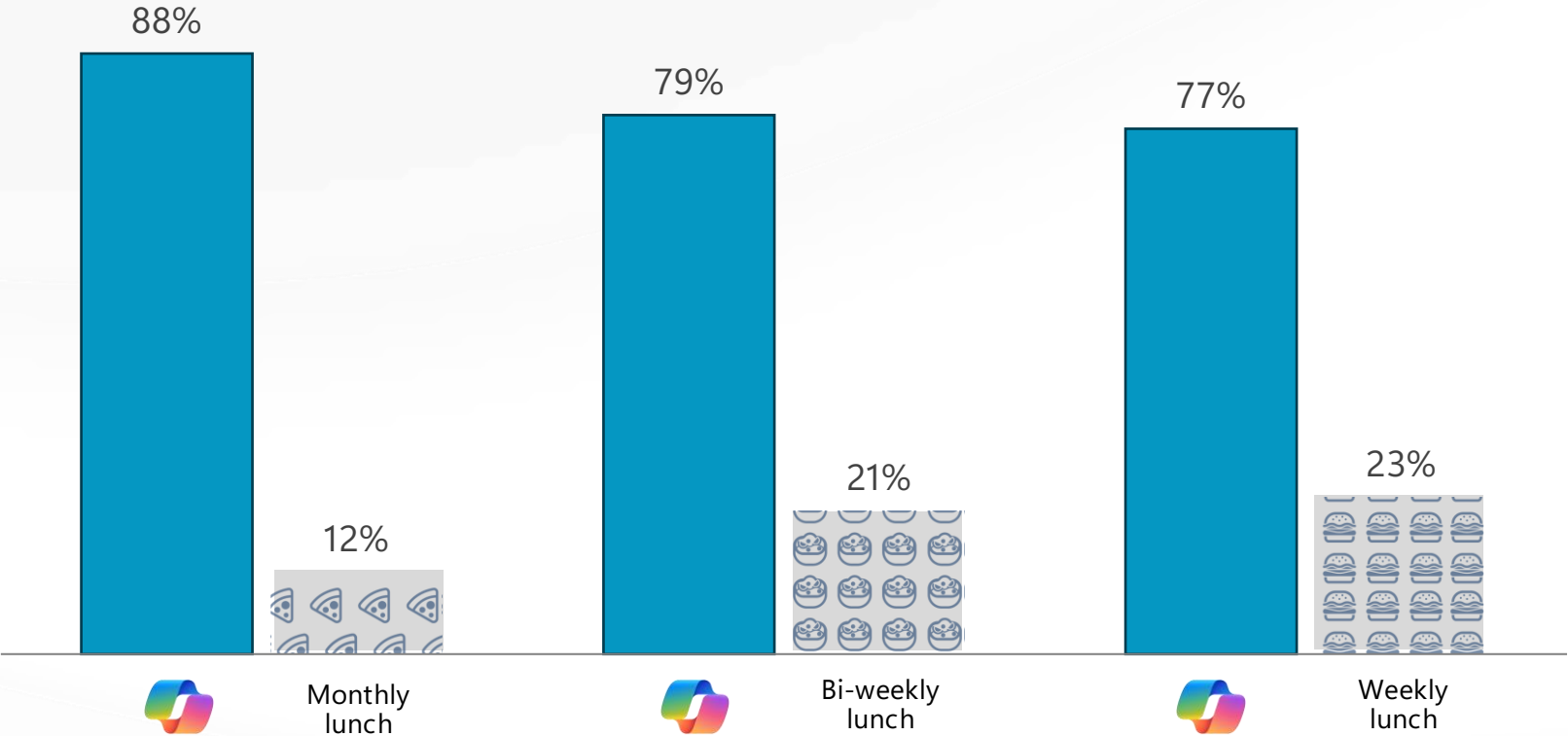**96%** would be disappointed if they **no longer had access to Copilot**

83% would not want to go back to **working without Copilot**

47% access to Copilot would influence my **choice of employer**

IS COPILOT WORTH MORE THAN A FREE LUNCH?

INVOKE

If offered the choice, users overwhelmingly said they would pick Copilot

88%

79%

77%

12%

21%

23%

Monthly lunch

Bi-weekly lunch

Weekly lunch

COMMON SECURITY AND COMPLIANCE QUESTIONS AND CONCERNS

invoke

How does Copilot access our data?

Can Copilot access data that an end user doesn't have access to?

Can a user get access to data via Copilot which they are not supposed to?

Where are the LLMs stored/hosted?

Does Copilot use our data to improve it?

What is Enterprise Data Protection?

How is the Sematic Index generated and where is it stored?

What data is stored in Sematic indexes?

Can Copilot over-share our data and how to prevent it?

How can we find out where the business critical and sensitive data resides?

How can we make sure that sensitive data (AI generated or not) isn't exposed to audiences not intended to?

Can Copilot access data that marked as sensitive?

What about encrypted data?

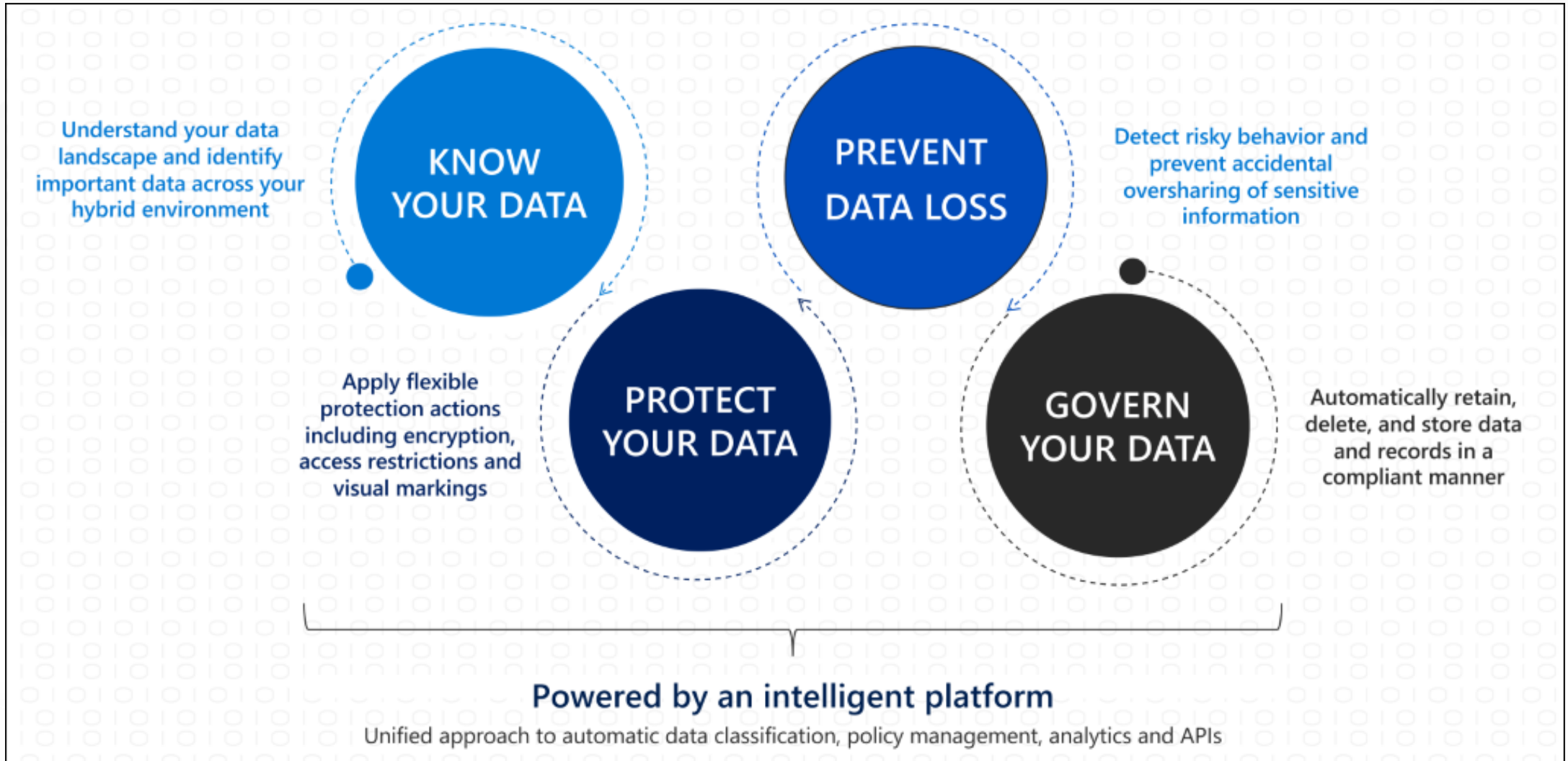What about content generated based on sensitive data?

Can we limit Copilot's access to certain data in our tenant? (or excluding certain data)

Are end users' interactions with Copilot auditable and discoverable?

Is it possible to prevent users from including sensitive information in their AI prompts?

MICROSOFT PURVIEW

Understand your data landscape and identify important data across your hybrid environment

KNOW YOUR DATA

PREVENT DATA LOSS

Detect risky behavior and prevent accidental oversharing of sensitive information

Apply flexible protection actions including encryption, access restrictions and visual markings

PROTECT YOUR DATA

GOVERN YOUR DATA

Automatically retain, delete, and store data and records in a compliant manner

Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs

PURVIEW CAPABILITIES

Data Security
- Data Loss Prevention*
- Information Barriers*
- Information Protection
- Insider Risk Management*
- Privileged Access Management

Data Governance*
- Data Catalog
- Data Estate Insights
- Data Map
- Data Policy
- Data Sharing

Risk & Compliance
- Audit
- Communication Compliance*
- Compliance Manager
- Data Lifecycle Management*
- eDiscovery*

SENSITIVITY LABELS

- Permissions and label settings are always honored by Copilot
- For Rights Managed items, users must have at least EXTRACT and VIEW usage rights for Copilot to return data
  - Even when items are NOT saved to Microsoft 365 repositories
- Copilot's responses are labeled with the most restrictive sensitivity label as referenced content
- When Copilot creates new content based on items that have sensitivity labels applied, the sensitivity labels from the source file are automatically inherited
  - If multiple files are used to create new content, the sensitivity label with the highest priority is used for label inheritance.
- Compliance management for Copilot supported by Purview

- Microsoft 365 Copilot messages are automatically included in the retention policy location named Teams chats and Copilot interactions

- If a user leaves your organization and their Microsoft 365 account is deleted, their Copilot messages that are subject to retention are stored in an inactive mailbox. The Copilot messages remain subject to any retention policy that was placed on the user before the mailbox was made inactive, and the contents are available to eDiscovery searches

MONITORING, AUDITING AND DISCOVERABILITY

Interactions with GenAI can be monitored on user level

Using Communication Compliance, you can analyze user prompts and Copilot responses to detect inappropriate or risky interactions or sharing of confidential information

User prompts to Copilot and responses from Copilot are stored in a user's mailbox and can be searched and retrieved when the user's mailbox is selected as the source for a search query in Content Search

This data can be put on hold and exported

This data can be permanently deleted as well

AI HUB (PREVIEW)

Microsoft Purview AI Hub and other security capabilities

Discover

> Discover generative AI activity, including sensitive data usage in and total users using AI

Protect

> Protect Copilot interactions to prevent sensitive data from unauthorized access
> Prevent users from pasting sensitive information or uploading sensitive documents to generative AI sites

Comply

> Detect and mitigate business risks and regulatory violations

INVOKE

We ignite **secure** innovation.

DEMO

Purview AI Hub

RESTRICTED SHAREPOINT SEARCH
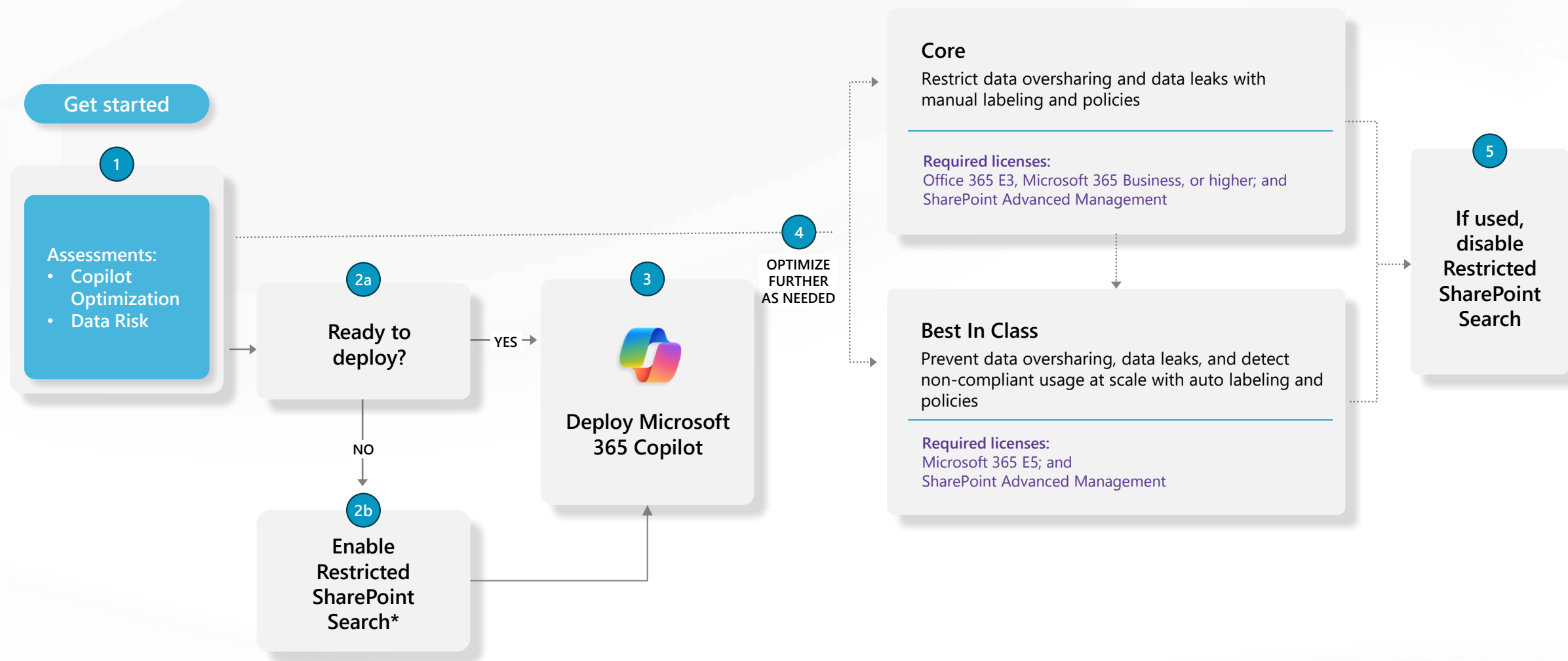
A setting to maintain a list of SharePoint sites ("allowed list") that you have checked the permissions and applied data governance for. The allowed list defines which SharePoint sites can participate in organization-wide search and Copilot experiences.

Allows you to restrict both organization-wide search and Copilot experiences to a curated set of SharePoint sites of your choice.

GET STARTED QUICKLY AND CONTINUE TO OPTIMIZE ALONG THE WAY

invoke

Get started

1

Assessments:
- Copilot Optimization
- Data Risk

2a

Ready to deploy?

— YES →

3

Deploy Microsoft 365 Copilot

NO

2b

Enable Restricted SharePoint Search*

4

OPTIMIZE FURTHER AS NEEDED

Core

Restrict data oversharing and data leaks with manual labeling and policies

Required licenses:
Office 365 E3, Microsoft 365 Business, or higher; and SharePoint Advanced Management

Best In Class

Prevent data oversharing, data leaks, and detect non-compliant usage at scale with auto labeling and policies

Required licenses:
Microsoft 365 E5; and SharePoint Advanced Management

5

If used, disable Restricted SharePoint Search

* 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.
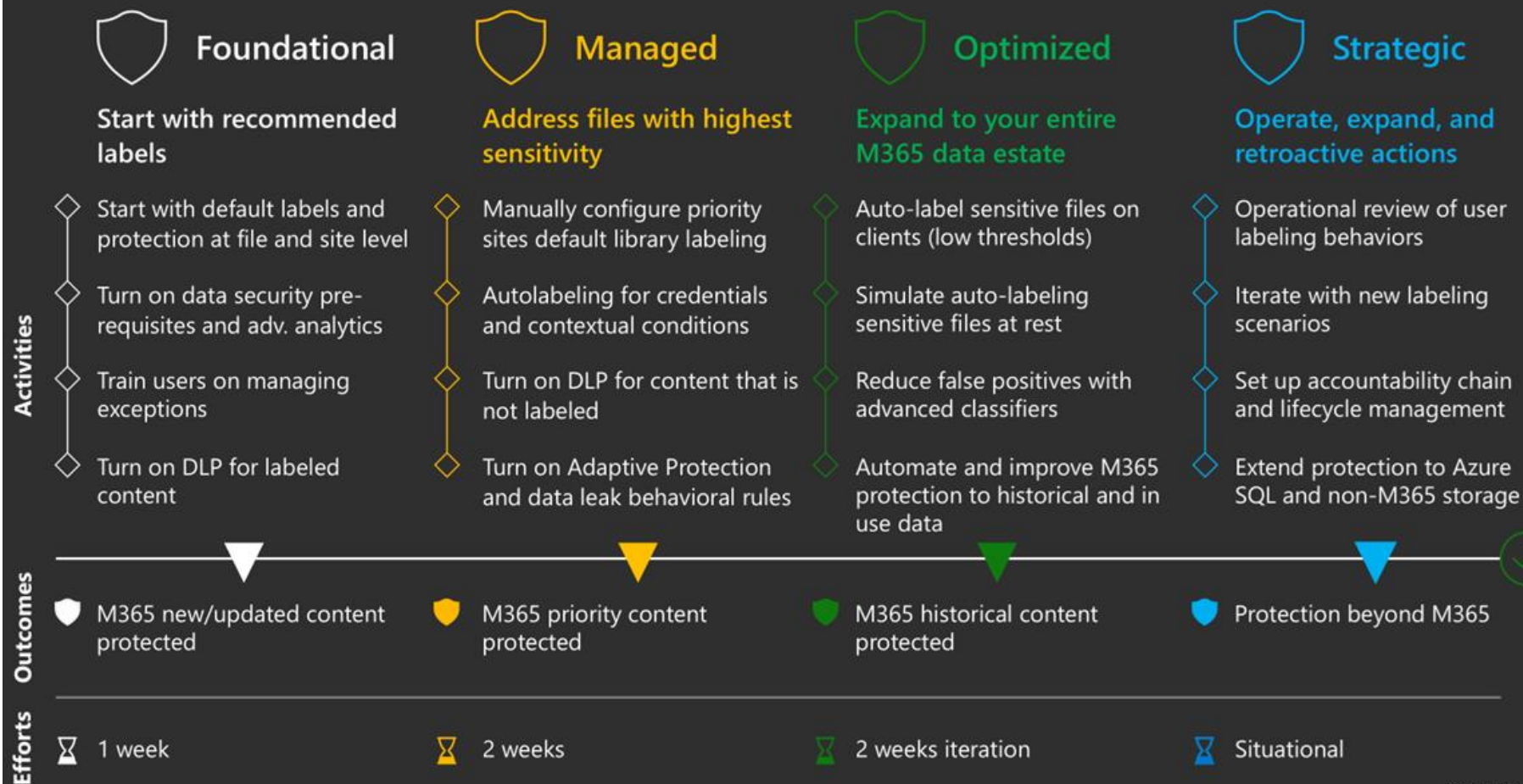
NEW QUESTIONS

- How do we start on data categorization?
  - What sensitivity data do we have, what classifiers should we use, trainable classifiers, custom SITs, EDM, …?
- What (sensitivity) labels should we create?
  - What are their settings, whom should we published them to, should we do encryption (RM), what about container level labels, auto-labeling, …?
- How do we manage our data's lifecycle?
  - Do we need retention policies, retention labels, for which containers, auto-labeling, records management, regulatory labels, …?
- Which eDiscovery capabilities should we use, which groups of people should we enable the capability for, …?
- Do we need to do DLP, what policies to define, where do we publish them to, …?
- What about other Purview capabilities, like insider risk, information barrier, communication compliance, …?
- How do we monitor all these?
- Should we set up RSS during pilot phare while we are derailing with all above, if yes which sites should we include in RSS?
- What about MDCA?
- ……
- **We need to start ASAP!**

PURVIEW DEPLOYMENT MODELS

Secure by default with Microsoft Purview and protect against oversharing

	Foundational	**Managed**	**Optimized**	**Strategic**
	Start with recommended labels	**Address files with highest sensitivity**	**Expand to your entire M365 data estate**	**Operate, expand, and retroactive actions**
Activities	Start with default labels and protection at file and site level	Manually configure priority sites default library labeling	Auto-label sensitive files on clients (low thresholds)	Operational review of user labeling behaviors
	Turn on data security pre-requisites and adv. analytics	Autolabeling for credentials and contextual conditions	Simulate auto-labeling sensitive files at rest	Iterate with new labeling scenarios
	Train users on managing exceptions	Turn on DLP for content that is not labeled	Reduce false positives with advanced classifiers	Set up accountability chain and lifecycle management
	Turn on DLP for labeled content	Turn on Adaptive Protection and data leak behavioral rules	Automate and improve M365 protection to historical and in use data	Extend protection to Azure SQL and non-M365 storage
Outcomes	M365 new/updated content protected	M365 priority content protected	M365 historical content protected	Protection beyond M365
Efforts	1 week	2 weeks	2 weeks iteration	Situational

Last updated: August 14, 2024

COPILOT JOURNEY – ASSESS & PLAN
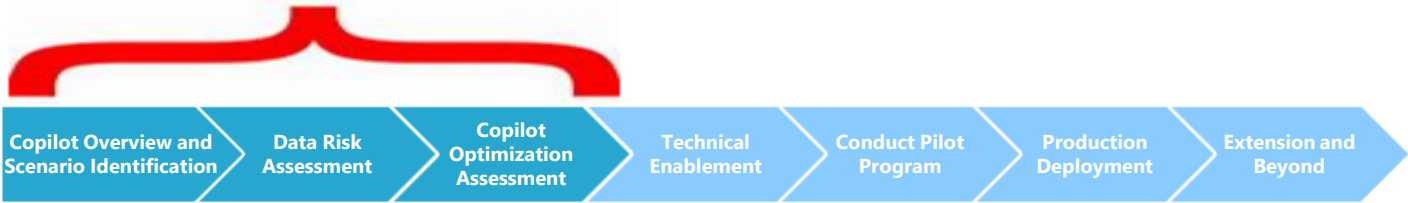
Value proposition

Assess your organization's environment, data and users for generative AI's deployment and plan to unlock its full potential with this engagement without financial commitment (no licensing purchase required and out-of-pocket consulting cost). This program is designed to facilitate business value conversations by function, providing a blueprint to determine the positive impact on your business in terms of increased revenue, reduced costs, and improved employee wellbeing. We will also dive into your environment, and asses its fitness for starting the generative AI journey.

Customer Benefits and Outcomes

- **Product Demonstration:** Conduct an "Art of the Possible" session to showcase the product capabilities of Microsoft Copilot.

- **Technical Assessment and Readiness:** Complete Optimization Assessment, and Data Risk Assessment to measure technical readiness and determine steps needed to prepare your environment, data and teams for your AI transformation with Microsoft Copilot.

- **Use Case Identification:** Identify the customer's high-value use cases that can benefit from Microsoft Copilot.

- **Business Case Development:** Build a business case for implementing Microsoft Copilot in terms of increased revenue, reduced costs, and improved employee wellbeing.

- **Roadmap Development:** Develop a roadmap to address gaps found in the optimization assessment and implement the high-value use cases.

Funding: Up to 100% by Microsoft, subject to qualifications and program cap. No Microsoft Copilot licenses purchase required.

Assess & Plan

| Copilot Overview and Scenario Identification | Data Risk Assessment | Copilot Optimization Assessment | Technical Enablement | Conduct Pilot Program | Production Deployment | Extension and Beyond |

Who is this Engagement is Intended for?

- Starting point for Customers who are beginning the Microsoft 365 Copilot Journey.

- Help customers understanding the benefits gained and activities required for their environment.

- Appropriate for Customers who have not yet made a licensing purchase for Microsoft 365 Copilot.

- Activities funded through Microsoft Programs (no out-of-pocket expense for qualified customers)

What are the Deliverables for this Engagement?

- Refined list of Use Cases tailored to the customers business needs.

- Technical Readiness Assessment.

- Roadmap to implement Copilot in your environment.

TAKEAWAYS

Generative AI is coming to workplace and Microsoft 365 Copilot has unique advantages for workplace productivity and innovation by seamlessly integrating generative AI capabilities with Microsoft 365 data and applications.

To ensure a successful Copilot journey, optimize data security and compliance posture is essential.

Microsoft Purview is the tool to govern, protect, and manage data across your entire data estate to prepare for Copilot deployment.

Restricted SharePoint Search can help jumpstart the deployment.

There are Microsoft funded services available to jumpstart!

Call to Action

- [Request a Microsoft 365 Copilot envisioning session](#) 🔗

- [Request more information on a Data Risk Assessment](#) 🔗

RESOURCES

Purview Overview: [Microsoft Purview | Microsoft Learn](#)

Purview Content Explorer: [Get started with content explorer | Microsoft Learn](#)

Data Classification: [Understand data classification in the Microsoft Purview governance portal | Microsoft Learn](#)

AI Hub: [Microsoft Purview data security and compliance protections for Microsoft 365 Copilot and other generative AI apps | Microsoft Learn](#)

Copilot Adoption: [Microsoft 365 Copilot – Microsoft Adoption](#)

Data Risk Assessment: [Data Risk Assessment – Microsoft AppSource](#)

Copilot Assess & Plan: [Copilot Journey – Assess & Plan](#)

Q & A

Thank you!

INVOKE

We ignite

secure innovation.