Morning sessions on the effective use of Artificial Intelligence (AI)

May 2025

Agenda

01 Welcome & Introduction

02 **AI Cybersecurity Threat Landscape** w. Kenneth Pedersen & Jørgen Sørensen

03 Inside **PwC's Compliance Journey with AI** w. CISO, Nicholas Jancey

04 **Security in the age of AI** w. Microsoft

05 **Tackling AI Security Threats** – What to do next?

06 Closing and Q&A

Kenneth Pedersen
Partner, Head of Cyber Risk Transformation, PwC
Kenneth.studsgaard.pedersen@pwc.com
+4531361073

Jørgen Sørensen
Partner, Head of Responsible AI, PwC
Jorgen.jgs.sorensen@pwc.com
+4524945254

Nicholas Jancey
CISO PwC Nordics & Africa
Nicholas.jancey@pwc.com
+4529614698

Kristoffer Rosenmeier
Sr. Specialist Manager, Security & Compliance at Microsoft
Kristoffer.rosenmeier@microsoft.com
+4529229873

The AI shift

AI Is Becoming Part of Everyday Life

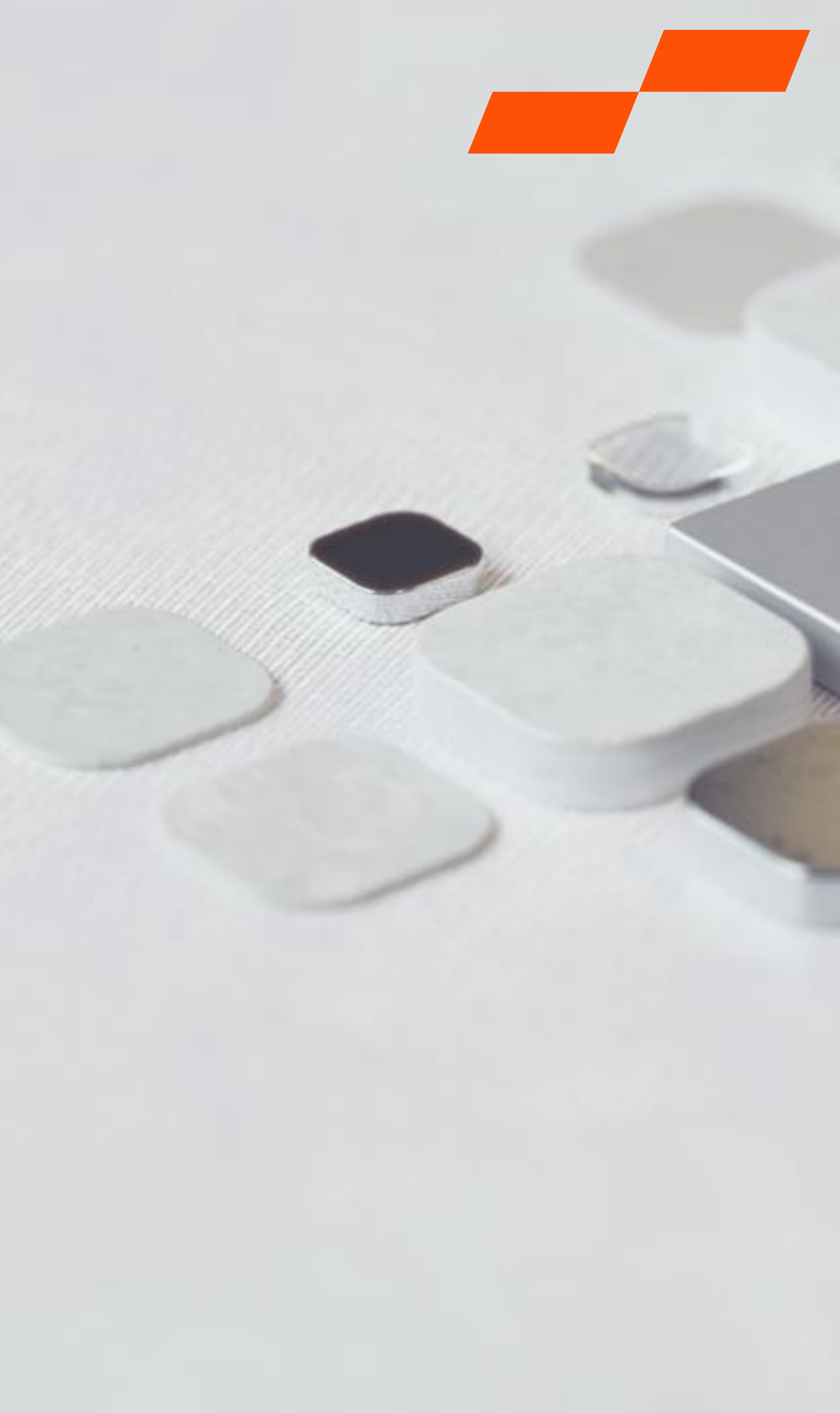
Tools like Microsoft Copilot, ChatGPT, and others are no longer optional – they're being integrated into workflows, communication, and decision-making.

Whether we're ready or not, the technology is advancing.
The challenge now is how to use AI **effectively and responsibly**.

AI is transforming how we work.
It automates routine tasks, supports faster insights, and opens for new ways of collaborating.

This shift brings new demands.
It requires **new skills, ethical awareness, and smarter strategies** from both individuals and organizations.

"We're not waiting for AI anymore. We're living with it."



61%

are using or planning to use AI in their cybersecurity efforts

60%

are more concerned about cyberthreats now than they were 12 months ago

Cybercrime Survey 2024

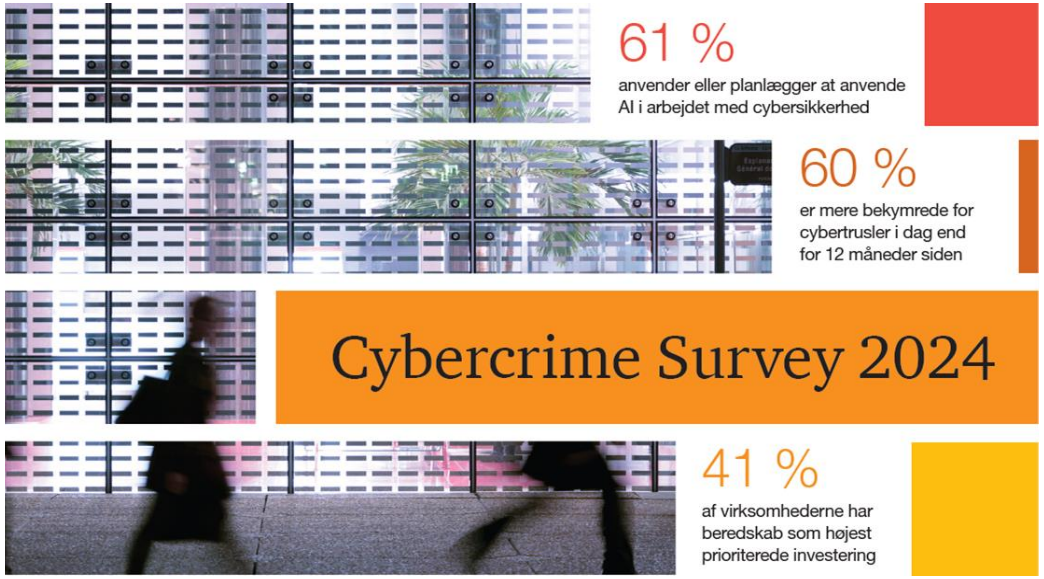
41%

of organisations have incident response as their highest-priority investment

About the **Cybercrime Survey**

In Brief

- For the **10th consecutive year**, PwC has evaluated cybersecurity efforts in Danish businesses.
- A total of **463 executives, security officers, and subject matter experts** participated in PwC's Cybercrime Survey 2024 making them reliable for statistical reporting.
- The respondents shared their insights on topics such as **concerns**, investments, challenges, and opportunities in cybersecurity.



61 %

anvender eller planlægger at anvende AI i arbejdet med cybersikkerhed

60 %

er mere bekymrede for cybertrusler i dag end for 12 måneder siden

Cybercrime Survey 2024

41 %

af virksomhederne har beredskab som højest prioriterede investering

You can download the complete survey on PwC's official website.

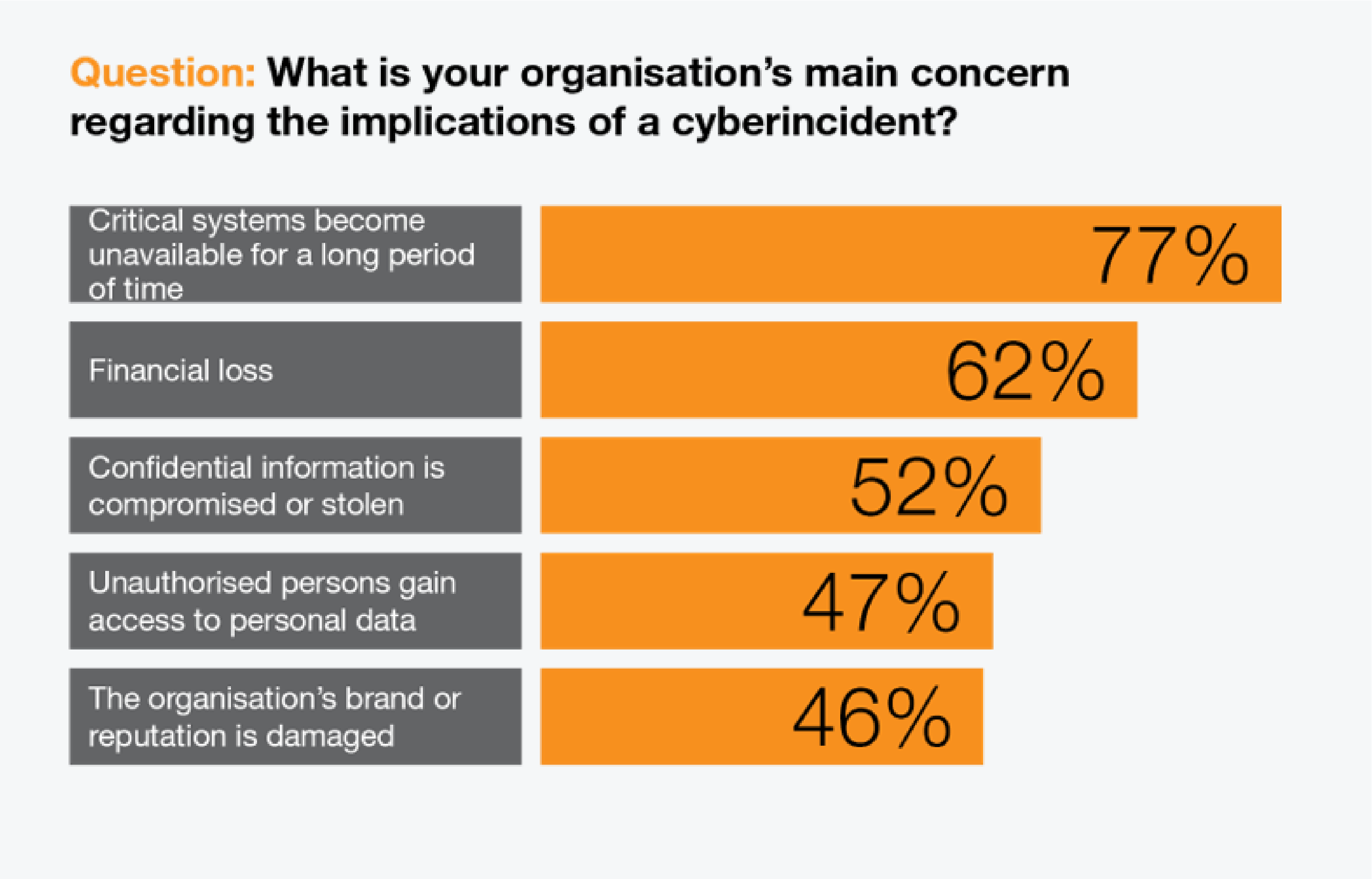
The biggest **cyber concerns**

77 %

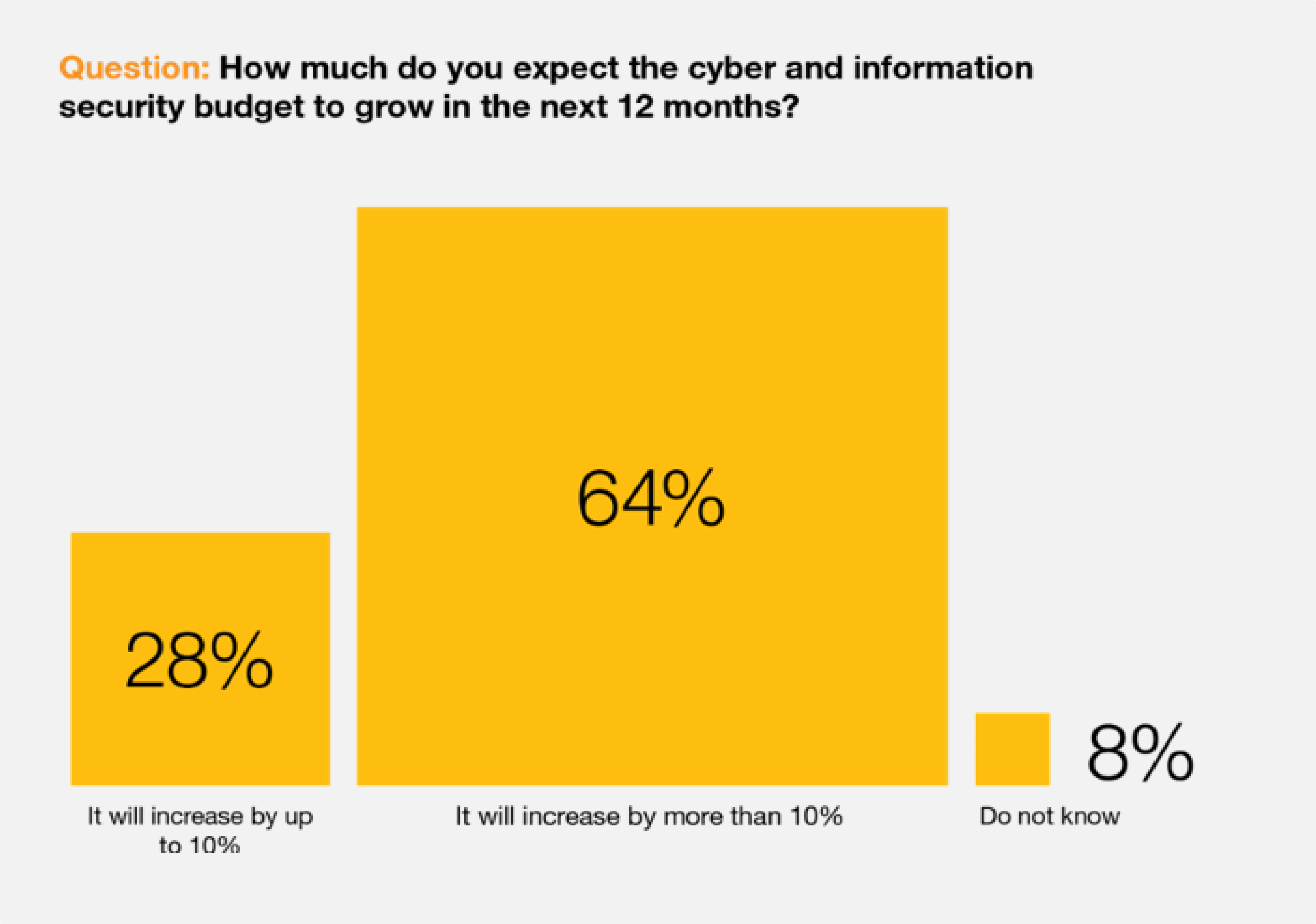
indicate that critical system outages are their biggest concern, while 62% point to the direct financial consequences of a cyberattack.

Cyber threats are no longer limited to hackers. Threats can also arise internally within the organization due to employees' unintentional actions. These actions are considered to represent a significant threat.

The cyber threat landscape is evolving in complexity, and comes with a cost.



Question: What is your organisation's main concern regarding the implications of a cyberincident?



Question: How much do you expect the cyber and information security budget to grow in the next 12 months?

How will the budget be invested

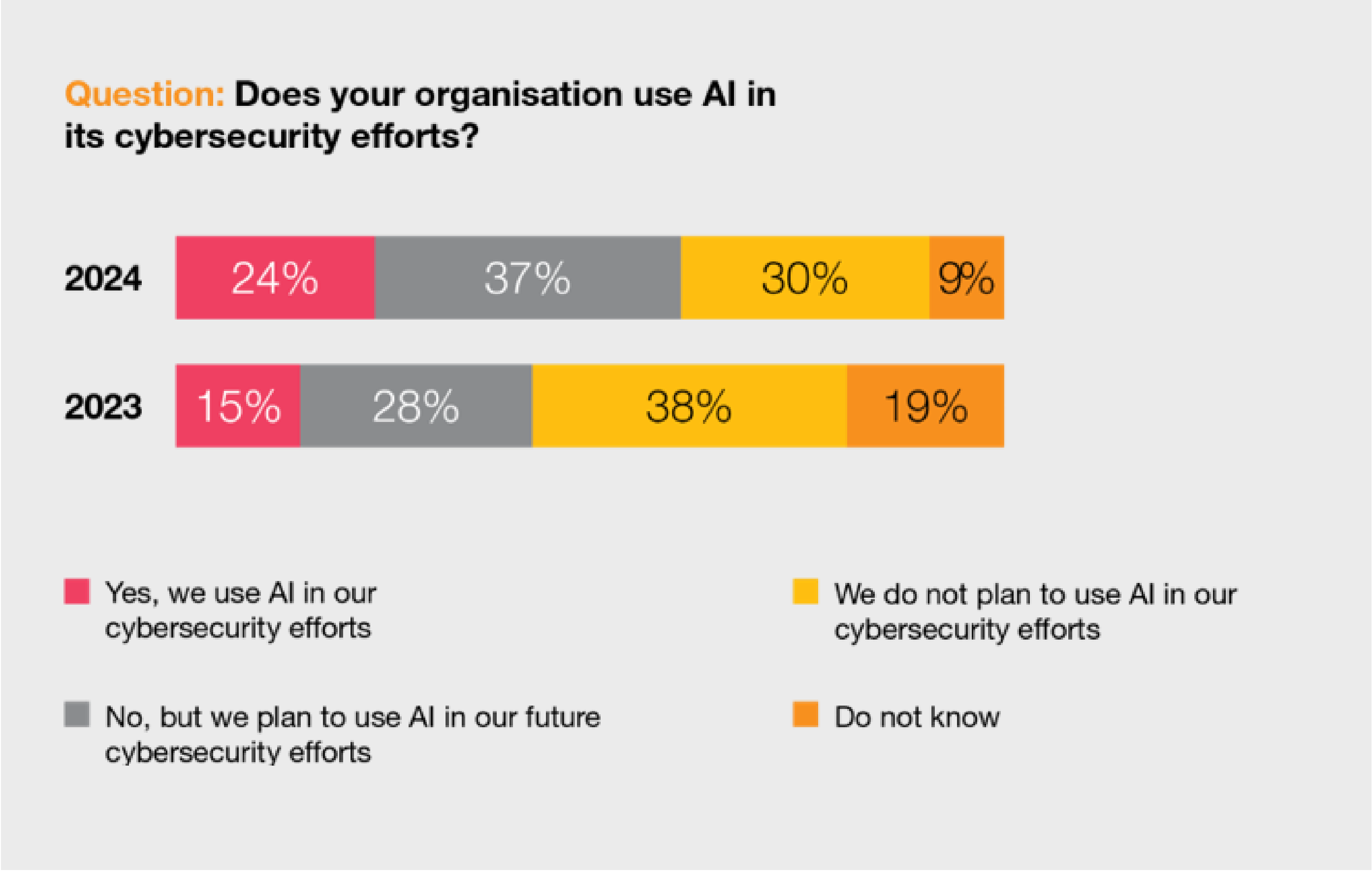
Measures that can help prevent companies from being affected by a cybersecurity incident.

Measures that can help strengthen a company's ability to manage cybersecurity incidents, should one occur — for example, contingency plans and policies for recovery.

"AI is one of the highest priority investments in cyber security"

AI has become a much bigger factor in cybersecurity work

AI is one of the highest priority investments in cyber security, rising from 12% in 2023 to a whopping 25% in 2024. Over the last 3 years the investment has increased fivefold



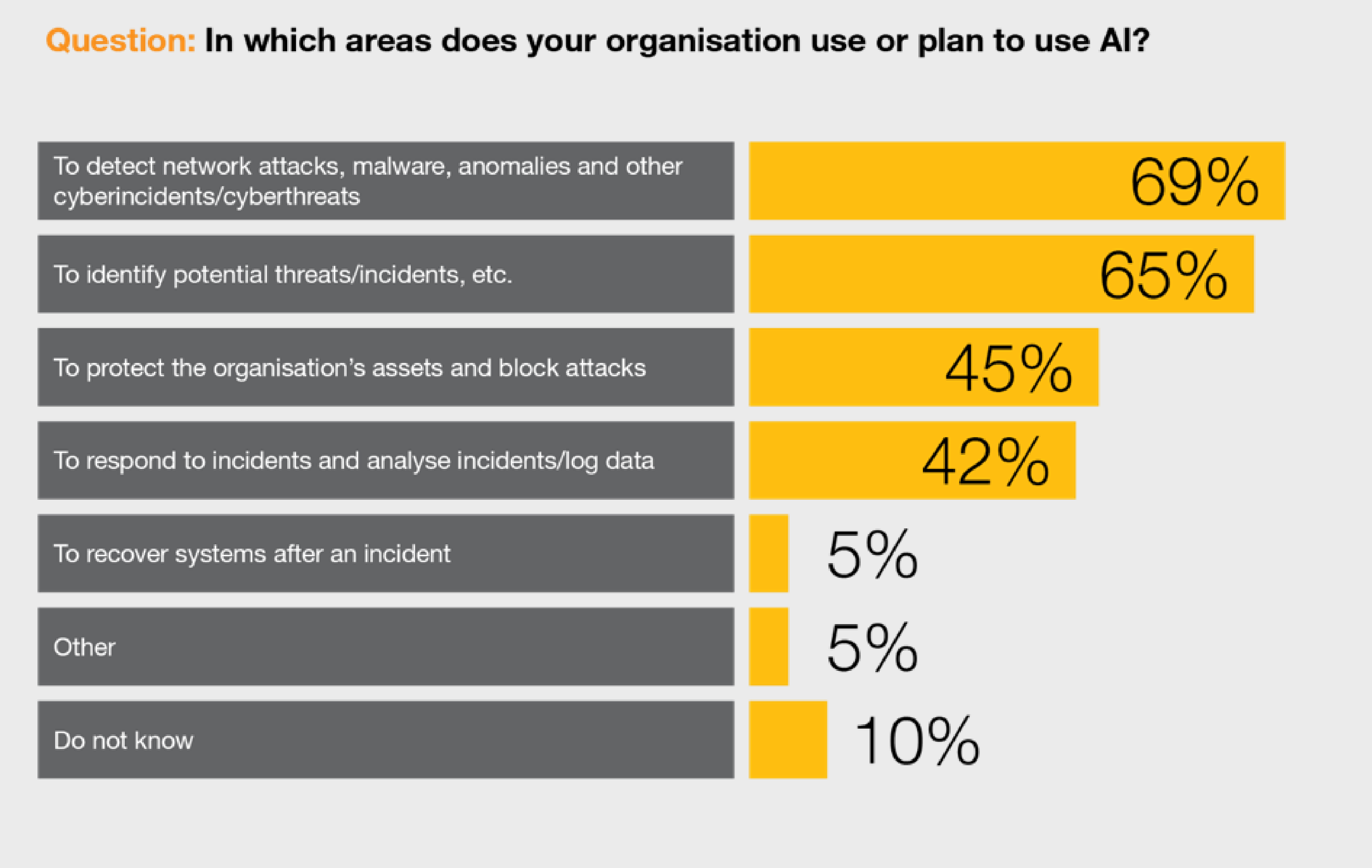
Question: Does your organisation use AI in its cybersecurity efforts?

61 %

of organizations indicate that they either use or plan to implement AI in their cybersecurity strategy. An increase from 43% in 2023.

- **AI is mainly perceived as a preventive measure,** companies primarily view AI as a tool to enhance the detection of cyberattacks.
- Only 5% of respondents consider AI useful for restoring systems after an incident.

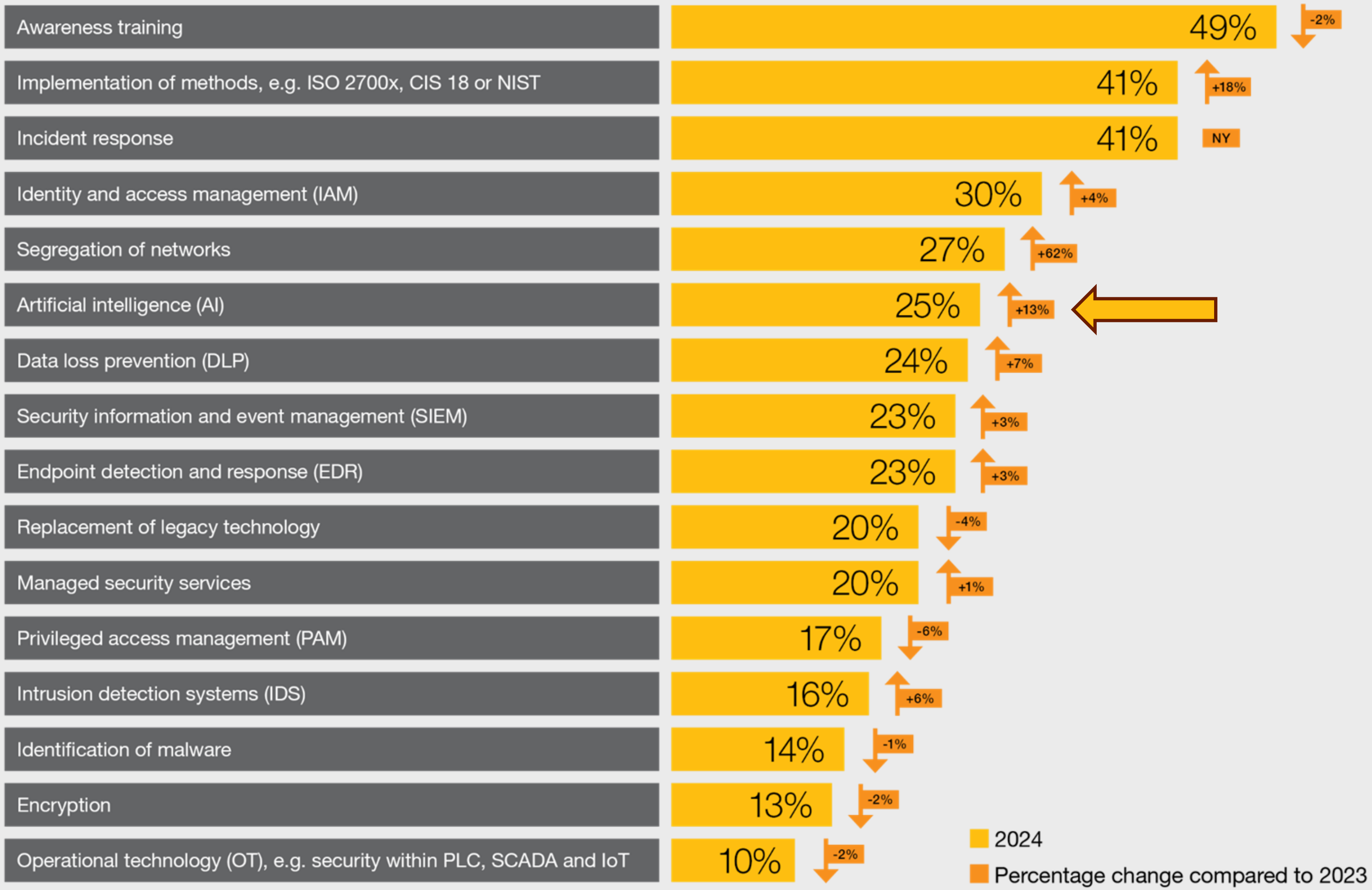
AI has become a much bigger factor in cybersecurity work


Question: In which areas does your organisation use or plan to use AI?

- PwC recommends that companies **integrate AI as a central component of their cybersecurity** strategy.
- **While AI can help detect threats faster** by, identify patterns, and automatically respond to potential security breaches, it is important to **combine AI with human oversight.**

*PwC has developed the “**Responsible AI framework** ” and offers tools and advisory services to help companies build and manage AI in a responsible way.*

Question: What are your organisation's highest-priority investments in IT security over the next 12 months?

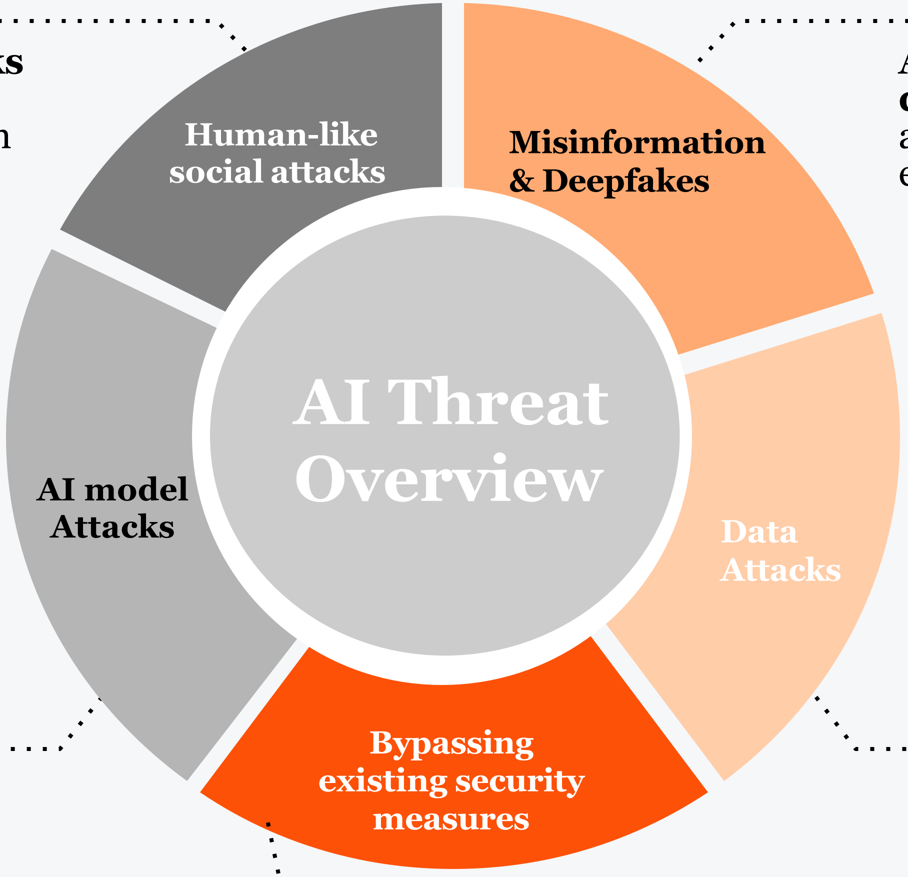


25%

of organizations now consider artificial intelligence (AI) a highest-priority investment in IT security.

It is clear that AI is growing the security threat landscape.

AI is growing the **security threat landscape**



AI Threat Overview

Human-like social attacks

Misinformation & Deepfakes

Data Attacks

Bypassing existing security measures

AI model Attacks

Generative Adversarial Networks (GANs) Attackers leverage AI-generated **fake content** derived from online recordings to **impersonate** individuals aiming to deceive others.

AI systems can generate **high-quality fake content** that appears real, impacting society or economy.

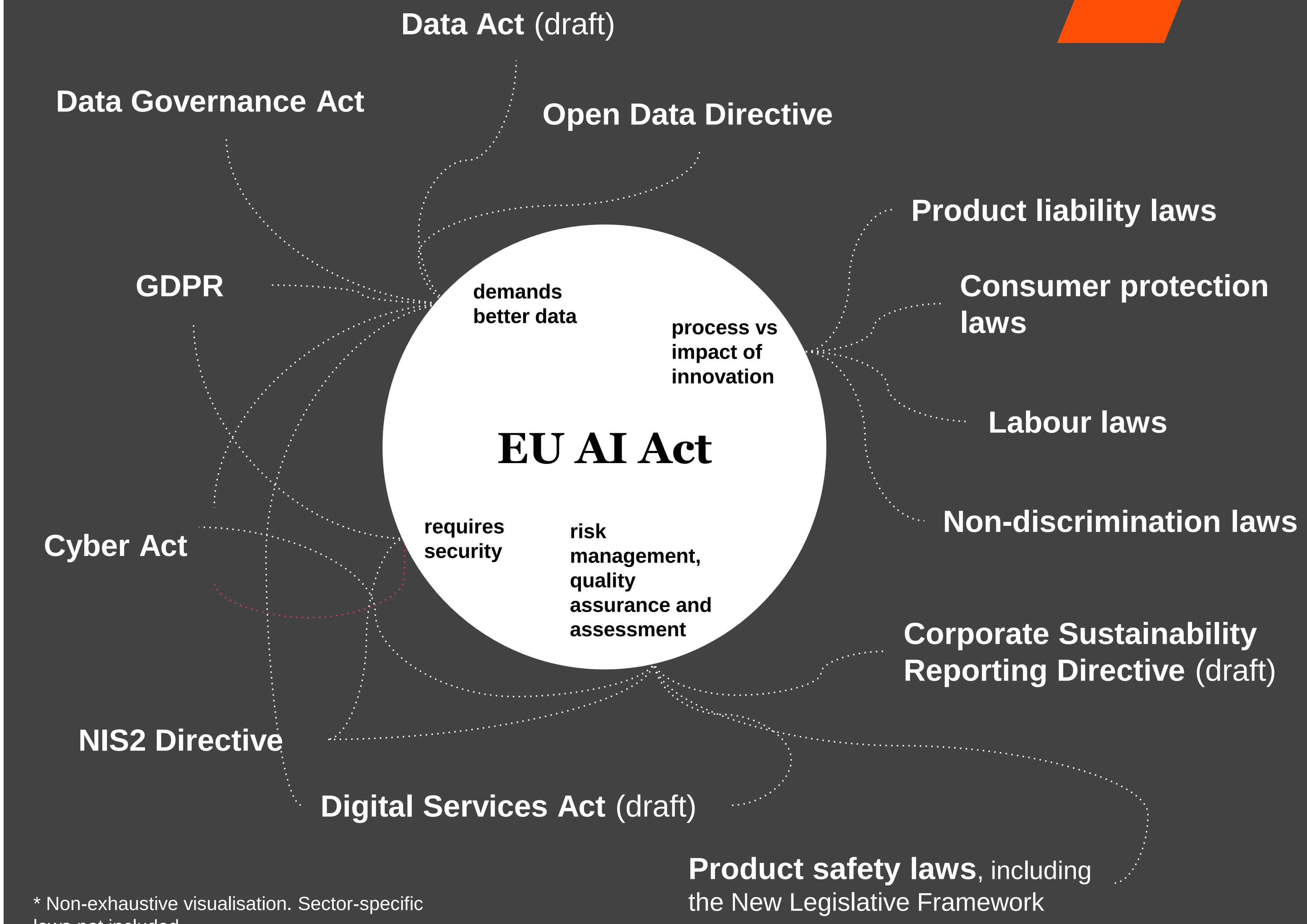
Adversarial attacks are a type of attack in which attackers **manipulate** input data to trick AI models into making mistakes. For example, small changes to an image can cause an image recognition model to classify it incorrectly.

Data Poisoning: Deliberately injecting corrupted data during model training to influence AI behavior.

AI-powered malware can learn from network behaviors and **exfiltrate data** in small, undetectable bursts. Having an AI solution could potentially bypass security measures increasing the risk of **data leakage.**

The AI Act should be viewed in the context of other laws and regulations

Especially the EU Charter of Fundamental rights

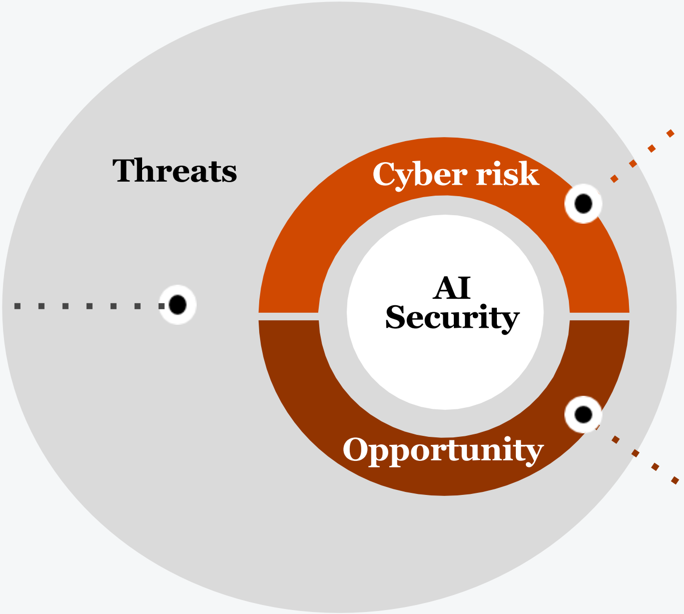

Data Act (draft)
Data Governance Act
Open Data Directive
Product liability laws
GDPR
Consumer protection laws
demands better data
process vs impact of innovation
EU AI Act
Labour laws
Non-discrimination laws
requires security
risk management, quality assurance and assessment
Cyber Act
Corporate Sustainability Reporting Directive (draft)
NIS2 Directive
Digital Services Act (draft)
Product safety laws, including the New Legislative Framework

* Non-exhaustive visualisation. Sector-specific laws not included

Why AI’s acceleration demands oversight

Threat Landscape

- Adversarial attacks include phishing, malware and deepfakes lead to significant risk
- Unauthorized access to AI models can compromise sensitive information and undermine system integrity



Threats

Cyber risk

AI Security

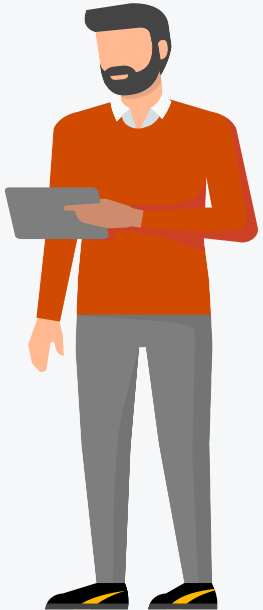
Opportunity

Cyber Security for AI

- Integrate AI-specific risks and controls into existing security governance frameworks
- Establish and enhance security processes and trainings

AI for Cyber Security

- Leverage AI for processing large datasets and documents
- Strengthen defense mechanisms against evolving threats and vulnerabilities



PwC's compliance journey with AI

Presentation by **Nicholas V. Jancey**
May 2025

Who am I?

Nicholas V. Jancey

Nordics & Africa CISO
Responsible for 23 PwC Member Firms,
including PwC Denmark

20 years experience
in Pharma, FMCG & Professional Services

Information Protection Committee

PwC's protection of personal data about individuals and confidential information we hold about our clients and others with whom we do business is critical to maintaining their trust and to comply with laws, regulations and other obligations.

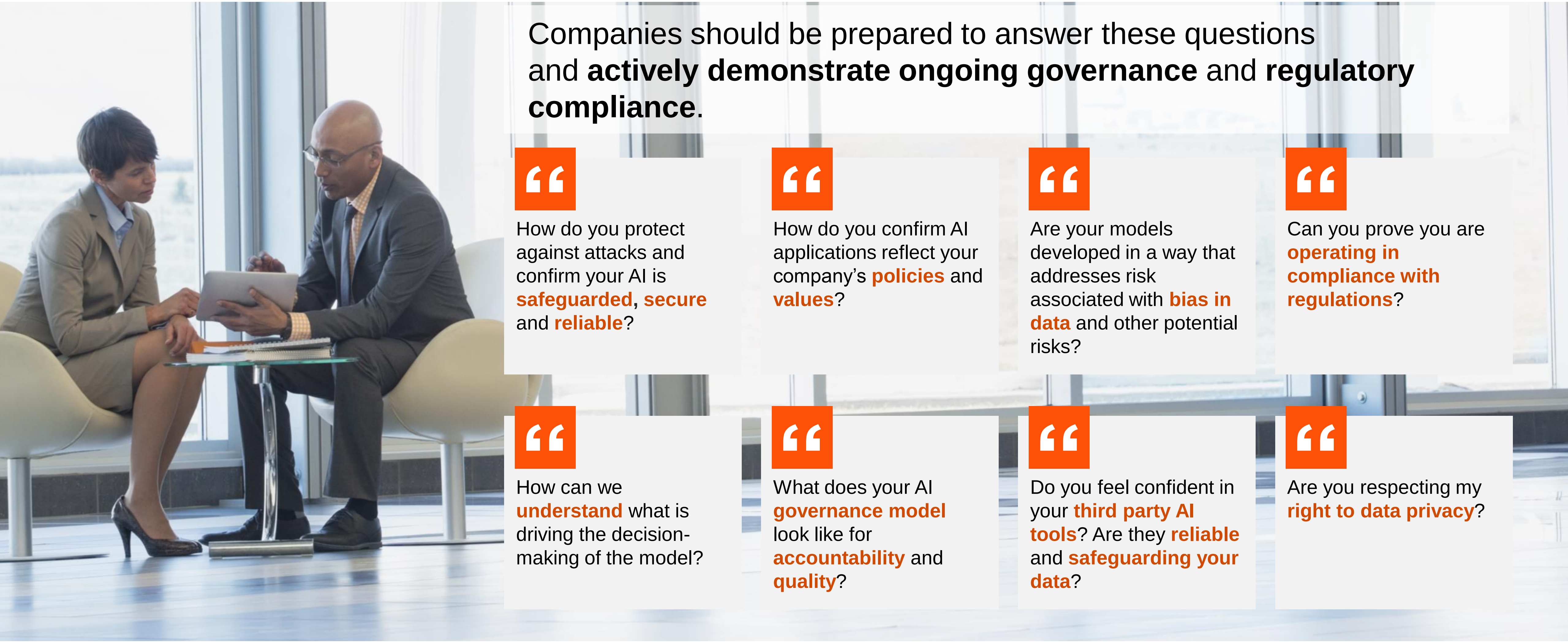
Technology Portfolio Management

PwC's process for registration and evaluation of new technology ensures that any technology in our portfolio is thoroughly documented and tested and is essential for managing the cybersecurity attack surface.

Global & Local compliance

Any new technology in PwC must comply with both global PwC policies and standards, as well as local legislation. There are many different compliance process that a new technology owner must navigate.

As AI adoption continues to accelerate, companies should address common questions around managing the risks of AI



Companies should be prepared to answer these questions and **actively demonstrate ongoing governance** and **regulatory compliance**.

How do you protect against attacks and confirm your AI is **safeguarded**, **secure** and **reliable**?

How do you confirm AI applications reflect your company's **policies** and **values**?

Are your models developed in a way that addresses risk associated with **bias in data** and other potential risks?

Can you prove you are **operating in compliance with regulations**?

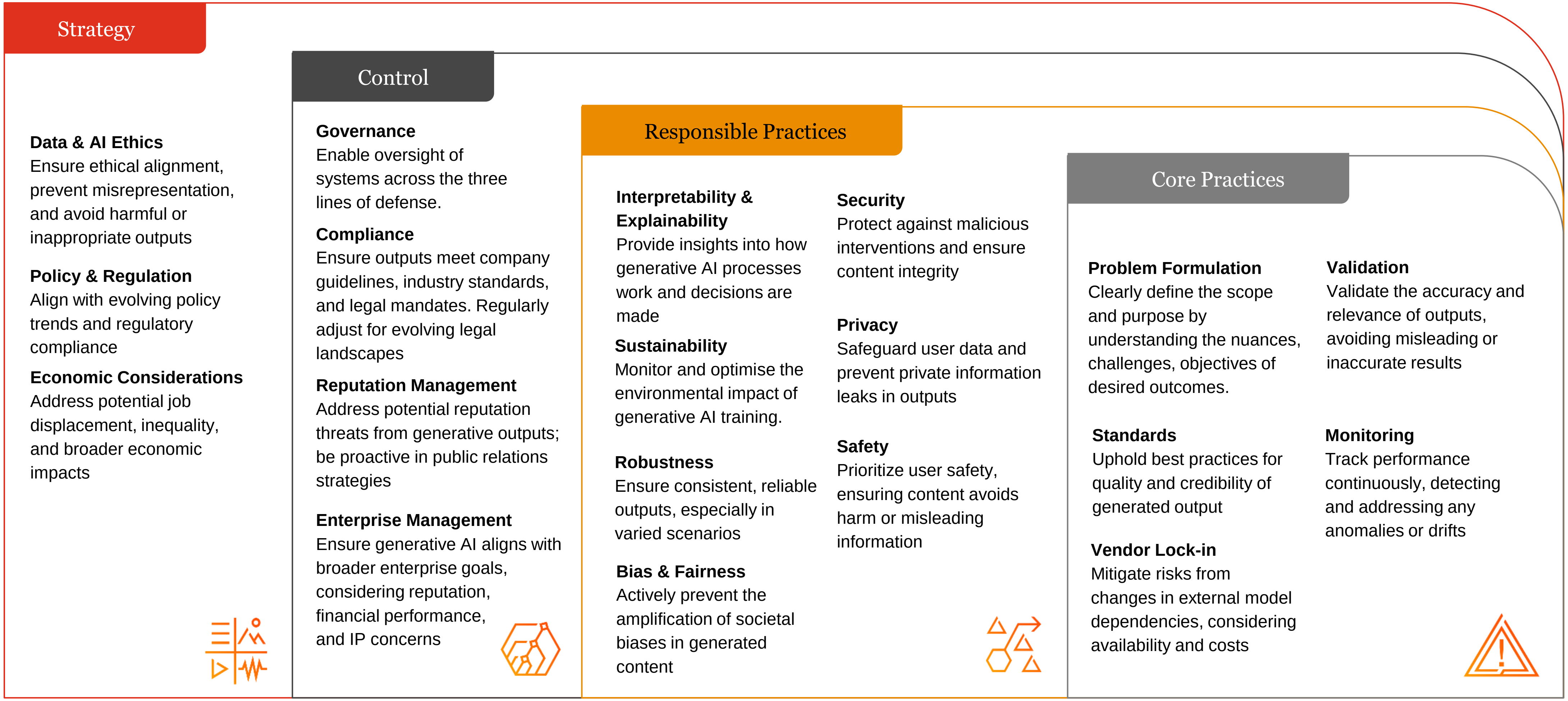
How can we **understand** what is driving the decision-making of the model?

What does your AI **governance model** look like for **accountability** and **quality**?

Do you feel confident in your **third party AI tools**? Are they **reliable** and **safeguarding your data**?

Are you respecting my **right to data privacy**?

PwC’s Responsible AI framework



Strategy

Data & AI Ethics
Ensure ethical alignment, prevent misrepresentation, and avoid harmful or inappropriate outputs

Policy & Regulation
Align with evolving policy trends and regulatory compliance

Economic Considerations
Address potential job displacement, inequality, and broader economic impacts

Control

Governance
Enable oversight of systems across the three lines of defense.

Compliance
Ensure outputs meet company guidelines, industry standards, and legal mandates. Regularly adjust for evolving legal landscapes

Reputation Management
Address potential reputation threats from generative outputs; be proactive in public relations strategies

Enterprise Management
Ensure generative AI aligns with broader enterprise goals, considering reputation, financial performance, and IP concerns

Responsible Practices

Interpretability & Explainability
Provide insights into how generative AI processes work and decisions are made

Sustainability
Monitor and optimise the environmental impact of generative AI training.

Robustness
Ensure consistent, reliable outputs, especially in varied scenarios

Bias & Fairness
Actively prevent the amplification of societal biases in generated content

Security
Protect against malicious interventions and ensure content integrity

Privacy
Safeguard user data and prevent private information leaks in outputs

Safety
Prioritize user safety, ensuring content avoids harm or misleading information

Core Practices

Problem Formulation
Clearly define the scope and purpose by understanding the nuances, challenges, objectives of desired outcomes.

Standards
Uphold best practices for quality and credibility of generated output

Vendor Lock-in
Mitigate risks from changes in external model dependencies, considering availability and costs

Validation
Validate the accuracy and relevance of outputs, avoiding misleading or inaccurate results

Monitoring
Track performance continuously, detecting and addressing any anomalies or drifts

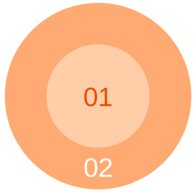
AI Ecosystem Building Blocks

We enable AI across every layer — from core infra, to AI agents & everyday assistants

PwC powers our enterprise **AI ecosystem** to drive **outcomes** for our clients, people and business.

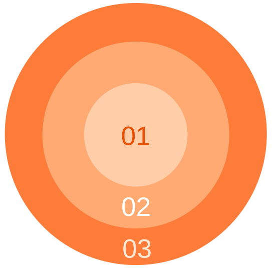
01. AI Core Data – Secure foundation to build and run AI at scale

Infrastructure	Cloud, Identify, Data Security
Models Access	Open AI, Google, Anthropic, Open Source
AI Dev Tools	Agent OS, CoPilot Studio, Azure AI



02. AI Tools & Agents – Smart tools that save time and amplify work

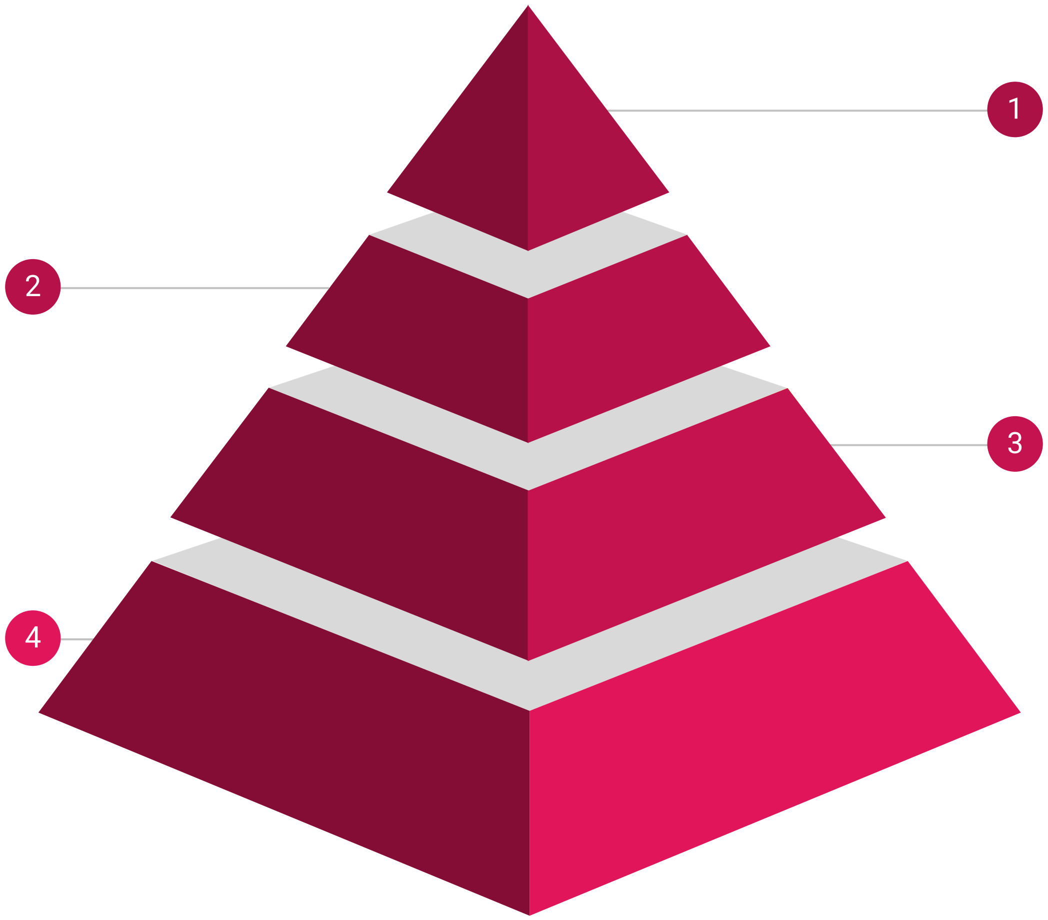
Client Service Delivery Tools	Audit, Tax, Advisory Delivery Agents
Vendor Tools	Harvey, Github CoPilot, Cursor, Phenom
PwC-Built Internal Agents	GC Learning Coach, Data Analyst, Resume Reviewer



03. AI Assistants & Applications – Where AI shows up in daily work

PwC-Built Everyday Assistants	ChatPwC, Astro (US)
Vendor AI Assistants	GPT-E (US & UK), CoPilot
AI Embedded in Enterprise Apps	Salesforce, ServiceNow, NGA, Concourse, etc.

EU AI Act



Unacceptable risk

All AI systems considered a clear threat to the safety, livelihoods and rights of people will be banned from social scoring by governments to toys using voice assistance that encourages dangerous behavior.

High risk

AI systems identified as high-risk include AI technology used in areas such as Critical infrastructures, Access to Education, Employment, Safety components, Law enforcement, migration and border control

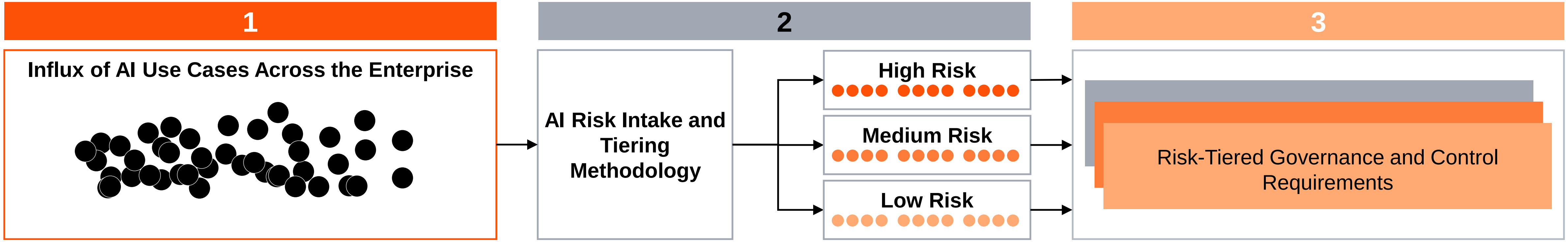
Limited risk

Duty to provide transparency such as labelling, or disclosure that content has been manipulated. Examples include: Chatbots, Emotion recognition and biometric categorisation systems.

Minimal risk

Applications such as spam filters or AI-enabled video games. The Commission proposes that these are mainly regulated by voluntary codes of conduct.

The AI risk intake and tiering methodology is a core requirement for effective and efficient AI governance and risk management



1

Influx of AI Use Cases Across the Enterprise

2

AI Risk Intake and Tiering Methodology

High Risk

Medium Risk

Low Risk

3

Risk-Tiered Governance and Control Requirements

1

Institutions are preparing for or are already facing a **large influx of internally developed or vendor-provided AI use cases**

Each use case's **inherent riskiness may be different** depending on characteristics such as the type of data used (e.g., PII vs. public), user type (internal vs. customer-facing) and area of use (e.g., embedded in product vs. internal process)

2

In line with expectations set by bodies such as **NIST, ISO and the EU AI Act**, institutions need to establish an **AI risk intake and tiering** methodology and process

This methodology must be able to **objectively and efficiently identify** the key risk factors relevant to a use case and designate a **risk tier based on the attributed risk factors**

The goal of this methodology is to **right-size governance requirements** for the inherent risk created by the use case

3

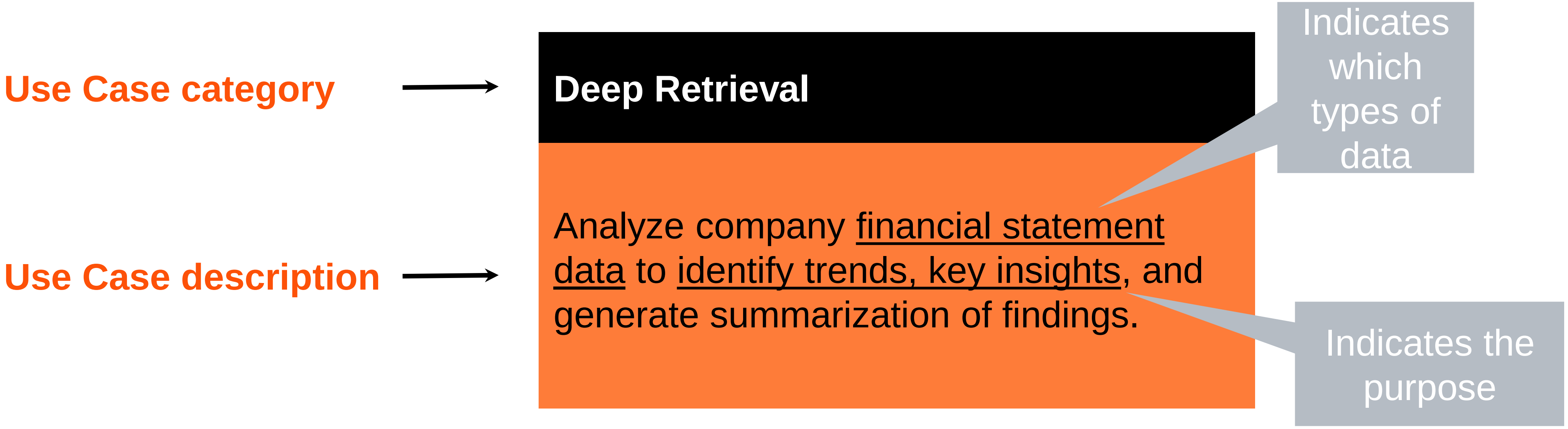
The risk tier and contributing factors then determine **which downstream assessments should be triggered** and which functions should be tagged (e.g., Legal, Cyber, Privacy) for additional review based on specific risk characteristics

This approach helps determine where **additional control and mitigation** is needed, and where use cases can be **deployed more quickly through lighter governance**

Use Case categories

Summarization	Deep Retrieval	Transformation	Augmentation	Q&A (dialogue)	Net-new Creation
Producing an abbreviated form of a given document, coded program, or other body of text.	Searching for specific information within a given document or set of documents.	Creating a transformed version of data, such as image style transfer, text translation, or text personalization.	Expanding upon existing content, such as auto complete or synthetic data creation.	Responding to a given question. Chatbots, service bots, and virtual assistants support Q&A.	Generating net new content based on a user provided prompt (instruction).
No-Go use cases	No-Go use cases	No-Go use cases	No-Go use cases	No-Go use cases	No-Go use cases

Example Use Case



Use Case category

Use Case description

Deep Retrieval

Analyze company financial statement data to identify trends, key insights, and generate summarization of findings.

Indicates which types of data

Indicates the purpose

Inherent Risks with any Use Case

- Model bias
- Overreliance
- Unauthorised Secondary Use of Data
- Infringement of 3rd party IP
- Disclosure of PwC IP, confidential information and personal data

To be addressed through controls in the specific technology implementation

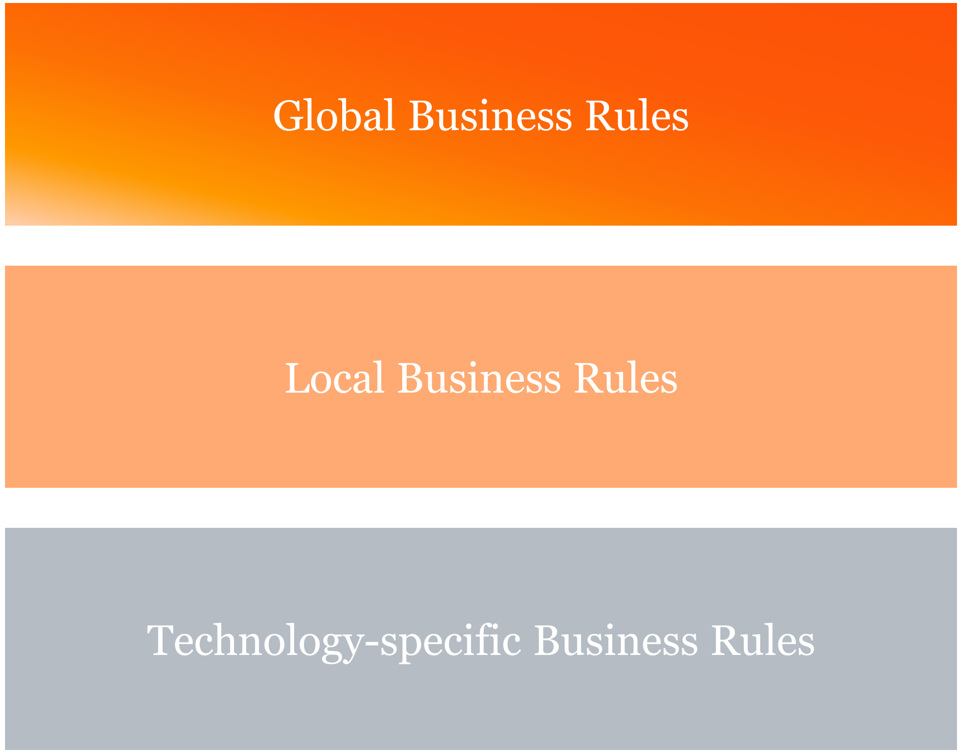
Business Rules

Non-technical controls

PwC applies non-technical controls to the use of AI through a hierarchy of Business Rules.

These rules contain the following:

- Required training
- Ethical values to apply to usage
- Data types that can be used, e.g. client data, PII, etc.
- Data classifications allowed
- Required verification and accuracy checks
- Areas of Attention, e.g. IP infringement risks, etc.



Global Business Rules

Local Business Rules

Technology-specific Business Rules

PwC AI Technology onboarding

Technology-specific controls

PwC applies a baseline of technical controls to each technology implementation.

Furthermore, each technology must go through the following steps:

- Registration
- Risk tiering – business criticality, data classification & Internet exposure
- Architecture Review
- Security testing – penetration testing, vulnerability scanning, etc.
- Code review & scanning (if applicable)
- Data Protection Risk Assessment
- Data Protection Impact Assessment (if applicable)
- Access Control model
- Business Continuity Plan

Pre-requisites for M365 Copilot

Understand the importance of data classification

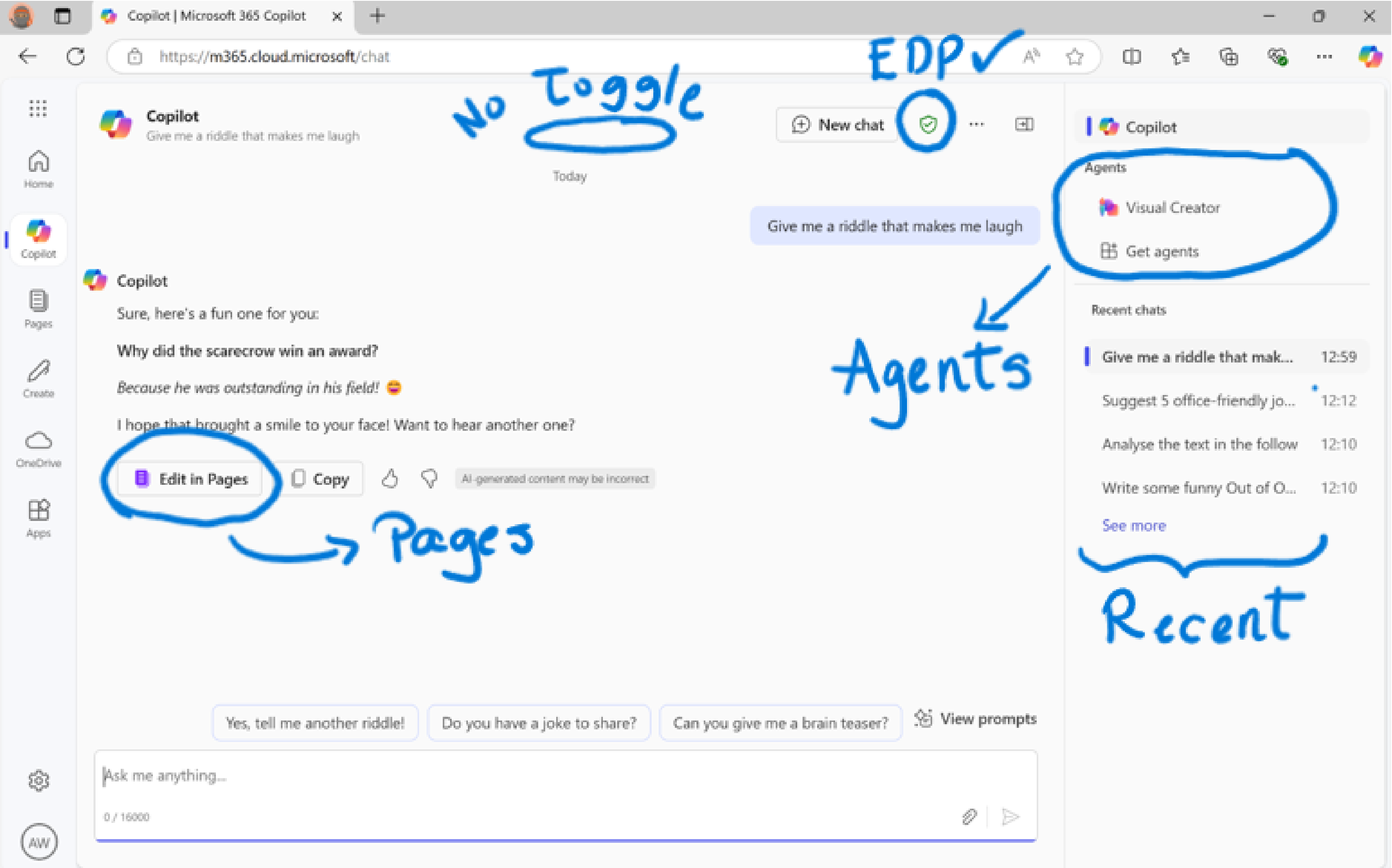
Data Classification is essential to consider prior to implementing M365 Copilot, as it is grounded in user data.

PwC implemented Data Classification using Azure Information Protection which is now Purview, in relation to the Confidentiality of data.

Purview allows the implementation of policies to exclude data, based on its classification, from processing by M365 Copilot.

What is Microsoft 365 Copilot Chat?

Copilot Chat is included at no additional cost within the M365 business subscription.


Copilot | Microsoft 365 Copilot
https://m365.cloud.microsoft/chat
EDP✓
No Toggle
Copilot
Give me a riddle that makes me laugh
New chat
Today
Home
Copilot
Pages
Create
OneDrive
Apps
AW
Copilot
Agents
Visual Creator
Get agents
Recent chats
Give me a riddle that mak... 12:59
Suggest 5 office-friendly jo... 12:12
Analyse the text in the follow 12:10
Write some funny Out of O... 12:10
See more
Agents
Recent
Edit in Pages
Copy
AI-generated content may be incorrect
Pages
Yes, tell me another riddle!
Do you have a joke to share?
Can you give me a brain teaser?
View prompts
Ask me anything...
0 / 16000

Give me a riddle that makes me laugh

Copilot

Sure, here's a fun one for you:

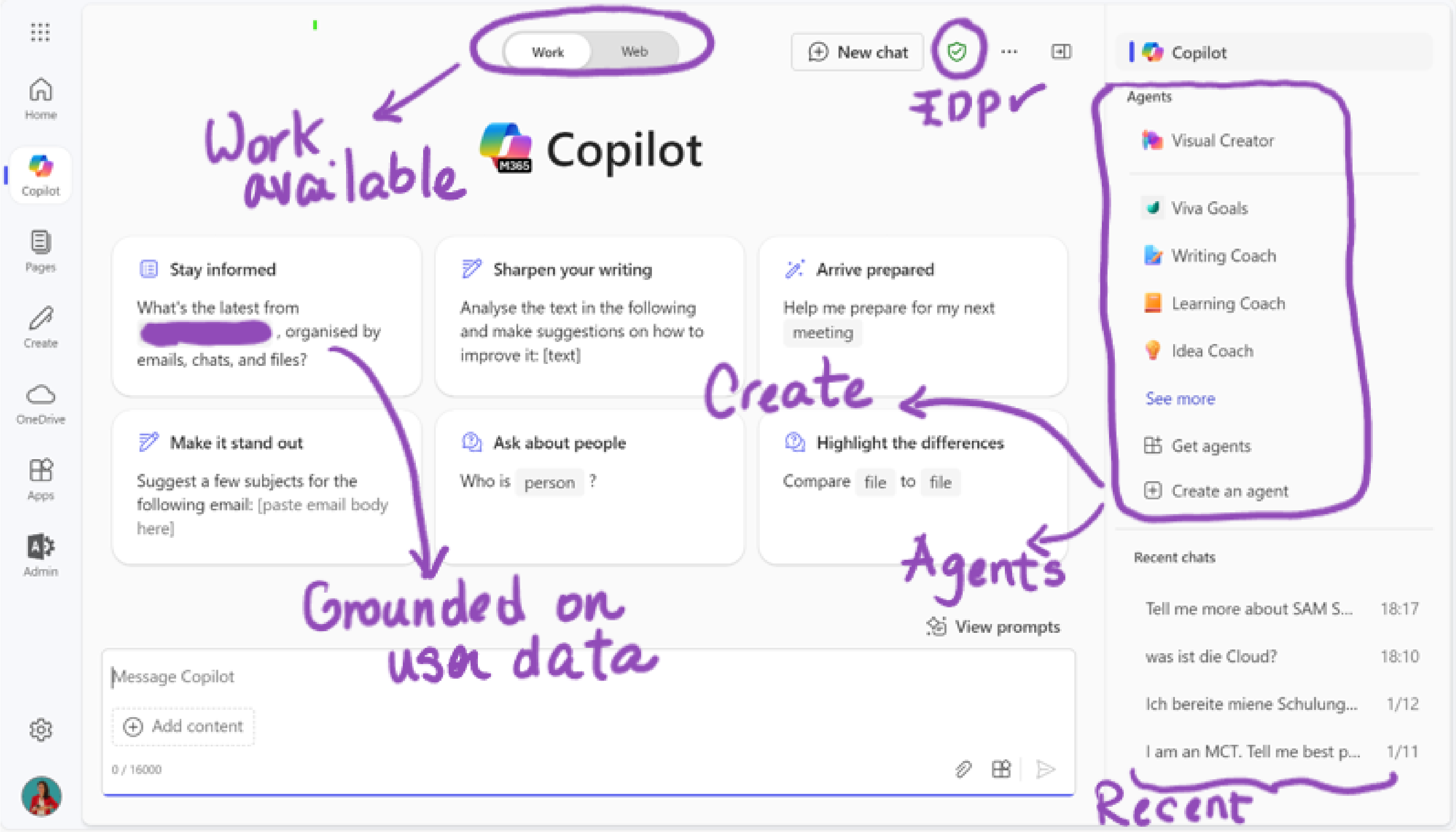
Why did the scarecrow win an award?

Because he was outstanding in his field! 😄

I hope that brought a smile to your face! Want to hear another one?

What is Microsoft 365 Copilot?

M365 Copilot is an add-on available for specific Microsoft 365 subscription with a license to be activated on top.



Stay informed

What's the latest from [redacted], organised by emails, chats, and files?

Sharpen your writing

Analyse the text in the following and make suggestions on how to improve it: [text]

Arrive prepared

Help me prepare for my next meeting

Make it stand out

Suggest a few subjects for the following email: [paste email body here]

Ask about people

Who is person ?

Highlight the differences

Compare file to file

Message Copilot

Tell me more about SAM S... 18:17

was ist die Cloud? 18:10

Ich bereite miene Schulung... 1/12

I am an MCT. Tell me best p... 1/11

Work available

EDP ✓

Create

Agents

Grounded on user data

Recent

PwC

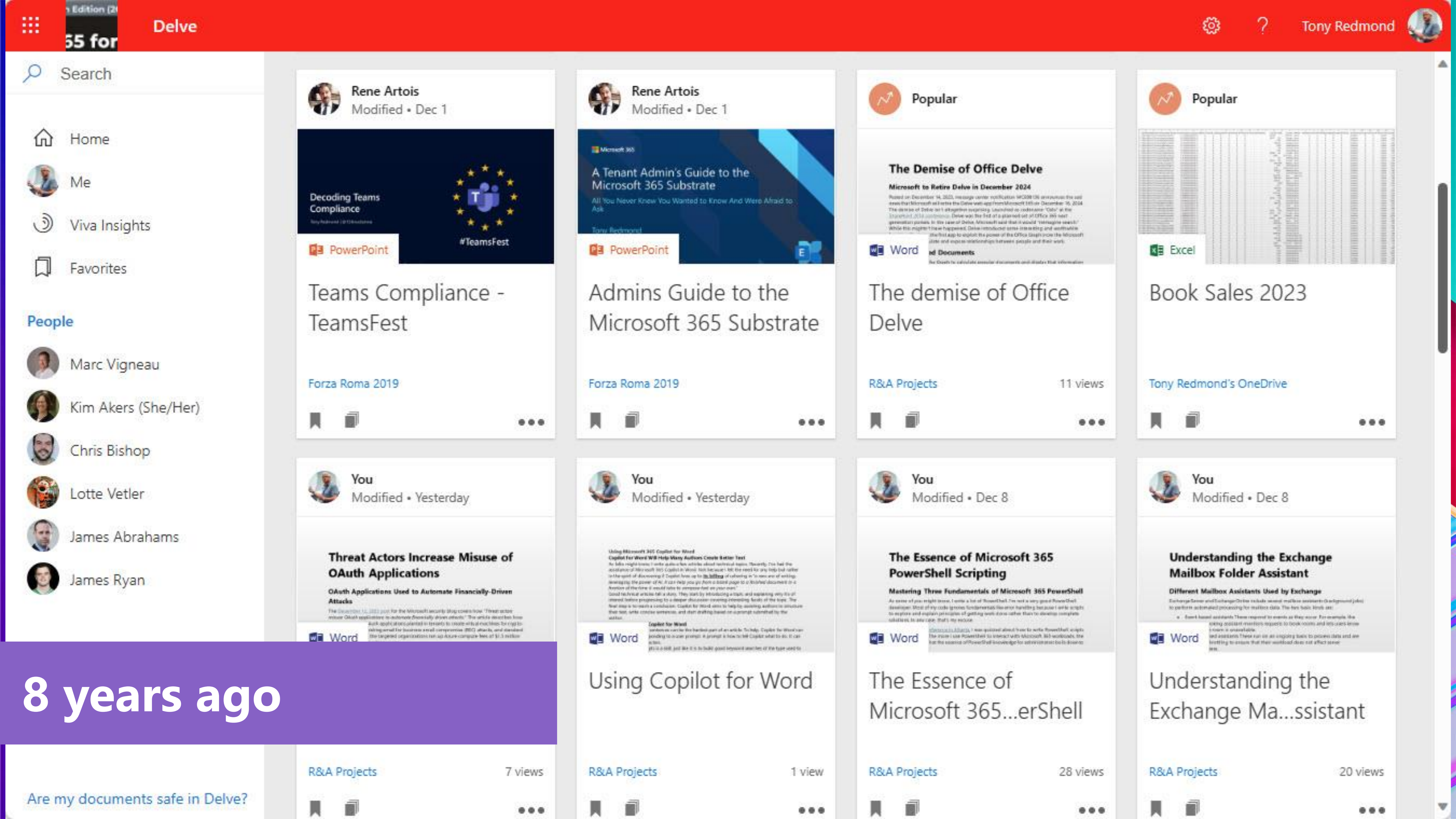
Microsoft

Security in the Age of AI

Kristoffer Rosenmeier, Microsoft

1. What does AI mean for our data security?

2. How can AI be used to improve our security?



Rene Artois
Modified • Dec 1
Decoding Teams Compliance
#TeamsFest
PowerPoint
Teams Compliance - TeamsFest
Forza Roma 2019

Rene Artois
Modified • Dec 1
A Tenant Admin's Guide to the Microsoft 365 Substrate
All You Never Knew You Wanted to Know And Were Afraid to Ask
PowerPoint
Admins Guide to the Microsoft 365 Substrate
Forza Roma 2019

Popular
The Demise of Office Delve
Microsoft to Retire Delve in December 2024
Word
The demise of Office Delve
R&A Projects
11 views

Popular
Excel
Book Sales 2023
Tony Redmond's OneDrive

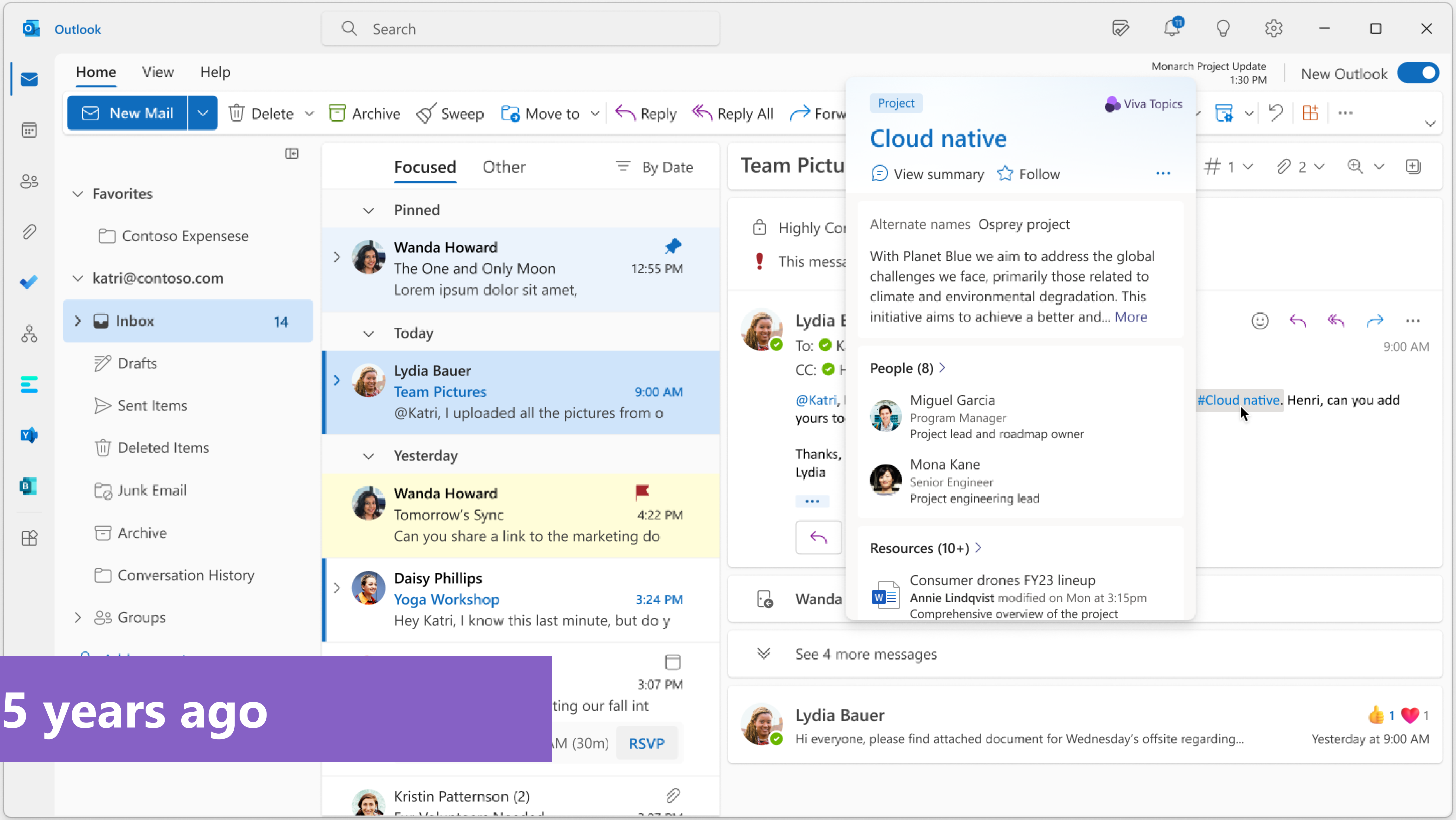
You
Modified • Yesterday
Threat Actors Increase Misuse of OAuth Applications
OAuth Applications Used to Automate Financially-Driven Attacks
Word
R&A Projects
7 views

You
Modified • Yesterday
Word
Using Copilot for Word
R&A Projects
1 view

You
Modified • Dec 8
The Essence of Microsoft 365 PowerShell Scripting
Mastering Three Fundamentals of Microsoft 365 PowerShell
Word
The Essence of Microsoft 365...erShell
R&A Projects
28 views

You
Modified • Dec 8
Understanding the Exchange Mailbox Folder Assistant
Different Mailbox Assistants Used by Exchange
Word
Understanding the Exchange Ma...ssistant
R&A Projects
20 views

8 years ago



Wanda Howard
The One and Only Moon 12:55 PM
Lorem ipsum dolor sit amet,

Lydia Bauer
Team Pictures 9:00 AM
@Katri, I uploaded all the pictures from o

Wanda Howard
Tomorrow's Sync 4:22 PM
Can you share a link to the marketing do

Daisy Phillips
Yoga Workshop 3:24 PM
Hey Katri, I know this last minute, but do y

3:07 PM
ting our fall int
M (30m)

Kristin Patternson (2)

Team Pictu

Highly Co

This messa

Lydia B
To: K
CC: H
9:00 AM

@Katri, #Cloud native. Henri, can you add yours to

Thanks,
Lydia

Wanda

Lydia Bauer
Hi everyone, please find attached document for Wednesday's offsite regarding...
1 1
Yesterday at 9:00 AM

Cloud native

Alternate names Osprey project

With Planet Blue we aim to address the global challenges we face, primarily those related to climate and environmental degradation. This initiative aims to achieve a better and... More

Miguel Garcia
Program Manager
Project lead and roadmap owner

Mona Kane
Senior Engineer
Project engineering lead

Consumer drones FY23 lineup
Annie Lindqvist modified on Mon at 3:15pm
Comprehensive overview of the project

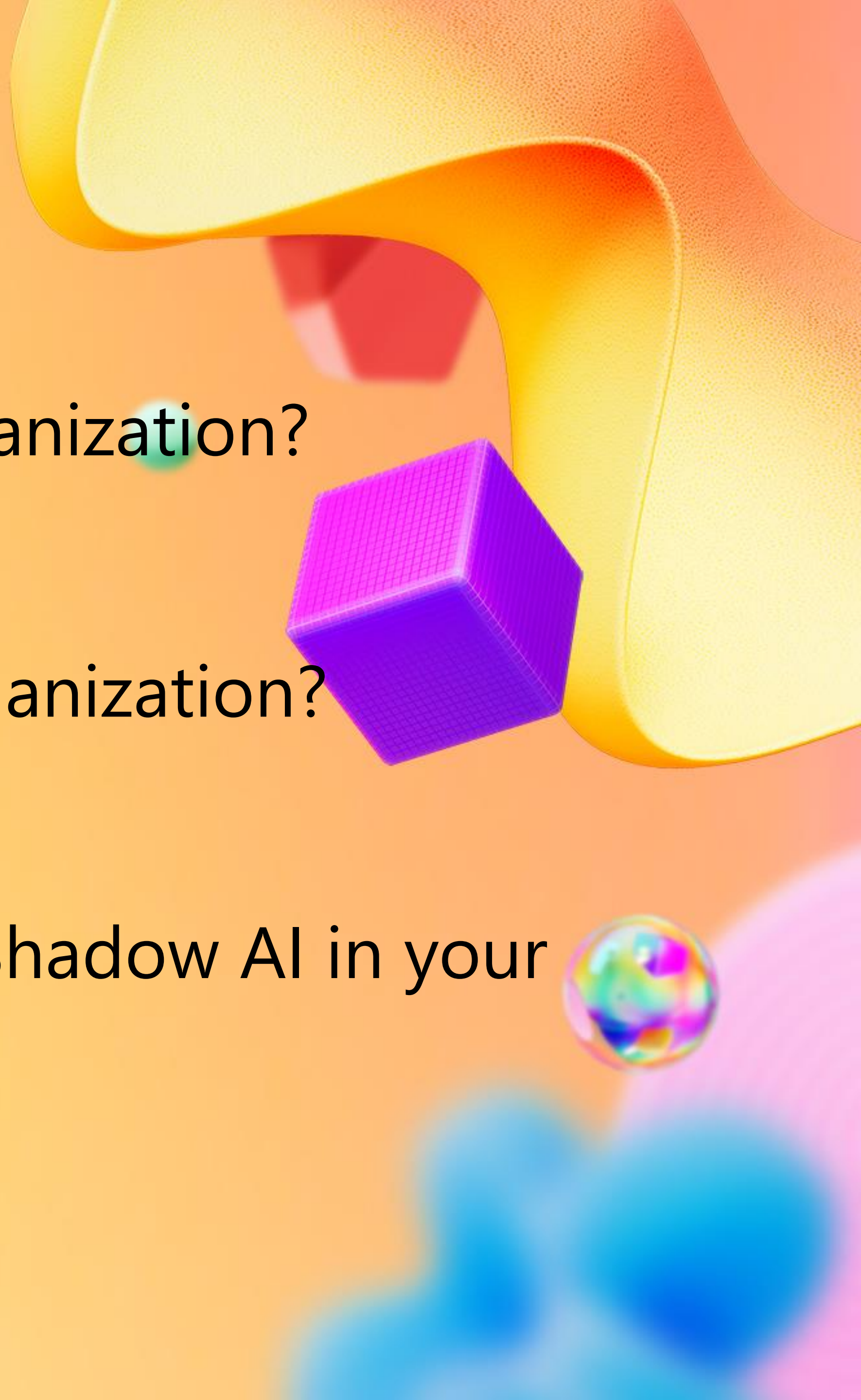
5 years ago

Your AI assistant for work

Last year

Conversation starters

- How do you secure the use of AI in your organization?
- How do you govern the use of AI in your organization?
- How do you monitor and secure the use of Shadow AI in your organization?



Conversation starters

- “We don’t have to, since we’ve built our own”

- “We don’t have to, we’re using a third party enterprise app”

- “We have a policy that states how employees should use Gen AI”

- “We trust our employees”

Top security and governance concerns about generative AI

Data oversharing and data leaks

80%

of leaders cited leakage of sensitive data as their main concern[1]

Identification of risky AI use

41%

of security leaders cited that the identification of risky users based on queries into AI was one of the top AI controls they want to implement[2]

AI governance and risk visibility

84%

Want to feel more confident about managing and discovering data input into AI apps and tools[2]

[1] First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

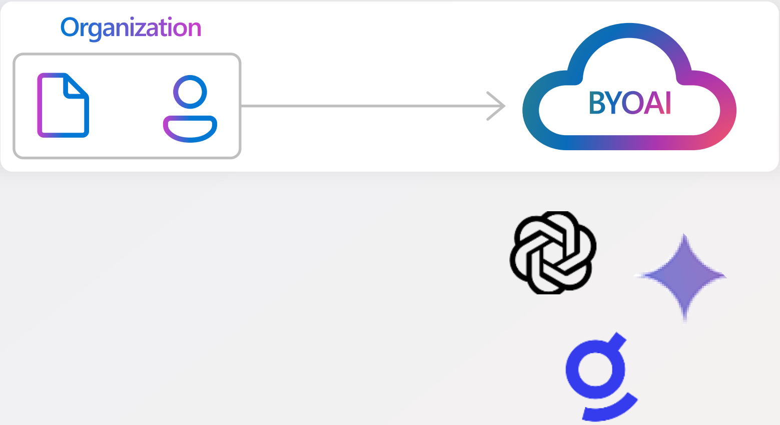
[2] Microsoft data security index 2024 report

Typical customer concerns

Shadow AI

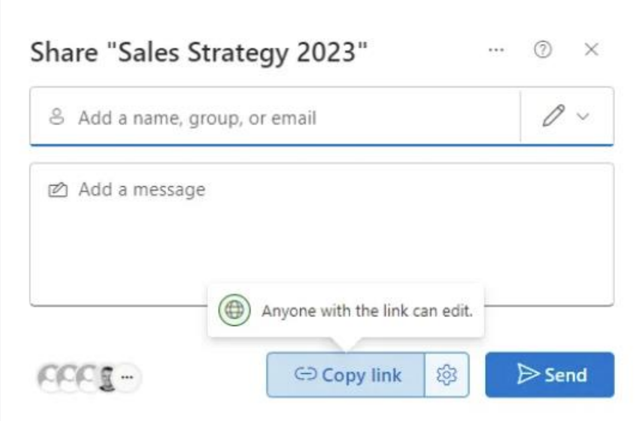
Sensitive data (e.g. PII, IP) might be shared with Shadow AI apps, creating risk of:

- Leakage
- Malicious use
- To train 3rd party algorithms



Oversharing

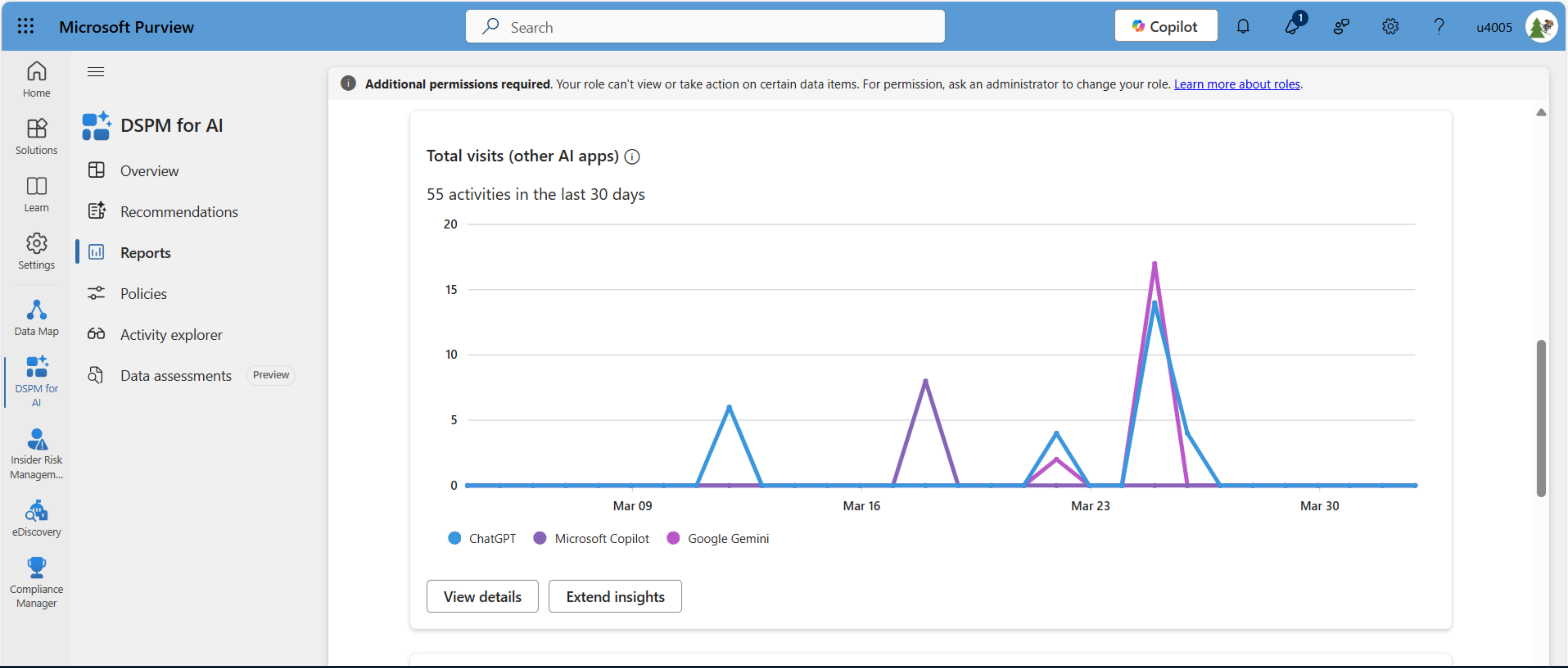
Organizations are worried about the risks of data oversharing and leaks, fearing that GenAI tools might provide quicker access to content without proper permissions, thereby making sensitive files easier to find


Share "Sales Strategy 2023"

Add a name, group, or email

Add a message

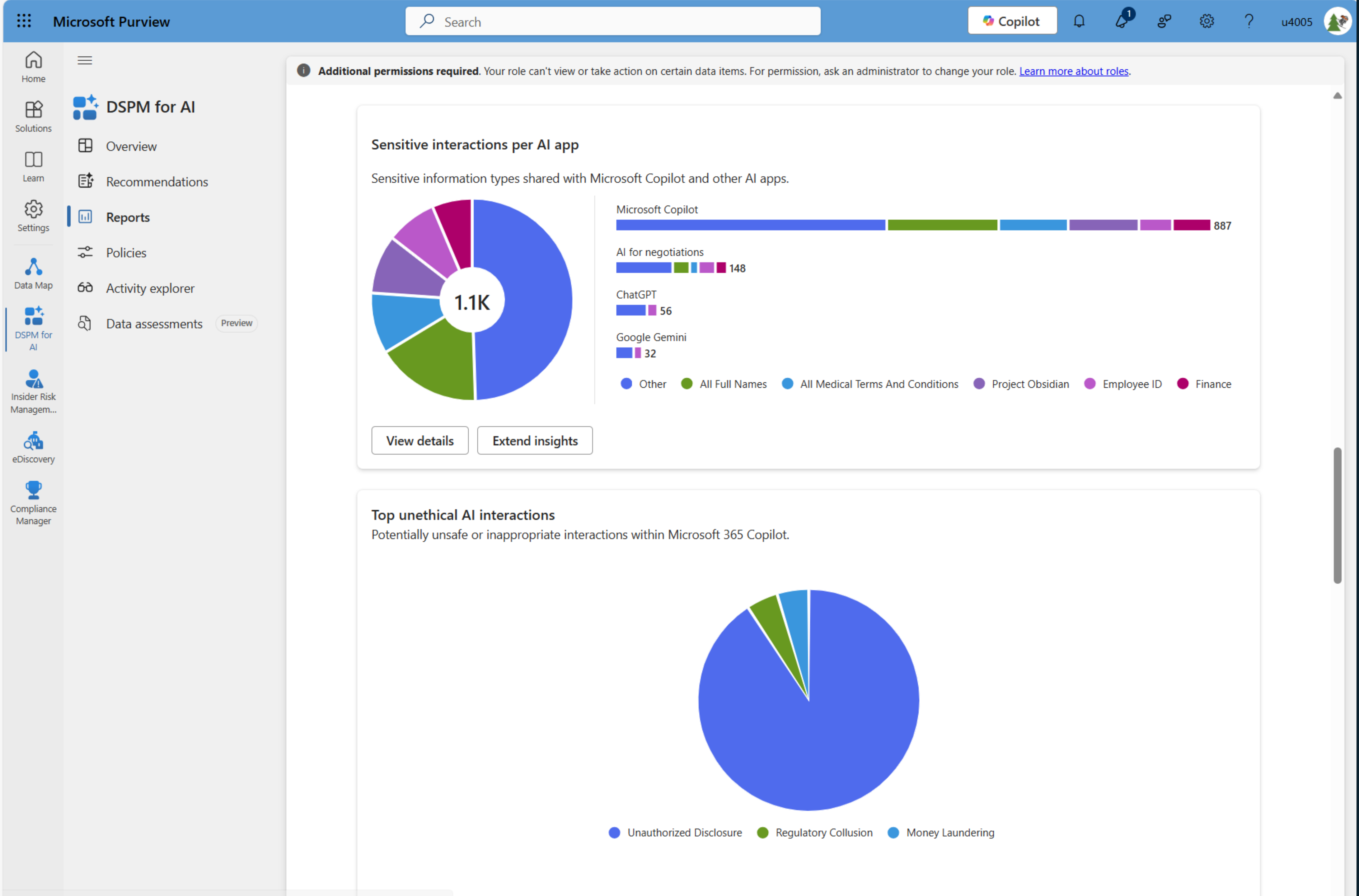
Anyone with the link can edit.



Additional permissions required. Your role can't view or take action on certain data items. For permission, ask an administrator to change your role. Learn more about roles.

Total visits (other AI apps)

55 activities in the last 30 days



Additional permissions required. Your role can't view or take action on certain data items. For permission, ask an administrator to change your role. Learn more about roles.

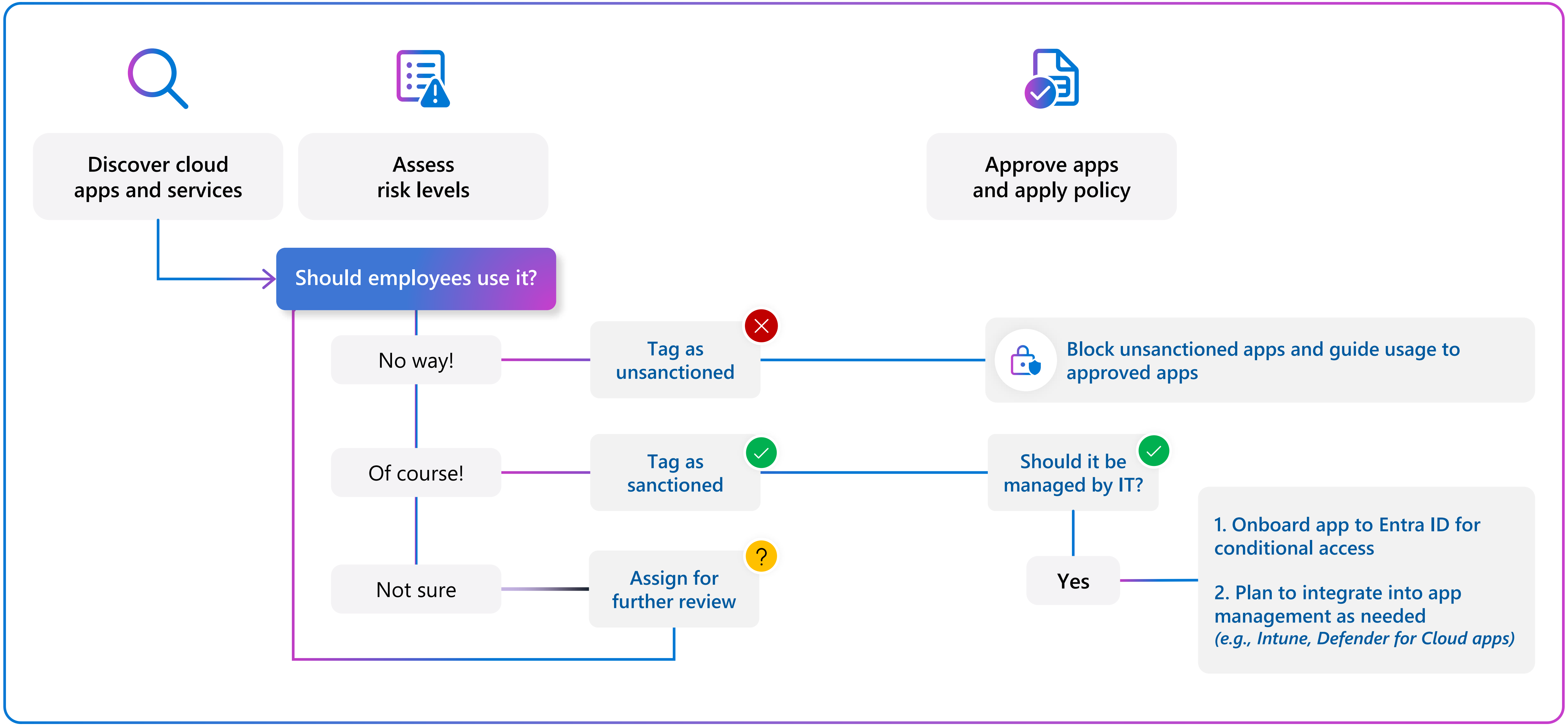
Sensitive interactions per AI app

Sensitive information types shared with Microsoft Copilot and other AI apps.

Top unethical AI interactions

Potentially unsafe or inappropriate interactions within Microsoft 365 Copilot.

Discover and manage apps in your environment



Discover cloud apps and services

Assess risk levels

Approve apps and apply policy

Should employees use it?

No way!

Tag as unsanctioned

Block unsanctioned apps and guide usage to approved apps

Of course!

Tag as sanctioned

Should it be managed by IT?

Yes

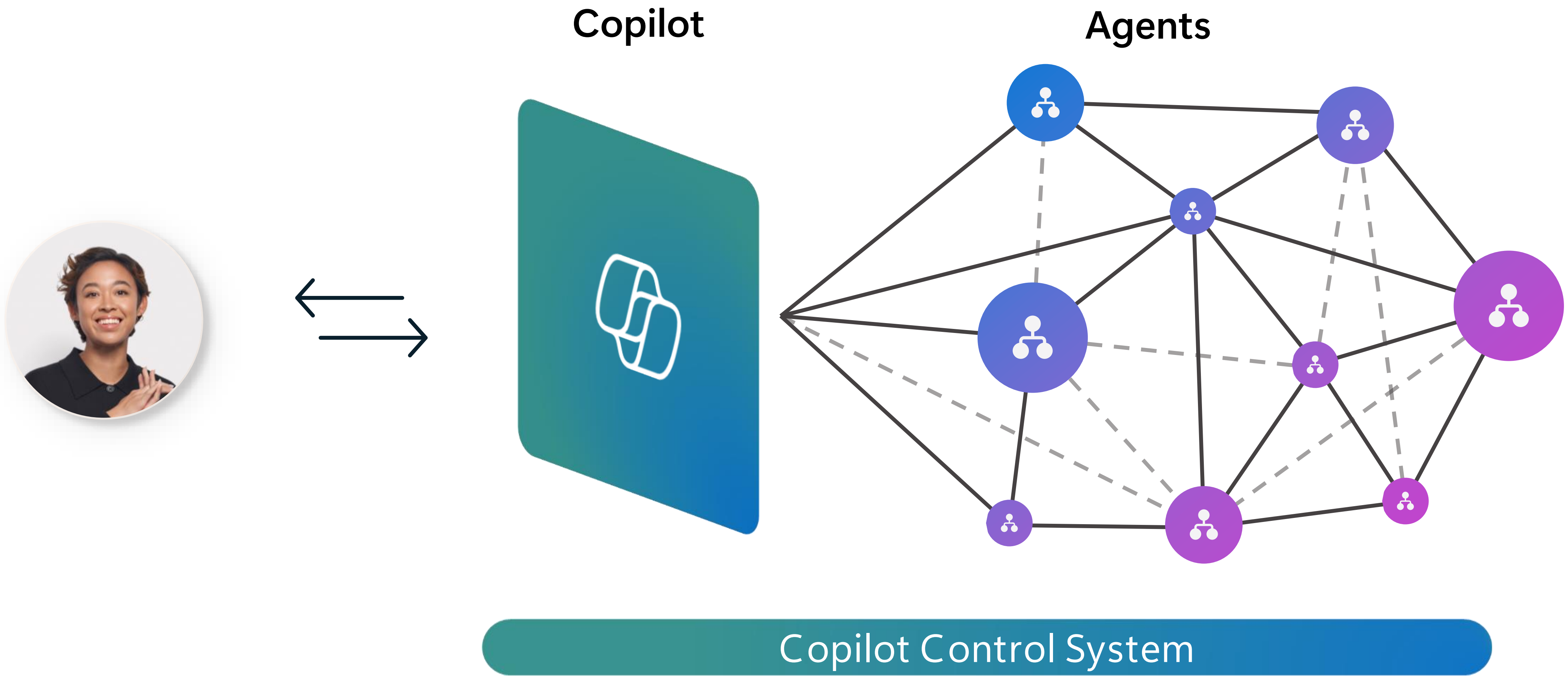
1. Onboard app to Entra ID for conditional access

2. Plan to integrate into app management as needed *(e.g., Intune, Defender for Cloud apps)*

Not sure

Assign for further review

Copilot is the UI for AI



M365

Microsoft 365 Copilot is built on trust

Microsoft commitments and controls

Tools to manage your data

M365 Copilot – Compliance Certifications

● Included	Microsoft 365 Copilot & Chat
SOC2 Type 1	●
SOC2 Type 2	In Progress
ISO 27001	●
ISO 27017	●
ISO 27018	●
ISO 27701	●
ISO 9001	N/A[1]
ISO 42001	●
CSA STAR	In Progress[2]
GDPR	●
CCPA	●
HIPAA	●
FedRAMP High	In Progress[3]
BSI C5	●

[1] Our other ISO certifications cover ISO 9001 clauses, as stated in customer-facing footnote. So far, we haven't seen customer demand for ISO 9001 certification, which focuses on quality management systems. If Marketing and CxE teams see demand for ISO 9001, we can then plan and resource accordingly.

[2] Like other M365 services, Microsoft 365 Copilot and Copilot Chat meet the requirements of the CSA STAR. We are planning to update our current CSA STAR attestation to formally include Microsoft 365 Copilot in the scope by Q3 CY25.

[3] Microsoft 365 Copilot and Copilot Chat are in the process of securing Fed RAMP High certification, with completion anticipated by Q4 CY25.

Microsoft commitments and controls

We secure your data at rest and in transit

You control your data

Your data is not used to train or enrich foundation models

You're protected against AI security and copyright risks[1]

M365

Microsoft 365 Copilot is built on trust

[1] Learn more about the Customer Copyright Commitment

Microsoft's new European digital commitments

1 We will help build a broad AI and cloud ecosystem across Europe.

2 We will uphold Europe’s digital resilience even when there is geopolitical volatility.

3 We will continue to protect the privacy of European data.

4 We will always help protect and defend Europe’s cybersecurity.

5 We will help strengthen Europe’s economic competitiveness, including for open source.

Prepare data for Copilot by ensuring correct access to files

What is oversharing?

Copilot only accesses data that an individual user is authorized to access

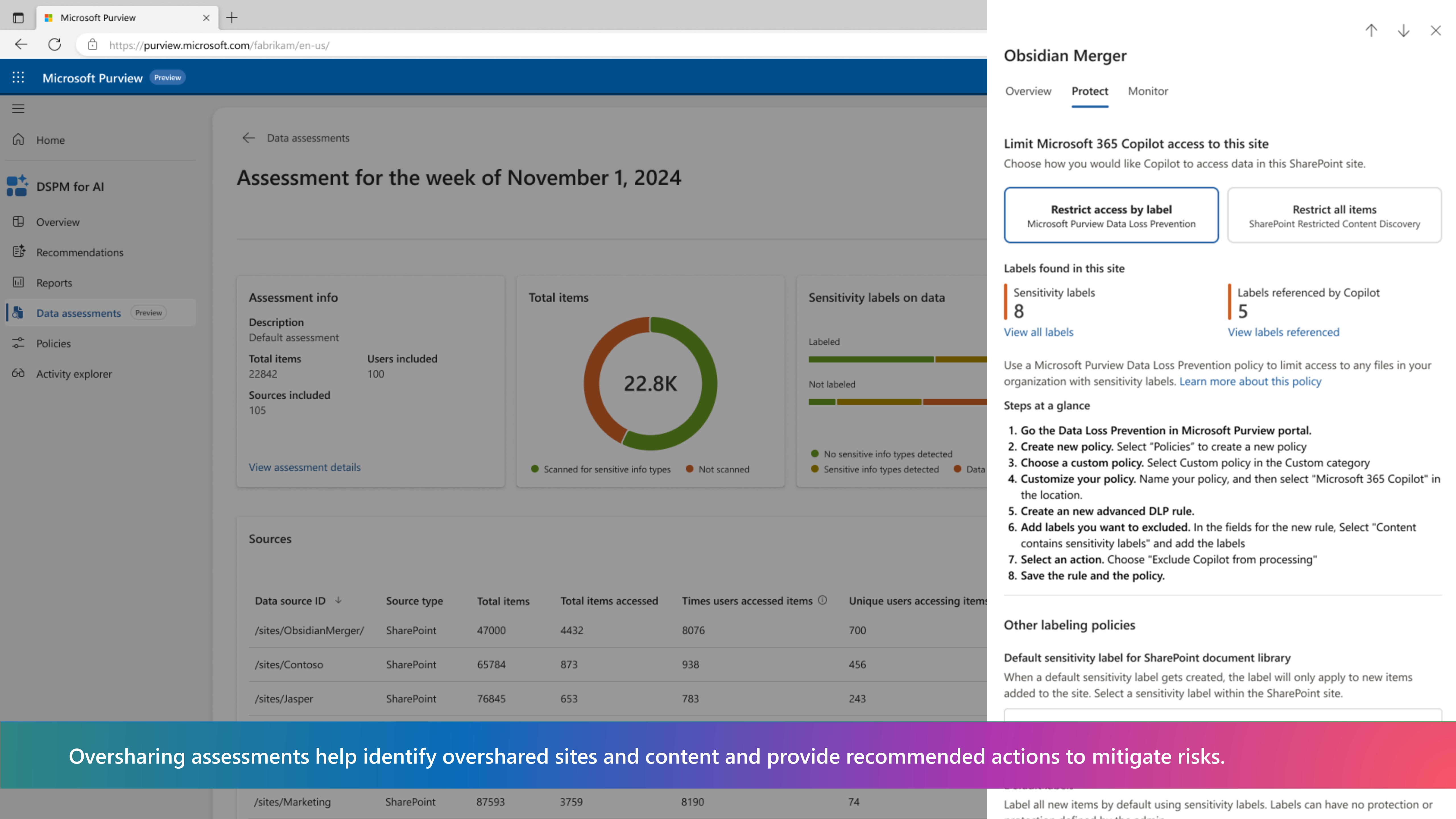
Oversharing happens when an employee has access to information beyond what is necessary to do their jobs

What causes oversharing?

Accidentally saving a file to a location with broad access permissions

A user sharing content with someone who should not have access

Files do not have access protections



Microsoft Purview

https://purview.microsoft.com/fabrikam/en-us/

Microsoft Purview Preview

Home

DSPM for AI

Overview

Recommendations

Reports

Data assessments Preview

Policies

Activity explorer

Data assessments

Assessment for the week of November 1, 2024

Assessment info

Description
Default assessment

Total items
22842

Users included
100

Sources included
105

View assessment details

Total items

Sensitivity labels on data

Labeled
Not labeled
● No sensitive info types detected
● Sensitive info types detected
● Data

Sources

Data source ID ↓	Source type	Total items	Total items accessed	Times users accessed items ⓘ	Unique users accessing items
/sites/ObsidianMerger/	SharePoint	47000	4432	8076	700
/sites/Contoso	SharePoint	65784	873	938	456
/sites/Jasper	SharePoint	76845	653	783	243
/sites/Marketing	SharePoint	87593	3759	8190	74

Obsidian Merger

Overview | **Protect** | Monitor

Limit Microsoft 365 Copilot access to this site

Choose how you would like Copilot to access data in this SharePoint site.

Restrict access by label
Microsoft Purview Data Loss Prevention

Restrict all items
SharePoint Restricted Content Discovery

Labels found in this site

Sensitivity labels
8
View all labels

Labels referenced by Copilot
5
View labels referenced

Use a Microsoft Purview Data Loss Prevention policy to limit access to any files in your organization with sensitivity labels. Learn more about this policy

Steps at a glance

1. **Go the Data Loss Prevention in Microsoft Purview portal.**
2. **Create new policy.** Select "Policies" to create a new policy
3. **Choose a custom policy.** Select Custom policy in the Custom category
4. **Customize your policy.** Name your policy, and then select "Microsoft 365 Copilot" in the location.
5. **Create an new advanced DLP rule.**
6. **Add labels you want to excluded.** In the fields for the new rule, Select "Content contains sensitivity labels" and add the labels
7. **Select an action.** Choose "Exclude Copilot from processing"
8. **Save the rule and the policy.**

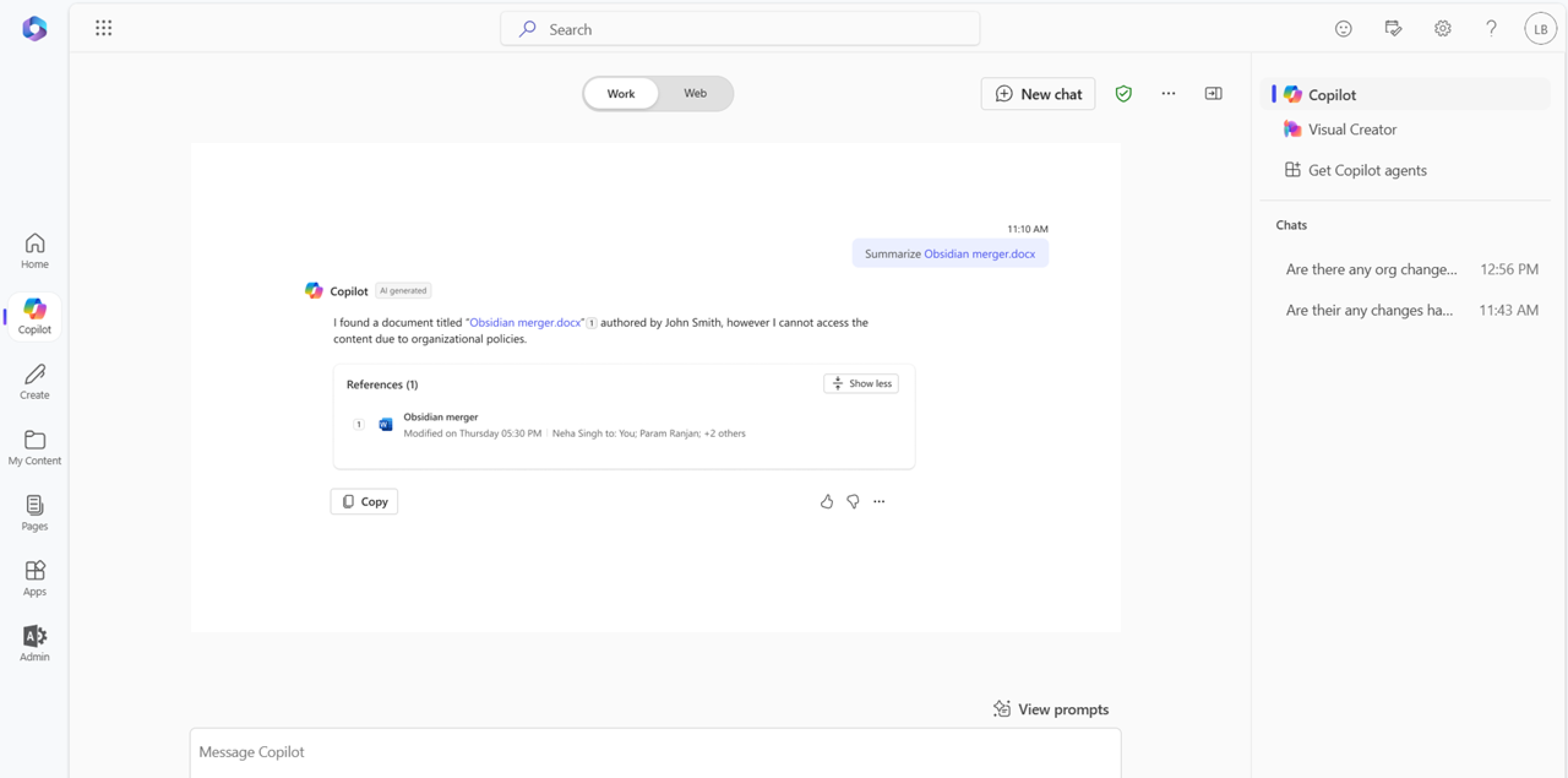
Other labeling policies

Default sensitivity label for SharePoint document library

When a default sensitivity label gets created, the label will only apply to new items added to the site. Select a sensitivity label within the SharePoint site.

Label all new items by default using sensitivity labels. Labels can have no protection or

Oversharing assessments help identify overshared sites and content and provide recommended actions to mitigate risks.



Chats

Are there any org change... 12:56 PM

Are their any changes ha... 11:43 AM

11:10 AM

Summarize Obsidian merger.docx

Copilot AI generated

I found a document titled "Obsidian merger.docx" 1 authored by John Smith, however I cannot access the content due to organizational policies.

References (1) Show less

1 Obsidian merger
Modified on Thursday 05:30 PM | Neha Singh to: You; Param Ranjan; +2 others

Copy

Purview DLP for Microsoft 365 Copilot policy can prevent Copilot from using sensitive data to generate responses.

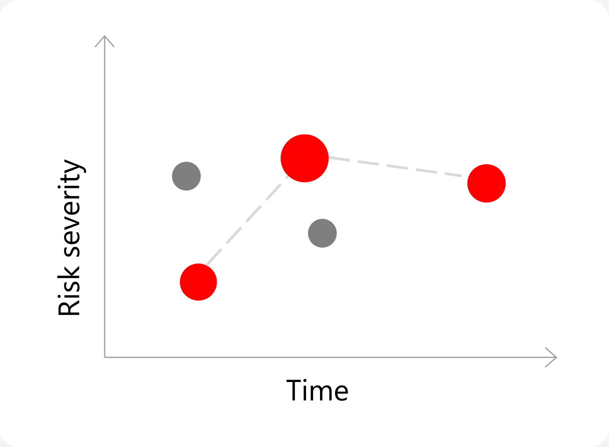
Dynamically apply security policies based on risky actions

A user performs a series of risky actions

Actions deviate from usual pattern of behavior

- Has a series of risky interactions via Copilot
- Downloads 100s of files containing sensitive data

Identifies the sequence of events as a risky pattern



Uses AI for risk analysis

Automatically adds the user to more strict security policies

Block actions until investigated

- Can't access content in sensitive sites
- Prevent sharing or downloading content
- Block from deleting content

Balance productivity and risk mitigation

Images for illustrative purposes only. Actual user experience may differ.

Powerful tools to address oversharing

Microsoft 365 Copilot*

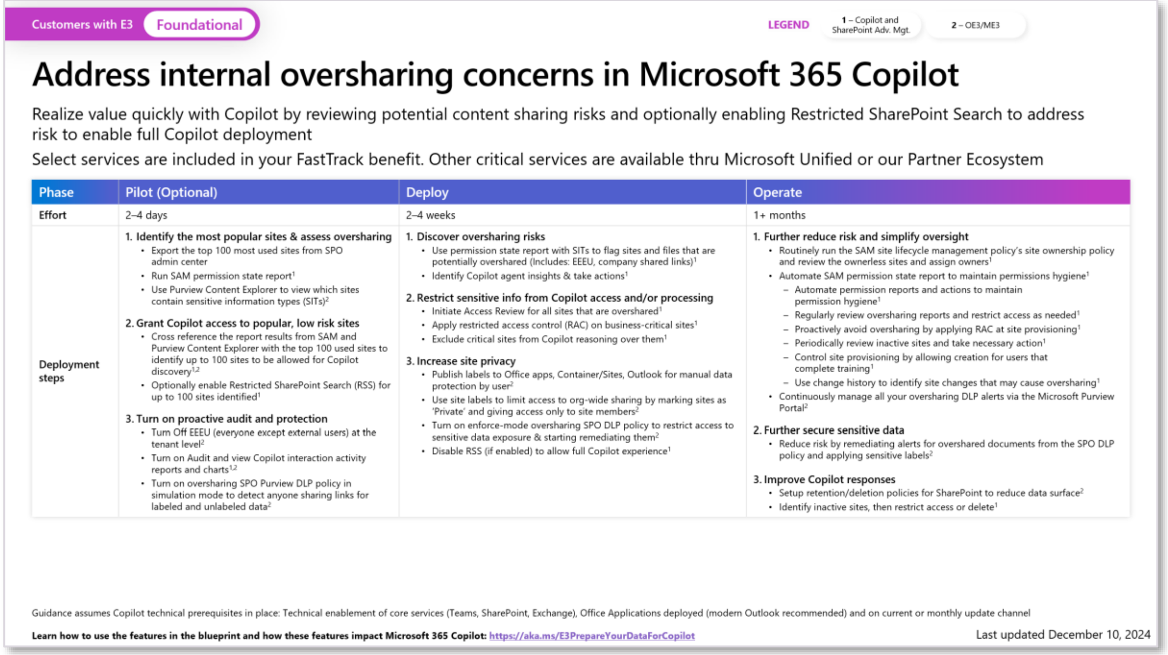
- Identify potentially overshared sites
- Enlist site owners to address access
- Restrict user and/or Copilot access to risky sites while remediating risks
- Remove organization-wide site access as needed
- Improve Copilot responses by archiving or deleting unneeded sites

Microsoft Purview

- Identify potentially overshared sites and files
- Create oversharing assessments targeted to specific Microsoft 365 locations
- Prevent Copilot from processing certain sensitive files and from using them in responses
- Receive and act on policy suggestions to mitigate your specific oversharing risks
- Get notifications when new oversharing occurs with options for remediation
- Secure sensitive data through file level access controls and Data Loss Prevention policies
- Improve Copilot responses by archiving or deleting unneeded files

* Provided by SharePoint Advanced Management.

Microsoft deployment blueprint to implement internal oversharing protections for Microsoft 365 Copilot



Customers with E3 Foundational

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

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

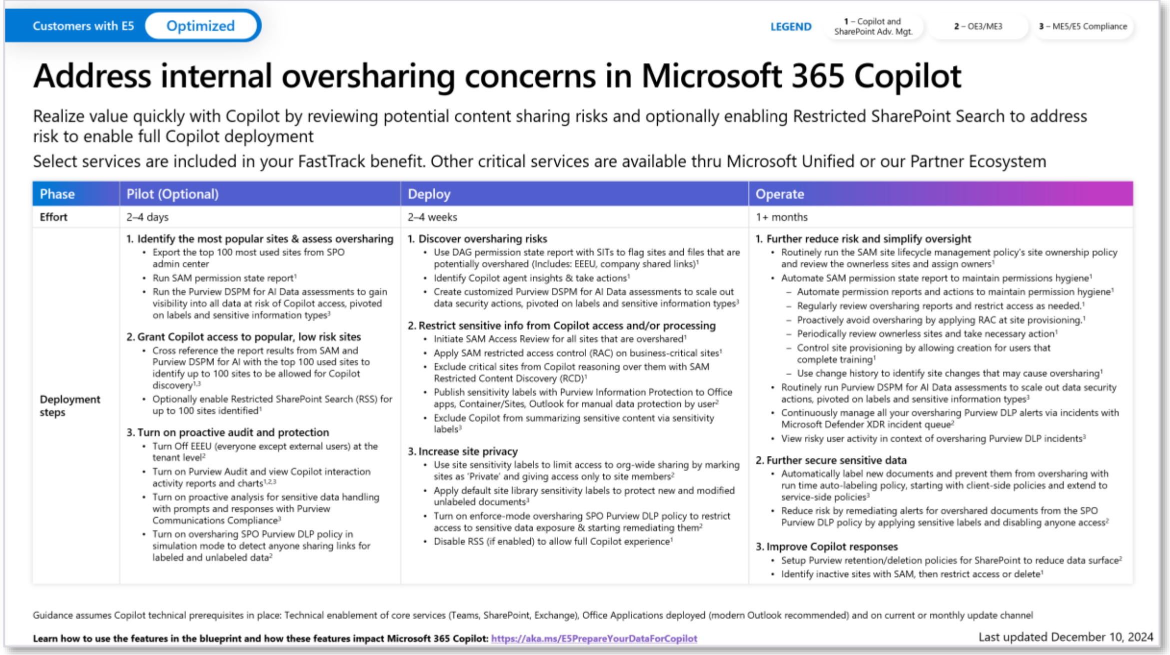
Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot (Optional)	Deploy	Operate
Effort	2–4 days	2–4 weeks	1+ months
Deployment steps	**1. Identify the most popular sites & assess oversharing** • Export the top 100 most used sites from SPO admin center • Run SAM permission state report[1] • Use Purview Content Explorer to view which sites contain sensitive information types (SITs)[2] **2. Grant Copilot access to popular, low risk sites** • Cross reference the report results from SAM and Purview Content Explorer with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery[1,2] • Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified[1] **3. Turn on proactive audit and protection** • Turn Off EEEU (everyone except external users) at the tenant level[2] • Turn on Audit and view Copilot interaction activity reports and charts[1,2] • Turn on oversharing SPO Purview DLP policy in simulation mode to detect anyone sharing links for labeled and unlabeled data[2]	**1. Discover oversharing risks** • Use permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)[1] • Identify Copilot agent insights & take actions[1] **2. Restrict sensitive info from Copilot access and/or processing** • Initiate Access Review for all sites that are overshared[1] • Apply restricted access control (RAC) on business-critical sites[1] • Exclude critical sites from Copilot reasoning over them[1] **3. Increase site privacy** • Publish labels to Office apps, Container/Sites, Outlook for manual data protection by user[2] • Use site labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members[2] • Turn on enforce-mode oversharing SPO DLP policy to restrict access to sensitive data exposure & starting remediating them[2] • Disable RSS (if enabled) to allow full Copilot experience[1]	**1. Further reduce risk and simplify oversight** • Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners[1] • Automate SAM permission state report to maintain permissions hygiene[1] – Automate permission reports and actions to maintain permission hygiene[1] – Regularly review oversharing reports and restrict access as needed[1] – Proactively avoid oversharing by applying RAC at site provisioning[1] – Periodically review inactive sites and take necessary action[1] – Control site provisioning by allowing creation for users that complete training[1] – Use change history to identify site changes that may cause oversharing[1] • Continuously manage all your oversharing DLP alerts via the Microsoft Purview Portal[2] **2. Further secure sensitive data** • Reduce risk by remediating alerts for overshared documents from the SPO DLP policy and applying sensitive labels[2] **3. Improve Copilot responses** • Setup retention/deletion policies for SharePoint to reduce data surface[2] • Identify inactive sites, then restrict access or delete[1]

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

Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: https://aka.ms/E3PrepareYourDataForCopilot

Last updated December 10, 2024



Customers with E5 Optimized

LEGEND 1 – Copilot and SharePoint Adv. Mgt. 2 – OE3/ME3 3 – ME5/E5 Compliance

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 (Optional)	Deploy	Operate
Effort	2–4 days	2–4 weeks	1+ months
Deployment steps	**1. Identify the most popular sites & assess oversharing** • Export the top 100 most used sites from SPO admin center • Run SAM permission state report[1] • Run the Purview DSPM for AI Data assessments to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types[3] **2. Grant Copilot access to popular, low risk sites** • Cross reference the report results from SAM and Purview DSPM for AI with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery[1,3] • Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified[1] **3. Turn on proactive audit and protection** • Turn Off EEEU (everyone except external users) at the tenant level[2] • Turn on Purview Audit and view Copilot interaction activity reports and charts[1,2,3] • Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance[3] • Turn on oversharing SPO Purview DLP policy in simulation mode to detect anyone sharing links for labeled and unlabeled data[2]	**1. Discover oversharing risks** • Use DAG permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)[1] • Identify Copilot agent insights & take actions[1] • Create customized Purview DSPM for AI Data assessments to scale out data security actions, pivoted on labels and sensitive information types[3] **2. Restrict sensitive info from Copilot access and/or processing** • Initiate SAM Access Review for all sites that are overshared[1] • Apply SAM restricted access control (RAC) on business-critical sites[1] • Exclude critical sites from Copilot reasoning over them with SAM Restricted Content Discovery (RCD)[1] • Publish sensitivity labels with Purview Information Protection to Office apps, Container/Sites, Outlook for manual data protection by user[2] • Exclude Copilot from summarizing sensitive content via sensitivity labels[3] **3. Increase site privacy** • Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members[2] • Apply default site library sensitivity labels to protect new and modified unlabeled documents[3] • Turn on enforce-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & starting remediating them[2] • Disable RSS (if enabled) to allow full Copilot experience[1]	**1. Further reduce risk and simplify oversight** • Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners[1] • Automate SAM permission state report to maintain permissions hygiene[1] – Automate permission reports and actions to maintain permission hygiene[1] – Regularly review oversharing reports and restrict access as needed.[1] – Proactively avoid oversharing by applying RAC at site provisioning.[1] – Periodically review ownerless sites and take necessary action[1] – Control site provisioning by allowing creation for users that complete training[1] – Use change history to identify site changes that may cause oversharing[1] • Routinely run Purview DSPM for AI Data assessments to scale out data security actions, pivoted on labels and sensitive information types[3] • Continuously manage all your oversharing Purview DLP alerts via incidents with Microsoft Defender XDR incident queue[2] • View risky user activity in context of oversharing Purview DLP incidents[3] **2. Further secure sensitive data** • 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 policies[3] • Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access[2] **3. Improve Copilot responses** • Setup Purview retention/deletion policies for SharePoint to reduce data surface[2] • Identify inactive sites with SAM, then restrict access or delete[1]

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

Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: https://aka.ms/E5PrepareYourDataForCopilot

Last updated December 10, 2024

Get the blueprint:

https://aka.ms/Copilot/OversharingBlueprintLearn

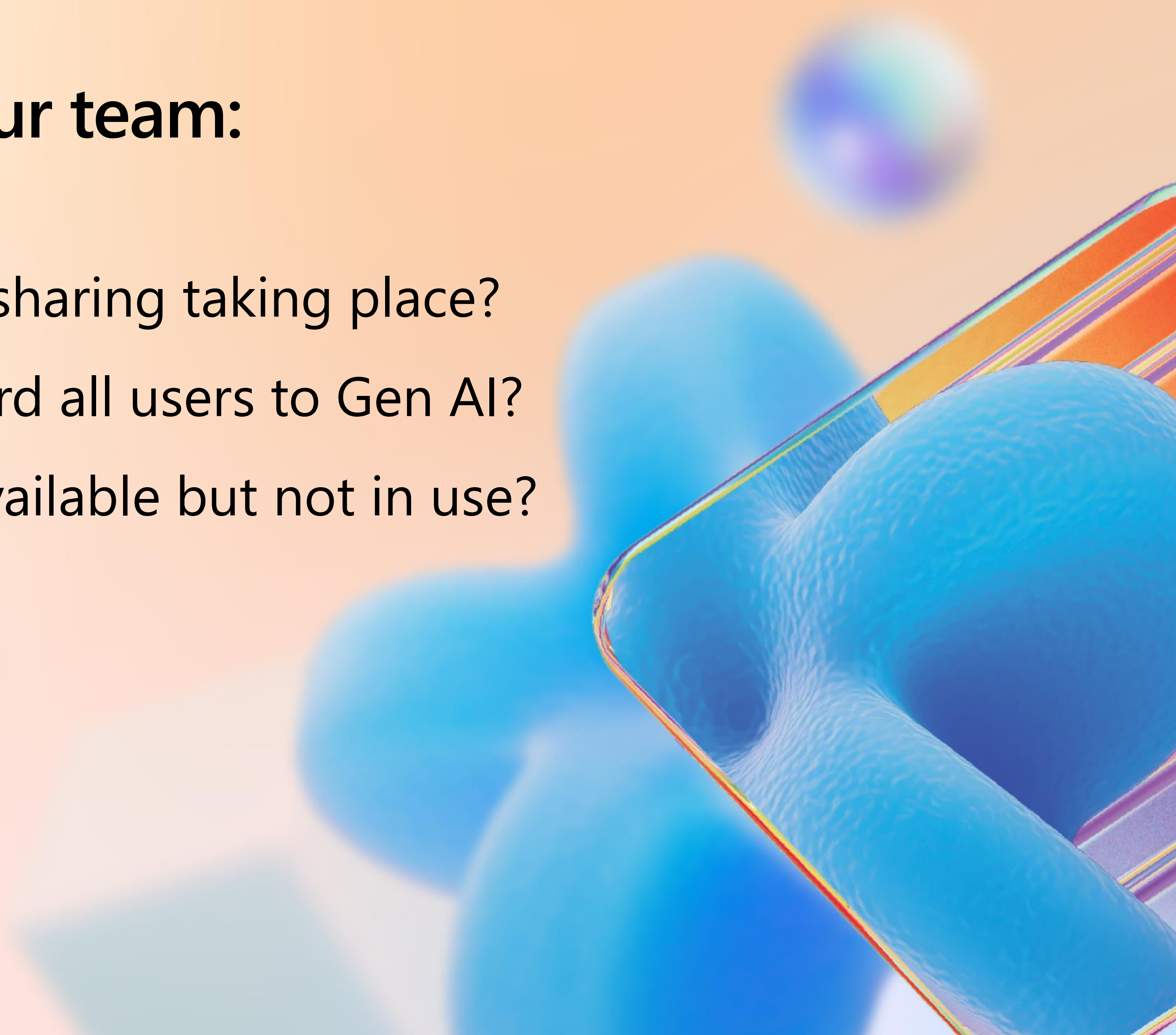
Secure and Govern Microsoft 365 Copilot licensing

		Foundational		Optimized
		Microsoft 365 Copilot*	Microsoft 365 Copilot* + Microsoft 365 E3	Microsoft 365 Copilot* + Microsoft 365 E5 Compliance
Address oversharing concerns	Identify potentially overshared sites and files across all of Microsoft 365	✓ Sites	✓ Sites	✓ Sites and files
	Create oversharing assessments targeted to specific Microsoft 365 locations			✓
	Restrict user and/or Copilot access to risky sites while remediating risks	✓	✓	✓
	Prevent Copilot from processing certain sensitive files and from using them in responses			✓
	Receive and act on policy suggestions to mitigate your specific oversharing risks			✓
	Remove organization-wide site access as needed	✓	✓	✓
	Get notifications when new oversharing occurs with options for remediation		✓	✓
	Secure sensitive data through file level access controls and Data Loss Prevention policies		✓	✓
	Improve Copilot responses by archiving or deleting unneeded content	✓ Sites	✓ Sites and files	✓ Sites and files
Protect against data loss and insider risk	View reports of sensitive data and unprotected files referenced in Copilot interactions		✓	✓
	Get alerted to risky AI use, such as an attempted prompt injection attack			✓
	View prompt and response text and referenced files		✓ via search	✓ via search or alerts
	Detect when content contains sensitive data and ask the user to manually apply protections		✓	✓
	Detect when content contains sensitive data and auto-apply protections			✓
	Copilot response and Copilot created documents inherit sensitivity label and protections		✓	✓
	Block Copilot access to files with a specific sensitivity label			✓
	Protect files even if they are moved or downloaded		✓	✓
	Get alerted to risky user actions that deviate from their usual pattern of behavior			✓
	Correlate and sequence risk alerts to identify high severity risk patterns for a user			✓
	Automatically add a user to more strict security policies based on their risk patterns			✓
Govern AI use to meet regulations & policies	Audit Copilot interactions to access detailed log information		✓	✓
	Enforce retention and deletion policies for Copilot interactions and meeting recordings + transcripts		✓	✓
	Include a user's Copilot prompts and responses in a legal hold		✓	✓
	Receive an alert if a possible compliance or ethical violation occurs and start an investigation			✓
	Perform an admin search for litigation or an investigation and include Copilot generated content		✓	✓
	Assess and track adherence to regulatory frameworks			✓

* Includes SharePoint Advanced Management

Questions to ask your team:

- To what degree is oversharing taking place?
- Are we ready to onboard all users to Gen AI?
- Do we have controls available but not in use?



Microsoft Security

How can AI be used to improve our security?

Submit a prompt

Navigating the complex threat landscape

1,500+

threat actors tracked by Microsoft

58%

of organizations use more than 40 security tools

4M+

global shortage of cybersecurity workers

Hackers use AI too…

Ransomware infection to full victim encryption

3 Days

2019

Ransomware infection to full victim encryption

1 Day

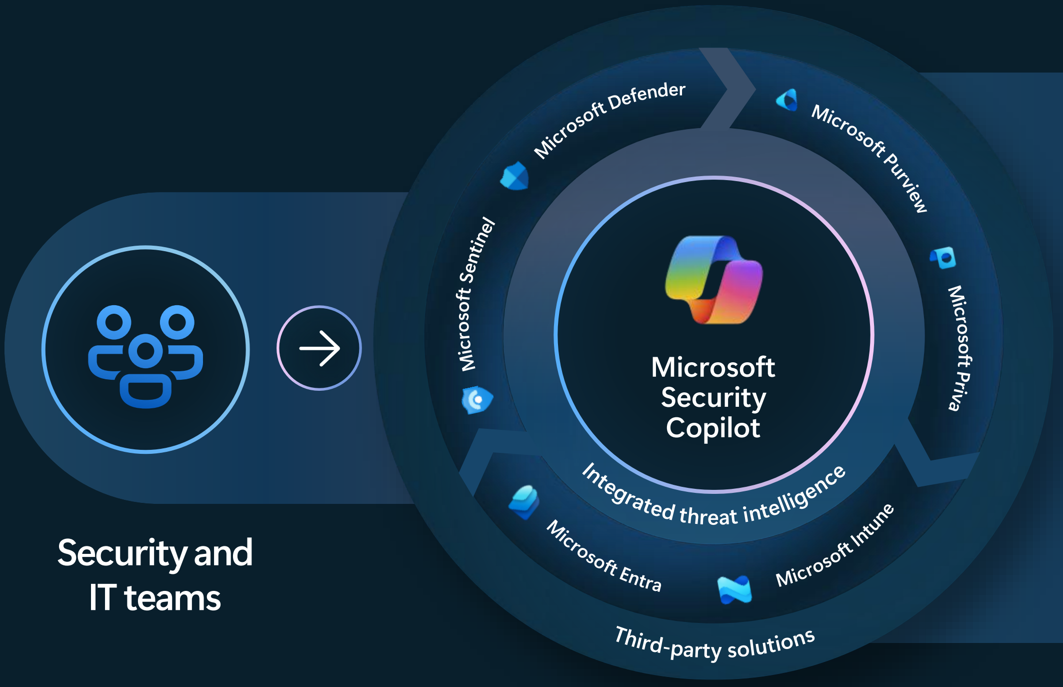
2021

Today

<15 Minutes

Security Copilot is built to solve these challenges

A generative AI-powered assistant for daily operations in security and IT
that empowers teams to protect at the speed and scale of AI



Security and IT teams

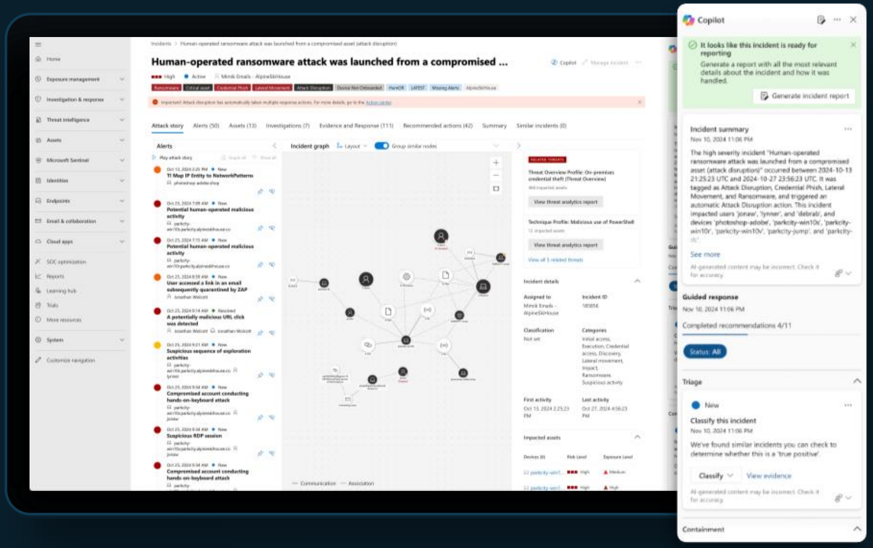
for many use cases like:

- Security investigation and remediation
- Building and reverse engineering scripts
- Risk exploration and posture management
- Troubleshooting IT issues
- Policy creation and management

Meet you where and how you work

Embedded

Offers the intuitive experience of getting Copilot guidance natively within the products that your team members already work from and are familiar with



Human-operated ransomware attack was launched from a compromised ...

Copilot

It looks like this incident is ready for reporting

Generate a report with all the most relevant details about the incident and how it was handled.

Generate incident report

Incident summary

Nov 10, 2024 11:06 PM

The high severity incident 'Human-operated ransomware attack was launched from a compromised asset (attack disruption)' occurred between 2024-10-13 21:25:23 UTC and 2024-10-27 23:56:23 UTC. It was tagged as Attack Disruption, Credential Phish, Lateral Movement, and Ransomware, and triggered an automatic Attack Disruption action. This incident impacted users 'jonaw', 'lynner', and 'debrab', and devices 'photoshop-adobe', 'parkcity-win10s', 'parkcity-win10r', 'parkcity-win10v', 'parkcity-jump', and 'parkcity-dc'.

See more

AI-generated content may be incorrect. Check it for accuracy.

Guided response

Nov 10, 2024 11:06 PM

Completed recommendations 4/11

Status: All

Triage

New

Classify this incident

Nov 10, 2024 11:06 PM

We've found similar incidents you can check to determine whether this is a 'true positive'.

Classify

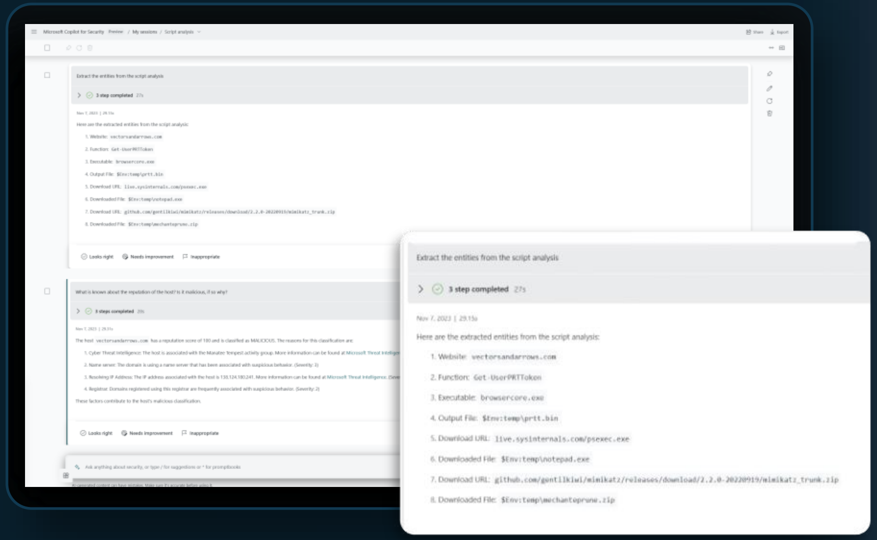
View evidence

AI-generated content may be incorrect. Check it for accuracy.

Containment

Standalone

Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot itself, with many use cases in one place, enabling enriched cross-product guidance



Extract the entities from the script analysis

3 step completed 27s

Nov 7, 2023 | 29.15s

Here are the extracted entities from the script analysis:

1. Website: `vectorsandarrows.com`
2. Function: `Get-UserPRTToken`
3. Executable: `browsercore.exe`
4. Output File: `$Env:temp\prtt.bin`
5. Download URL: `live.sysinternals.com/psexec.exe`
6. Downloaded File: `$Env:temp\notepad.exe`
7. Download URL: `github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip`
8. Downloaded File: `$Env:temp\mechanteprune.zip`

Automation

Helps teams accelerate response with built-in and custom promptbooks as well as integration with Logic Apps

Copilot in Microsoft Purview

Scaled visibility

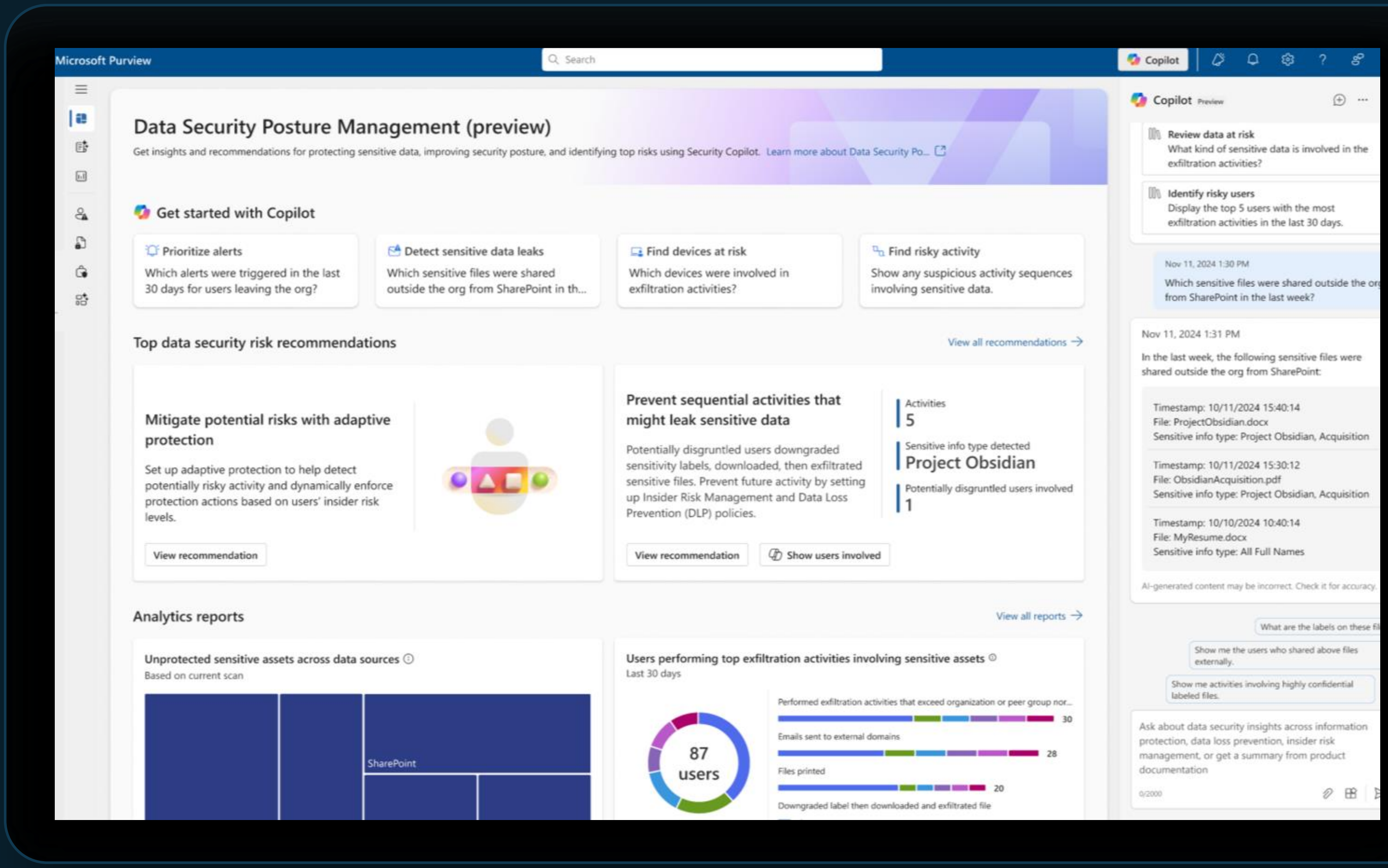
Gain comprehensive, integrated visibility across solutions and insight into relevant compliance regulatory requirements.

Summarization for speed

Quickly summarize alerts containing a breadth of signals and lengthy content to review in the lens of data security and compliance policies.

Unlock expert skills

Receive step-by-step guidance, conduct searches in natural language, and conduct advanced investigations without keyword query language.



Data Security Posture Management (preview)

Get insights and recommendations for protecting sensitive data, improving security posture, and identifying top risks using Security Copilot. Learn more about Data Security Po...

Get started with Copilot

Prioritize alerts
Which alerts were triggered in the last 30 days for users leaving the org?

Detect sensitive data leaks
Which sensitive files were shared outside the org from SharePoint in th...

Find devices at risk
Which devices were involved in exfiltration activities?

Find risky activity
Show any suspicious activity sequences involving sensitive data.

Top data security risk recommendations

Mitigate potential risks with adaptive protection

Set up adaptive protection to help detect potentially risky activity and dynamically enforce protection actions based on users' insider risk levels.

Prevent sequential activities that might leak sensitive data

Potentially disgruntled users downgraded sensitivity labels, downloaded, then exfiltrated sensitive files. Prevent future activity by setting up Insider Risk Management and Data Loss Prevention (DLP) policies.

Activities
5

Sensitive info type detected
Project Obsidian

Potentially disgruntled users involved
1

Analytics reports

Unprotected sensitive assets across data sources
Based on current scan

Users performing top exfiltration activities involving sensitive assets
Last 30 days

87
users
Performed exfiltration activities that exceed organization or peer group nor...
30
Emails sent to external domains
28
Files printed
20
Downgraded label then downloaded and exfiltrated file

Review data at risk
What kind of sensitive data is involved in the exfiltration activities?

Identify risky users
Display the top 5 users with the most exfiltration activities in the last 30 days.

Nov 11, 2024 1:30 PM
Which sensitive files were shared outside the or
from SharePoint in the last week?

Nov 11, 2024 1:31 PM

In the last week, the following sensitive files were shared outside the org from SharePoint:

Timestamp: 10/11/2024 15:40:14
File: ProjectObsidian.docx
Sensitive info type: Project Obsidian, Acquisition

Timestamp: 10/11/2024 15:30:12
File: ObsidianAcquisition.pdf
Sensitive info type: Project Obsidian, Acquisition

Timestamp: 10/10/2024 10:40:14
File: MyResume.docx
Sensitive info type: All Full Names

AI-generated content may be incorrect. Check it for accuracy.

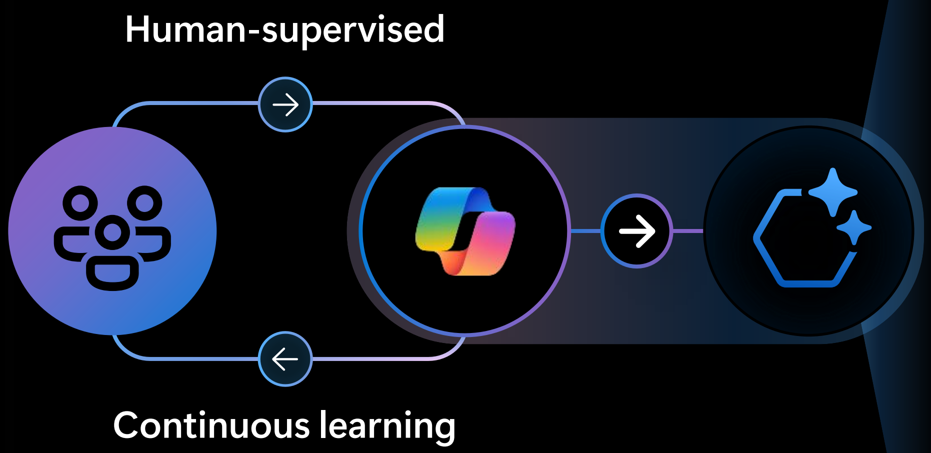
What are the labels on these fi

Show me the users who shared above files externally.

Show me activities involving highly confidential labeled files.

Ask about data security insights across information protection, data loss prevention, insider risk management, or get a summary from product documentation

Agents to empower roles across security and IT



Microsoft Security

- Phishing Triage
- Alert Triage in DLP
- Alert Triage in IRM
- Conditional Access Optimization
- Vulnerability Remediation
- Threat Intelligence Briefing

Partner ecosystem

- Privacy Breach Response by OneTrust
- SecOps Tooling by BlueVoyant
- Network Supervisor by Aviatrix
- Alert Triage by Tanium
- Task Optimizer by Fletch
- Email Threat Analyst by Performanta
- IAM Supervisor by Performanta

Use cases for prompting across your security and IT team

Security operations

CISO

- ✓ Get executive summary and detailed reporting

SOC analyst

- ✓ Accelerate investigation and remediation
- ✓ Reverse engineer malicious scripts

Threat intelligence (TI) analyst

- ✓ Enrich analysis with unified TI
- ✓ Accelerate threat hunting

Beyond the SOC

Data security admin

- ✓ Proactive data security posture management
- ✓ Discover protection gaps and streamline controls

IT admin

- ✓ Risk investigation
- ✓ Accelerate IT troubleshooting

Identity admin

- ✓ Sign-in and risky user exploration
- ✓ Lifecycle workflow management

Questions to ask your team:

- Can we break down the siloes in the security team?
- Can we handle incidents and/or report on security across teams?
- Can we automate tasks to free up resources?
  - Security
  - Operations/management

Hopefully we have addressed…

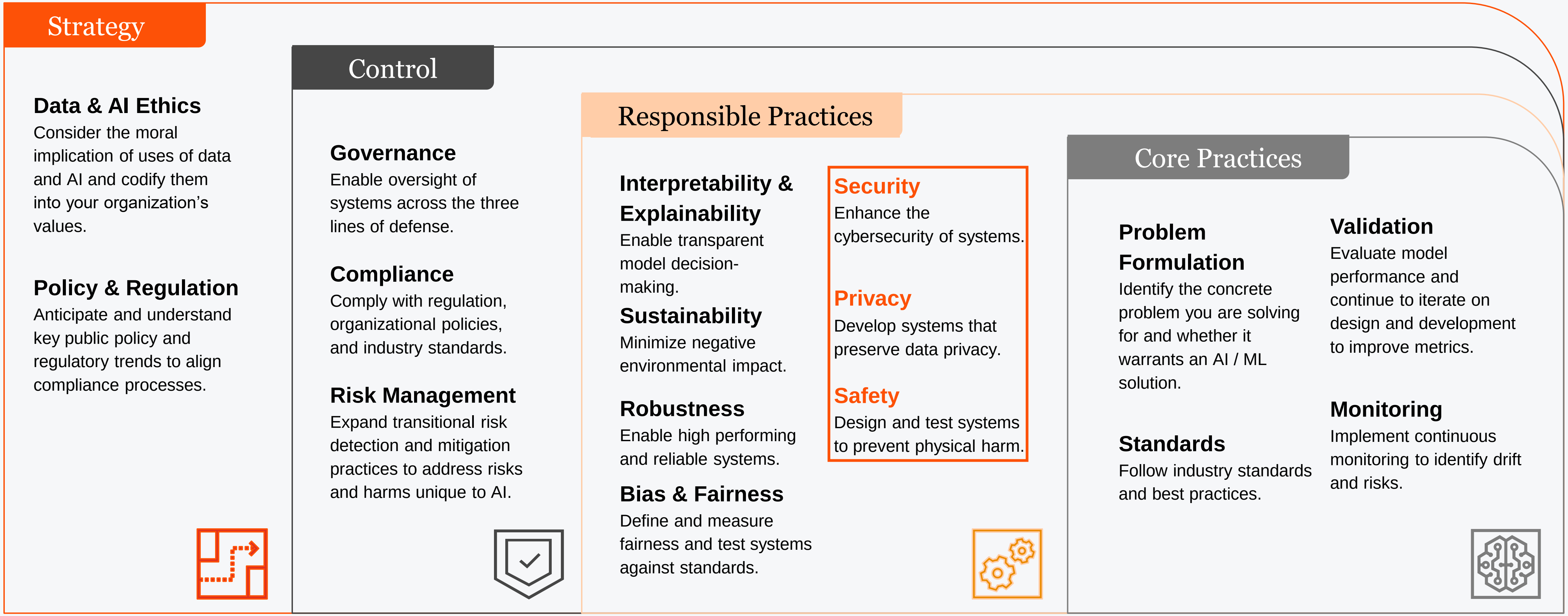
What AI means for your data security.

How AI can be used to improve your security.

Tackling AI Security Threats – What to do next?

PwC’s Responsible AI Framework

Responsible AI at its core is simply good data science, governed by key guiding principles **from strategy to execution**



Strategy

Data & AI Ethics
Consider the moral implication of uses of data and AI and codify them into your organization’s values.

Policy & Regulation
Anticipate and understand key public policy and regulatory trends to align compliance processes.

Control

Governance
Enable oversight of systems across the three lines of defense.

Compliance
Comply with regulation, organizational policies, and industry standards.

Risk Management
Expand transitional risk detection and mitigation practices to address risks and harms unique to AI.

Responsible Practices

Interpretability & Explainability
Enable transparent model decision-making.

Sustainability
Minimize negative environmental impact.

Robustness
Enable high performing and reliable systems.

Bias & Fairness
Define and measure fairness and test systems against standards.

Security
Enhance the cybersecurity of systems.

Privacy
Develop systems that preserve data privacy.

Safety
Design and test systems to prevent physical harm.

Core Practices

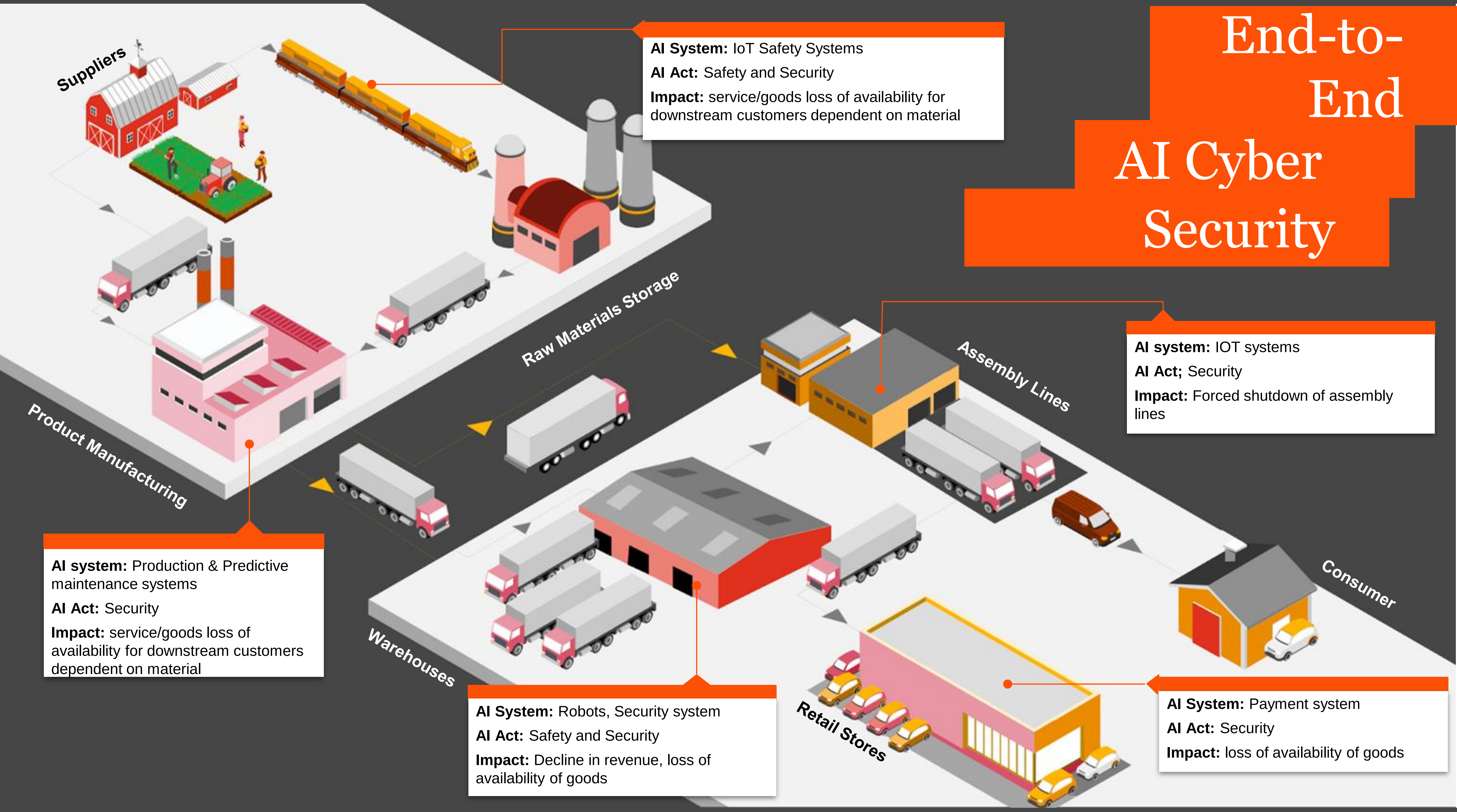
Problem Formulation
Identify the concrete problem you are solving for and whether it warrants an AI / ML solution.

Standards
Follow industry standards and best practices.

Validation
Evaluate model performance and continue to iterate on design and development to improve metrics.

Monitoring
Implement continuous monitoring to identify drift and risks.

End-to-End AI Cyber Security



AI System: IoT Safety Systems

AI Act: Safety and Security

Impact: service/goods loss of availability for downstream customers dependent on material

AI system: IOT systems

AI Act; Security

Impact: Forced shutdown of assembly lines

AI system: Production & Predictive maintenance systems

AI Act: Security

Impact: service/goods loss of availability for downstream customers dependent on material

AI System: Robots, Security system

AI Act: Safety and Security

Impact: Decline in revenue, loss of availability of goods

AI System: Payment system

AI Act: Security

Impact: loss of availability of goods

How to get started:

A “simple” Guide your Next Steps

1. Create a full overview of the use of AI in your organization.

2. Classify each AI Application according to the EU AI Act by following guidelines and a structured methodology.

3. Perform formal risk assessments for each high-risk AI Application.

4. Implement relevant security controls.

AI Use-case vs. Application - Examples

Use case 1

General assistance: Employees using GenAI such as Microsoft CoPilot and ChatGPT.

Use case 2

Customer support: Routine customer queries, reducing support workload and improving response times.

Use case 3

Sales forecasting: Predict future sales trends to help organizations make data-driven decisions.

Use case 4

Fraud detection: Detect suspicious transactions or behaviors in real time to prevent fraud and financial loss.

Use case 5

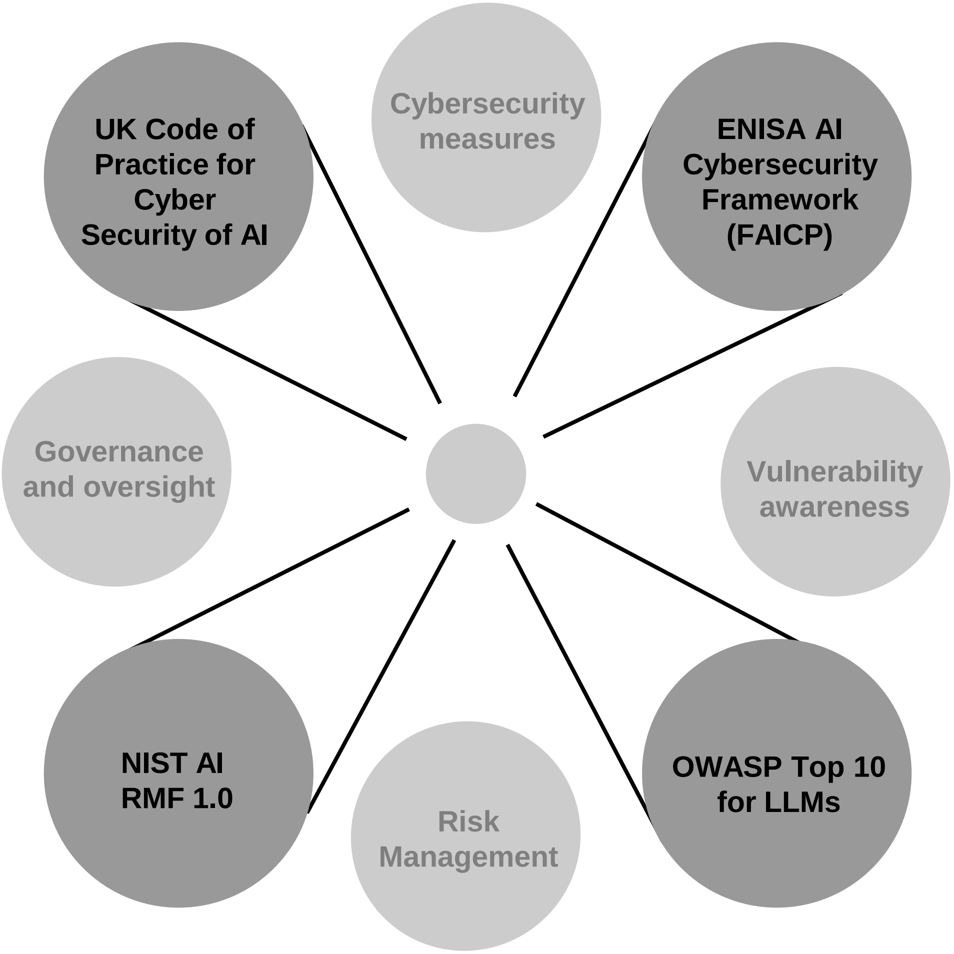
Document and invoice processing: extracting data from documents, automating general tasks.

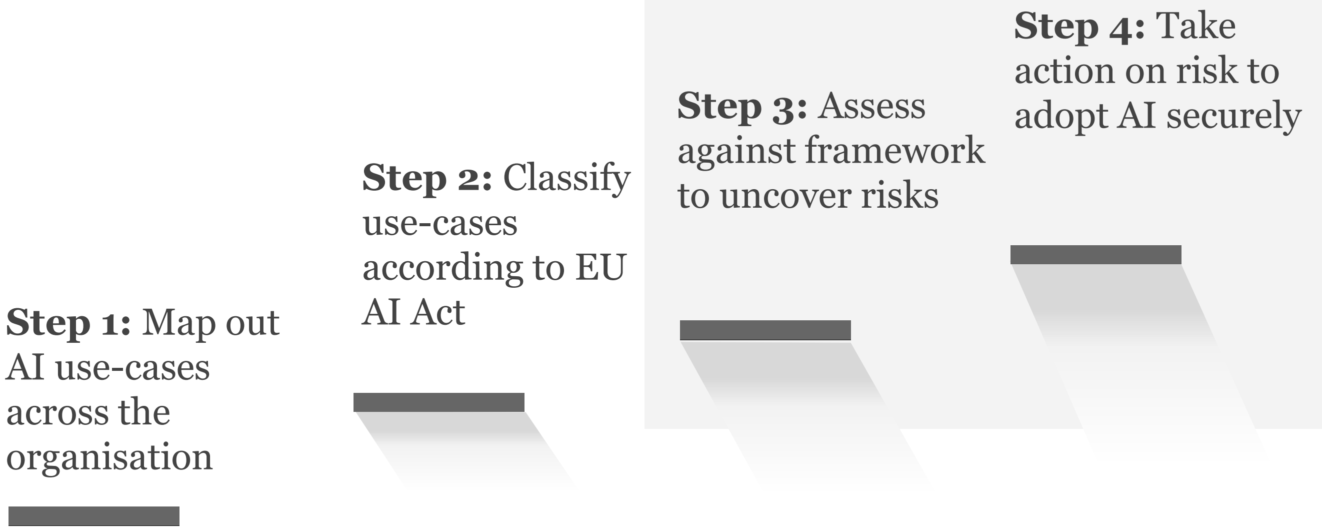
Use case 6

Recruiting and HR: AI Screens resumes and matches candidates to roles.

Application 1	Microsoft Copilot
Application 2	ChatGPT
Application 3	HireVue
Application 4	Darktrace
Application 5	Grammarly
Application 6	Microsoft Defender with AI
Application 7	Google Gemini
Application 8	Salesforce
Application 9	Mailchimp AI

PwC's Combined **AI Security Assessment Framework** will support all the steps




Step 1: Map out AI use-cases across the organisation
Step 2: Classify use-cases according to EU AI Act
Step 3: Assess against framework to uncover risks
Step 4: Take action on risk to adopt AI securely

Morning sessions on the effective use of AI

Thank you!

Kenneth Pedersen
Partner, Head of Cyber Risk Transformation, PwC
Kenneth.studsgaard.pedersen@pwc.com
+4531361073

Jørgen Sørensen
Partner, Head of Responsible AI, PwC
Jorgen.jgs.sorensen@pwc.com
+4524945254

Nicholas Jancey
CISO PwC Nordics & Africa
Nicholas.jancey@pwc.com
+4529614698

Kristoffer Rosenmeier
Sr. Specialist Manager, Security & Compliance at Microsoft
Kristoffer.rosenmeier@microsoft.com
+4529229873