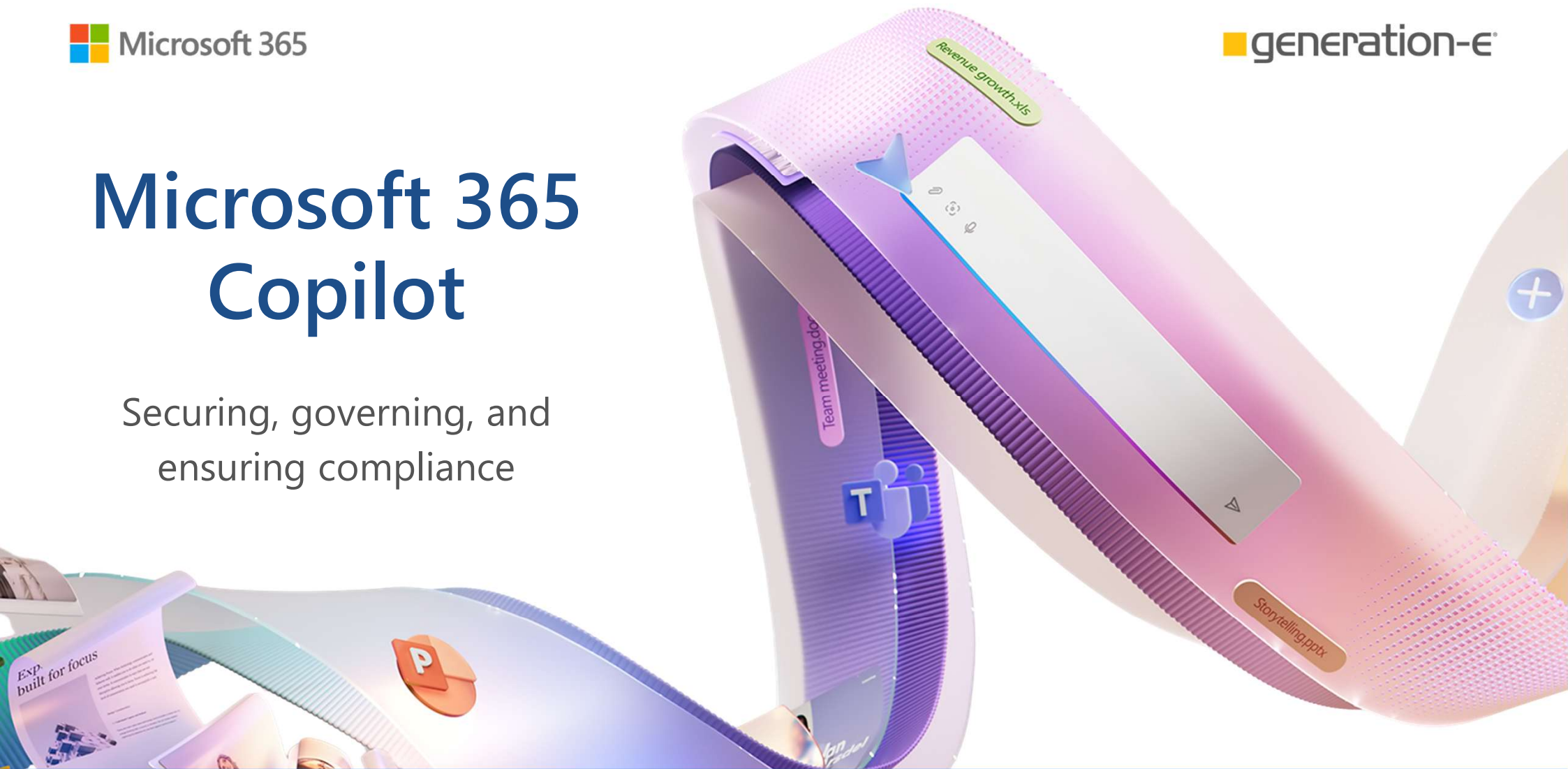




Microsoft 365 Copilot

Securing, governing, and
ensuring compliance



Welcome

Sean Hartman

Head of Information Architecture, Risk, & Compliance

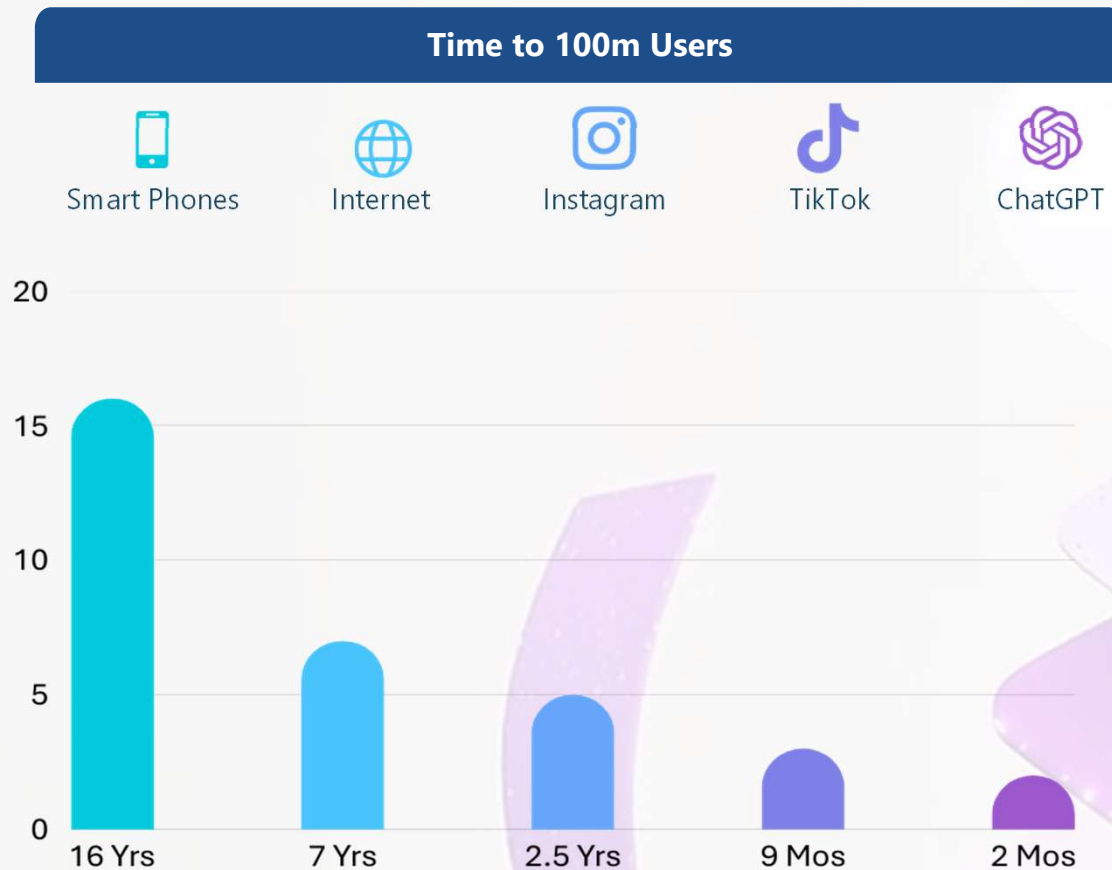
Generation-e





The AI Revolution

Generative AI technology is here



And can help to:



Unleash Creativity

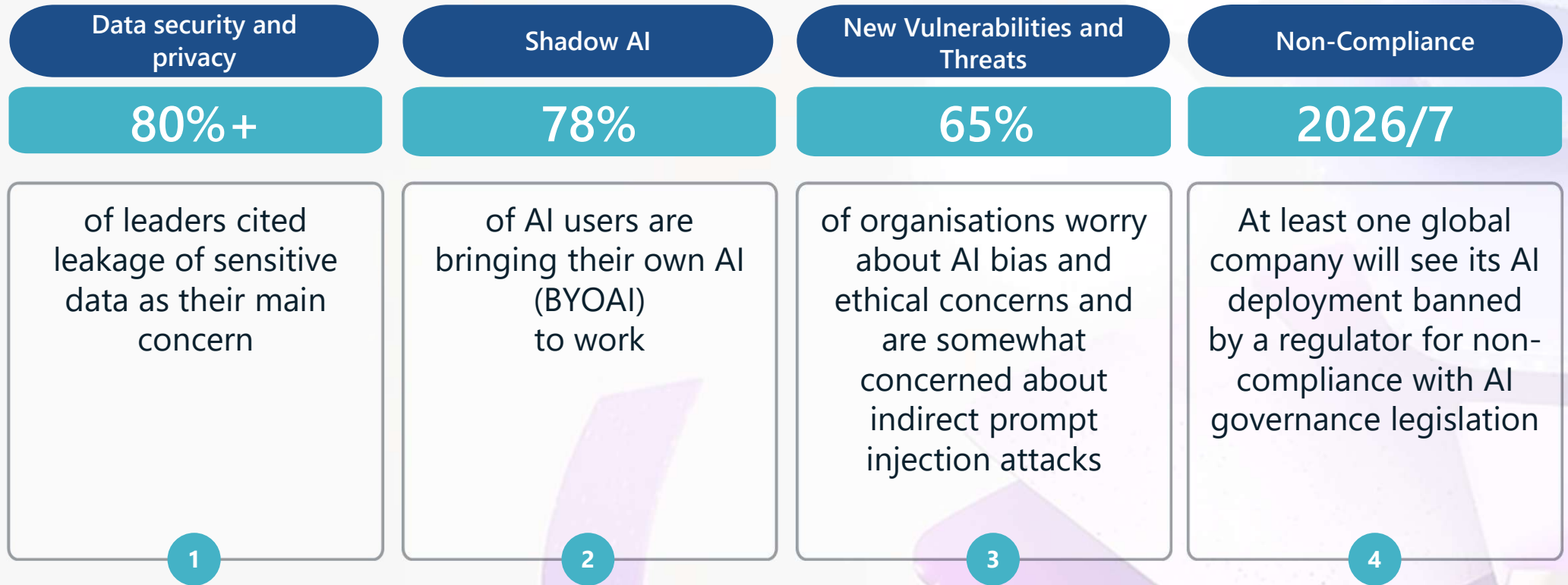


Unlock Productivity



Uplevel Skills

But there are associated risks



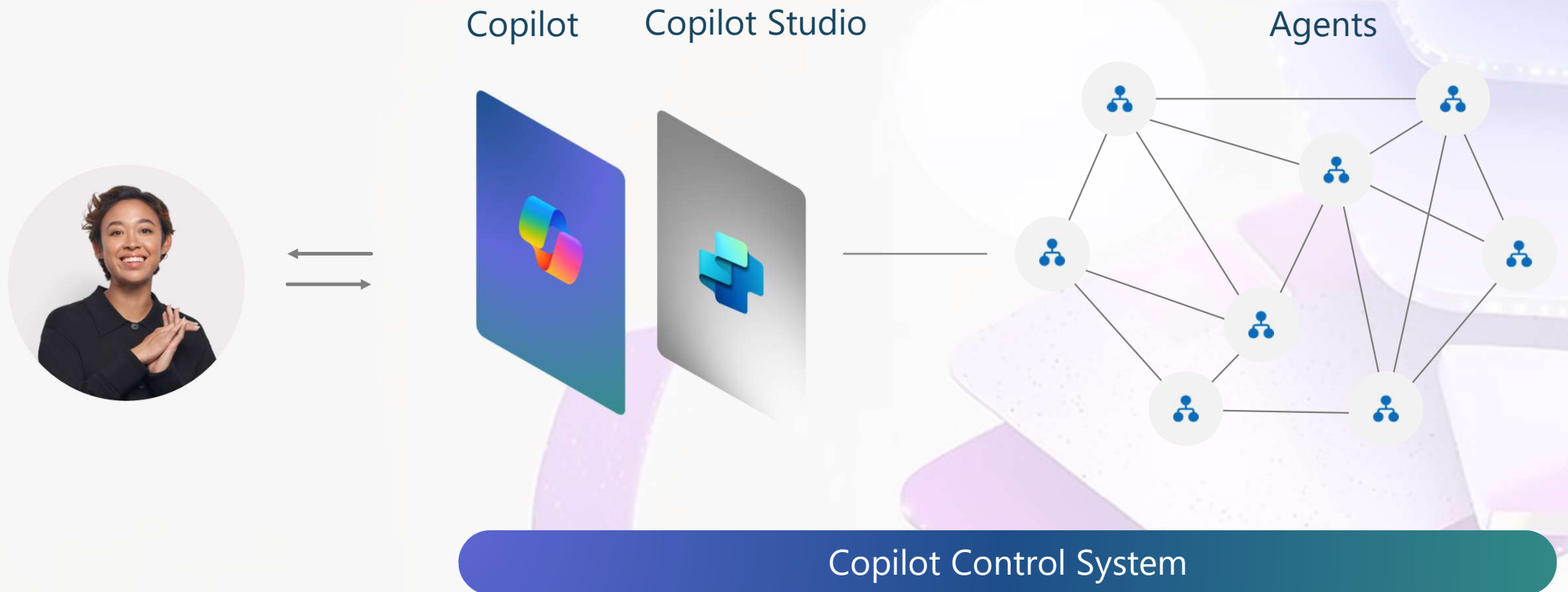
1. [First Annual Generative AI study: Business Rewards vs. Security Risks](#), Q3 2023, ISMG, N=400

2. [2024 Work Trend Index Annual Report](#), Microsoft and LinkedIn, May 2024, N=31,000.

3. [Gartner®, Gartner Peer Community Poll](#)

4. [Gartner Security Leaders Guide to Data Security](#), Sep 2023

Copilot is the UI for AI



Copilot Security Fundamentals

The background of the slide is a dark, blue-toned image of a modern office interior. Several human figures are depicted as glowing blue wireframe models, standing and moving. In the center, a large digital display shows green code or data. The overall aesthetic is high-tech and digital.

Microsoft commitments & controls

Whatever your business goals, trust is foundational



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



Microsoft 365
Copilot is built on
trust

Shared Responsibility of security for AI



Copilot for Microsoft 365

Inherits your security, compliance, and privacy policies

1

Manage
overprivileged and
risky users



Microsoft Entra ID

2

Mitigate
device risk



Microsoft Intune

3

Prevent over-
exposure of data



Microsoft Purview

4

Discover and
control the use of
AI apps



Microsoft Defender
for Cloud Apps



Secure and govern Copilot with Microsoft Security



Baseline



Copilot for Microsoft 365
+ Office 365 E3

Multi-factor authentication
Audit Logging

Core



Copilot for Microsoft 365
+ Microsoft 365 E3
+ SharePoint Advanced MGMT

Conditional access
Manual sensitivity labels
Data loss prevention policies
Advanced SharePoint site-wide
access controls & reports
Unified endpoint management

Best-in-class



Copilot for Microsoft 365
+ Microsoft 365 E5
+ SharePoint Advanced MGMT

Risk-based Conditional access
Automatically apply sensitivity
labels
Automatically remove inactive
content
Prevent data leak on devices
Detect non-compliant usage



Preparing for Copilot

Pre-deployment readiness

- Establishing governance policies:
 - **Acceptable Use Policy:** Define clear rules for employees on how to use Copilot responsibly and ethically.
 - **Data Sharing Guidelines:** Create policies for when and how sensitive data can be used in Copilot prompts and responses.
 - **Audit and Monitoring:** Explain the importance of auditing Copilot interactions to detect suspicious or inappropriate usage.

AI + Data Leakage: A Threat Hiding in Plain Sight



Over the past 12 months, our team has conducted **five in-depth investigations** into data leakage incidents involving **online AI platforms**. In every case, the root cause wasn't malicious intent—it was **staff who were simply unaware of the privacy and security implications** of uploading sensitive data to tools like ChatGPT, Gemini, or other generative AI models.

report suspected of containing AI invented quote

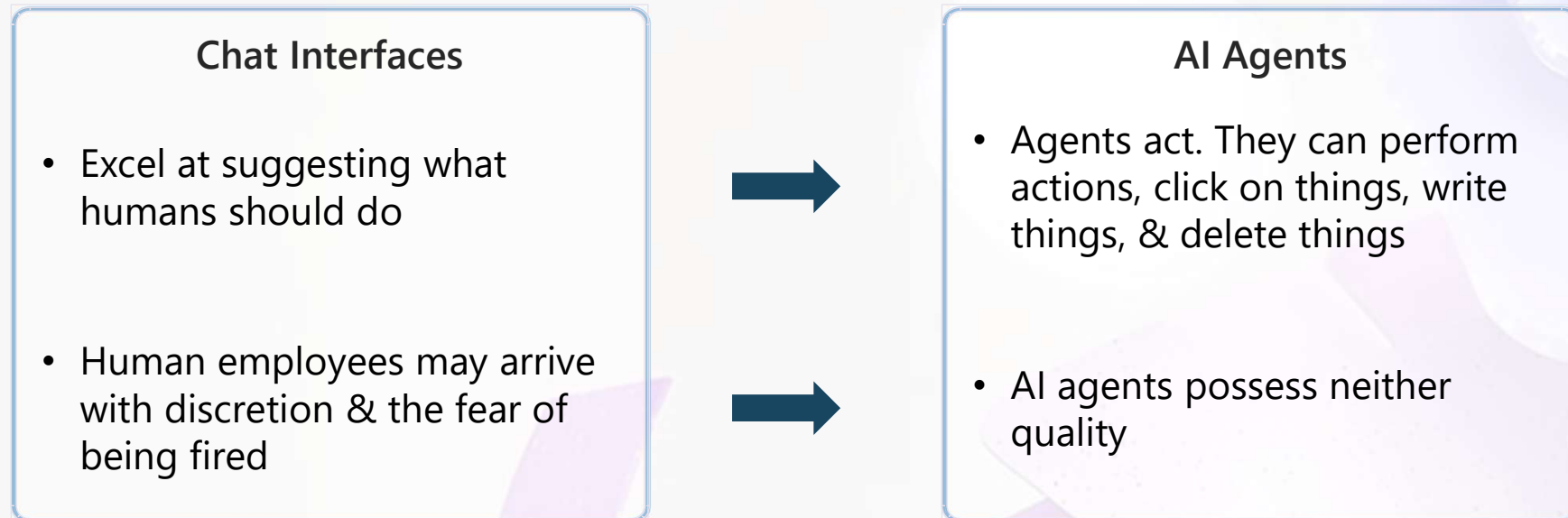


New errors have been found in a major report
...raising further suspicions some of the content was
generated by artificial intelligence.

On Friday [The Australian Financial Review revealed](#) that ... report for
the ... on welfare
compliance systems. ... contained at least half
a dozen references to academic works that do not exist.

Evolution from chat to action

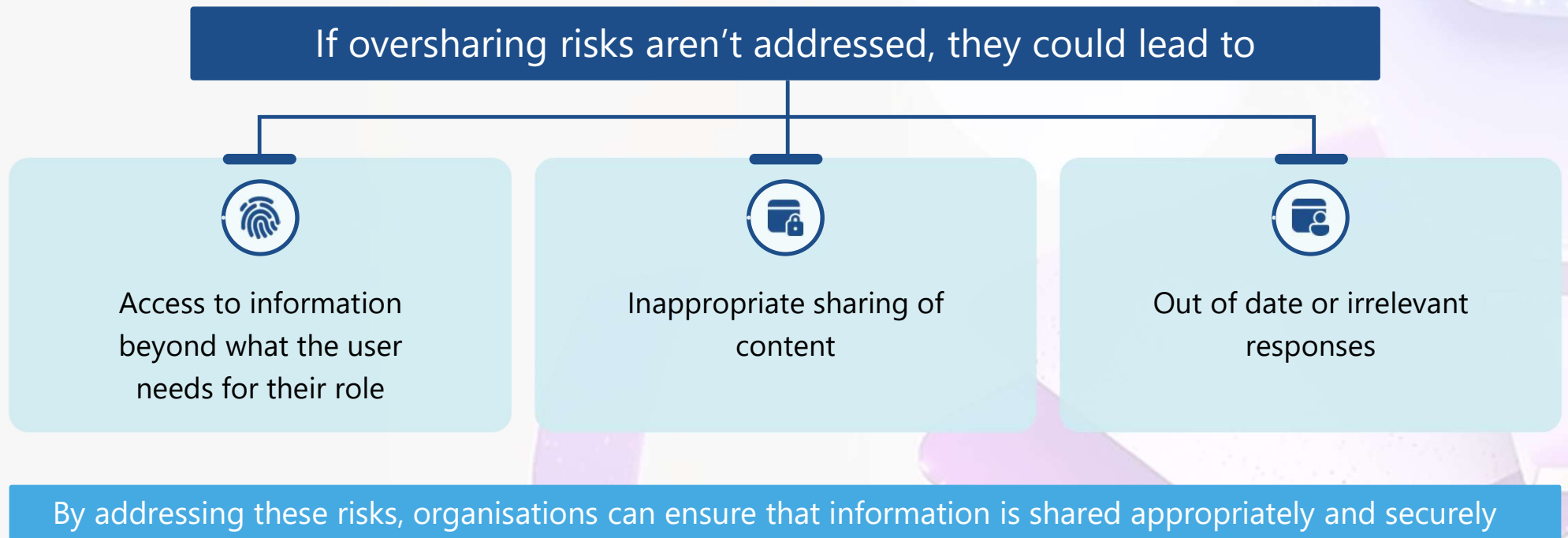
There is a critical transition taking place



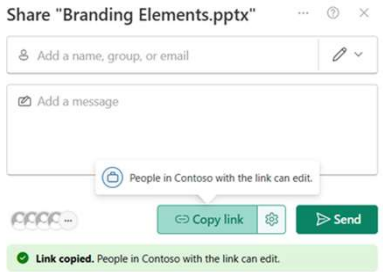
The biggest challenges in Agent governance is not just technical, they're cultural

Principle of “least privilege”

Copilot’s ability to leverage information available to employees has raised concerns for organisations about overshared permissions



Common causes of oversharing



Share "Branding Elements.pptx"

Add a name, group, or email

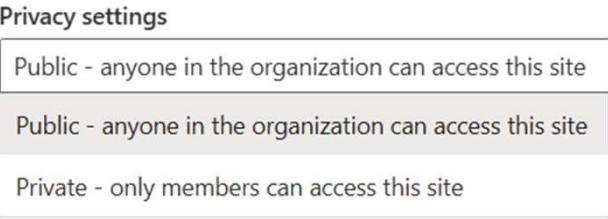
Add a message

People in Contoso with the link can edit.

Copy link Send

Link copied. People in Contoso with the link can edit.

Default sharing option is everyone



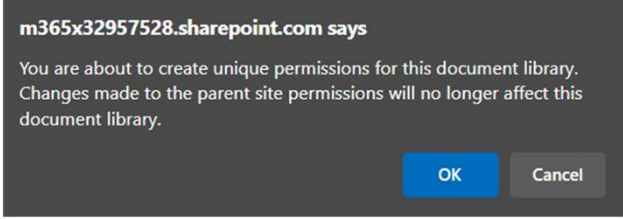
Privacy settings

Public - anyone in the organization can access this site

Public - anyone in the organization can access this site

Private - only members can access this site

Site privacy set to public

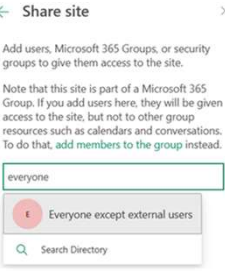


m365x32957528.sharepoint.com says

You are about to create unique permissions for this document library. Changes made to the parent site permissions will no longer affect this document library.

OK Cancel

Broken permission inheritance



Share site

Add users, Microsoft 365 Groups, or security groups to give them access to the site.

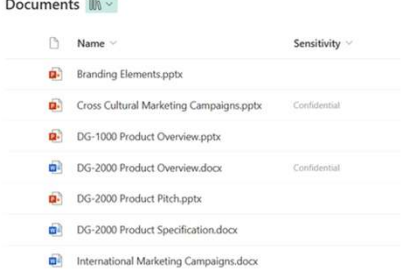
Note that this site is part of a Microsoft 365 Group. If you add users here, they will be given access to the site, but not to other group resources such as calendars and conversations. To do that, add members to the group instead.

everyone

Everyone except external users

Search Directory

Use of "everyone except external users" domain group



Documents

| Name | Sensitivity |
|---|--------------|
| Branding Elements.pptx | |
| Cross Cultural Marketing Campaigns.pptx | Confidential |
| DG-1000 Product Overview.pptx | |
| DG-2000 Product Overview.docx | Confidential |
| DG-2000 Product Pitch.pptx | |
| DG-2000 Product Specification.docx | |
| International Marketing Campaigns.docx | |

Sites and files without sensitivity labels

SharePoint Advanced Management

- SharePoint Advanced Management (SAM) is an essential add-on for M365:
 - Equips IT admins with a suite of tools to bolster content governance
 - Helps organisations prepare for the Copilot journey



Manage content sprawl

Governing ever-increasing digital content is important for every SharePoint admin



Prevent oversharing

Lack of built-in tools to identify oversharing and broken content inheritance put the content at risk, especially in the AI era



Control Copilot access to content

Existing tools take too long to act. Capabilities that can take actions near real time will be important to control content that Copilot can access and disseminate



Manage content lifecycle

Lack of advanced management tools to continuously monitor and govern inactive/active SharePoint sites make it hard to meet various access and regulatory requirements

Content access management dashboard

- A new SharePoint CMA dashboard is rolling out in October through November 2025
- Key features will include:
 - **Centralised dashboard:** Consolidates multiple governance reports into a single actionable interface
 - **Site health evaluation:** Assess permissions, inactive content, & potential oversharing risks
 - **Lifecycle readiness:** Helps evaluate content readiness and lifecycle compliance, aiding in better retention and archival decisions
 - **Automated governance:** Automates manual governance tasks, saving time and reducing human error
 - **Copilot preparation:** Surface key issues in permissions and lifecycle to better prepare SharePoint environments for Copilot integration
 - **Improved UI:** User-friendly interface with improved navigation, categorised issues, and in-tool tips for better insight and management



Microsoft Purview

Microsoft Purview



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

- Compliance Manager
- DSPM for AI
- Communication Compliance
- Data Lifecycle Management
- Records Management
- Audit & eDiscovery
- Privacy Management (Priva)

- Data Catalogue
- Data Estate Insights
- Data Map
- Data Policy
- Data Sharing

Regulatory & Corporate Compliance

- ISO 27018
- SOC 1&2
- HIPAA
- GDPR
- FedRAMP
- NIST
- EU AI Act
- NIST AI RMF
- ISO/IEC 42001
- ISO/IEC 23894
- Many more...



Microsoft 365 Copilot



Microsoft Purview

Secure

Honors your existing permissions

Protects against data loss and insider risk

Assess oversharing risks and apply recommended corrections

Govern

Supports your lifecycle policies and audit requirements

Detect and investigate non-compliant and unethical usage

Guided assistance to remain compliant with AI regulations

A complete solution to secure and govern Copilot

Information Protection & Governance



Unified Approach



Discover



Classify

Apply Policy

Protection:



- Watermark
- Restrict access
- Encryption
- Prevent data loss

Governance:



- Archiving
- Retention & disposition
- Records management
- Disposition reviews

Monitor

- Sensitive information discovery
- Content explorer
- Activity explorer

- Audit trails
- Proof of disposal

Sensitive information comes in many forms

Internal



Business intellectual property

Business plans, product designs, confidential projects



Employee or customer information

HR Information, resumés, employment records, salary information



Highly confidential information

Mergers and Acquisition, workforce reduction

External



Geographical requirements

GDPR (Europe), CCPA (US: California)



Industry requirements

PCI-DSS, HIPAA



Regulatory requirements

GLBA(US), PIOCP (UK), DPA (France)

Classifiers

Sensitive info types



300+ out of the box info types like Credit card, Passport Numbers, etc.

Clone, edit, or create your own

Supports regex, keywords, and dictionaries

Named entities



50+ entities covering person name, medical terms, and drug names

Best used in combination with other sensitive info types

Trainable classifiers



23+ pre-trained ready-to-use trainable classifiers

More in product preview
Create your own classifier based on business data

Credentials SITs



42+ SITs for digital authentication credential types

Use in auto-labelling and DLP policies to detect sensitive credentials in files



Information Protection & Classification

- For many organisations, information must be classified (labelled) in some way
- Once classified, it can be protected based on the classification
- Microsoft Purview provides both classification and built-in protection mechanisms

Sensitivity

🛡️ No Label

sean.hartman@generation-e.com.au

🛡️ Non-Business (Personal)

🛡️ Public

🛡️ General

Confidential >

Highly Confidential >

🛡️ Unrestricted

🛡️ Employees Only

🛡️ Trusted Recipients

 Government of Western Australia
Department of Transport

VL17

Application to License a Vehicle

When blank, this form is classed as **OFFICIAL**, when completed, this form is classed as **OFFICIAL SENSITIVE**
SEE OVER PAGE FOR IMPORTANT INFORMATION

If the vehicle is not currently licensed in WA or has not previously been licensed in your name, the application must be presented in person by the proposed licence holder or an authorised representative of a Motor Vehicle Dealership with proof of ownership. The 'Sellers Declaration' must be completed by a Motor Vehicle Dealer. **See over for acceptable proof of ownership.** Where the vehicle has previously been licensed in your name, this application and proof of your identity can be presented by a third party, who must also provide proof of their identity.

Current or previous plate number (if factory new write NEW)

Vehicle licensed in name previously ☐

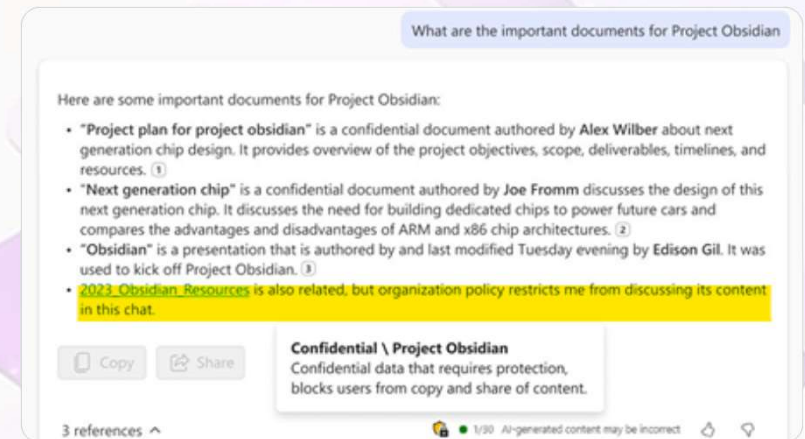
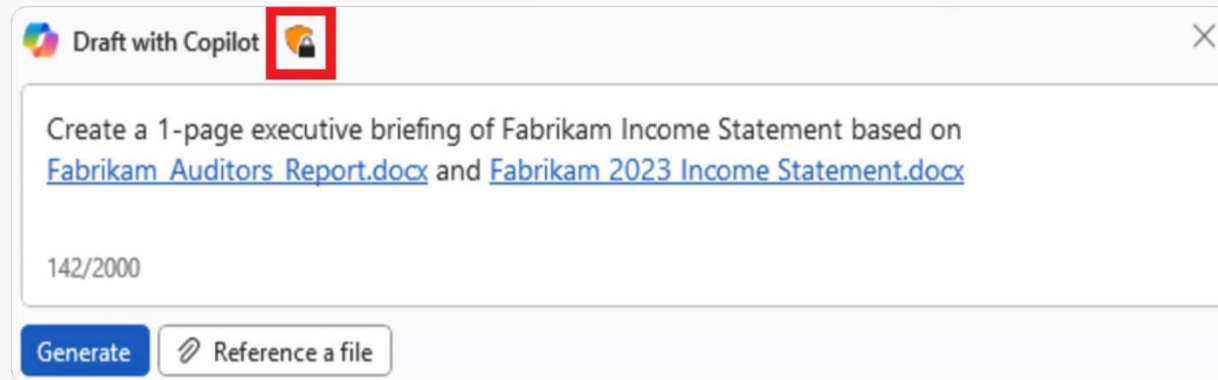
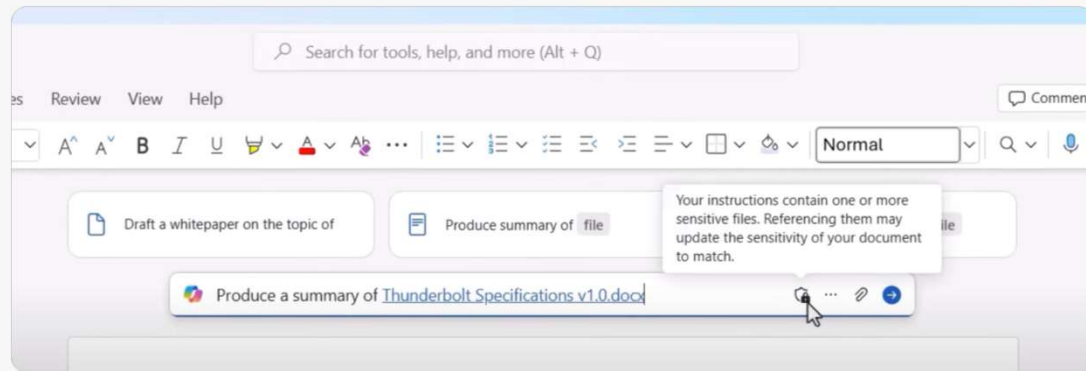
Vehicle to be licensed in new name ☐

PROPOSED LICENCE HOLDER DECLARATION

SELLER'S DECLARATION (Motor Vehicle Dealers)

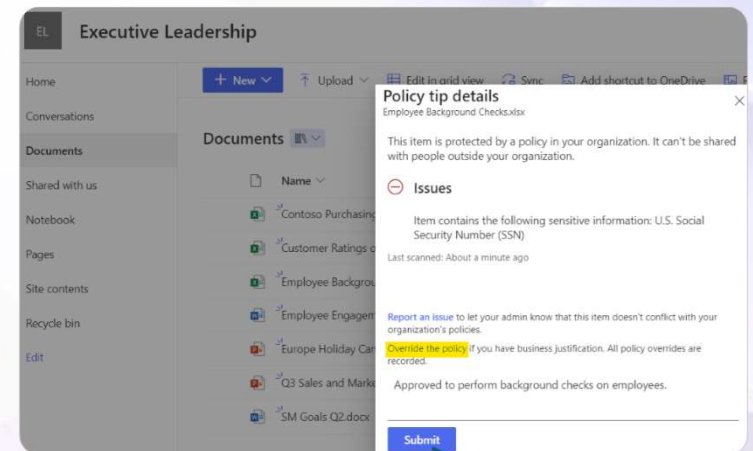
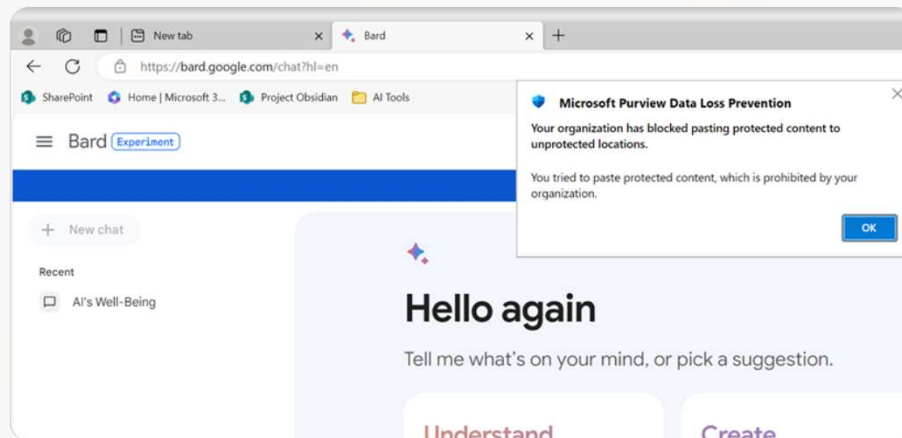
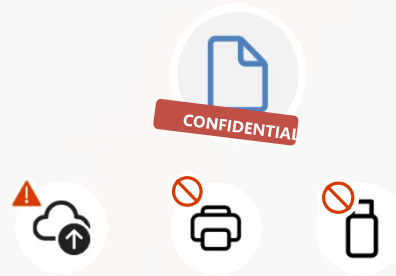
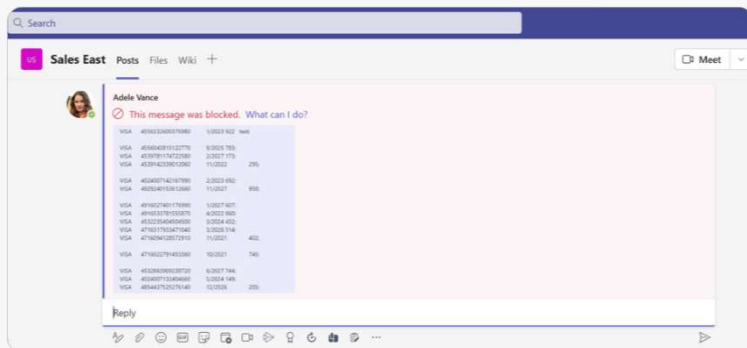
Copilot respects configured protections

Creating new content from or summaries of protected content is respected by Copilot



Data loss prevention

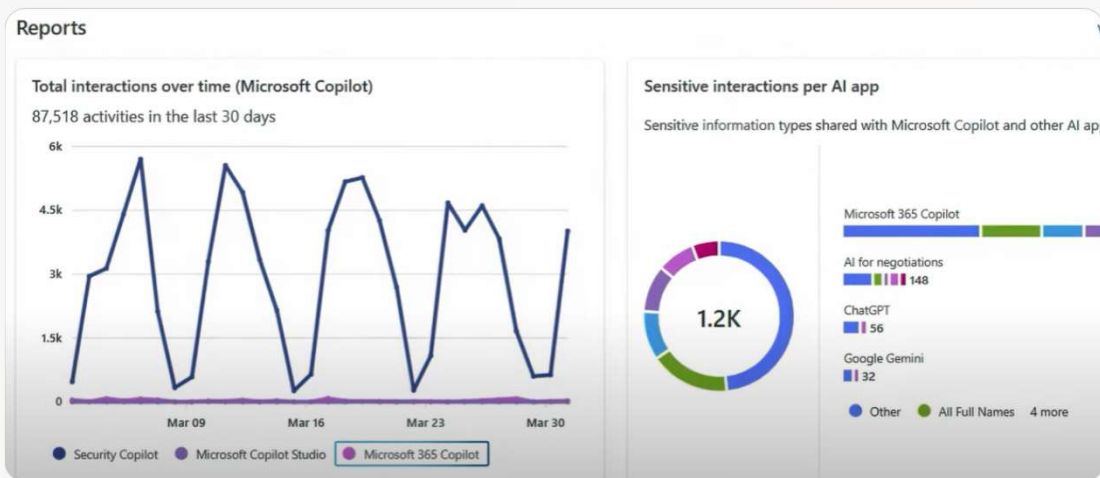
Prevent unauthorised use of data across apps, services, and devices



Prevent sensitive data from being pasted into consumer AI apps

Data Security Posture Management for AI

- DSPM for AI can help protect AI models, data, and applications from various threats
- It provides visibility into AI systems, identifying sensitive data and monitoring its usage
- Two common scenarios for DSPM for AI:
 - **Shadow AI:** DSPM can provide insights and analytics into the usage of third-party public generative AI applications
 - **Copilot Interactions:** DSPM will offer insights into usage, data sensitivity, and related security risks



Insider Risk solutions

Organisations face a broad range of risks from insiders

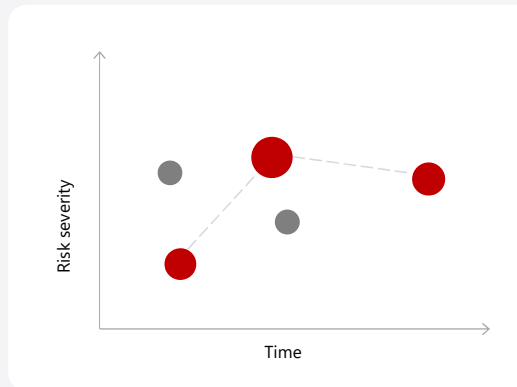
A user performs a series of risky actions



Actions deviate from usual pattern of behaviour

- 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

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

Investigate for compliance & ethical violations



Copyright violation
Insider trading
Corporate sabotage
Regulatory collusion
And more

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

EU AI Act
NIST AI Risk Management Framework
ISO standards 42001 and 23894

Assess and track adherence to regulatory frameworks with Compliance Manager

Communication compliance

Communication Compliance detects non-compliant content in Copilot interactions

The screenshot displays the Microsoft Purview Communication Compliance interface for Contoso Electronics. The left sidebar shows the navigation menu with 'Communication compliance' selected. The main area shows a list of communication items under the 'Pending (19)' tab. The table columns include Subject, Tags, Sender, Recipients, Sentiment, and Date (UTC). One item is selected, and its details are shown on the right.

| Subject | Tags | Sender | Recipients | Sentiment | Date (UTC) |
|-----------------------|------|-------------------------|------------|-----------|--------------|
| Copilot in Word | ... | Alex Wilber <Alex...> | Copilot | Positive | Feb 14, 2024 |
| Copilot in BizChat | ... | Alex Wilber <Alex...> | Copilot | Positive | Feb 14, 2024 |
| Copilot in BizChat | ... | Diego Siciliani <Di...> | Copilot | Positive | Feb 13, 2024 |
| Copilot in BizChat | ... | Diego Siciliani <Di...> | Copilot | Positive | Feb 12, 2024 |
| Copilot in BizChat | ... | Diego Siciliani <Di...> | Copilot | Positive | Feb 1, 2024 |
| Copilot in BizChat | ... | Diego Siciliani <Di...> | Copilot | Positive | Feb 1, 2024 |
| Copilot in BizChat | ... | Diego Siciliani <Di...> | Copilot | Positive | Feb 1, 2024 |
| Copilot in PowerPo... | ... | Alex Wilber <Alex...> | Copilot | Neutral | Jan 30, 2024 |
| Copilot in PowerPo... | ... | Alex Wilber <Alex...> | Copilot | Negative | Jan 30, 2024 |
| Copilot in BizChat | ... | Alex Wilber <Alex...> | Copilot | Neutral | Jan 30, 2024 |
| Copilot in BizChat | ... | Alex Wilber <Alex...> | Copilot | Neutral | Jan 30, 2024 |
| Copilot in Word | ... | Alex Wilber <Alex...> | Copilot | Neutral | Jan 30, 2024 |
| Copilot in Word | ... | Alex Wilber <Alex...> | Copilot | Positive | Jan 30, 2024 |
| Copilot in BizChat | ... | Diego Siciliani <Di...> | Copilot | Positive | Jan 30, 2024 |
| Copilot in BizChat | ... | Diego Siciliani <Di...> | Copilot | Neutral | Jan 29, 2024 |

Copilot in BizChat

Source Plain Text User history

Conditions detected: Gifts & entertainment (take these tickets as a gift) [View all](#)

From: Diego Siciliani <DiegoS@MODERNCOMMS382604.OnMicrosoft.com>
Sent on: Monday, February 12, 2024 6:38:32 PM
To: Copilot <>
Subject: Copilot in BizChat

can you help rephrase this sentence so it's less obvious that I am giving our free gifts to clients? "I would love for you to take these tickets as a gift as an expression of my gratitude for all of the hard work you put in"



Data quality & hygiene

Copilot performance & security are directly tied to the quality & structure of the data it can access

What we hear

- 1 Organisations reaching—and exceeding—storage limits
- 2 Unexpected data overage fees
- 3 No strategy to manage data footprint and mitigate growth
- 4 Retention and disposal requirements are not being appropriately met
- 5 Employees are wasting time searching for relevant information

Data governance

- In the digital age, data is often referred to as the new oil or currency
- However, improper management of data can lead to digital clutter and increased costs
- Address data hoarding by implementing retention, disposition, and archiving policies
- Especially relevant in the age of generative AI where access to outdated information::
 - Can lead to productivity loss
 - Potentially missed opportunities
 - Risk of poor or incorrect decisions

Some organisations are using version history and retention in place of a backup/archival strategy

We should also consider our regulatory requirements for retaining content. Where should it go if not retained in M365?



Decide if you want to retain content, delete it, or both

☒ Retain items for a specific period
Items will be retained for the period you choose.

Retain items for a specific period
7 years

Start the retention period based on
When items were created

At the end of the retention period

☐ Delete items automatically

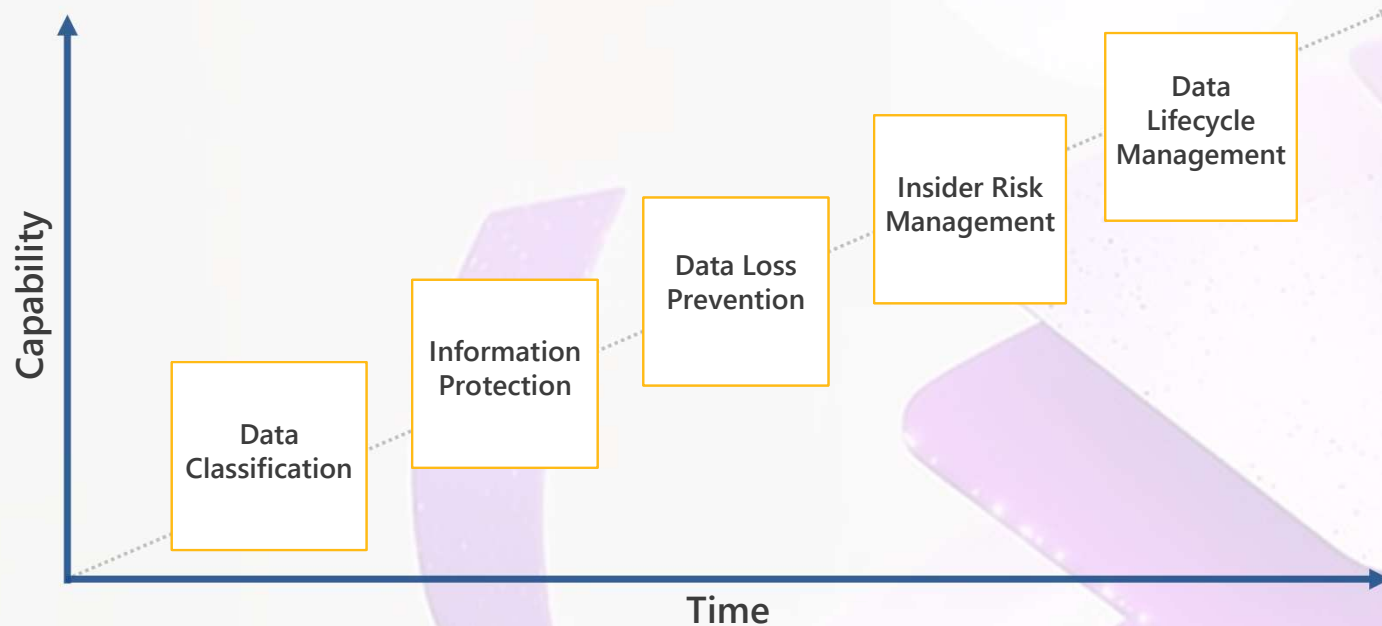
☒ Do nothing

☐ Retain items forever
Items will be retained forever, even if users delete them.

☐ Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Building a data protection strategy

- Implementing a data protection solution is a journey
- A core set of capabilities enables you to have better visibility over the data
 - Data classification to assist with discovery
 - Information protection to assist with labelling of sensitive data
 - Data loss prevention to control the use of sensitive data
- Build your capability over time – the appetite to start again will be low if you get it wrong



Contact Us

Website : www.generation-e.co

Email: sales@generation-e.com.au

Contact us: www.generation-e.co/contact

The deck and recording will be available after this session on our website

[Generation-e | Webinars](#)

Thank you

