

Microsoft 365 Copilot

Security and Compliance controls





Microsoft 365 Copilot

Unlock productivity and unleash creativity

Natural Language



Large Language
Models



Microsoft Graph
- Your Data -



Microsoft 365
Apps



The
Internet



Microsoft 365 Copilot

Built on Microsoft's comprehensive approach



Security



Compliance



Privacy



Responsible AI

Microsoft 365 Copilot

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
Information Protection

4

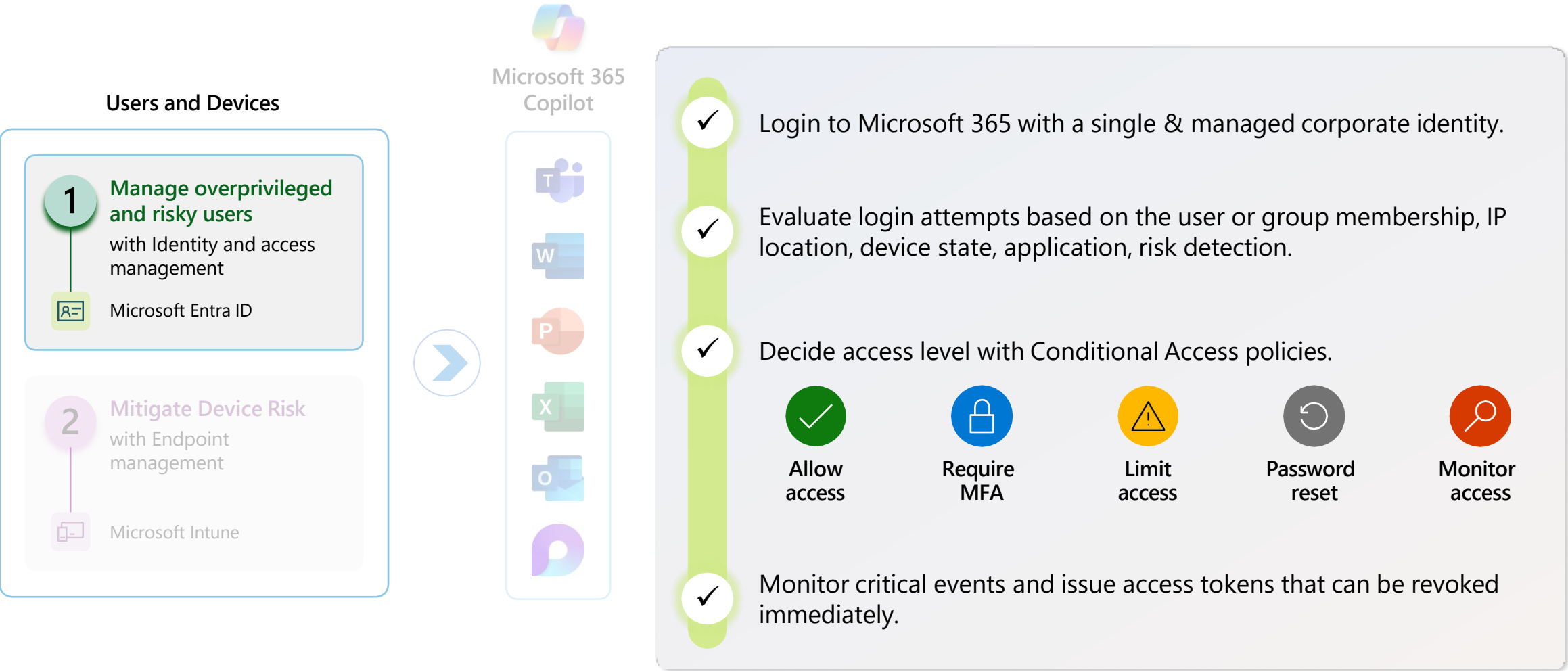
**Discover and
control the use
of AI apps**



Microsoft Defender for
Cloud Apps

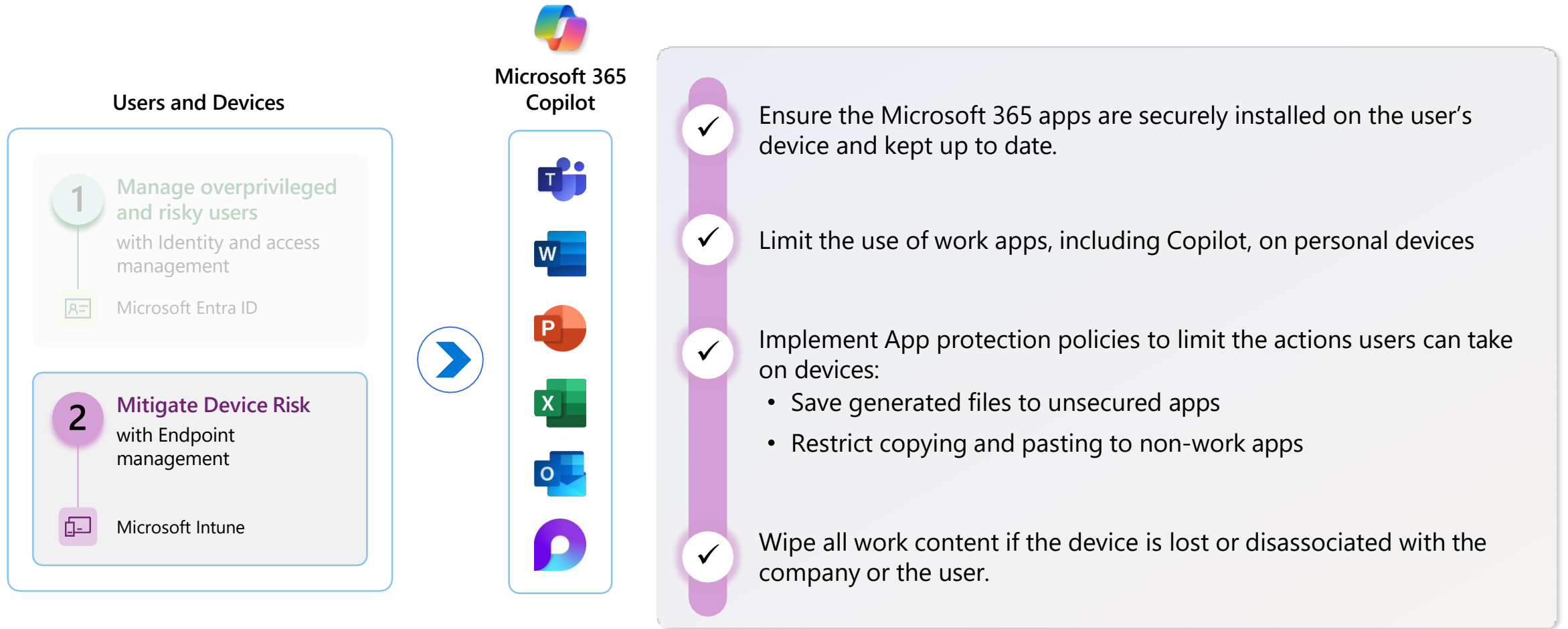
Govern access to Copilot

Microsoft Entra ID



Manage device real-estate

Microsoft Intune



Protect business information and restrict actions

Microsoft Purview Information Protection



Data consumption and processing with Copilot is limited to the user's permissions.



Copilot inherits sensitive documents' sensitivity labels and applies them to its output and references.



If Copilot generates sensitive data and saves it in Microsoft 365, Data Loss Prevention policies will apply.



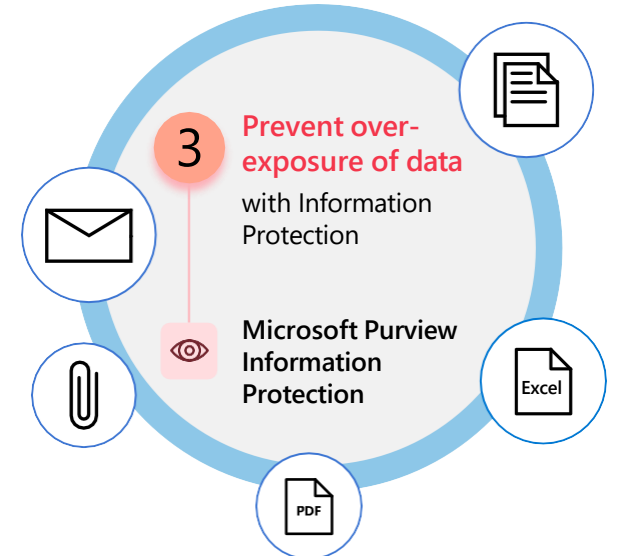
Interactions with Copilot are logged for auditing purposes and business, or code of conduct violations can be detected.



Microsoft 365
Copilot

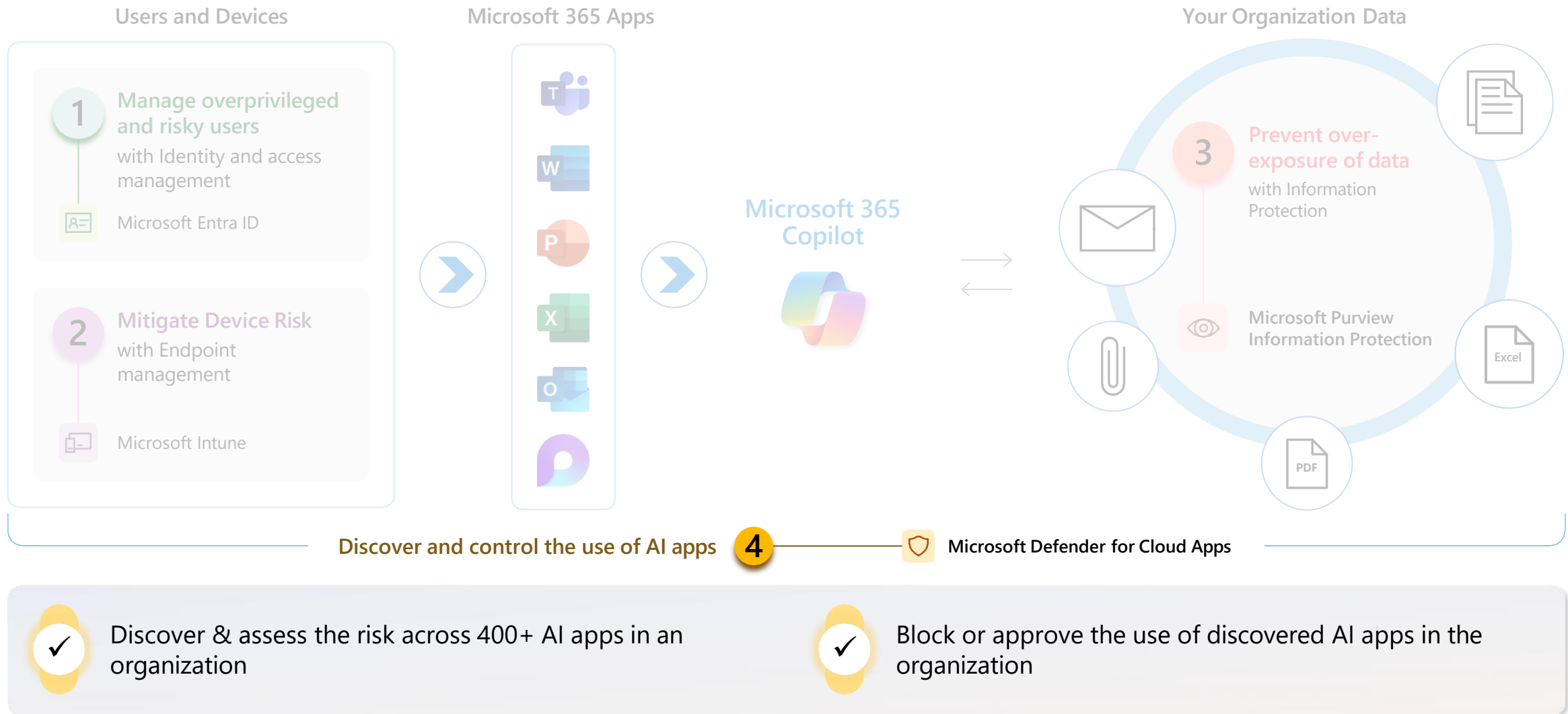


Your Organization Data

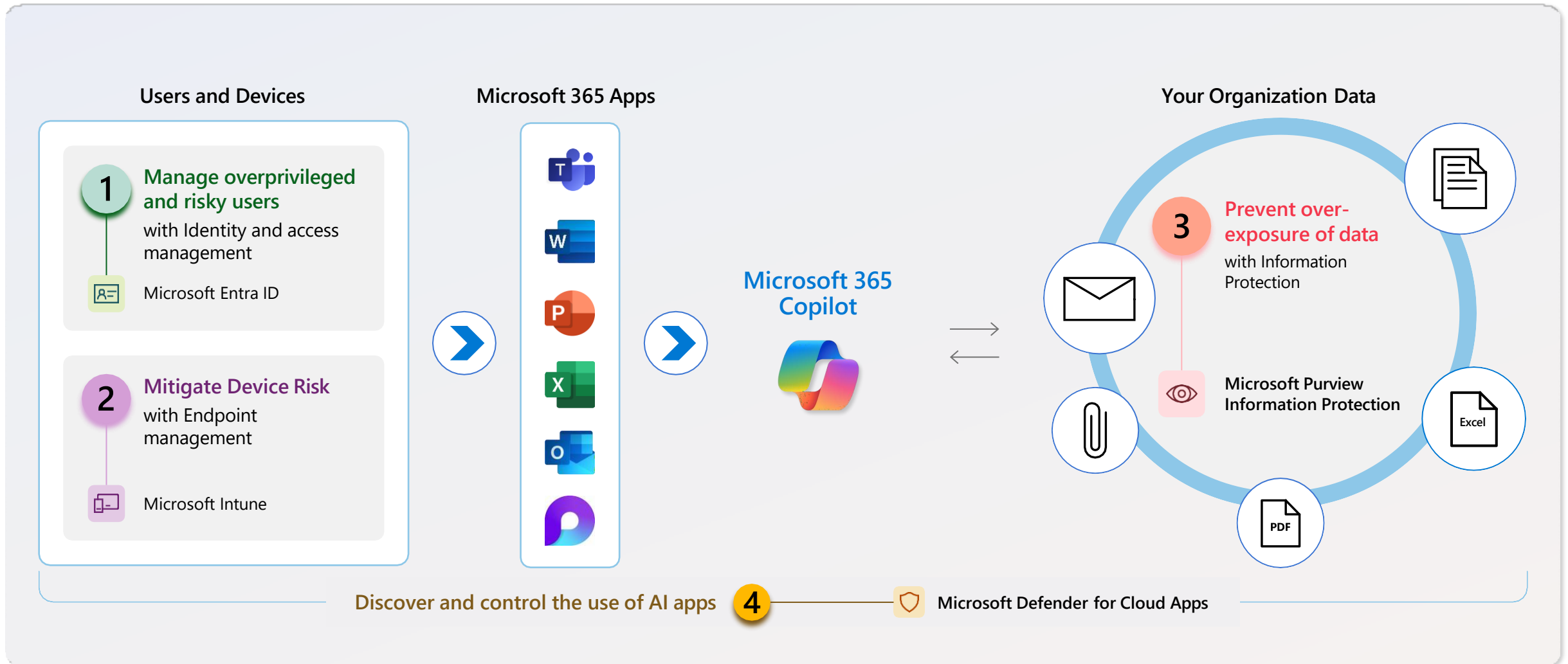


Discover and control the use of AI apps

Microsoft Defender for Cloud Apps



Security and compliance controls for Microsoft 365 Copilot



Licensing options



Security and Compliance controls for Microsoft 365 Copilot

Baseline security



**Copilot +
Office 365 E3**

Multi-factor Authentication
with security defaults

Manual sensitivity labels
for Copilot generated content
(Office only)

Core security controls



**Copilot +
Microsoft 365 E3**

Conditional Access
policies based on identity, device,
location, & network

Manual sensitivity labels
for **non-Microsoft** documents
(e.g., pdf)

Endpoint management
capabilities

Best in class security controls



**Copilot +
Microsoft 365 E5**

User/session risk
and access control

Automatic sensitivity labels
for **non-Microsoft** documents
(e.g., pdf)

Discover and evaluate the
risk of 400+ **AI apps** & implement
controls to for their use at work

O365 and M365 security value for Copilot

Scenario		O365 E3	M365 E3	M365 E5
Identity & Access Management	Login to Microsoft 365 Copilot with a single identity	•	•	•
	Enforce MFA when accessing Microsoft 365 to use Copilot	Basic MFA	•	•
	Enable end-user password reset, change, and unlock when accessing Microsoft 365	Cloud only	•	•
	Implement Conditional Access policies based on identity, device, and location when accessing Microsoft 365 to use Copilot		•	•
	Enable near real-time access policies enforcement, evaluate critical events, and immediately revoke access to Microsoft 365		•	•
	Control access over cloud apps (Microsoft 365 and third party)			•
	Review who has access to content in Microsoft 365 – Copilot – to reduce oversharing			•
	Require just-enough and just-in-time approval for admin roles that can manage Copilot app access			•
Endpoint Management	Push/deploy the Microsoft 365 apps to devices and grant access to Copilot in these apps		•	•
	Manage Microsoft 365 apps updates		•	•
	Restrict the use of the Microsoft 365 apps and Teams – as well as Copilot in these apps – on personal devices		•	•
	Prevent saving files – including those generated by Copilot – to unprotected apps		•	•
	Wipe all work content – including content generated by Copilot – if a device is lost		•	•
	Revoke work access on noncompliant devices		•	•
Data security & compliance	Search for Copilot generated data by content, keyword search, apply legal hold, and export the search results; investigate incidents related to Copilot and respond to litigations	Standard	Standard	Premium
	Audit logs for Copilot interactions	Standard	Standard	Premium
	Apply a retention policy for Copilot interactions	Standard	Standard	Automated
	Data Loss Prevention policies to protect sensitive data, generated by Copilot and saved in Microsoft 365 locations, from exfiltration	Files & email	Files & email	+ Endpoint, Teams
	Inherit sensitivity labels and cite sensitivity label in output and references in Copilot	•	•	•
	Prohibit Copilot from summarizing or including data that users have no extract permissions in its response messages for the said users	•	•	•
	Exclude sensitive files that users have no view permission from being processed by Copilot for the said users	•	•	•
	Label and protect Microsoft 365 content, used by Copilot	Office only	Manual	Automated
	Detect business or code of conduct violations for Copilot prompts and responses			•
	Prevent Copilot access to content encrypted with Double Key Encryption			•
	Use ready-to-use machine learning trainable classifiers to identify sensitive information and create custom classifiers			•
Threat Protect	Discovery and risk evaluation across 400+ AI apps in an organization			•
	Ability to block or sanction the use of any discovered AI app in the organization			•

Thank you.

