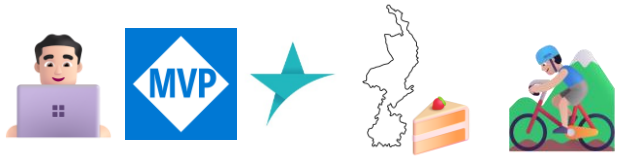
International Data Security User Group

Protect Your Microsoft 365 Data in the Age of AI

(Extended Ignite Edition)

Hi,
I’m Dominique



- Dominique Hermans
- Microsoft Security MVP (Technology Area Microsoft Purview)
- Work at InSpark as Data Security Consultant
- Live in Limburg (NL)
- Data Security | Community | Blogging | Music | Cycling

Agenda

- ➡️ Todays Challenge
- ➡️ Techniques already in store
- ➡️ Licensing
- ➡️ Example Case
- ➡️ One More Thing...

Todays Challenge

Because yes, I believe most organizations have a challenge when it comes to AI use

The Gen AI Wave: Todays challenge

More and more employees are using generative AI tools to be more productive. They use:

- A generative AI tool that has been provided or allowed by the users' organization or
- A generative AI tool of choice has **not** been provided or allowed by the users' organization.

The challenge however remains the same, how do you maintain control over your data?

Techniques already in store

Why reinvent the wheel?

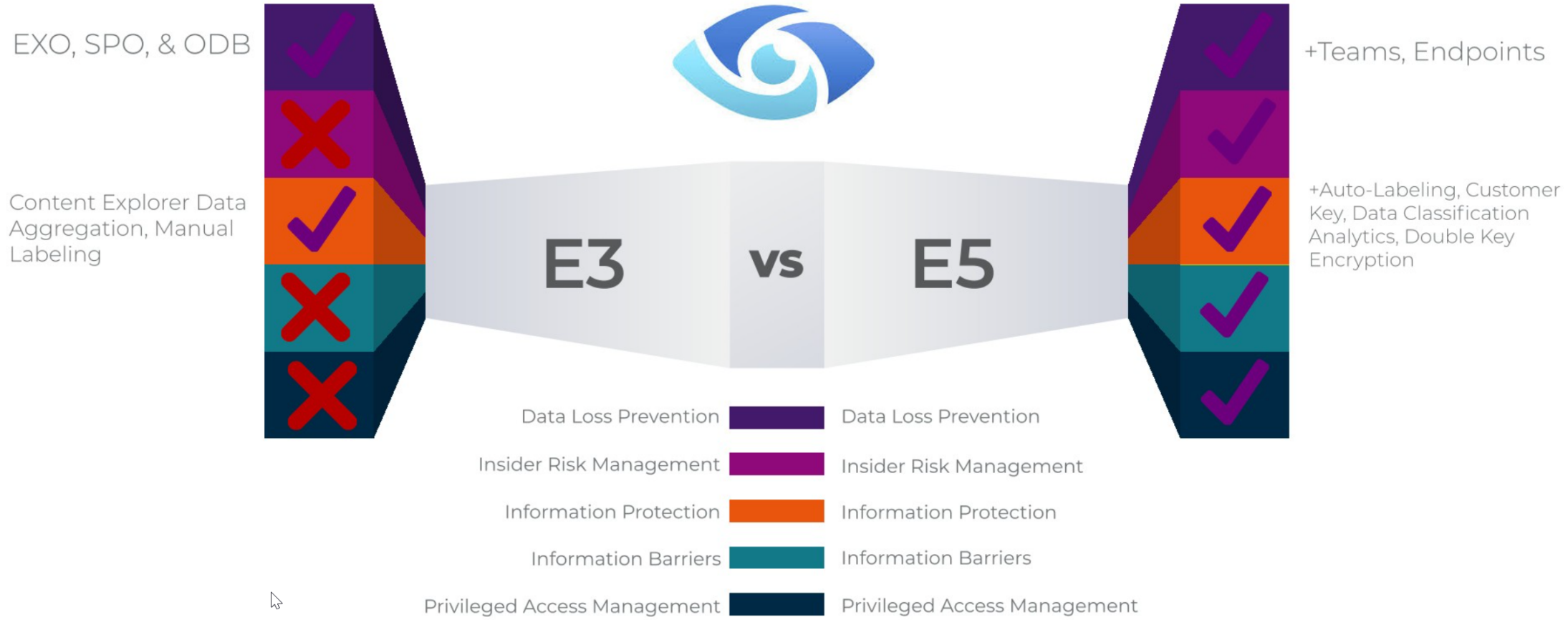
DSPM (for AI)

Create quick out-of-the-box policies for creating insight in and securing data against generative AI platforms

Licensing

Always save the best for last

MICROSOFT PURVIEW
DATA SECURITY



Picture by Matthew Silcox

DominiqueHermans.com

- For AI apps other than Microsoft 365 Copilot and Microsoft Facilitator, you've set up pay-as-you-go billing for your organization. When this billing model is applicable for specific configurations, you'll see notifications and instructions in the UI.

  Considerations for deploying Microsoft Purview Data Security Posture Management (DSPM) for AI | Microsoft Learn

Solution	Applies to	Unit of Measure	Details
On-demand classification (preview)	Applies when you run a scan to identify and classify sensitive content in data stored in SharePoint and OneDrive	Asset, based on the number classified per scan	Learn more about On-demand classification (preview)
Security Copilot	Applies for all Security Copilot functions	Security Compute Units	Get started with Security Copilot
Network Data Security (preview)	Requests from an endpoint device to a website, cloud app, or generative AI app	Number of requests sent from the endpoint device to the website, cloud app, or generative AI app	Network data security only counts requests that are outbound from the device.
Data Security for Gen AI Appications	Applies to classification and protection of sensitive content for non-M365 AI interactions (prompts/responses)	Number of requests or messages for non-Microsoft 365 AI interactions (prompts or responses)	Learn more about data security for AI interactions

Learn about Microsoft Purview billing models | Microsoft Learn

DominiqueHermans.com

Requests

A request as a unit of measure for pay-as-you-go billing purposes is defined as each network call made from a devices or browser to a website or API. This doesn't include the responses to the requests. Requests are counted in the monthly pay-as-you-go bill you receive from Azure on a monthly basis. Microsoft Purview network data security pay-as-you-go uses requests as its unit of measure. Here are some examples:

Expand table

Activity	Data type	Example
Text sent to or shared with cloud or AI app	human readable strings transmitted inline	- submitting a form with textual information - Sending raw text or a prompt to a generative AI - the body of an email - sending JDSON data to an API
File uploaded to or shared with cloud or AI app	Byte streams, including text based file, binary files, txt files, source code, documents, images, videos, .exe's, .pdf's, archive files	- Uploading a profile picture to social media - sending a document or PDF file as an email attachment - sharing a document with generative AI - transferring a document or .ZIP files to a cloud storage solution

Learn about Microsoft Purview billing models | Microsoft Learn

DominiqueHermans.com

Data Security | In Transit Protection (Public Preview)

Microsoft Purview In Transit Protection is billed based on the number of requests, or packets of information sent back and forth from a device or non-Microsoft browser to a website or application through the internet. With In Transit Protection, Purview data security controls such as classification, labeling, or DLP policy verdicts can be applied to the data contained within these requests. The volume of requests can vary based on the website or application with which users are interacting or the activity they are performing. Customers will only be billed for requests that are detected within the scope of a Purview policy (e.g. collection policy, labeling policy, or DLP policy). See the FAQ below for more details on requests.

Note: Advanced classification using Exact Data Match and Optical Character Recognition is not included in the In Transit Protection pricing.

Feature	SKU	Price
In Transit Protection	Standard	**$0.50**/10K Requests

Pricing - Microsoft Purview | Microsoft Azure

DominiqueHermans.com

Example Case:

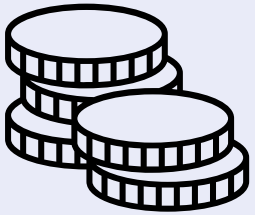
Cashanova Capital

For the charming approach to capital management. 

Scenario

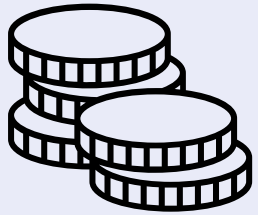
We are a capital management company.
We want to comply with the following conditions:

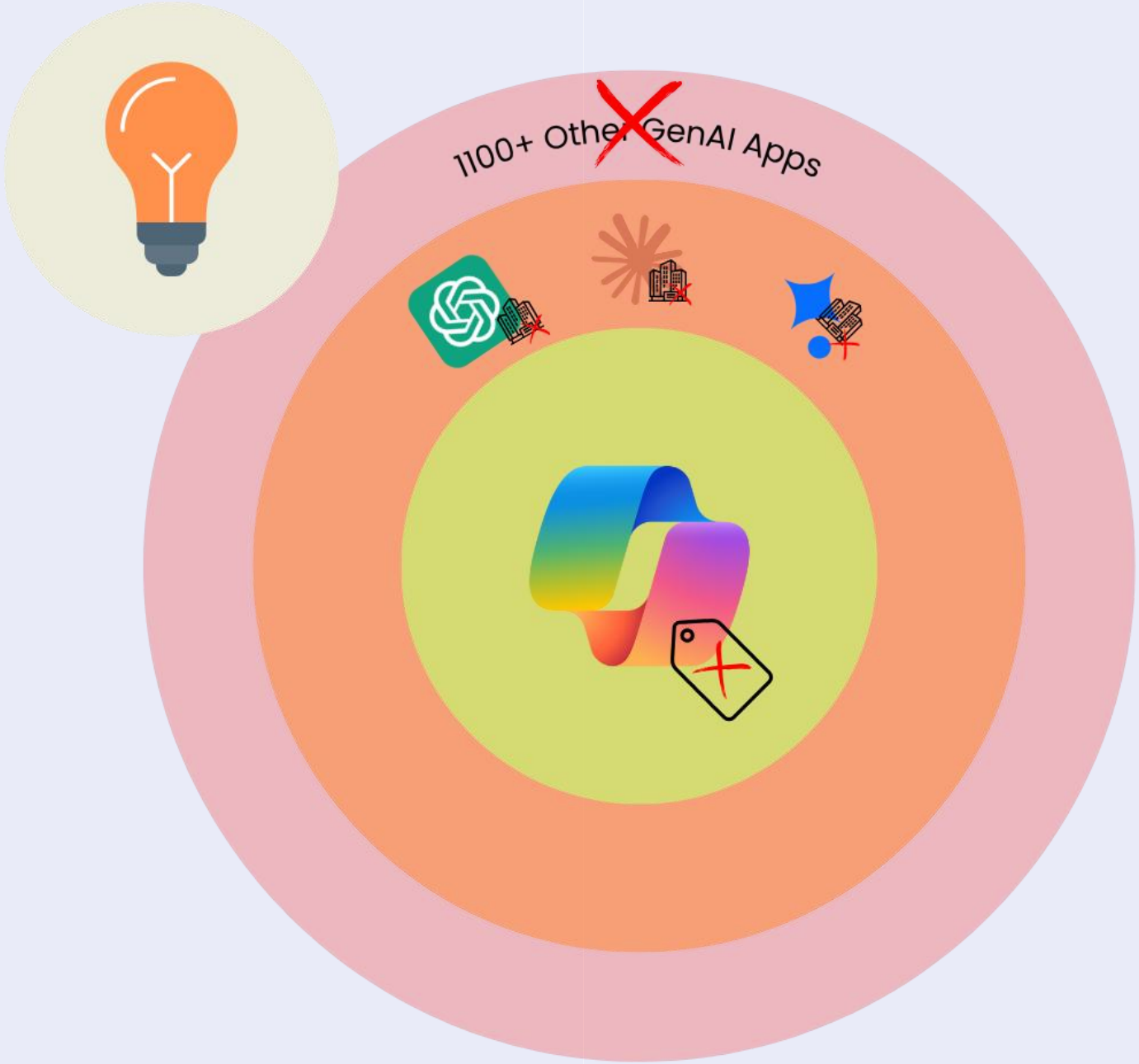
1. Create insight in the use of sensitive info shared with GenAI apps in our company.
2. Allow the use of M365 Copilot but prohibit its use on files labeled as sensitive.
3. Allow third-party GenAI apps such as ChatGPT, Claude, and Google Gemini, but block the sharing of the following sensitive information: [next slide]
4. Block usage of other GenAI apps completely.



Scenario

ABA Routing Number, Azure SAS, Azure Storage Account Key (Generic), Belgium National Number, **Credit Card Number**, Drug Enforcement Agency (DEA) Number, Germany Identity Card Number, Germany Tax Identification Number, Germany Value Added Tax Number, International Banking Account Number (IBAN), IP Address, IP Address v4, IP Address v6, **Netherlands Citizen's Service (BSN) Number**, Netherlands Tax Identification Number, Netherlands **Value Added Tax Number**, SWIFT Code, U.S. Bank Account Number, U.S. Driver's License Number, U.S. Individual Taxpayer Identification Number (ITIN), U.S. Social Security Number (SSN), **Ordernumber**




1100+ Other GenAI Apps

Prerequisites

Condition 1

Create insight in the use of sensitive info shared with GenAI apps in our company.

Condition 2

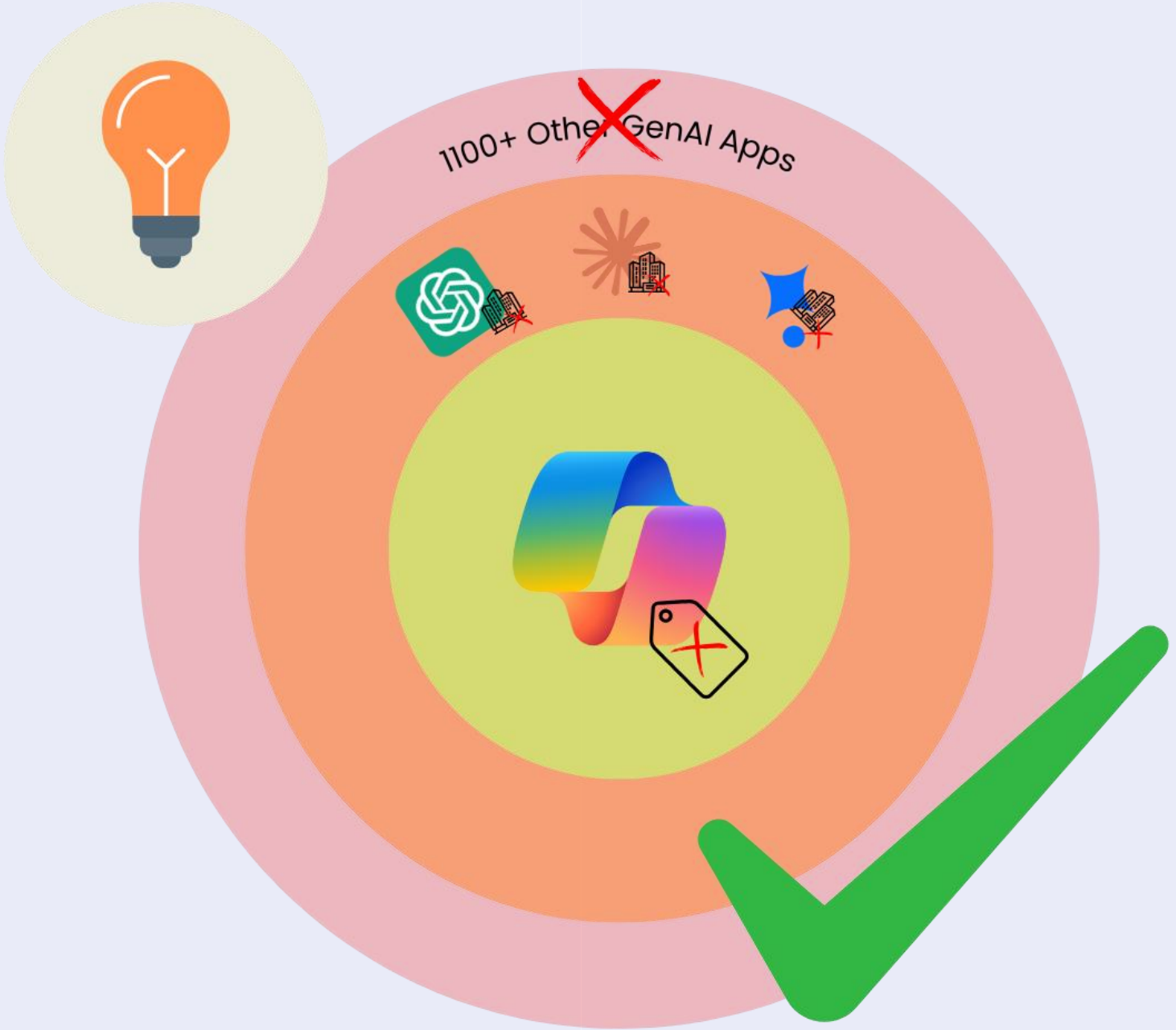
Allow the use of M365 Copilot but prohibit its use on files labeled as sensitive.

Condition 3

Allow third-party GenAI apps such as ChatGPT, Claude, and Google Gemini, but block the sharing of sensitive information.

Condition 4

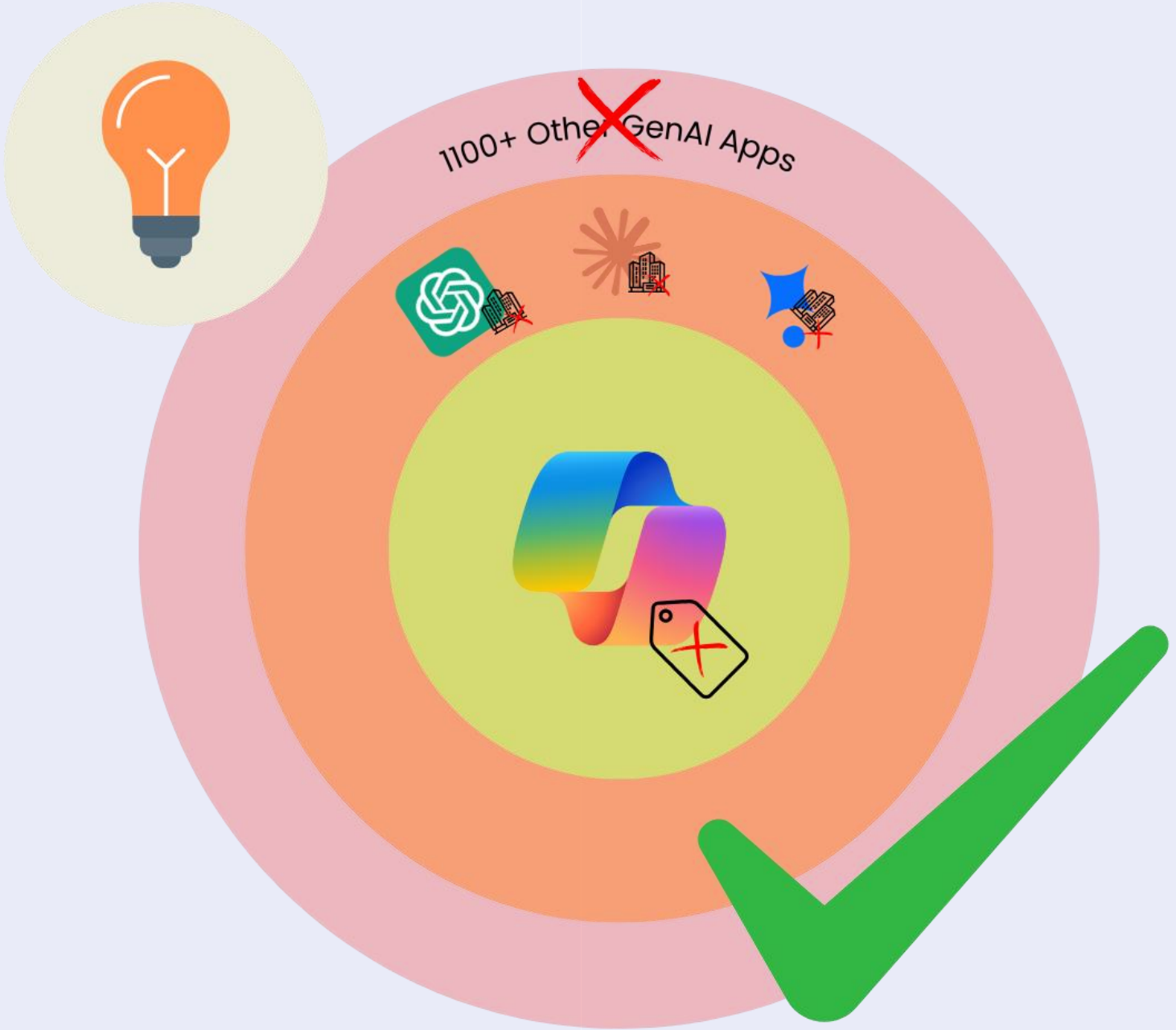
Block usage of other GenAI apps completely.


1100+ Other GenAI Apps

One More Thing...

~~One~~ A Couple More Things...

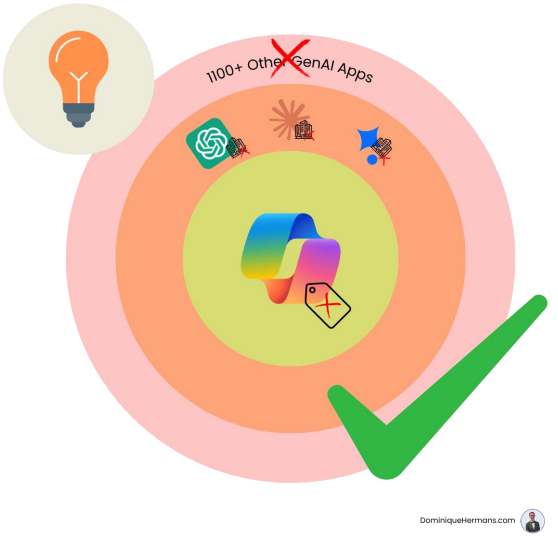
Microsoft Ignite


1100+ Other GenAI Apps

~~One~~ A Couple More Things...

Agent 365

AI Adoption Needs for Enterprises

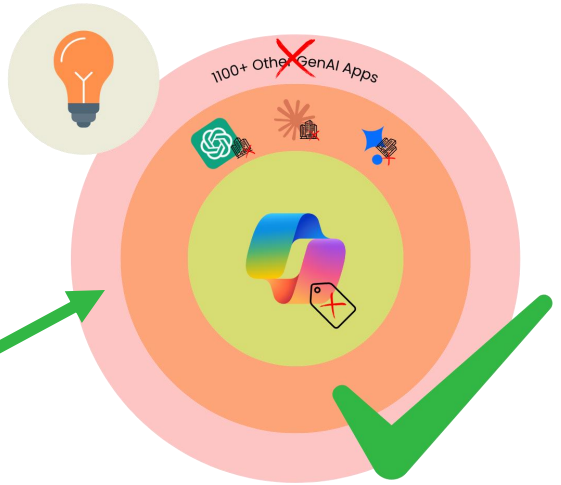


1.3B

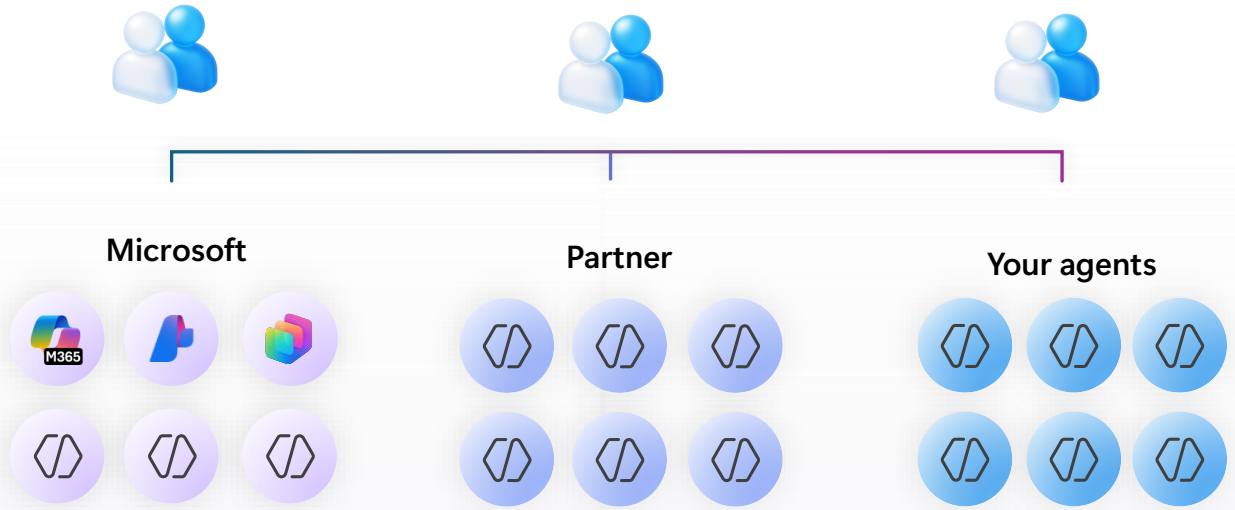
projected number of agents by 2028

Source: IDC Info Snapshot, 1.3 Billion AI Agents by 2028, doc #US53361825, May 2025

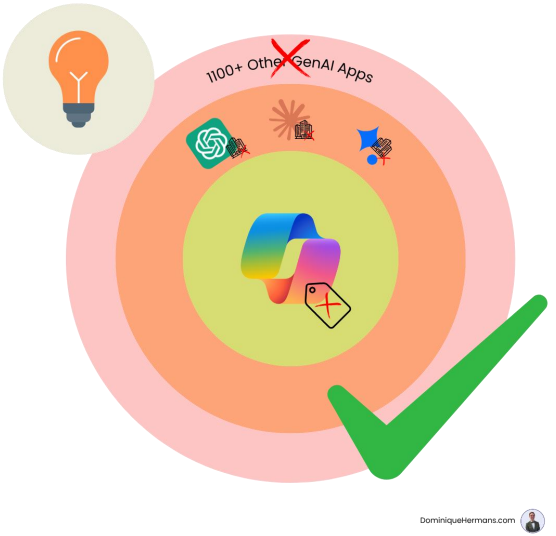
Every organization has a mix of agents



DominiqueHermans.com




M365
Agent 365


1100+ Other GenAI Apps
DominiqueHermans.com

Home
Copilot
Agents
Overview
All agents
Settings
Users
Teams & groups
Marketplace
Billing
Setup
Customize navigation
Show all

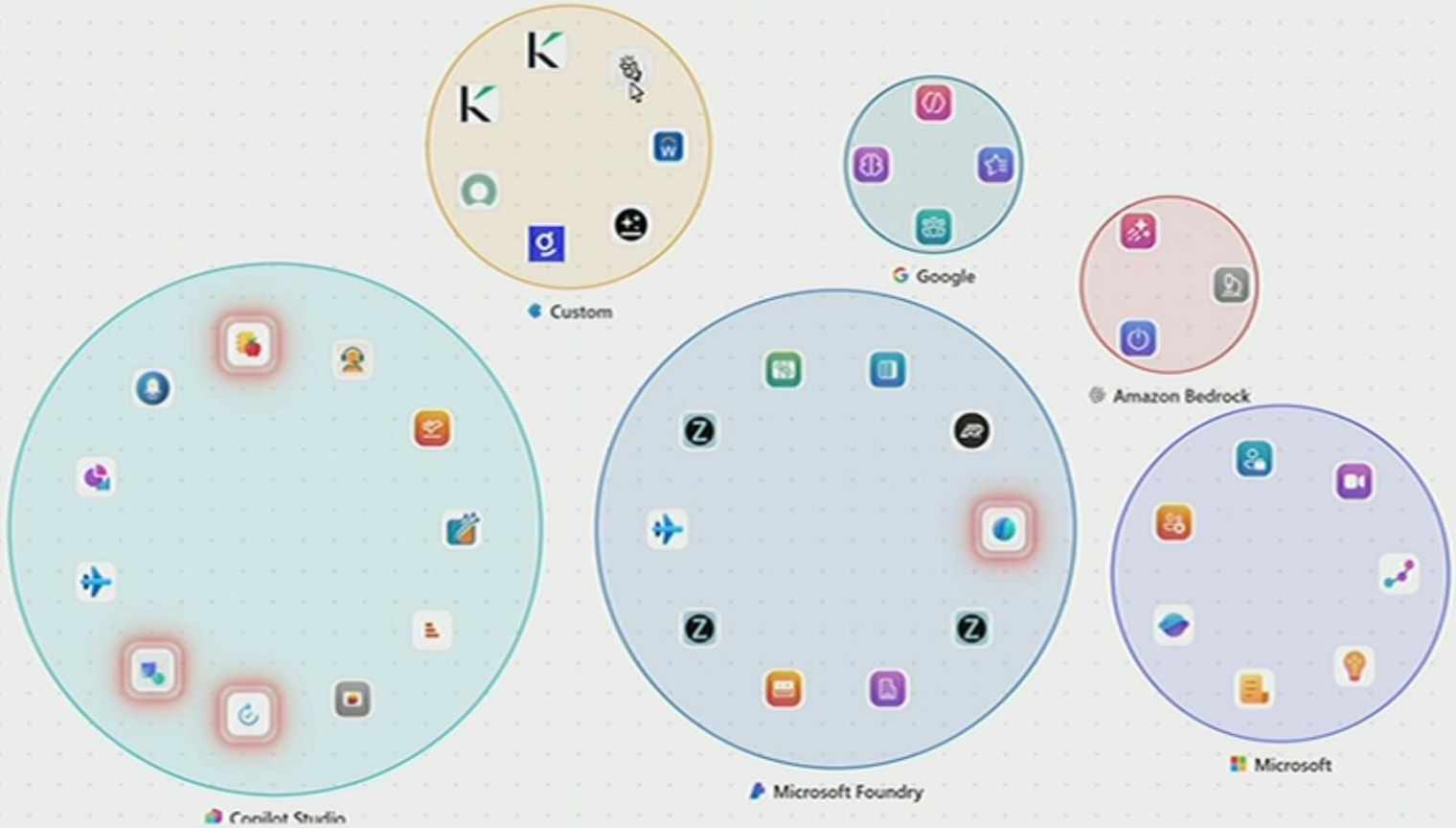
All agents

Agent 365

Monitor and manage agents powered by Microsoft Entra in your organization. Manage in Entra | Learn more about managing agents

Map | Registry | Requests | Catalog

Filters: Publisher | Availability | Channel | Deployment | Platform | Alert : Yes



Home
Copilot
Agents
Overview
All agents
Settings
Users
Teams & groups
Marketplace
Billing
Setup
Customize navigation
Show all

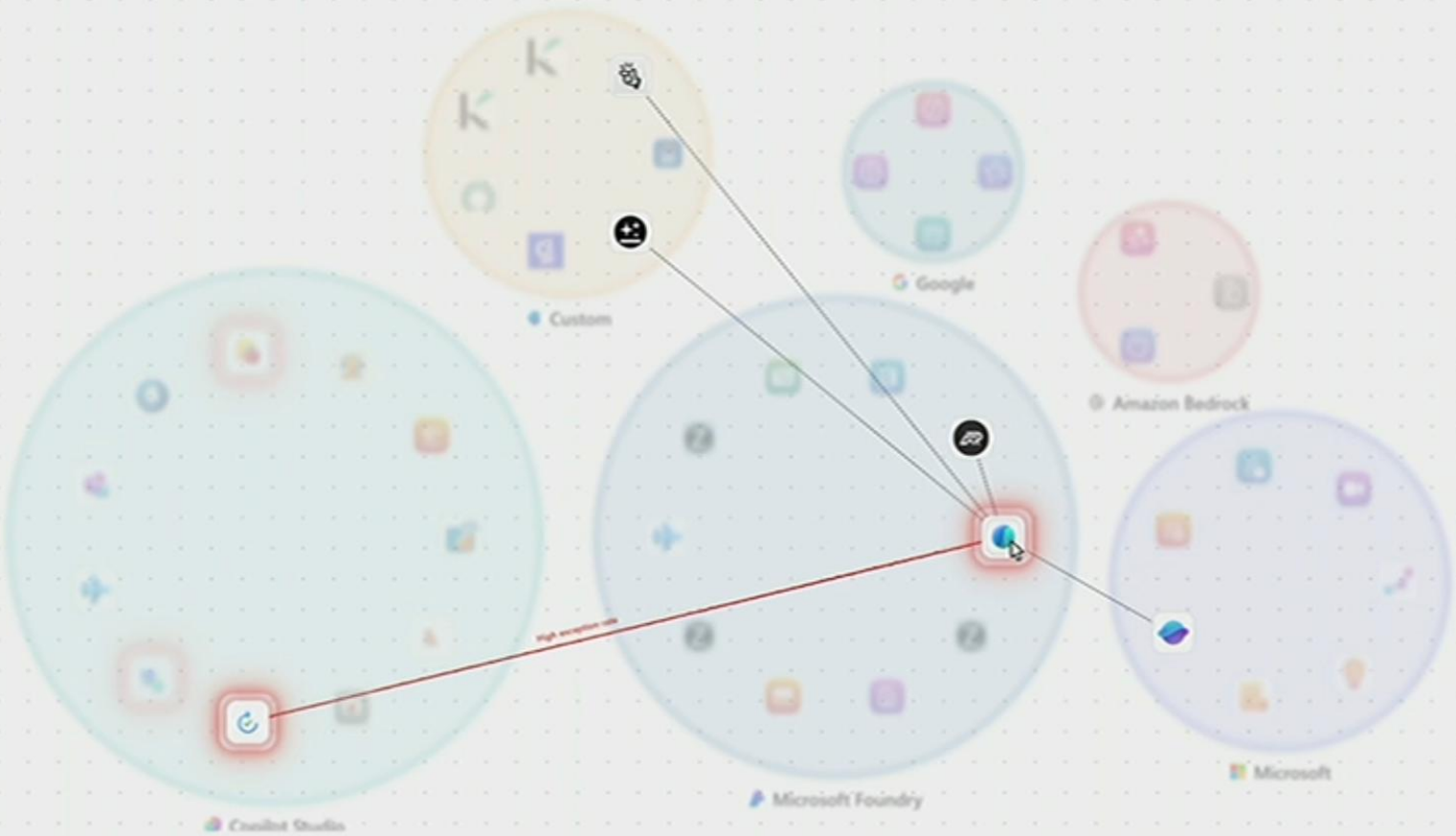
All agents

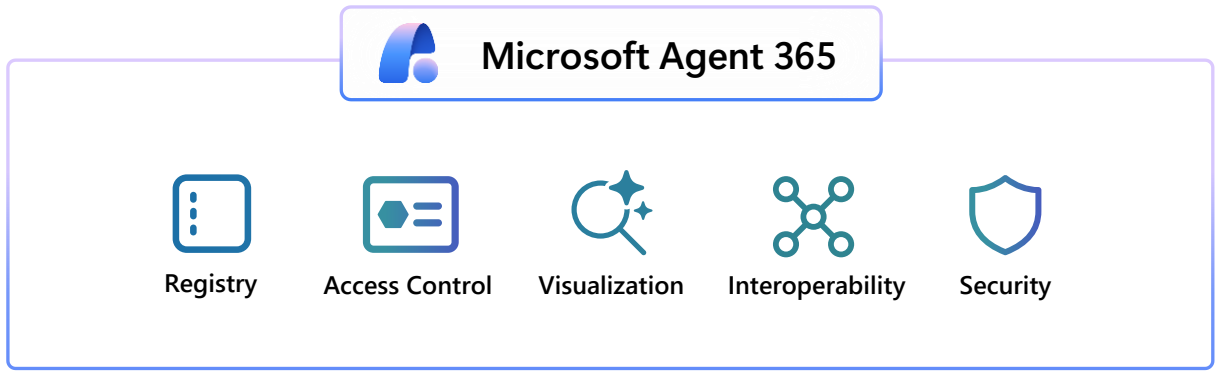
Agent 365

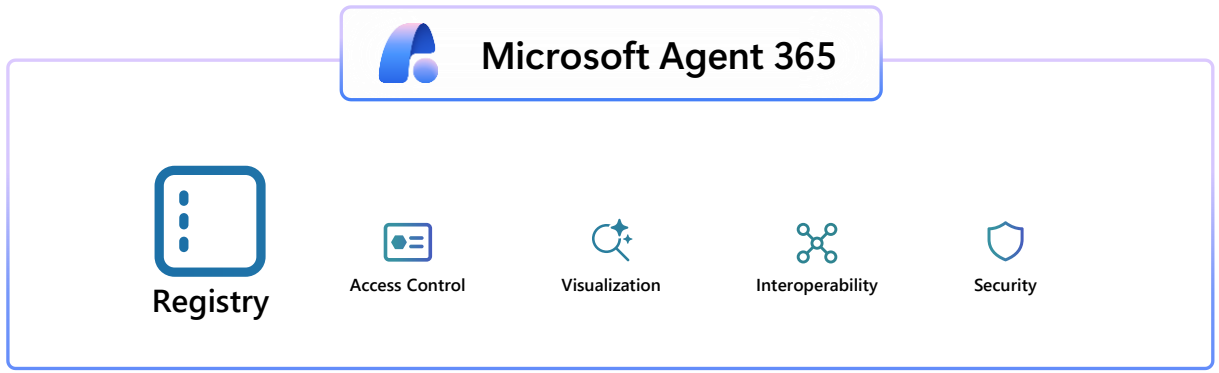
Monitor and manage agents powered by Microsoft Entra in your organization. Manage in Entra | Learn more about managing agents

Map | Registry | Requests | Catalog

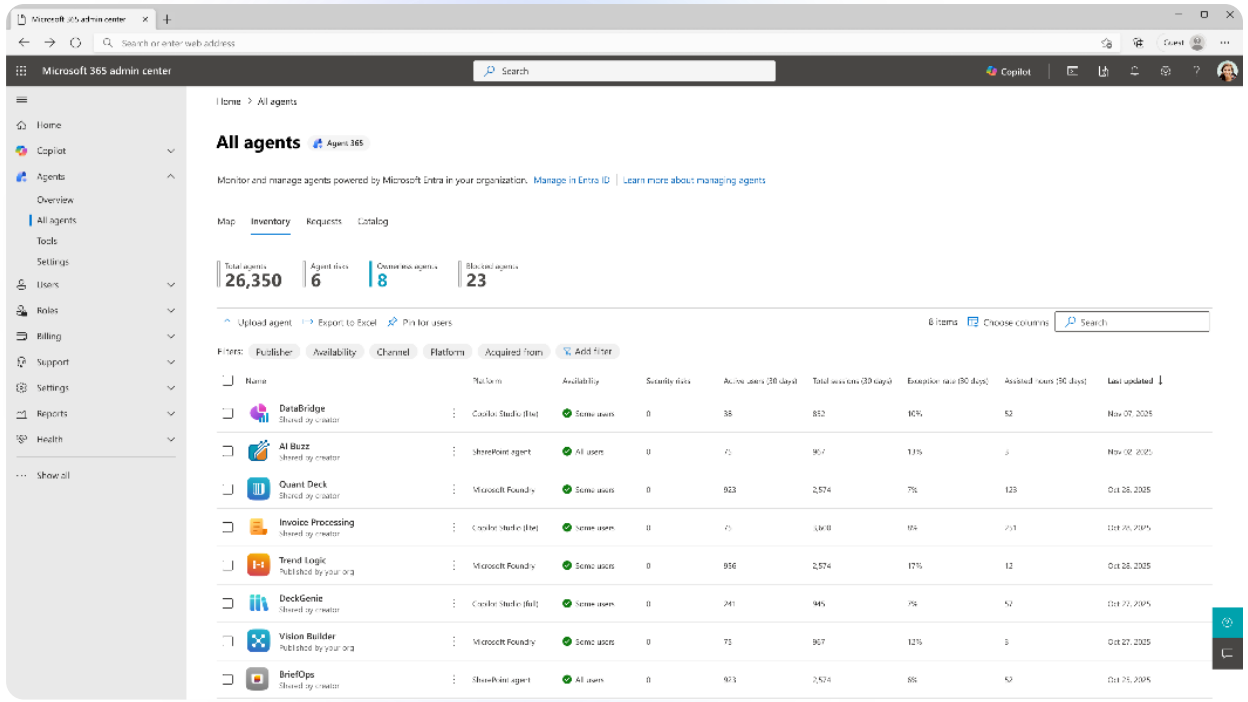
Filters: Publisher | Availability | Channel | Deployment | Platform | Alert : Yes

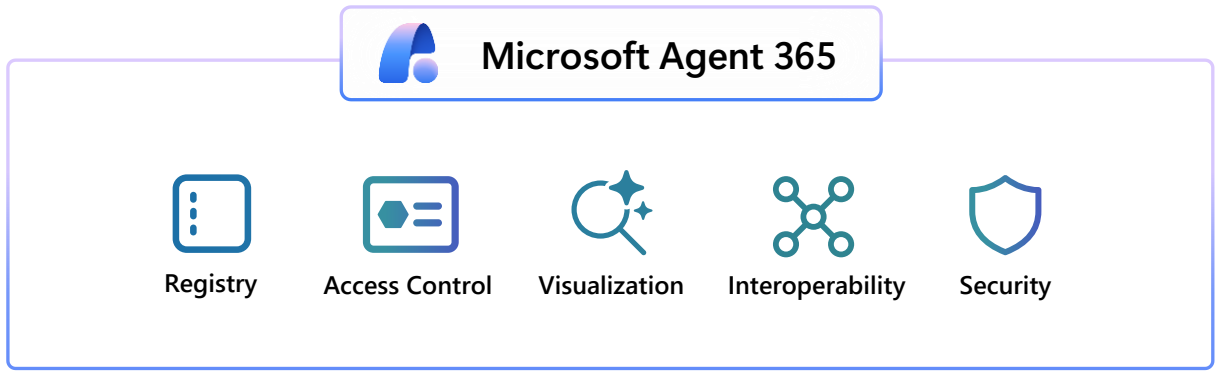


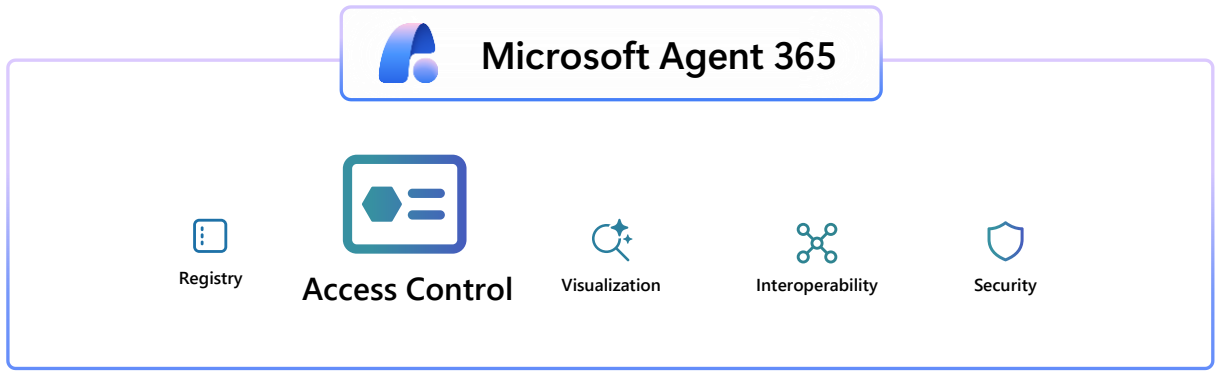

Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security


Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security

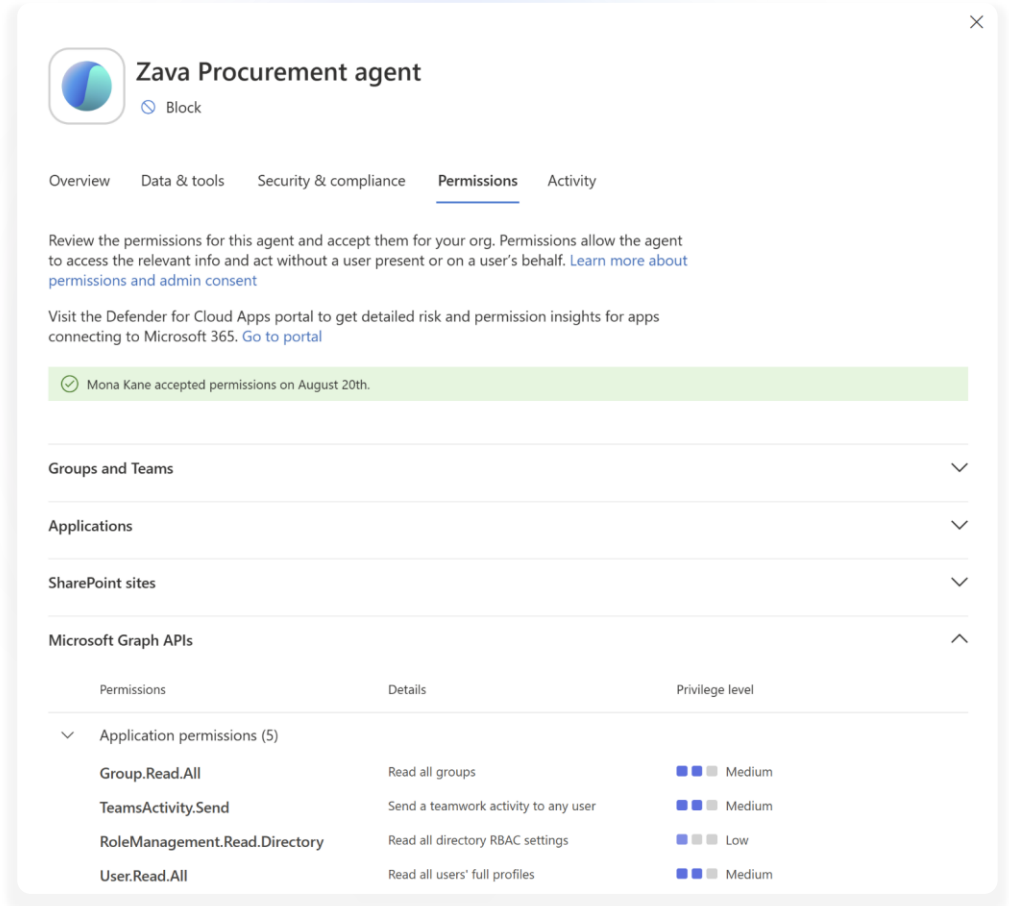
Registry

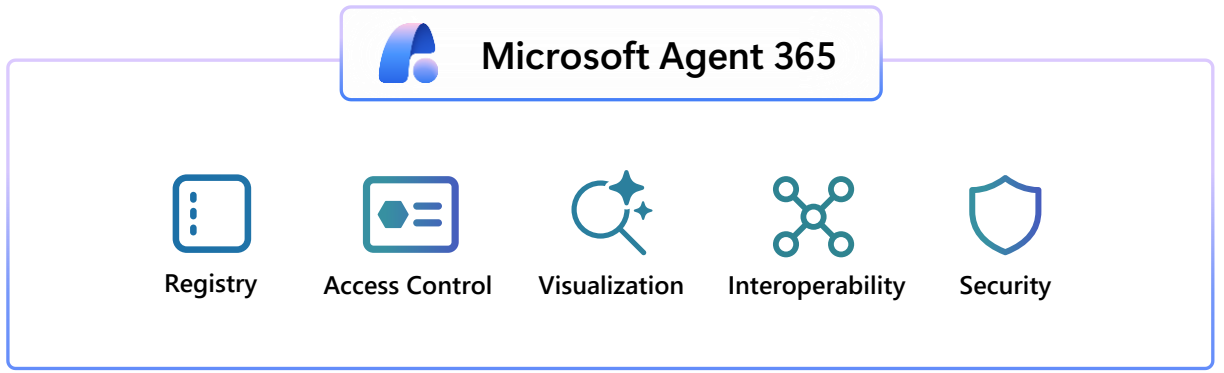

Microsoft 365 admin center
Search
Copilot
Home
Copilot
Agents
Overview
All agents
Tools
Settings
Users
Roles
Billing
Support
Settings
Reports
Health
Show all
Home > All agents
All agents
Agents 365
Monitor and manage agents powered by Microsoft Entra in your organization. Manage in Entra ID | Learn more about managing agents
Map
Inventory
Requests
Catalog
Total agents
26,350
Agent risks
6
Connected agents
8
Blocked agents
23
Upload agent
Export to Excel
Pin for users
8 items
Choose columns
Search
Filters:
Publisher
Availability
Channel
Platform
Acquired from
Add filter
Name
Platform
Availability
Security risks
Active users (28 days)
Total sessions (30 days)
Escalation rate (90 days)
Assisted hours (90 days)
Last updated
DataBridge
Shared by creator
Some users
AI Buzz
Shared by creator
All users
Quant Deck
Shared by creator
Some users
Invoice Processing
Shared by creator
Some users
Trend Logic
Published by your org
Some users
DeckGenie
Shared by creator
Some users
Vision Builder
Published by your org
Some users
BriefOps
Shared by creator
All users

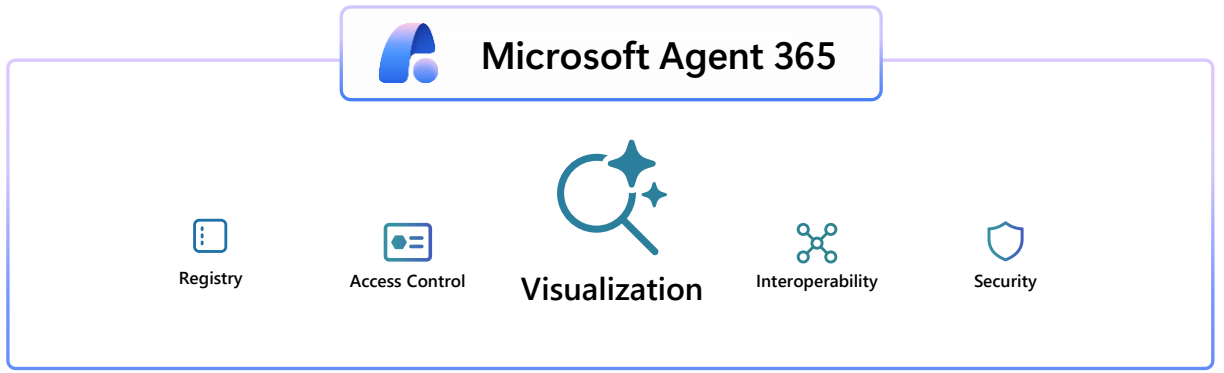

Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security


Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security

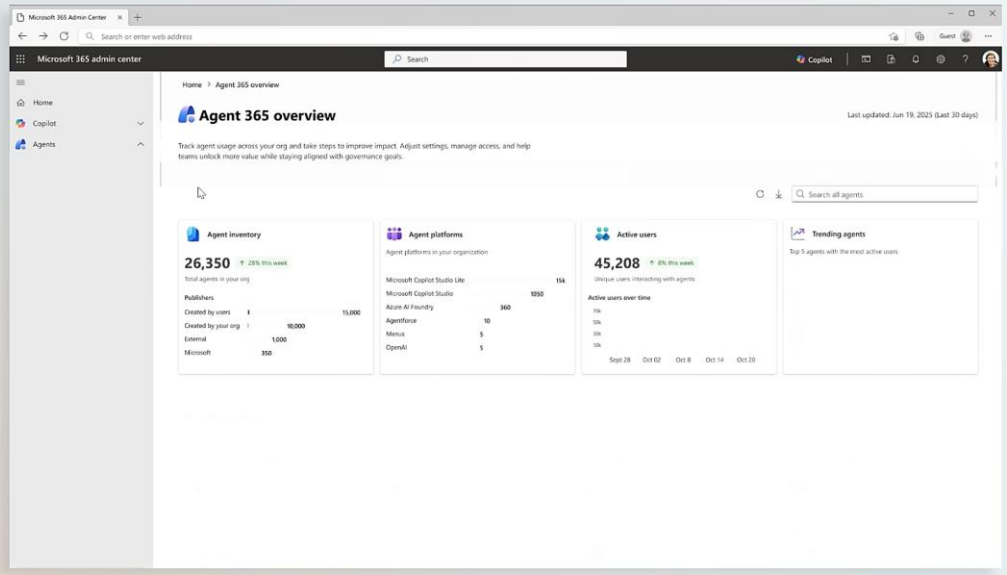
Access Control

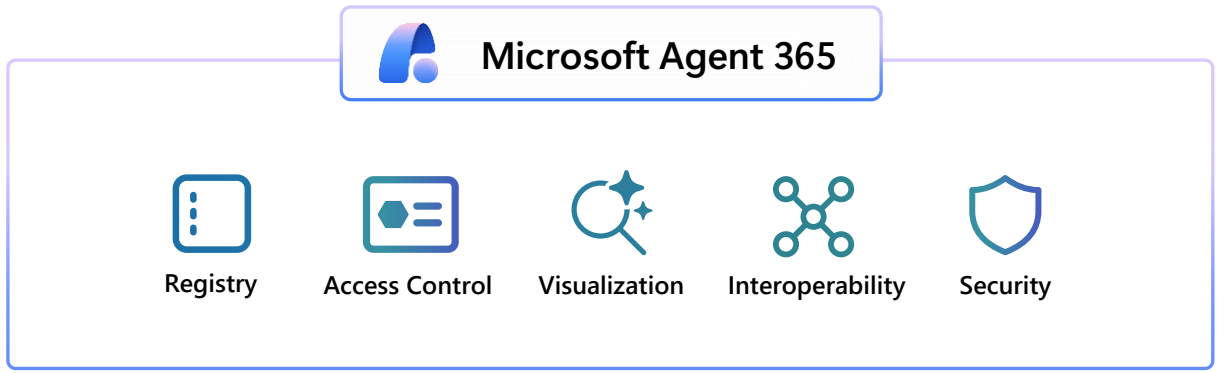


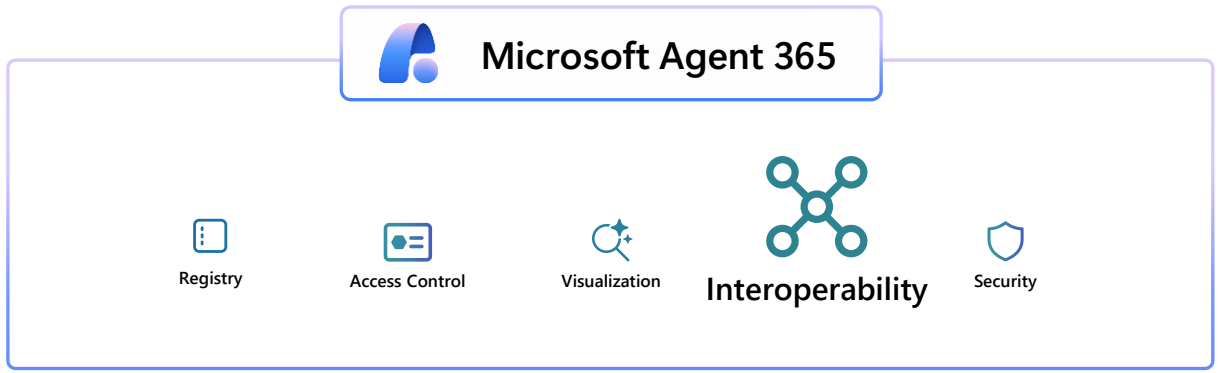

Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security


Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security

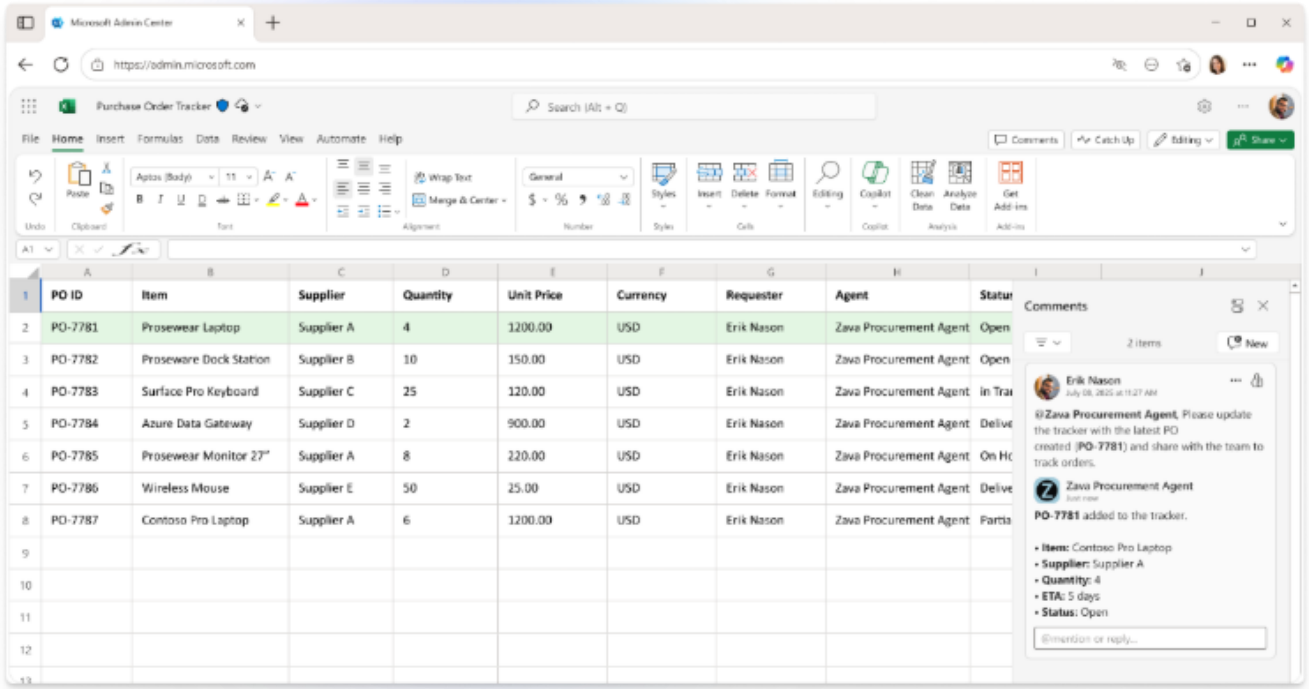
Visualization

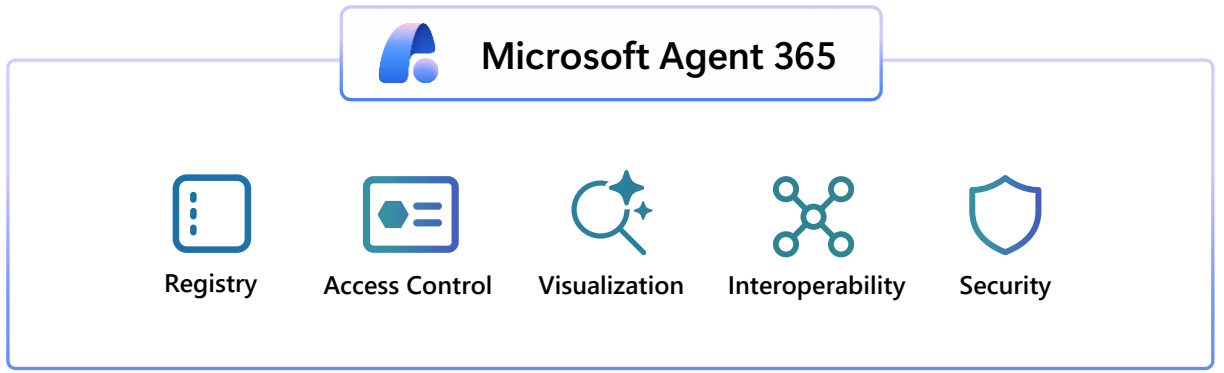


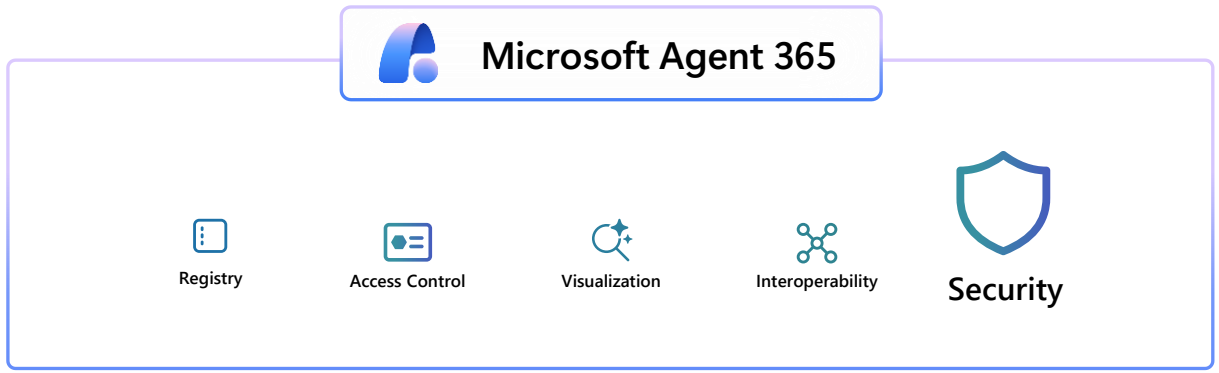

Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security


Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security

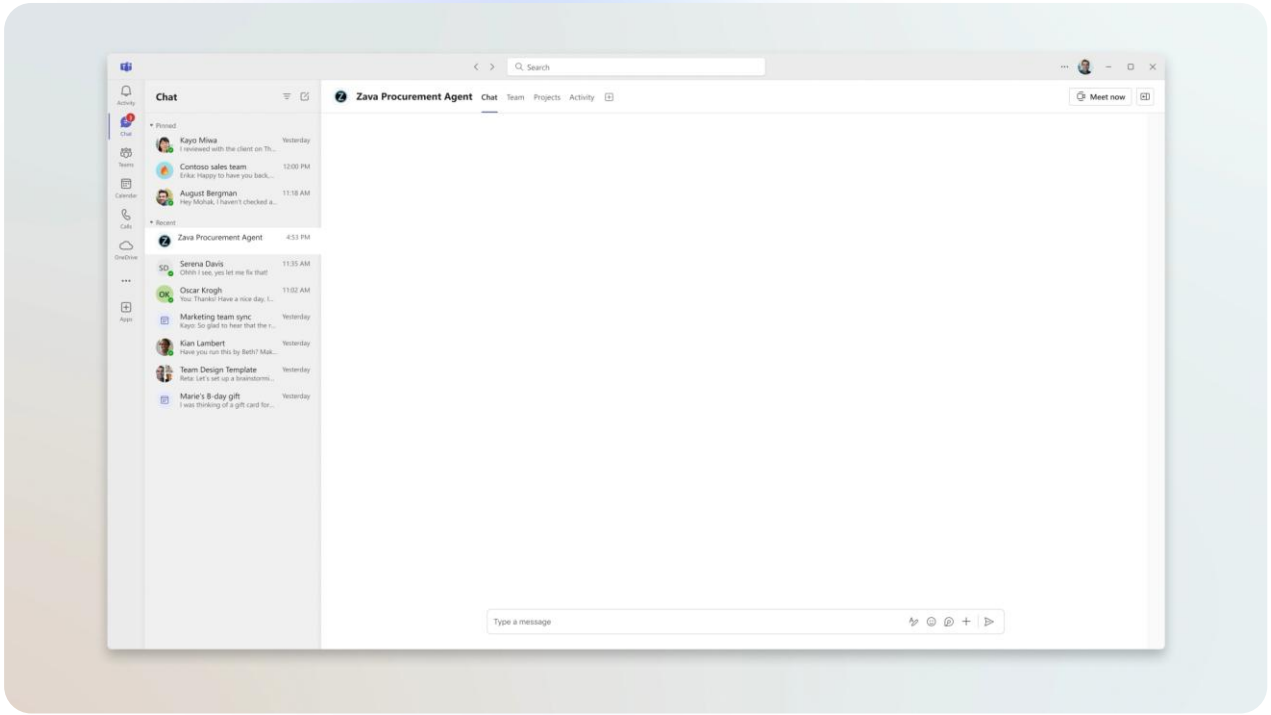
Interoperability




Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security


Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security

Security


Search
Chat
Zava Procurement Agent
Chat
Team
Projects
Activity
Meet now
Pinned
Kayo Miwa
Contoso sales team
August Bergman
Recent
Zava Procurement Agent
Serena Davis
Oscar Krogh
Marketing team sync
Kian Lambert
Team Design Template
Marie's B-day gift
Type a message

~~One~~ A Couple More Things...

AI Baseline Assessment & AI Powered Regulatory Templates

AI regulations are emerging across all regions

Global standards

ISO 42001
ISO 23894

AI Baseline: Automatic Compliance Posture

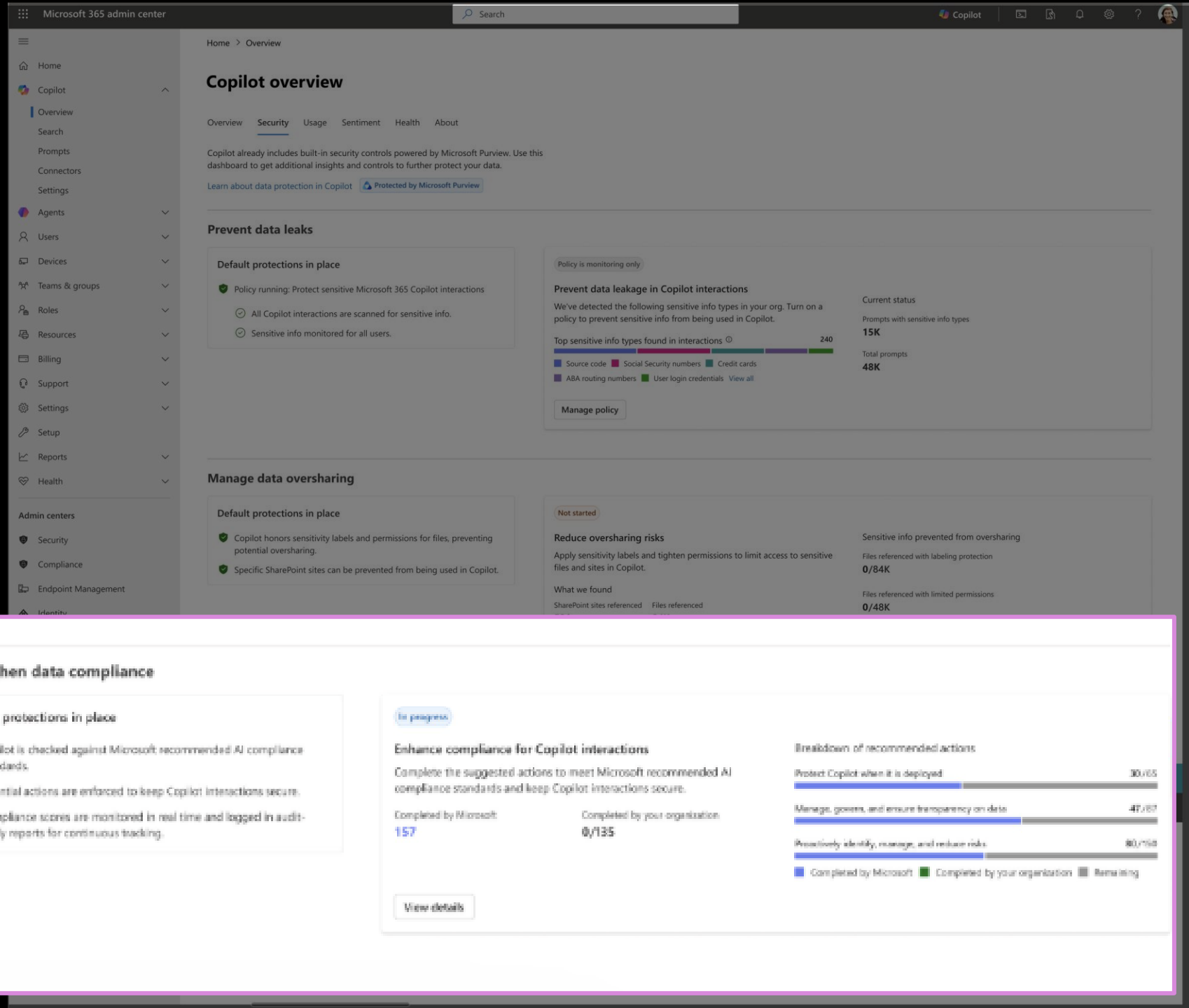
Helps organizations quickly evaluate their compliance posture and take remediation actions

AI Baseline assessment derives from global AI regulations for example EU AI act, NIST AI RMF

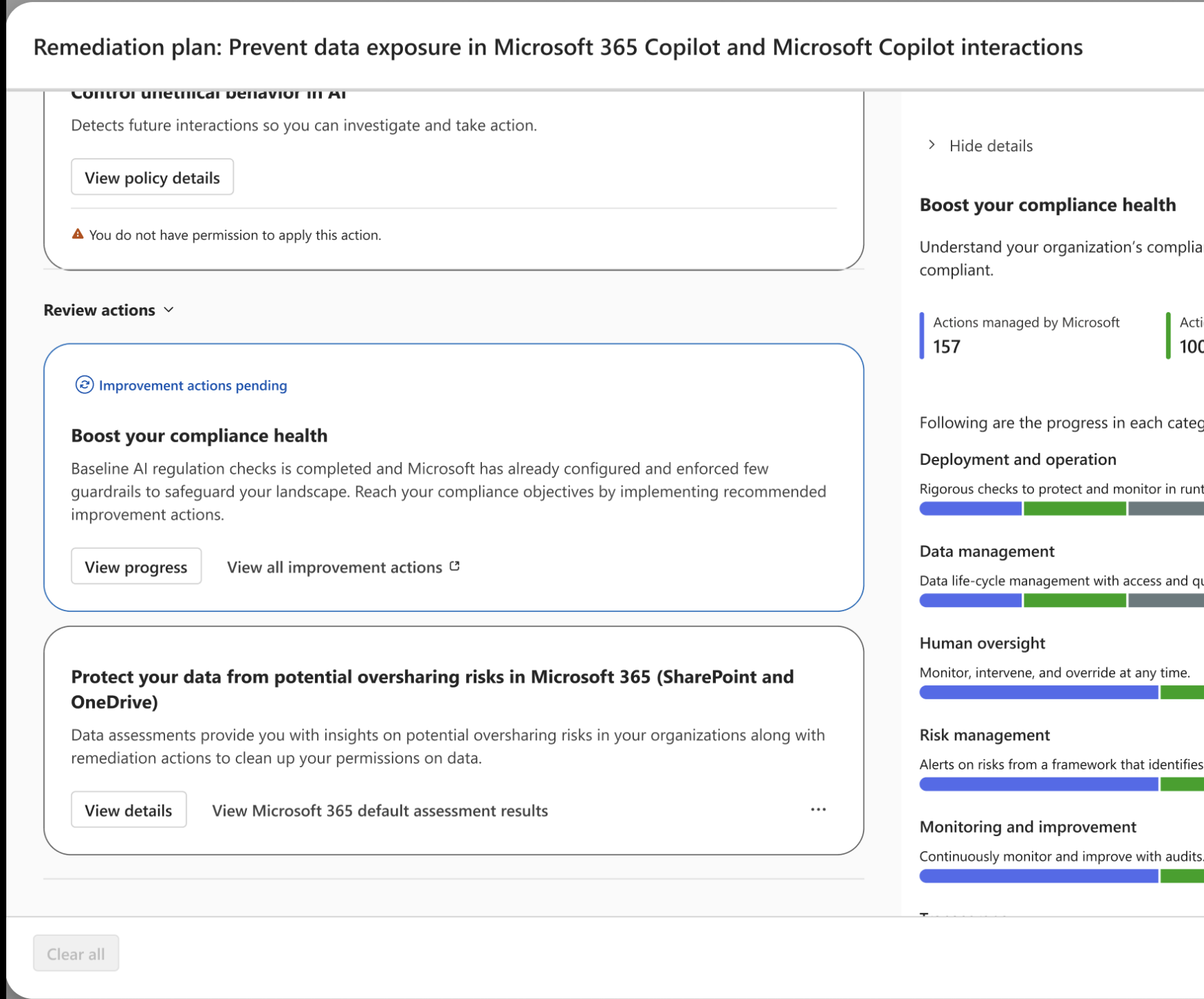
Evaluates compliance posture automatically against AI Baseline assessment and highlights regulatory gaps

Recommends remediation actions such as setting up policies or configuring settings in Purview, ENTRA, Defender and other Microsoft products

AI Baseline in Microsoft 365 Admin Center



AI Baseline in Purview DSPM vNext



Remediation plan: Prevent data exposure in Microsoft 365 Copilot and Microsoft Copilot interactions

Control unethical behavior in AI

Detects future interactions so you can investigate and take action.

View policy details

You do not have permission to apply this action.

Review actions

Improvement actions pending

Boost your compliance health

Baseline AI regulation checks is completed and Microsoft has already configured and enforced few guardrails to safeguard your landscape. Reach your compliance objectives by implementing recommended improvement actions.

View progress | View all improvement actions

Protect your data from potential oversharing risks in Microsoft 365 (SharePoint and OneDrive)

Data assessments provide you with insights on potential oversharing risks in your organizations along with remediation actions to clean up your permissions on data.

View details | View Microsoft 365 default assessment results | ...

Clear all

Hide details

Boost your compliance health

Understand your organization's compliance health objectives to keep the environment secure and compliant.

Actions managed by Microsoft	Actions implemented by you	Recommended actions pending
157	100	35

Following are the progress in each category included in your compliance objectives.

Deployment and operation

Rigorous checks to protect and monitor in runtime. — 3 pending actions /10

Data management

Data life-cycle management with access and quality controls. — 2 pending actions /10

Human oversight

Monitor, intervene, and override at any time. — 1 pending actions /10

Risk management

Alerts on risks from a framework that identifies them. — 2 pending actions /10

Monitoring and improvement

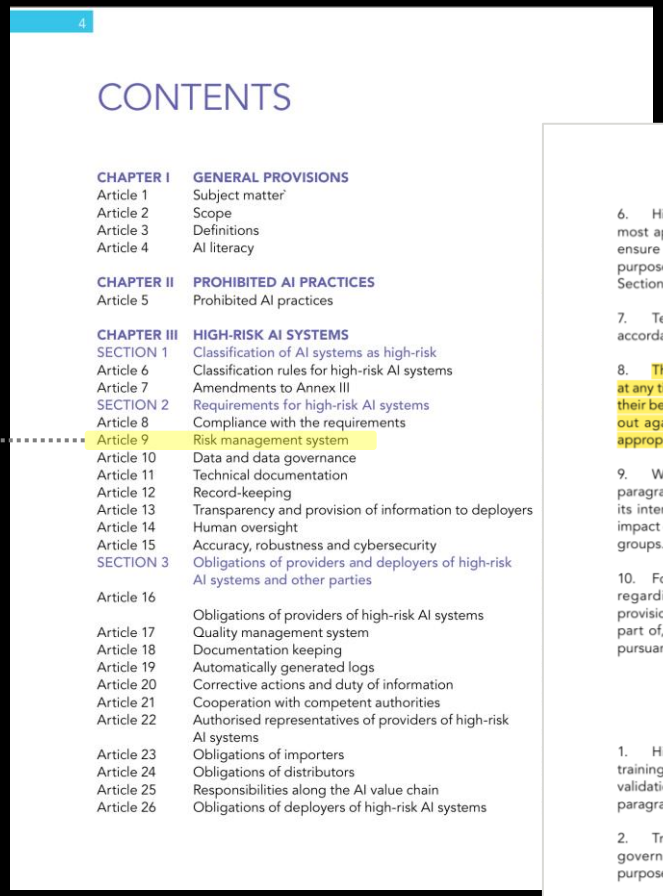
Continuously monitor and improve with audits. — 4 pending actions /10

Apply | Cancel

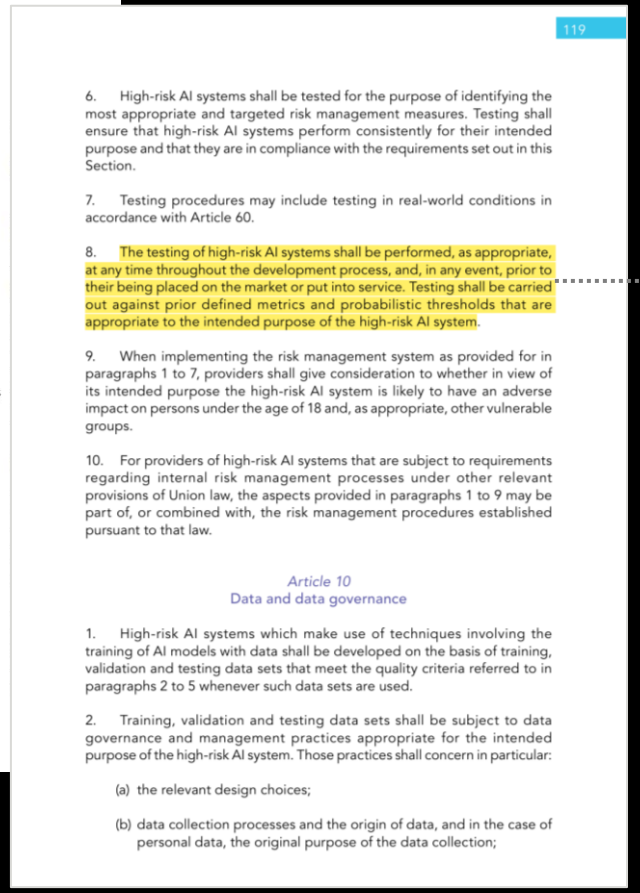
Anatomy of Regulation

Regulations

Regulations are official rules set by authorities to manage activities and ensure legal compliance.



CONTENTS



6. High-risk AI systems shall be tested for the purpose of identifying the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the requirements set out in this Section.

7. Testing procedures may include testing in real-world conditions in accordance with Article 60.

8. The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

9. When implementing the risk management system as provided for in paragraphs 1 to 7, providers shall give consideration to whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups.

10. For providers of high-risk AI systems that are subject to requirements regarding internal risk management processes under other relevant provisions of Union law, the aspects provided in paragraphs 1 to 9 may be part of, or combined with, the risk management procedures established pursuant to that law.

Article 10
Data and data governance

1. High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.

2. Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

(a) the relevant design choices;

(b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;

Controls

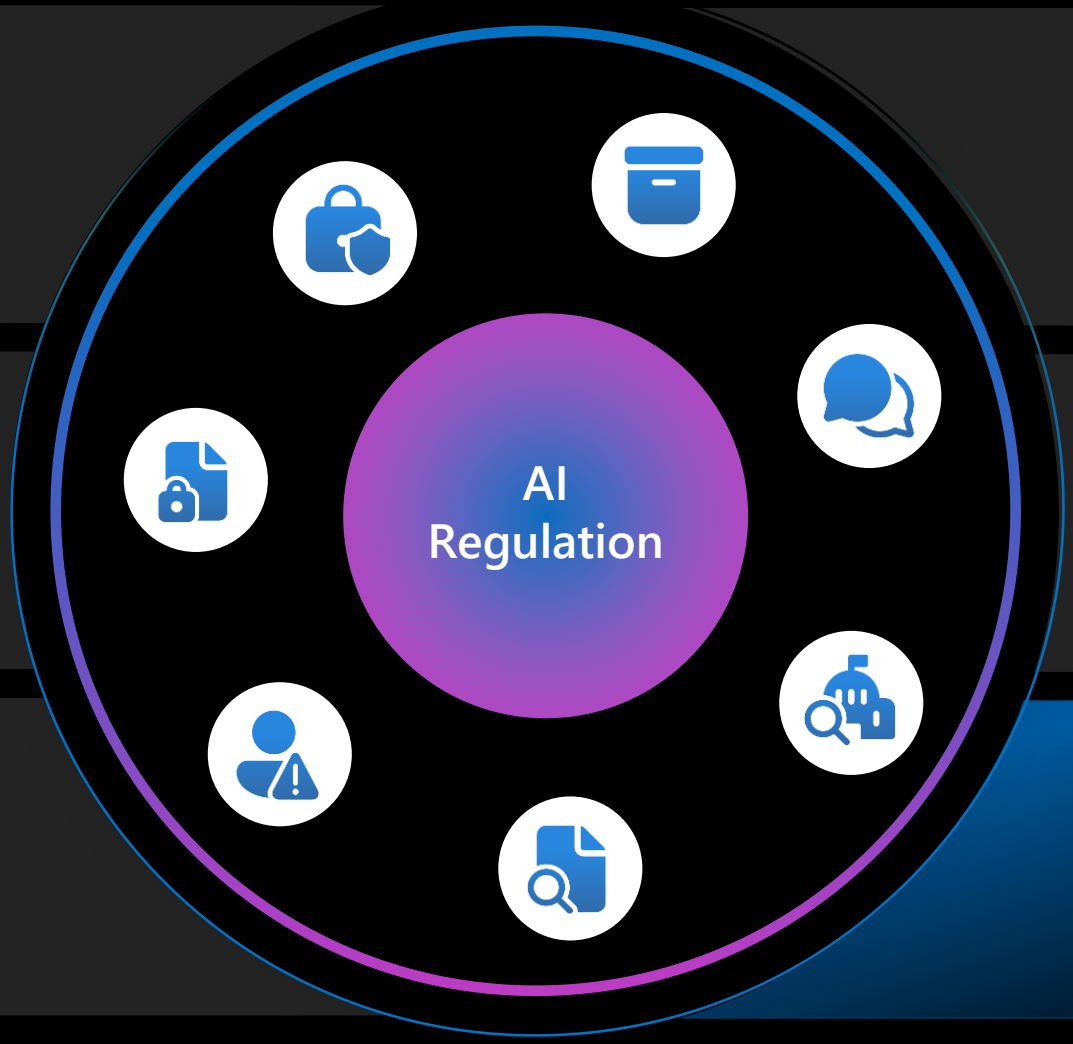
Controls are individual rules in regulations. Meeting its requirement means you comply with part of the regulation.

AI Regulatory controls mapping to Microsoft Purview

Information Protection:
Protect sensitive data from use by AI systems

Data Loss Prevention & Insider Risk Management: Robust cybersecurity and human oversight to prevent misuse

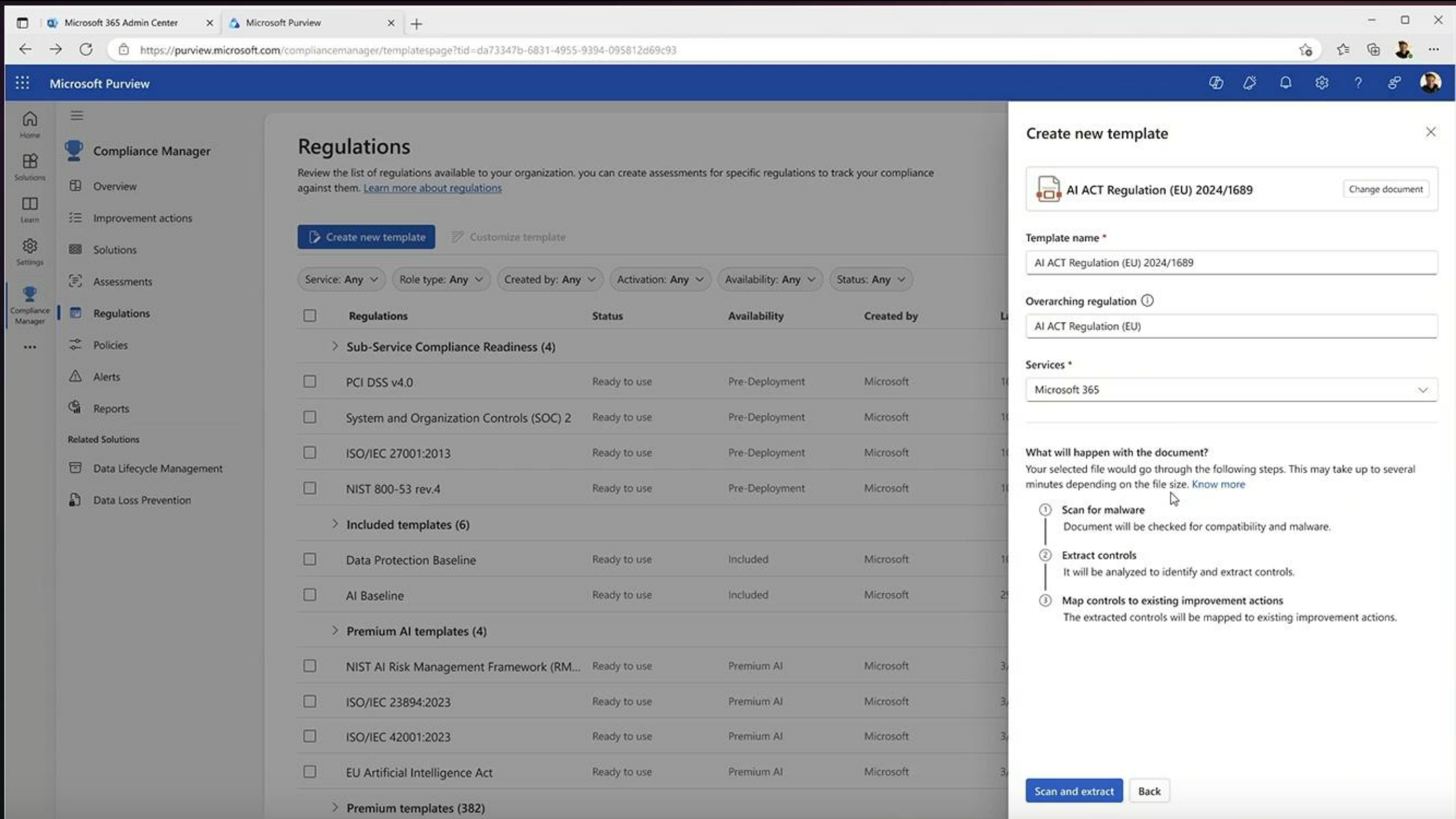
Purview Audit & eDiscovery:
High-risk systems need conformity assessments and auditability

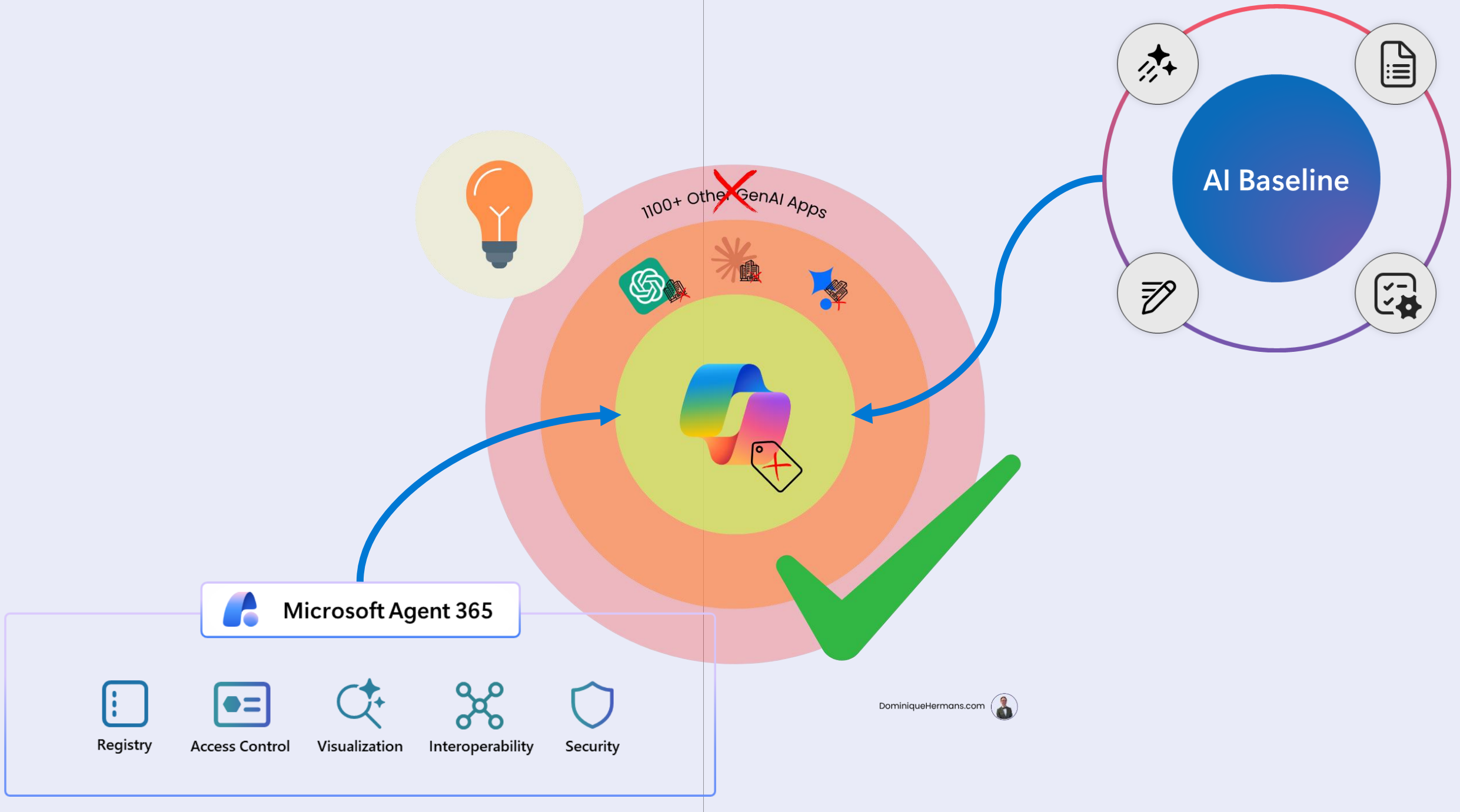


Data Lifecycle Management:
Controlled retention and deletion of sensitive data and AI data

Communication Compliance:
Detecting biased, unfair and other sensitive data in AI responses

Outcome:
E2E security, governance and compliance controls for AI deployments


Microsoft 365 Admin Center
Microsoft Purview
https://purview.microsoft.com/compliancemanager/templatespage?tid=da73347b-6831-4955-9394-095812d69c93
Microsoft Purview
Home
Solutions
Learn
Settings
Compliance Manager
Compliance Manager
Overview
Improvement actions
Solutions
Assessments
Regulations
Policies
Alerts
Reports
Related Solutions
Data Lifecycle Management
Data Loss Prevention
Regulations
Review the list of regulations available to your organization. you can create assessments for specific regulations to track your compliance against them. Learn more about regulations
Create new template
Customize template
Service: Any
Role type: Any
Created by: Any
Activation: Any
Availability: Any
Status: Any
Regulations
Status
Availability
Created by
Sub-Service Compliance Readiness (4)
PCI DSS v4.0 Ready to use Pre-Deployment Microsoft
System and Organization Controls (SOC) 2 Ready to use Pre-Deployment Microsoft
ISO/IEC 27001:2013 Ready to use Pre-Deployment Microsoft
NIST 800-53 rev.4 Ready to use Pre-Deployment Microsoft
Included templates (6)
Data Protection Baseline Ready to use Included Microsoft
AI Baseline Ready to use Included Microsoft
Premium AI templates (4)
NIST AI Risk Management Framework (RM... Ready to use Premium AI Microsoft
ISO/IEC 23894:2023 Ready to use Premium AI Microsoft
ISO/IEC 42001:2023 Ready to use Premium AI Microsoft
EU Artificial Intelligence Act Ready to use Premium AI Microsoft
Premium templates (382)
Create new template
AI ACT Regulation (EU) 2024/1689
Change document
Template name *
AI ACT Regulation (EU) 2024/1689
Overarching regulation
AI ACT Regulation (EU)
Services *
Microsoft 365
What will happen with the document?
Your selected file would go through the following steps. This may take up to several minutes depending on the file size. Know more
1 Scan for malware
Document will be checked for compatibility and malware.
2 Extract controls
It will be analyzed to identify and extract controls.
3 Map controls to existing improvement actions
The extracted controls will be mapped to existing improvement actions.
Scan and extract
Back


AI Baseline
1100+ Other GenAI Apps
Microsoft Agent 365
Registry
Access Control
Visualization
Interoperability
Security
DominiqueHermans.com

Thank you!

Feel free to connect on the socials:

https://dominiquehermans.com

https://www.linkedin.com/in/dominiquehermans1/

Dominiquehermans.bsky.social