Je omgeving op orde

voor veilig en optimaal Copilot gebruik

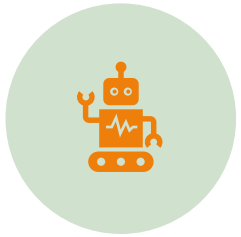
Over mij…

- **Jeroen Bijdevier**
- **AVK Training & Coaching**
- **Security Architect | Microsoft Certified Trainer | Project Manager | Change Manager**
- **www.linkedin.com/in/jeroenbijdevier**
- **Focus op: Data veiligheid & de mens**

AI is gaaf

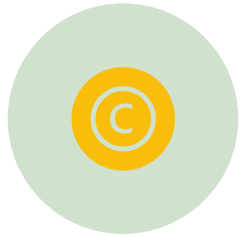
AI Act

Juridische aspecten AI



AI Verordening

Privacy (AVG)



Auteursrecht

Security (BIO/NIS2)

Overheid? WoO, Archiefwet, algoritme kader …

BIO: Baseline Informatiebeveiliging Overheid
NIS2: Europeese security wetgeving voor kritische infrastructuur
WoO: Wet open Overheid

Risico niveau's AI Act

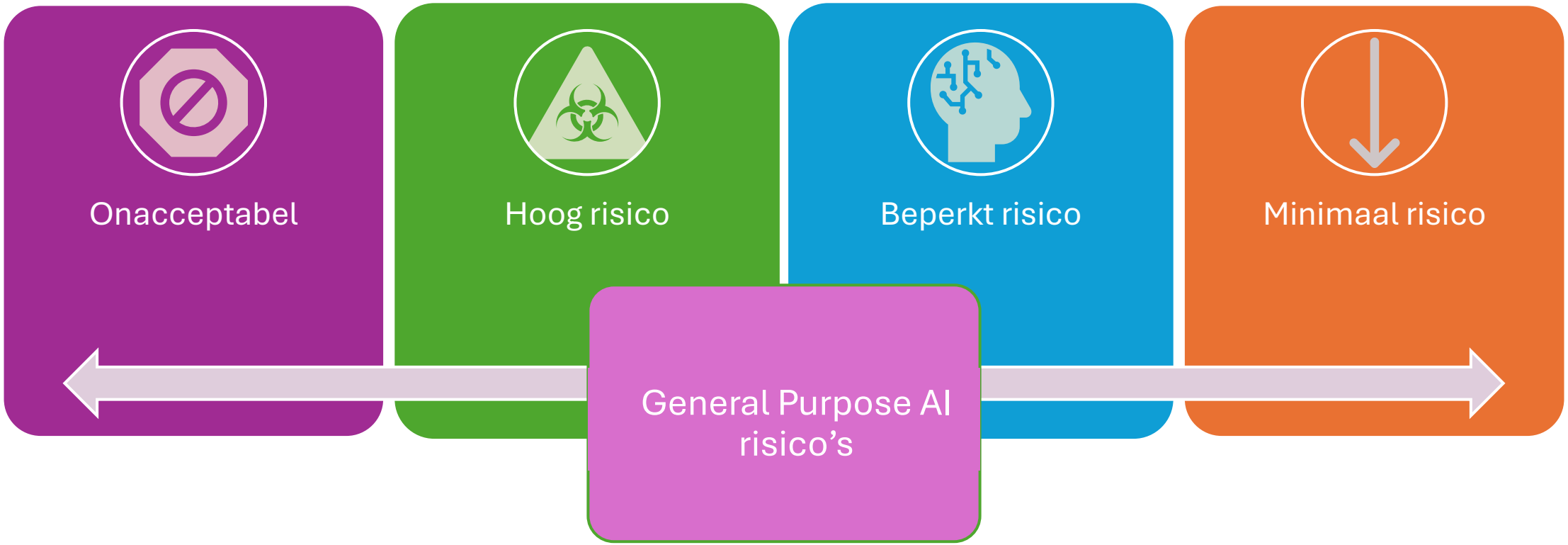
Voorbeelden:
•Sociale scoring (zoals gedragsscores voor burgers)
•Manipulatieve AI die gedrag stuurt
•Real-time gezichtsherkenning in publieke ruimtes

👉 Deze systemen zijn **niet toegestaan** in de EU.

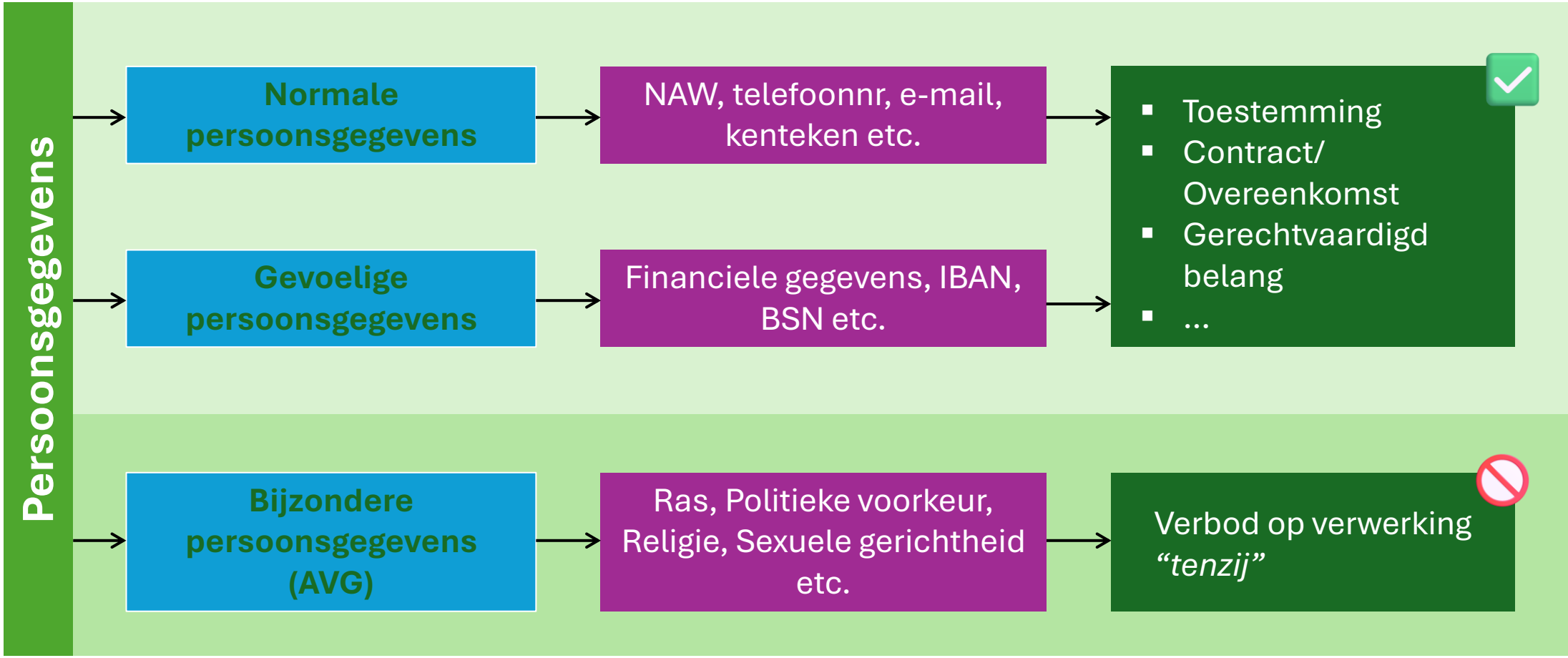
Voorbeelden:
•AI in sollicitatieprocedures (CV-selectie)
•Medische AI (diagnoses)
•AI in kritieke infrastructuur (zoals energie)

Voorbeelden:
•Chatbots
•Deepfakes
•AI die tekst of beelden genereert

Voorbeelden:
•Spamfilters
•AI in videogames
•Aanbevelingssystemen (zoals Netflix)



Soorten persoonsgegevens



Sprake van “tenzij”? Dan ook voldoen aan een juridische grondslag

Ethische aspecten

Bias

Discriminatie

Transparantie

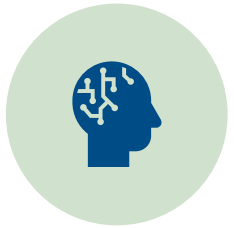
Vertrouwen en kwaliteit

Uitlegbaarheid

Hallucinatie

Duurzaamheid

Werkgelegenheid



AGI / ASI

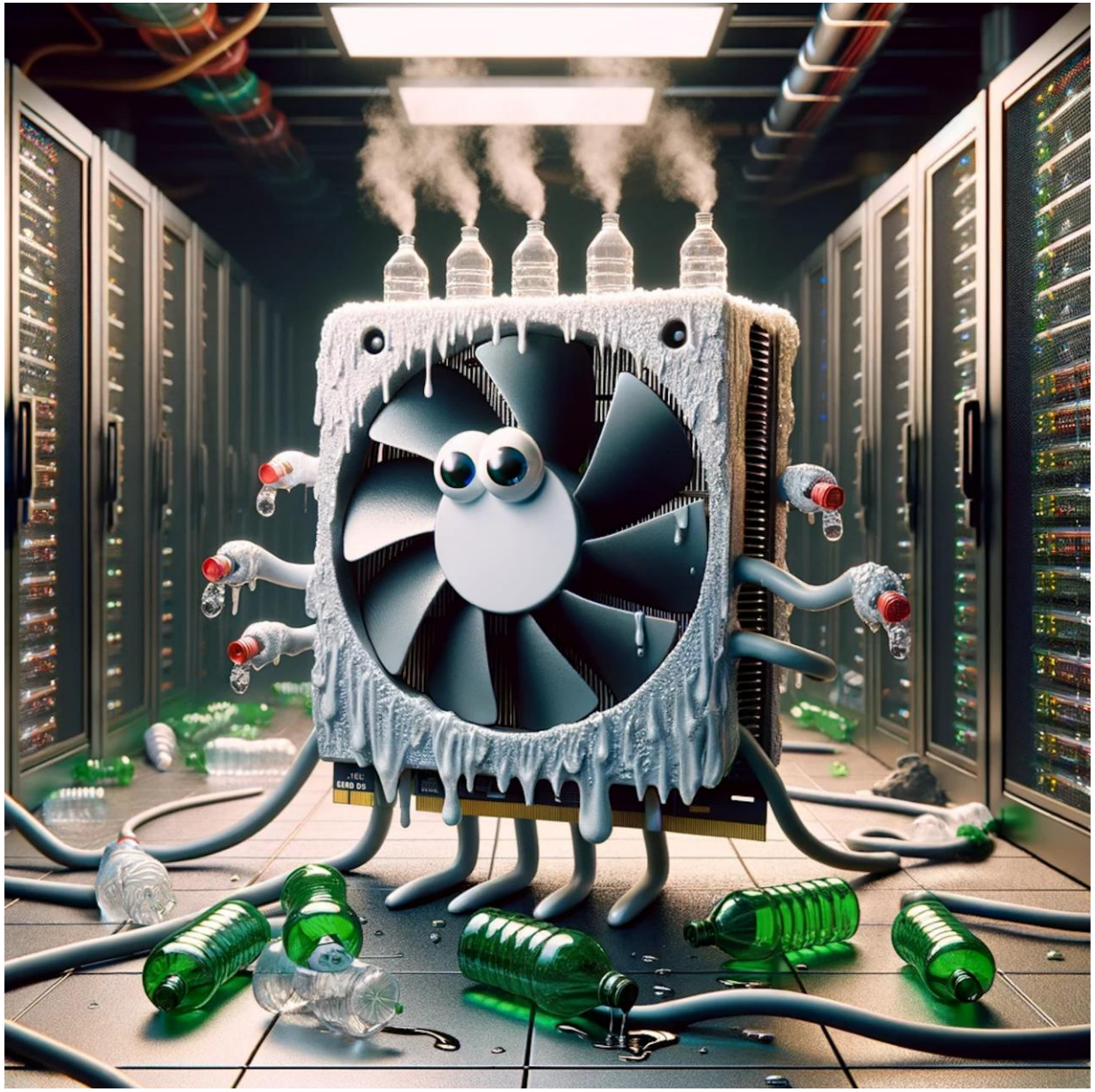
Milieu impact

<u>AI servers</u>

- Gebruiken zeldzame grondstoffen
- Produceren e-waste
- Verbruiken energie
- Verbruiken (koel)water

ChatGPT verbruikt 10x meer energie dan een Google search.

(bron: International Energy Agency)



Risicobeheersing

Agenda

SharePoint Advanced Management

Purview

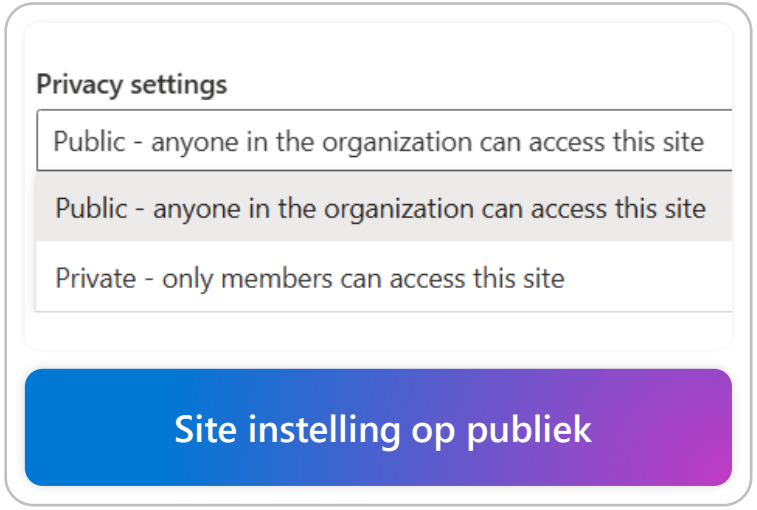
Prioriteren en aanpakken risico’s

Gefaseerde uitrol Copilot

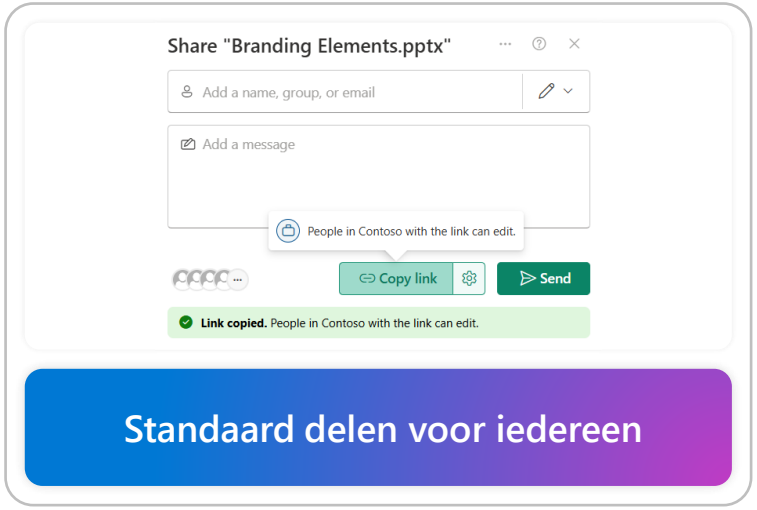
AI draait op goede data

Het data fundament / data veiligheid

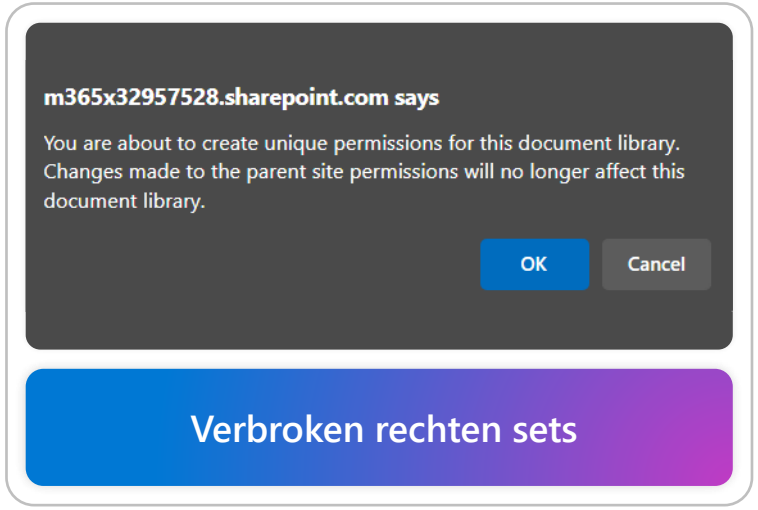
Problemen met rechten structuren (oversharing)



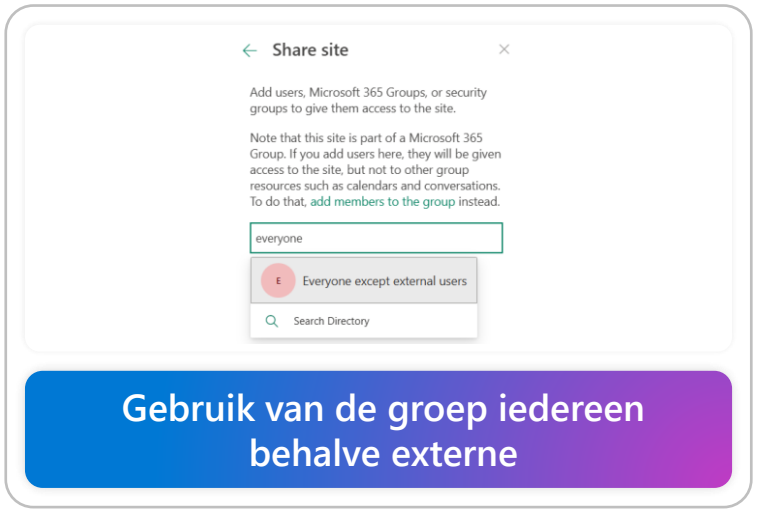
Site instelling op publiek



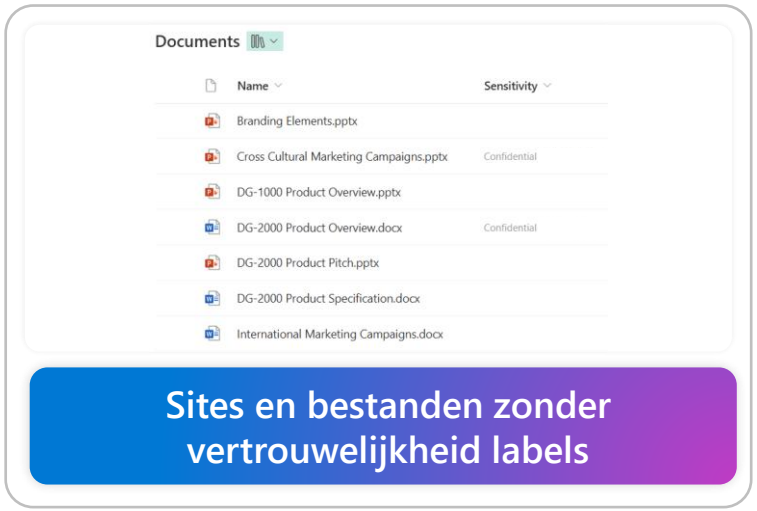
Standaard delen voor iedereen



Verbroken rechten sets



Gebruik van de groep iedereen behalve externe



Sites en bestanden zonder vertrouwelijkheid labels

Digitale vervuiling (ROT)

Redundant	Obsolete	Trivial
• Meerdere kopieën van hetzelfde document met deels verschillende informatie: • ProjectPlanDefinief.docx • ProjectPlanDefinitief_V4.docx • ProjectPlanDefinitief_review.docx	• Een strategie plan wat inmiddels achterhaald is • Een oude HR handboek wat vervangen is door een nieuwe versie maar nog wel beschikbaar is	• Persoonlijk aantekeningen op een algemene plek • Foto’s van feesten van verschillende jaren • Informele notulen van vergaderingen

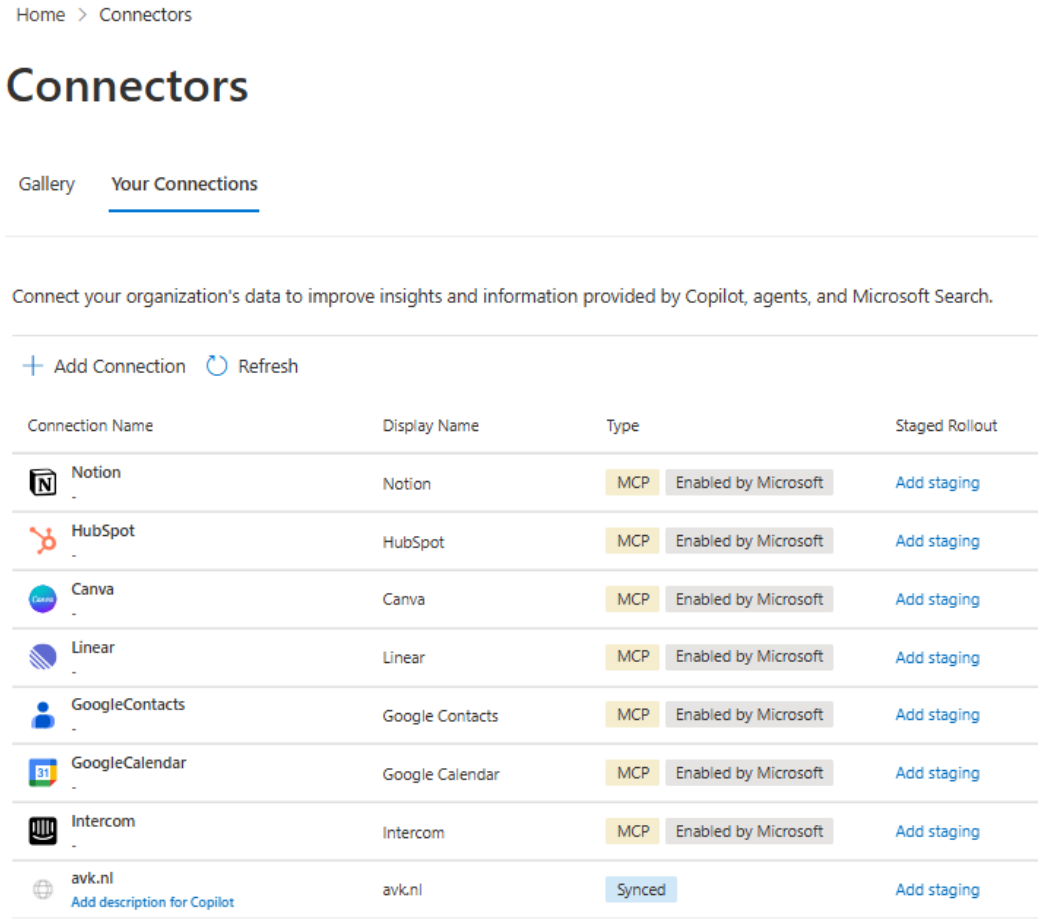
Digitale vervuiling (ROT)

Redundant	Obsolete	Trivial
• Meerdere kopieën van hetzelfde document met deels verschillende informatie: • ProjectPlanDefinief.docx • ProjectPlanDefinitief_V4.docx • ProjectPlanDefinitief_review.docx	• Een strategie plan wat inmiddels achterhaald is • Een oude HR handboek wat vervangen is door een nieuwe versie maar nog wel beschikbaar is	• Persoonlijk aantekeningen op een algemene plek • Foto's van feesten van verschillende jaren • Informele notulen van vergaderingen
• Procedure: **Enkelvoudig opslag meervoudig gebruik**	• Procedure: **Archief stukken**	• Procedure: **Ik, Wij, Ons**

Digitale etiquette

Bronnen die Copilot kan gebruiken

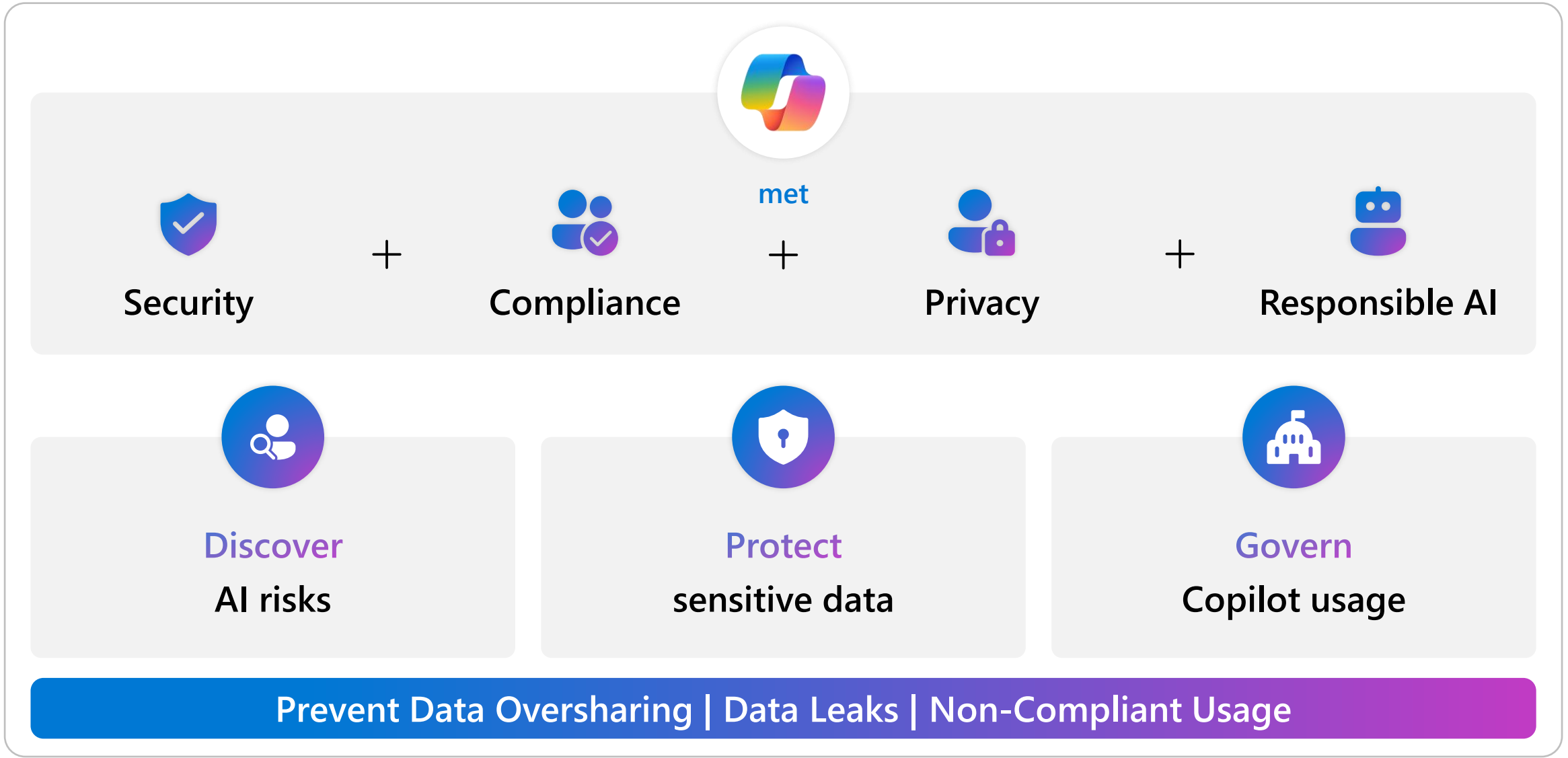
- SharePoint Online
- OneDrive for Business
- Exchange Online
- Teams
- OneNote
- Loop
- Planner en To Do
- Word, Excel en PowerPoint
- Fabric
- Connectors
- Copilot search locaties



Copilot Control System

Framework

Copilot Control System framework



Links

- aka.ms/copilot/oversharing
- aka.ms/copilotcontrolsystemddd
- aka.ms/copilotcontrolsystemddd/s3
- aka.ms/oversharingMechanics
- aka.ms/m365copilotwithpurview
- aka.ms/copilotacedemie
- aka.ms/DSPMforAI/deploy
- aka.ms/DSPMforAI/oversharing
- aka.ms/PurviewDeploymentModels

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

De primaire tools

SharePoint Advanced Management

Voor SharePoint beheer en governance

Microsoft Purview

Voor data veiligheid, archiveren en rapporteren

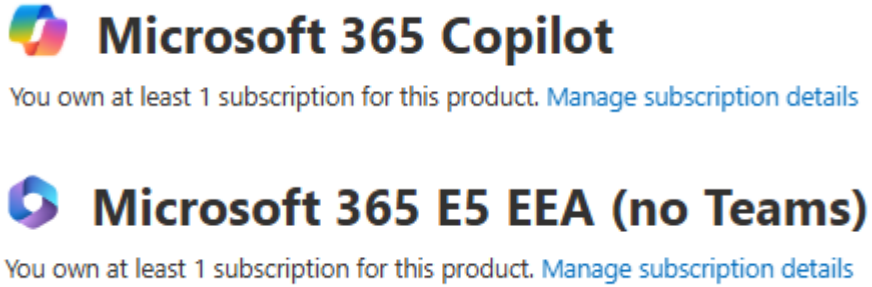
Rollen en licentie

- **Global Administrator**

- **SharePoint Administrator**

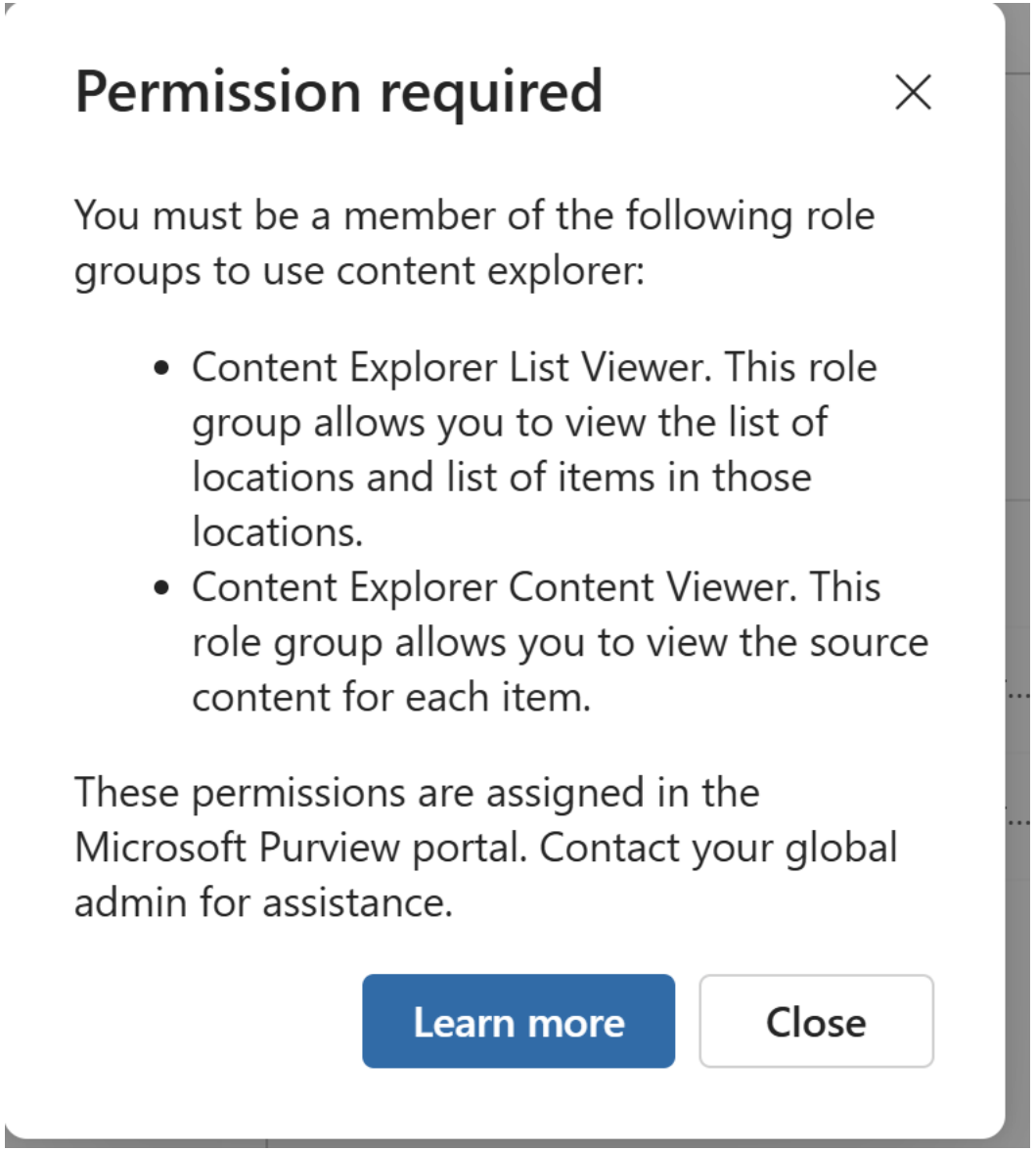
- **Compliance Administrator**
  Geeft toegang tot de meeste compliance-functionaliteiten

- **Content view en list**



DLP for endpoints
Insider risk managent

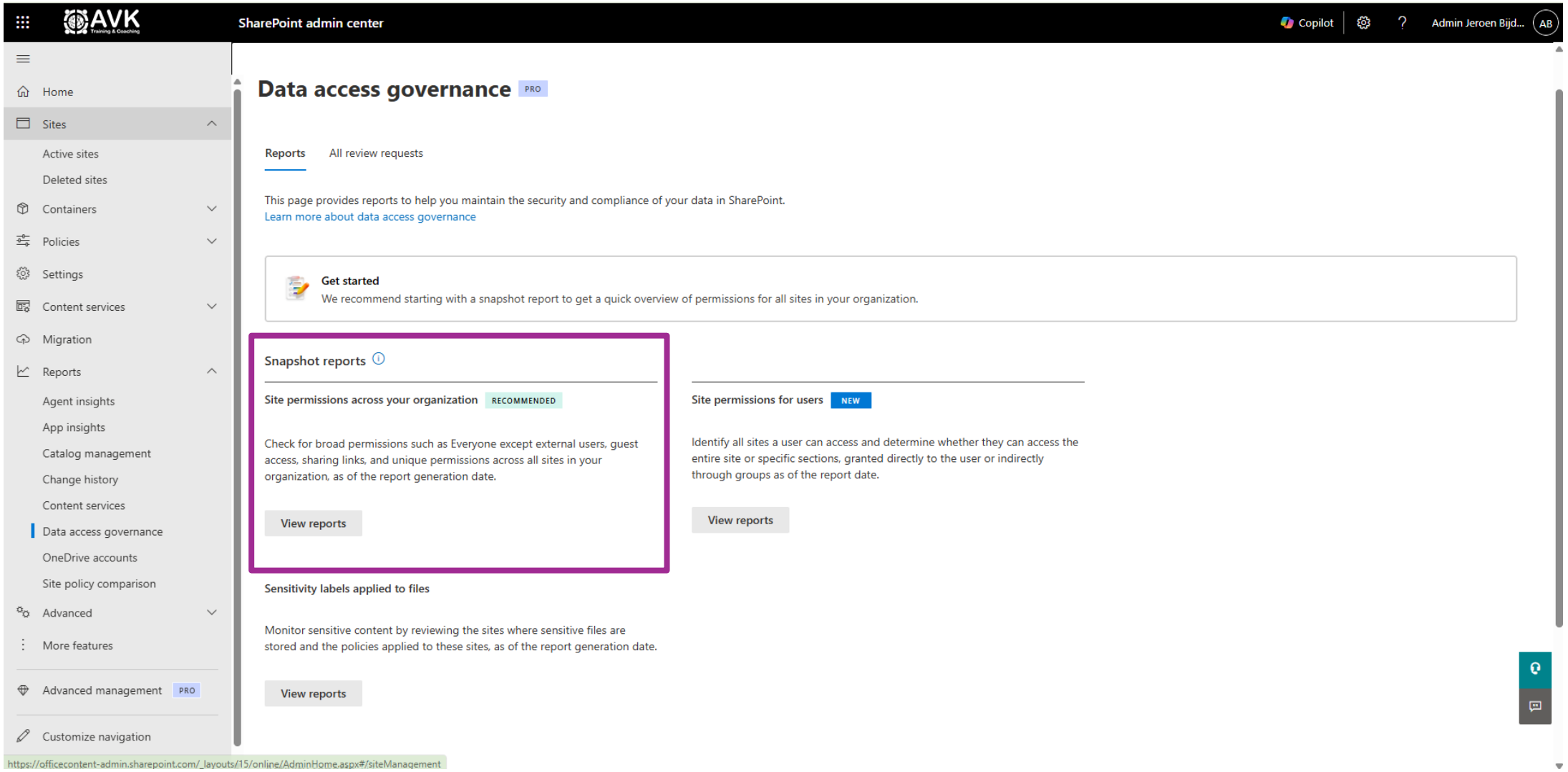
Business Premium + Purview suite


Permission required
You must be a member of the following role groups to use content explorer:
Content Explorer List Viewer. This role group allows you to view the list of locations and list of items in those locations.
Content Explorer Content Viewer. This role group allows you to view the source content for each item.
These permissions are assigned in the Microsoft Purview portal. Contact your global admin for assistance.
Learn more
Close

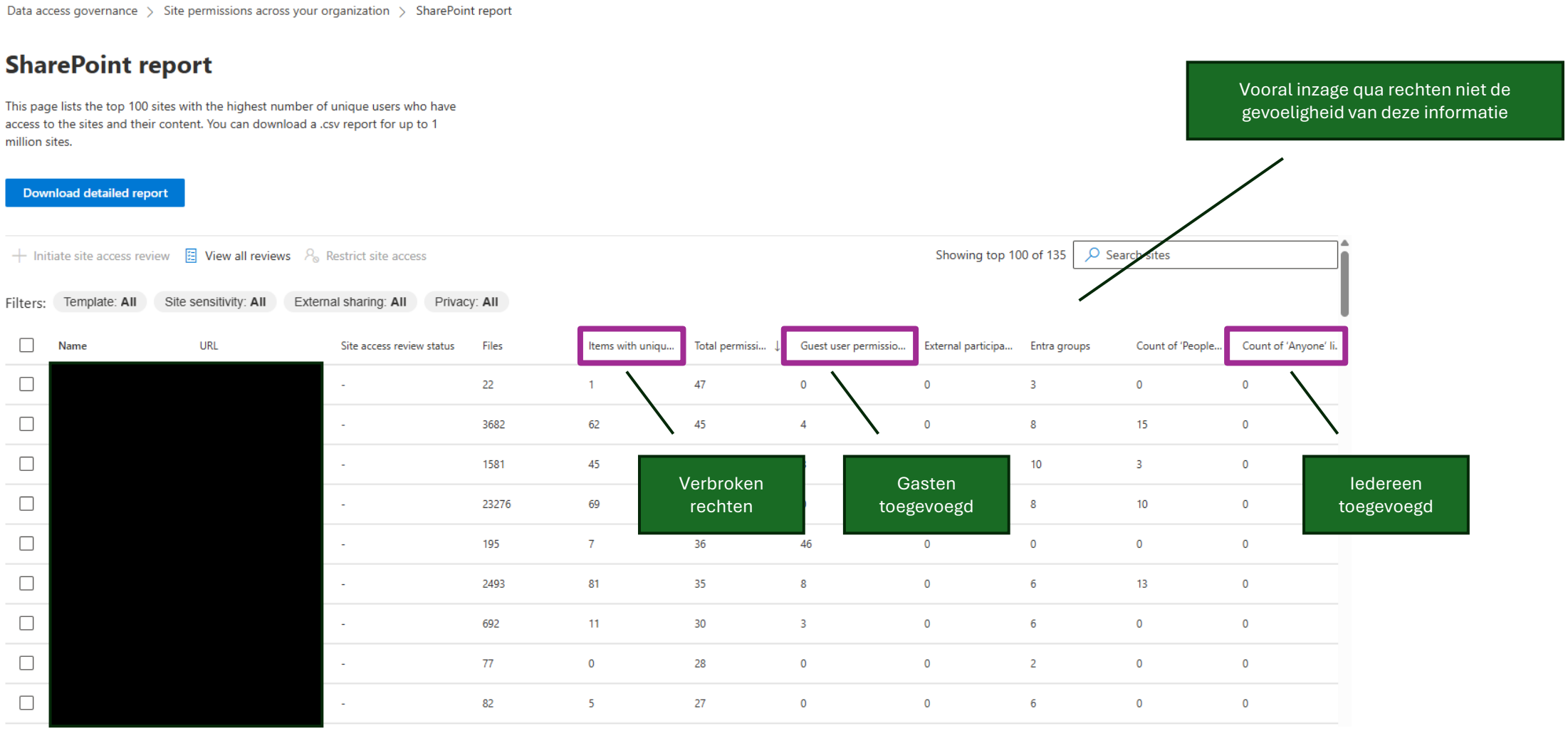
SharePoint Advanced Management

Inventarisatie

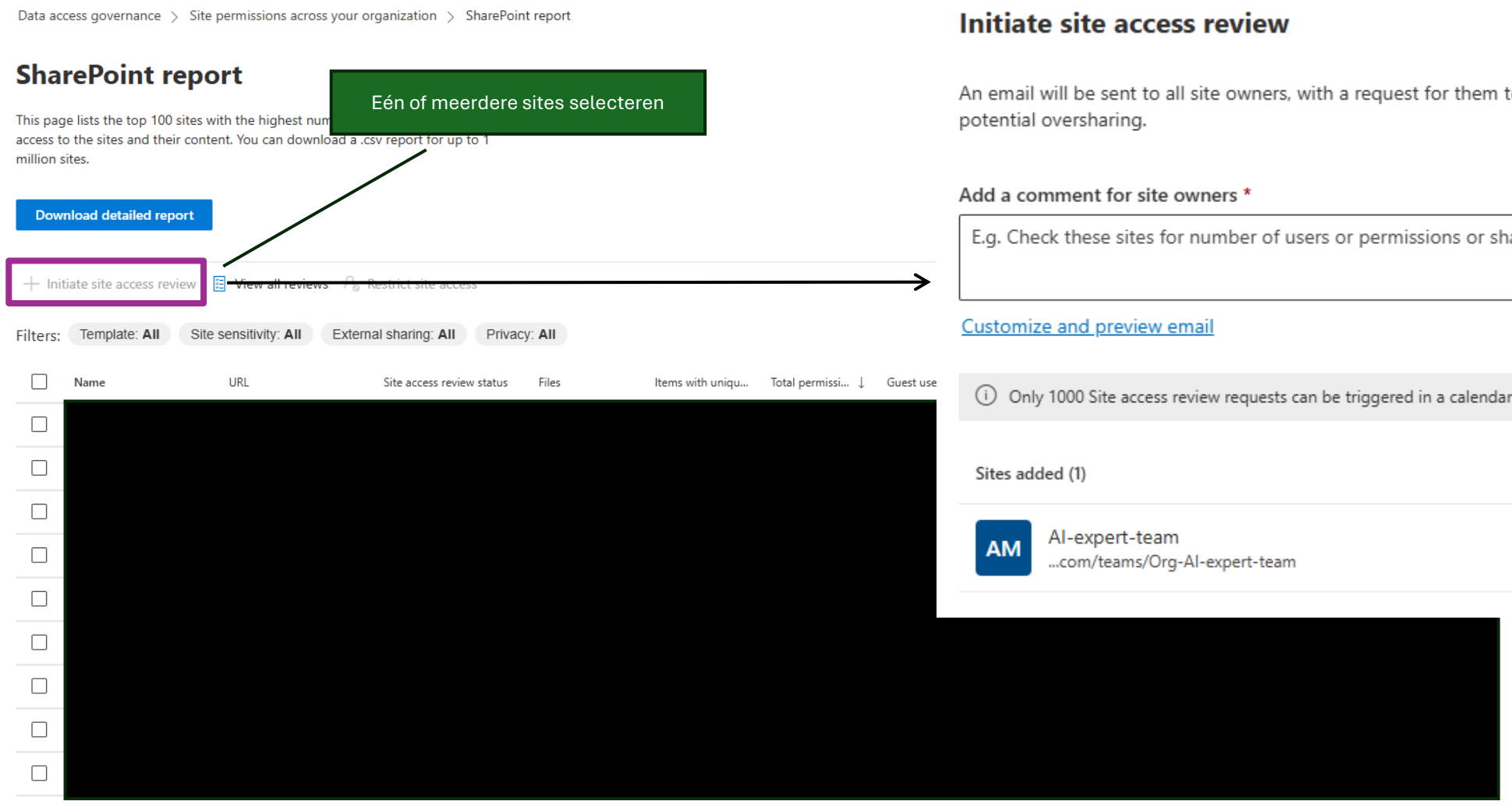
SharePoint Advanced Management



Site permissions across your organization



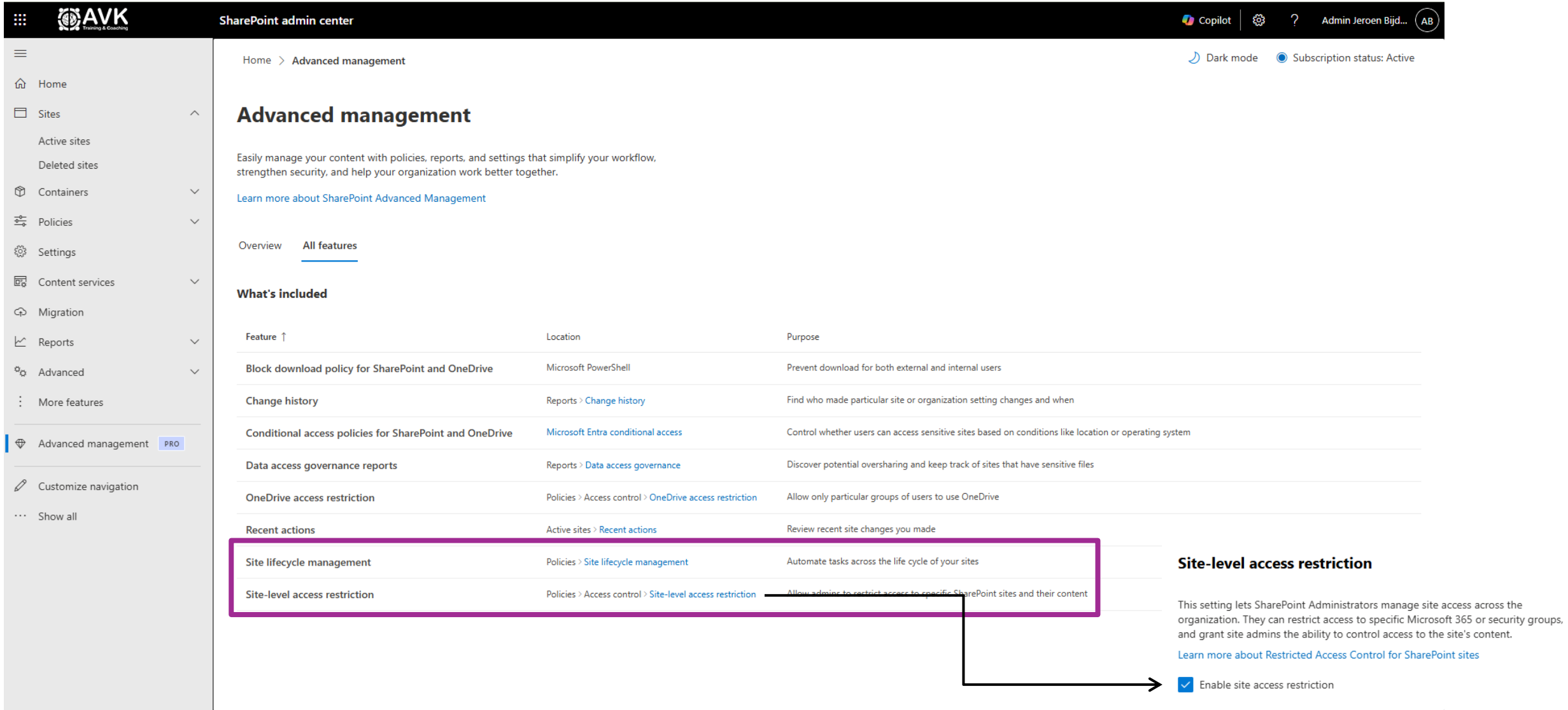
Site permissions across your organization



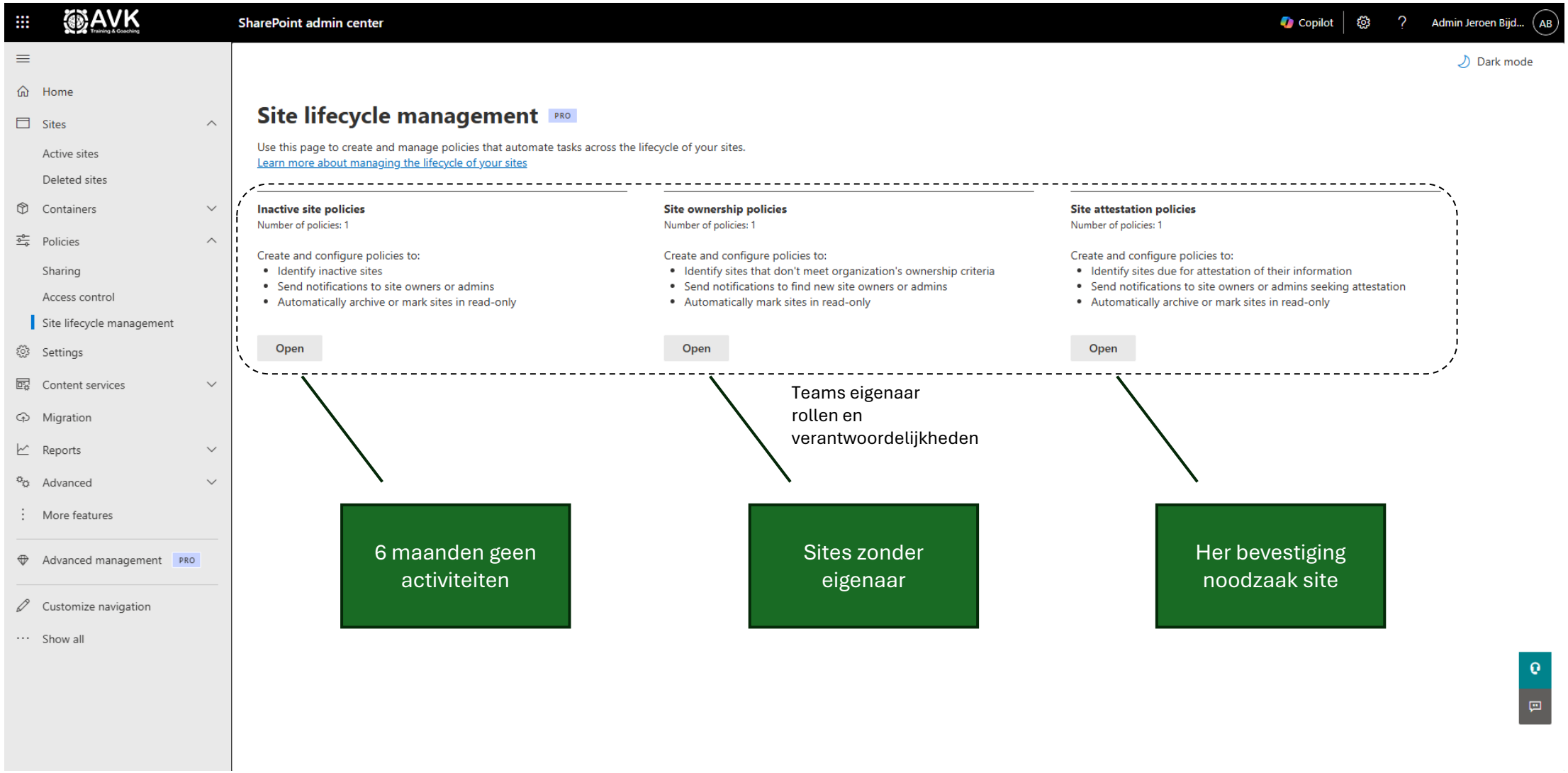
SharePoint Advanced Management

Rechten structuren

SharePoint Advanced Management



Site lifecycle management



Site lifecycle management

Create a site attestation policy

- Overview
- Scope
- Configuration
- Finish

Manage site attestation

With a site attestation policy, you can ensure your sites are secure and compliant by reducing the risk of unmanaged sites. This involves regular reviews by site owners or admins to check and confirm the accuracy of site information, including the site's necessity, its owners, members, permissions, and sharing settings.

This policy will:

Generate monthly report of sites that are due for attestation

You can specify how often sites should be attested while configuring the policy. It will then run monthly to identify sites that are due for attestation and generate a report.

Sites excluded from policy: OneDrive, System, App catalog, Root, Home and Admin sites.

Send attestation notifications to site owners or admins

For sites identified as due for attestation, site owners or admins will receive email notifications every month asking them to review and confirm that their site's information is accurate.

Act on sites that have not been attested after 3 notifications

If there is no confirmation from site owners or admins after 3 notifications, you can configure the policy to:

- Archive or set access to read-only
- Take no action

Learn how site attestation can improve governance

Begeleidende email met instructies

Active sites

Use this page to sort and filter sites and change site settings.
Learn more about managing sites

+ Create | Edit | Membership | Hub | Sharing | Delete

Site name	URL	Teams	Channe
Jeroens Demo site	.../teams/JeroensDemosite	-	-

Site-level access restriction

This setting lets SharePoint Administrators manage site access across the organization. They can restrict access to specific Microsoft 365 or security groups, and grant site admins the ability to control access to the site's content.

Learn more about Restricted Access Control for SharePoint sites

Enable site access restriction

JS

Jeroens Demo site

Private group

Email | View site | Delete

General | Activity | Membership | **Settings**

Email

Let people outside the organization email this team

Send copies of team emails and events to team members' inboxes

Don't show team email address in Outlook

Privacy

Private

Public

External file sharing

New and existing guests

More sharing settings

Sensitivity label

None

Restrict content from Microsoft 365 Copilot PRO

On

Off

Restricted site access PRO

Ambachtelijk Vliegende Koekjes, Jeroens Demo site

Edit

Custom scripts

Blocked

Edit

Version history limit

Same as Organization-level (Automatic)

Save

Delen stoppen door groepen toe te voegen

Active sites

Use this page to sort and filter sites and change site settings.
Learn more about managing sites

Create | Edit | Membership | Hub | Sharing | Delete

Site name	URL	Teams	Channe
Jeroens Demo site	.../teams/JeroensDemosite	-	-

JS

Jeroens Demo site

Private group

Email | View site | Delete

General | Activity | Membership | **Settings**

Changes saved.

Email

- [ ] Let people outside the organization email this team
- [ ] Send copies of team emails and events to team members' inboxes
- [ ] Don't show team email address in Outlook

Privacy

- (•) Private
- ( ) Public

External file sharing

New and existing guests

More sharing settings

Sensitivity label

None

Restrict content from Microsoft 365 Copilot PRO

- (•) On
- ( ) Off

Restricted site access PRO

Ambachtelijk Vliegende Koekjes, Jeroens Demo site

Edit

Custom scripts

Blocked

Edit

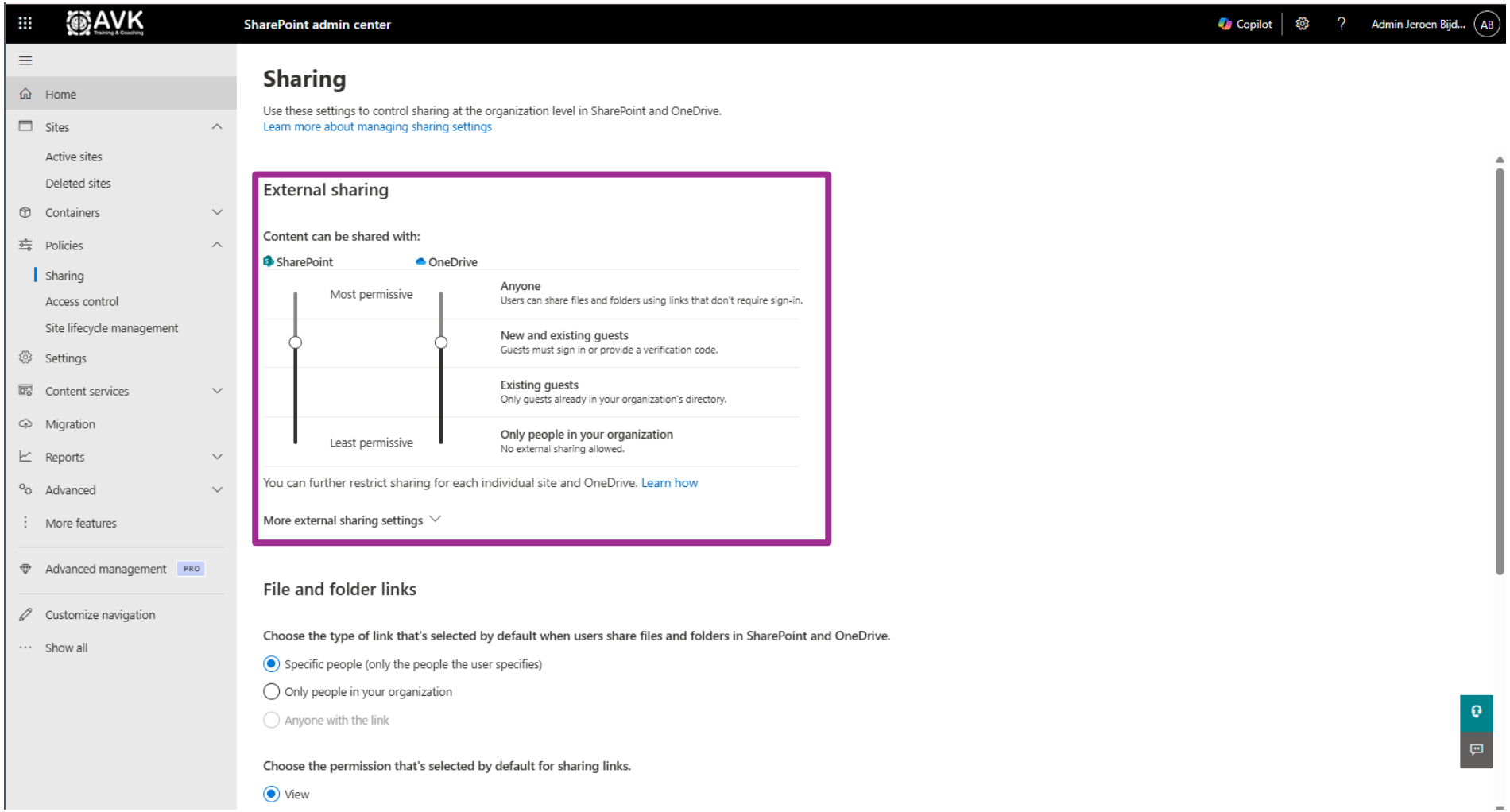
Version history limit

Same as Organization-level (Automatic)

Save

Site in zijn geheel uitsluiten voor Copilot

Overige SharePoint instellingen



Purview

Overzicht

Enkele Purview tools om risico’s te beperken

- Gevoeligheidslabels (openbaar, intern, vertrouwelijk, zeer vertrouwelijk)
- Vereist in ISO27001, NIS2, NEN7510, BIO

Dataclassificatie

- Data Loss Prevention
- Voorkom delen van (vertrouwelijke) informatie met AI
- Beperkingen voor de gebruiker

DLP

- Onderzoek doen naar een incident, voldoen aan openbaringseisen, doorzoeken specifieke bronnen naar specifieke inhoud
- Voorbeeld: inzage verzoek

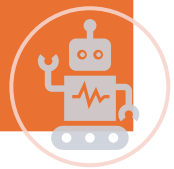
eDiscovery

- Retentielabels en beleid
- Bewaar en vernietigings-termijnen voor e-maisl documenten en e-mails
- Voorbeeld: email archivering volgens Capstone methode

Retentie

- **Data Security Posture Management**
- Inzicht in AI gebruik, gevoelige interacties met AI,
- Afdwingen van beleid

DSPM



- Toets je omgeving aan bestaande regelgeving zoals NIS2, ISO27001 en de AI Act

Compliancebeheer

- Detecteren van pesten en discriminatie
- Onethische communicatie preventie

Communicatie compliance

- Instellen van waarschuwingen zoals:
  - aanmaken of verwijderen van een team,
  - delen van vertrouwelijke informatie

Alerts

Purview

Information protection

Defense in dept

Youtuber kraakt BitLocker-versleuteling binnen minuut met Raspberry Pi Pico

Een beveiligingsonderzoeker is erin geslaagd een laptop die met BitLocker is versleuteld binnen een minuut te kraken met behulp van een aangepaste Raspberry Pi Pico. Voor de aanval is wel fysieke toegang tot de laptop nodig.

De BitLocker-tool van Microsoft beschermt gegevens op harde schijven door ze te versleutelen. Stacksmashing ontdekte echter dat de sleutel die hiervoor gebruikt wordt, gemakkelijk te onderscheppen is via een 'sniffing attack'. Daarbij wordt netwerkverkeer afgeluisterd om informatie te onderscheppen.

Bij BitLocker gaat het om het verkeer dat wordt uitgewisseld tussen een losstaande Trusted Platform Module, ofwel TPM, en de cpu in een laptop. BitLocker gebruikt de TPM-chip in een laptop om de decryptiesleutel op te slaan. Om de schijf bij het opstarten van de laptop toegankelijk te maken, wordt de sleutel naar de cpu verstuurd. De communicatie tussen de processor en de TPM is echter niet versleuteld, wat betekent dat de sleutel in cleartext wordt verzonden. Door deze communicatie af te luisteren, kon Stacksmashing de sleutel achterhalen.

Stacksmashing maakte daarvoor een zogeheten TPM-sniffer van een Raspberry Pi Pico. Hij sloot de singleboardcomputer aan op de LPC Bus in de laptop, waardoor hij het verkeer kon onderscheppen. Nadat de onderzoeker de sleutel in handen had gekregen, gebruikte hij de opensourcetool Disclocker om de schijf te ontsleutelen. Vervolgens kon hij alle data inzien.

Microsoft is al langer op de hoogte van dit soort aanvallen, maar benadrukt dat aanvallers hiervoor 'voldoende tijd' nodig hebben. Stacksmashing had echter slechts 43 seconden nodig om de laptop open te maken, de TPM-sniffer aan te sluiten op de LPC Bus en de sleutel te stelen. De benodigde hardware om de TPM-sniffer te maken, kostte hem slechts tien dollar.

Stacksmashing gebruikte voor zijn aanval een Lenovo-laptop, maar ook andere laptops zijn kwetsbaar. De aanval werkt echter alleen als een laptop een aparte TPM en cpu heeft. Zijn de twee samengevoegd, wat op veel laptops het geval is, dan werkt de aanval niet. Gebruikers die zich tegen een dergelijke aanval willen beschermen, kunnen volgens Microsoft mitigerende maatregelen nemen door een pincode te configureren. Overigens werkt de aanval in theorie ook op vergelijkbare processen die informatie vanuit de TPM naar de cpu sturen en niet alleen op BitLocker.

Microsoft BitLocker encryption hacked by a cheap off-the-shelf Raspberry Pi Pico

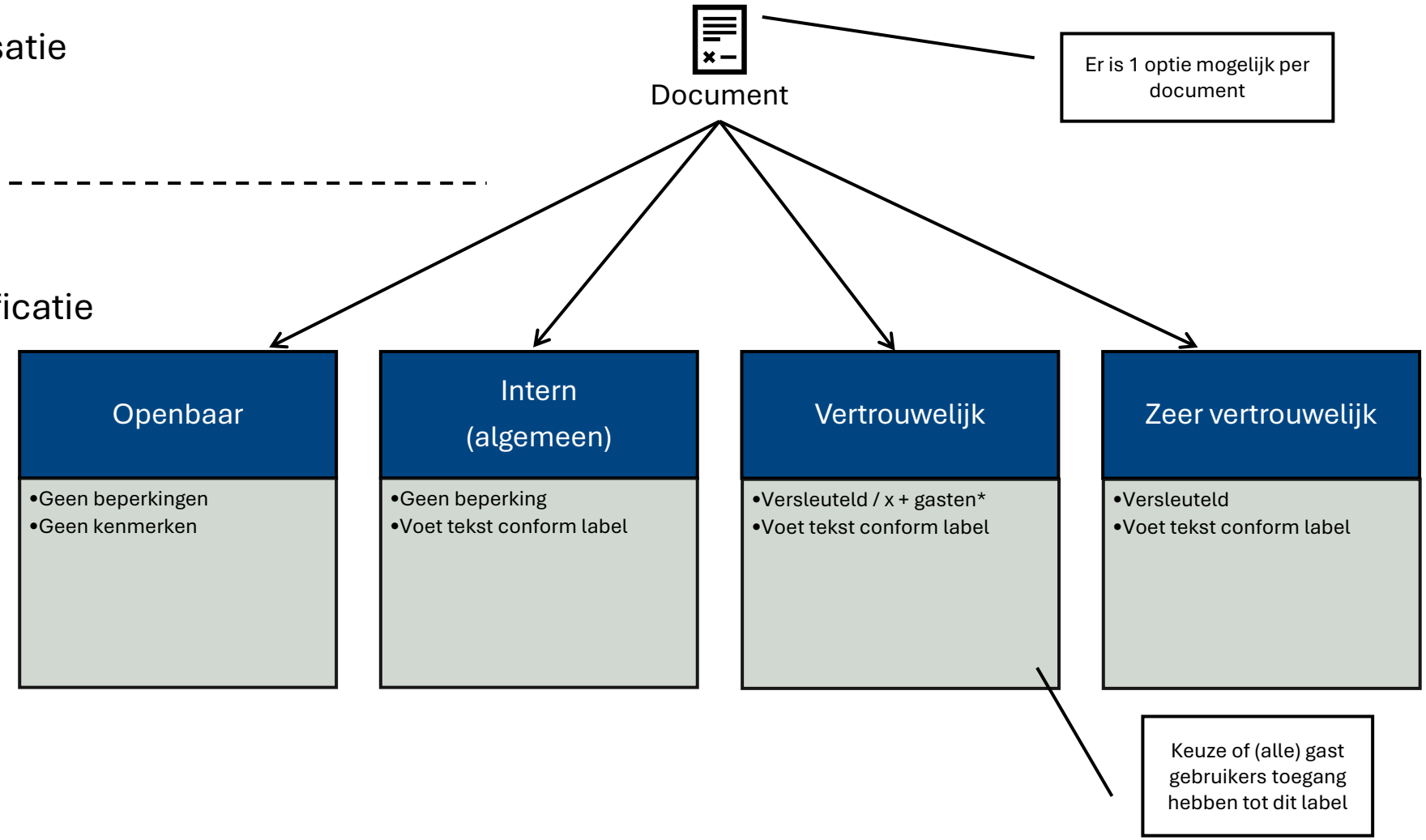
Deanna Ritchie / Last Updated: Feb 7, 2024 / AI / Data and Security / News / Security

Security researcher Stacksmashing showed how hackers may use a $4 Raspberry Pi Pico to retrieve the BitLocker encryption key from Windows PCs in just 43 seconds, in a YouTube video. The researcher claims that specific attacks can get beyond BitLocker's encryption by directly accessing the hardware and retrieving the encryption keys kept in the computer's Trusted Platform Module (TPM) viz the LPC bus.

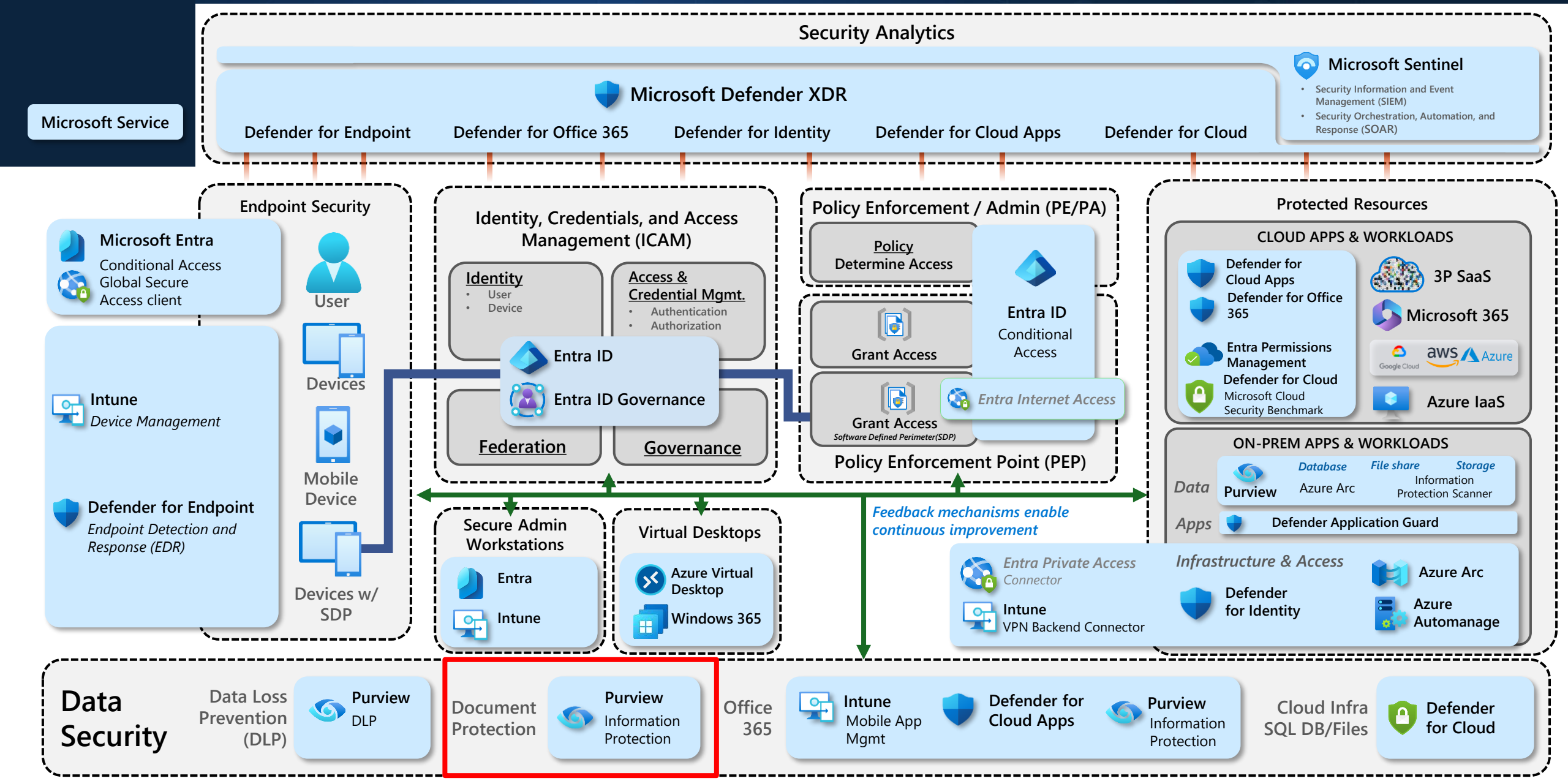
Vertrouwelijkheidslabels

Autorisatie

Classificatie



Microsoft Tools Mapping



Sluit Co-Pilot uit

Vertrouwelijkheidslabel maken

Set-Label -Identity "Niet voor Co-pilot" -AdvancedSettings @{Tooltip="Deze inhoud wordt niet gebruikt door Co-Pilot";BlockContentAnalysisServices="True"}

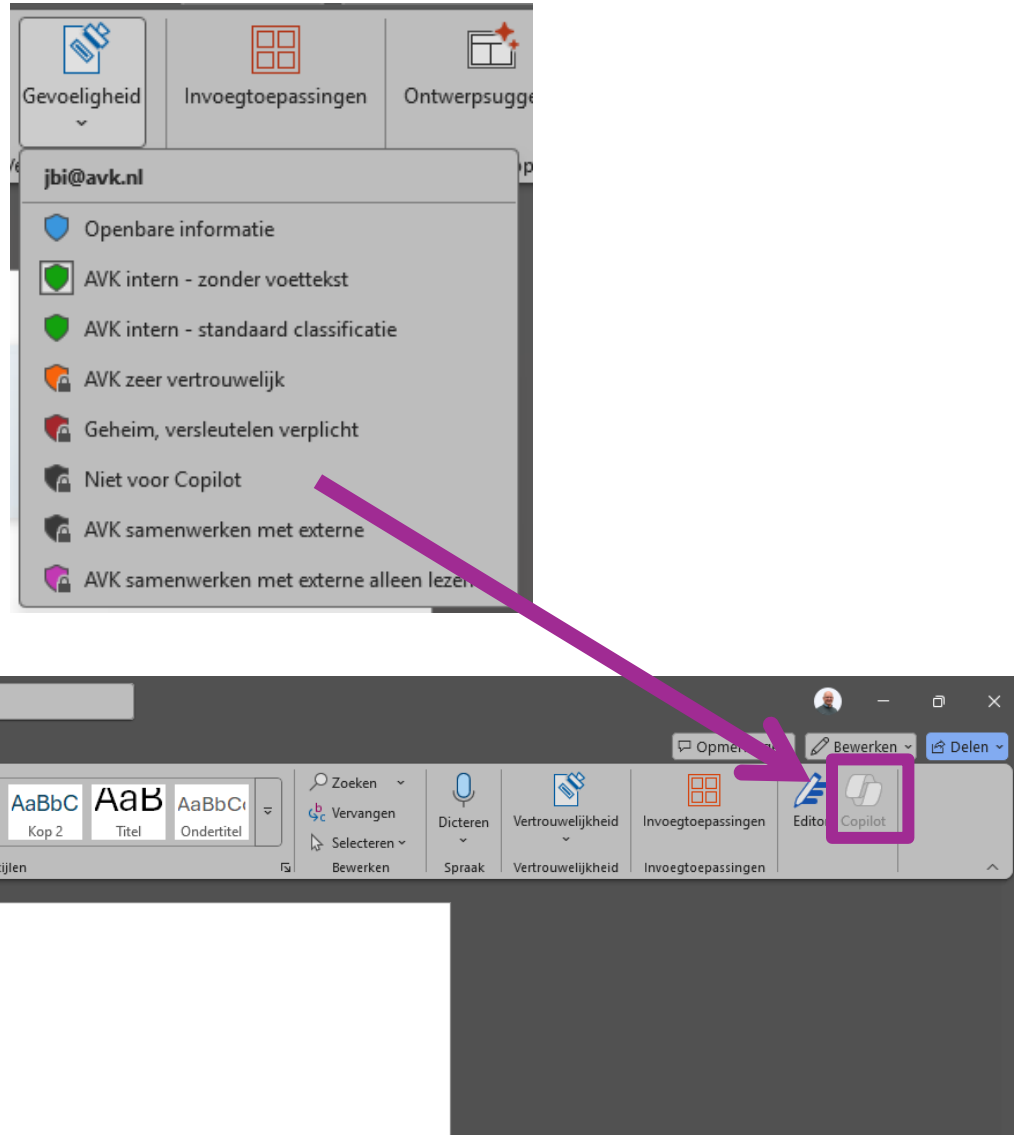
```
PS C:\Windows\system32> Set-Label -Identity "Niet voor Co-Pilot" -AdvancedSettings @{Tooltip="Deze inhoud wordt miet gebruikt
door Co-Pilot";BlockContentAnalysisServices="True"}
```

(Get-Label -Identity 'Niet voor Co-pilot').Settings

```
PS C:\Windows\system32> (Get-Label -Identity 'Niet voor Co-Pilot').Settings
[color, #393939]
[isparent, False]
[contenttype, File, Email]
[tooltip, Dit label voorkomt dat Co-Pilot in inhoud gebruikt]
[displayname, Niet voor Co-Pilot]
[blockcontentanalysisservices, True]
```

https://practical365.com/block-access-to-content-services/

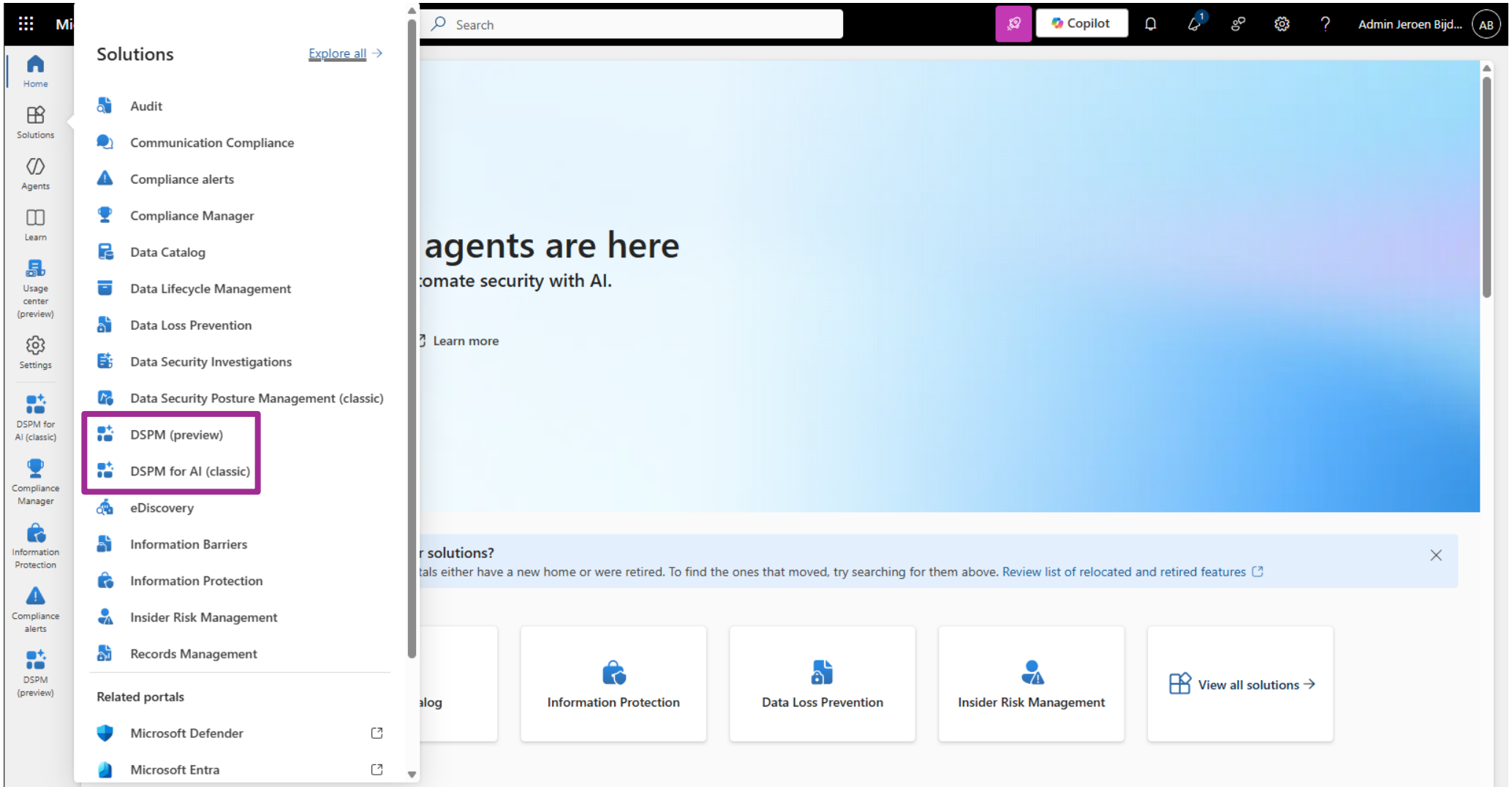
Sluit Co-Pilot uit



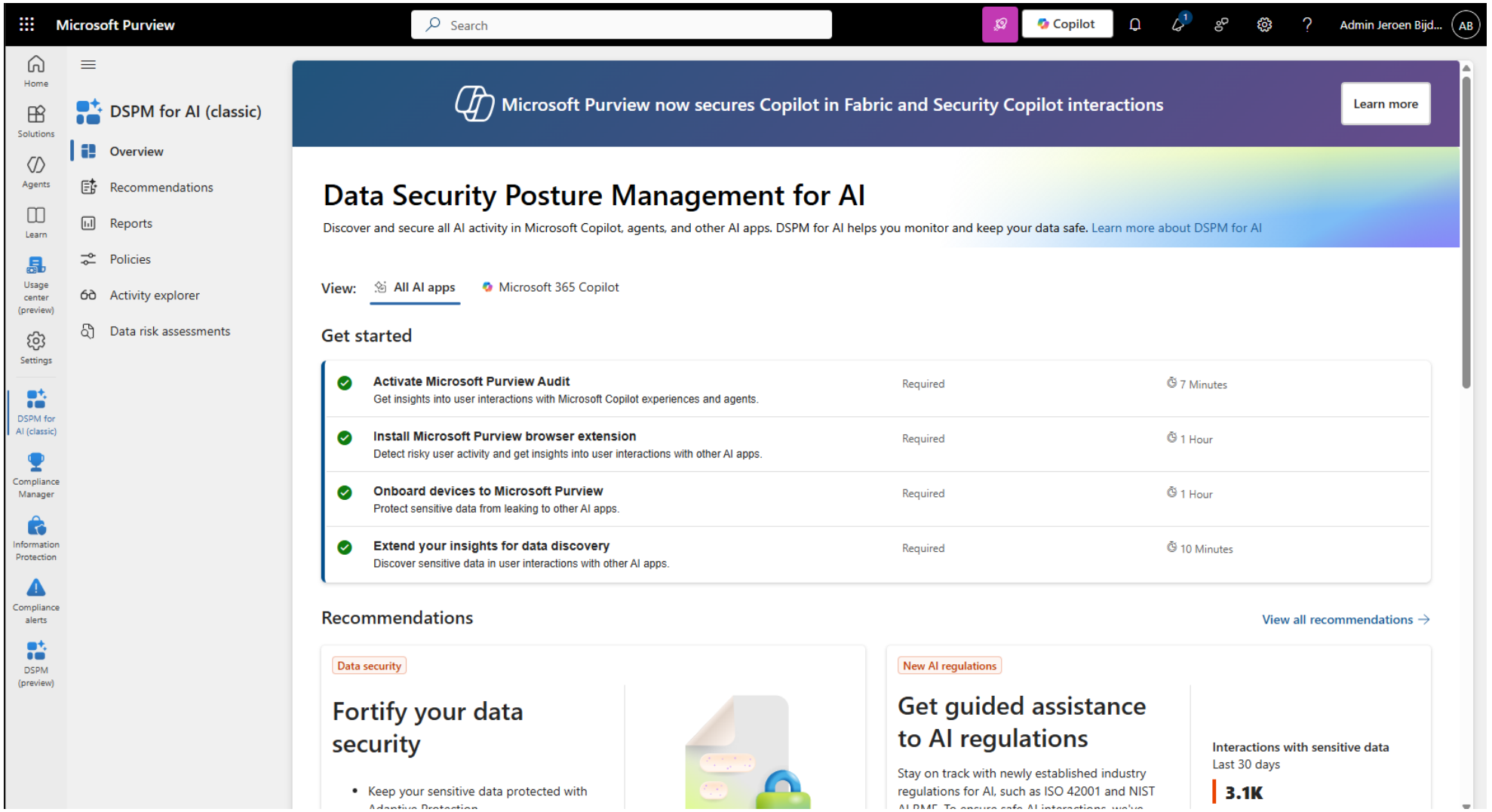
Purview DSPM

Overzicht

Purview overzicht



DSPM for AI


Microsoft Purview
Search
Copilot
Admin Jeroen Bijd...
AB
Home
Solutions
Agents
Learn
Usage center (preview)
Settings
DSPM for AI (classic)
Compliance Manager
Information Protection
Compliance alerts
DSPM (preview)
DSPM for AI (classic)
Overview
Recommendations
Reports
Policies
Activity explorer
Data risk assessments
Microsoft Purview now secures Copilot in Fabric and Security Copilot interactions
Learn more
Data Security Posture Management for AI
Discover and secure all AI activity in Microsoft Copilot, agents, and other AI apps. DSPM for AI helps you monitor and keep your data safe. Learn more about DSPM for AI
View:
All AI apps
Microsoft 365 Copilot
Get started
Activate Microsoft Purview Audit
Get insights into user interactions with Microsoft Copilot experiences and agents.
Required
7 Minutes
Install Microsoft Purview browser extension
Detect risky user activity and get insights into user interactions with other AI apps.
Required
1 Hour
Onboard devices to Microsoft Purview
Protect sensitive data from leaking to other AI apps.
Required
1 Hour
Extend your insights for data discovery
Discover sensitive data in user interactions with other AI apps.
Required
10 Minutes
Recommendations
View all recommendations
Data security
Fortify your data security
Keep your sensitive data protected with
New AI regulations
Get guided assistance to AI regulations
Stay on track with newly established industry regulations for AI, such as ISO 42001 and NIST
Interactions with sensitive data
Last 30 days
3.1K

DSPM (preview)

Microsoft Purview: New Microsoft Purview Data Security Posture Management Experience

IN DEVELOPMENT

PREVIEW AVAILABLE
December 2025

ROLLOUT START
April 2026

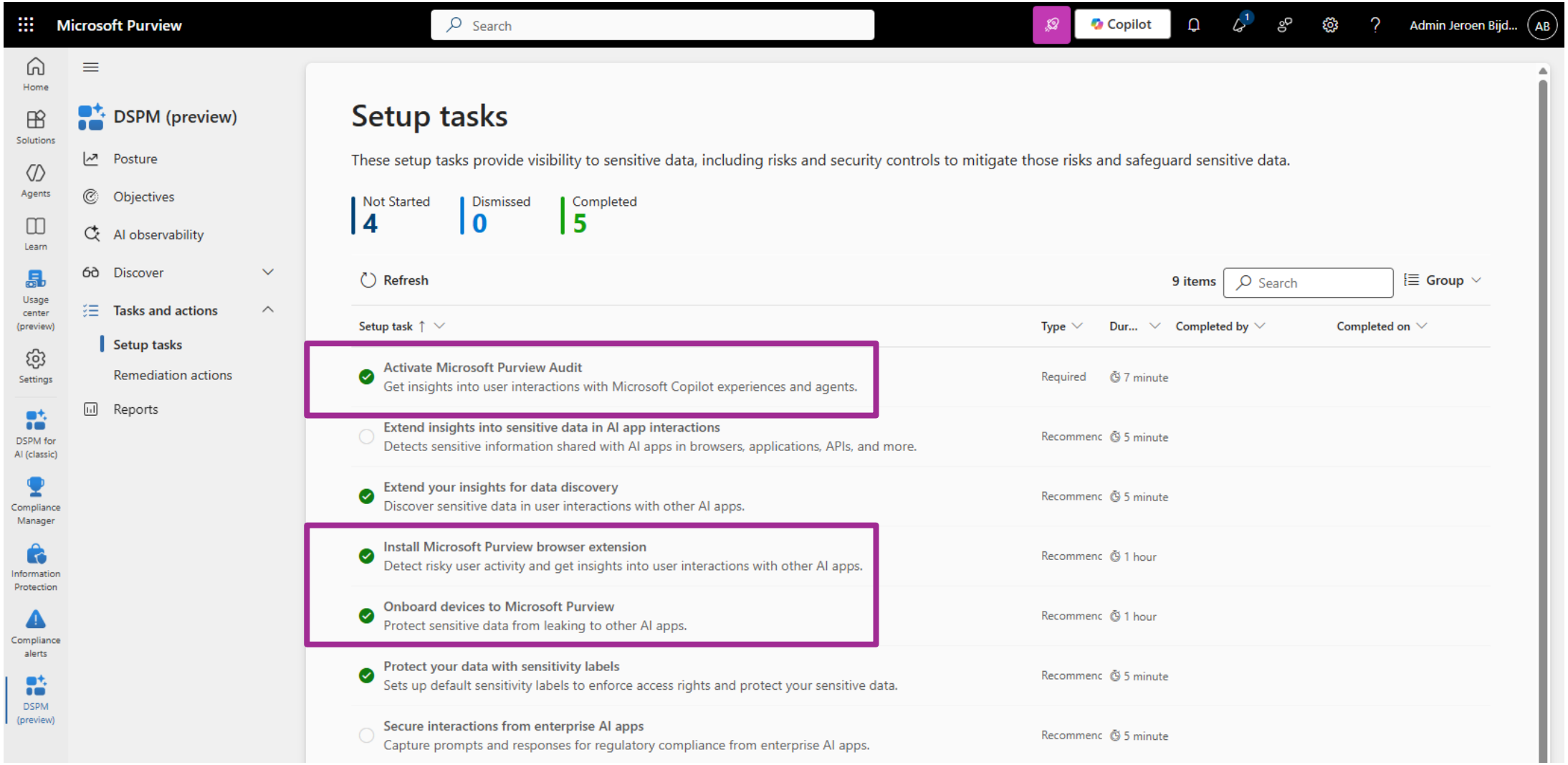
Microsoft Purview

At Ignite, Microsoft is introducing a major evolution of Purview Data Security Posture Management (DSPM) to help organizations strengthen data security and confidently embrace AI. The new DSPM experience unifies visibility and control across traditional data and AI-driven environments, delivering outcome-based guided workflows that turn insights into actionable steps—so teams can prioritize risks and remediate faster. It brings AI observability, enhanced posture reporting, and intelligent Security Copilot agents to automate tasks like triage and policy management. Plus, Purview now extends coverage beyond Microsoft data with third-party signals from partners like BigID, Cyera, OneTrust, and Varonis, giving security teams a single, streamlined view of sensitive data across clouds and platforms. Together, these innovations make DSPM the central hub for managing data security posture in the era of AI. We are also extending Data Risk Assessments to Fabric and to item-level analysis with new remediation actions like bulk disabling of overshared SharePoint links.

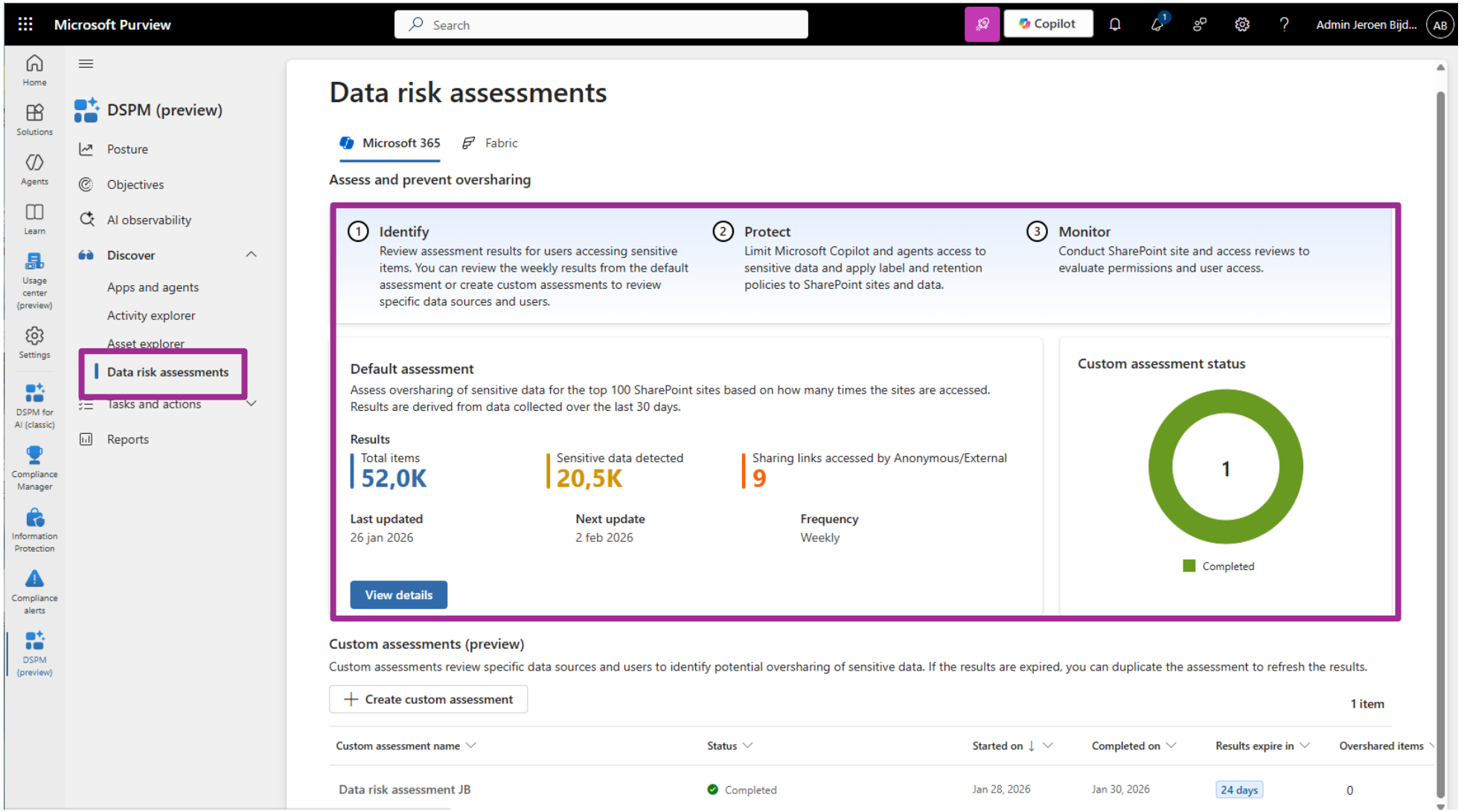
Roadmap ID	Cloud instances(s)	Platform(s)	Release phases(s)
532728	Worldwide (Standard Multi-Tenant)	Web	General Availability, Preview

Added to roadmap: 11/25/2025 | **Last modified:** 11/25/2025

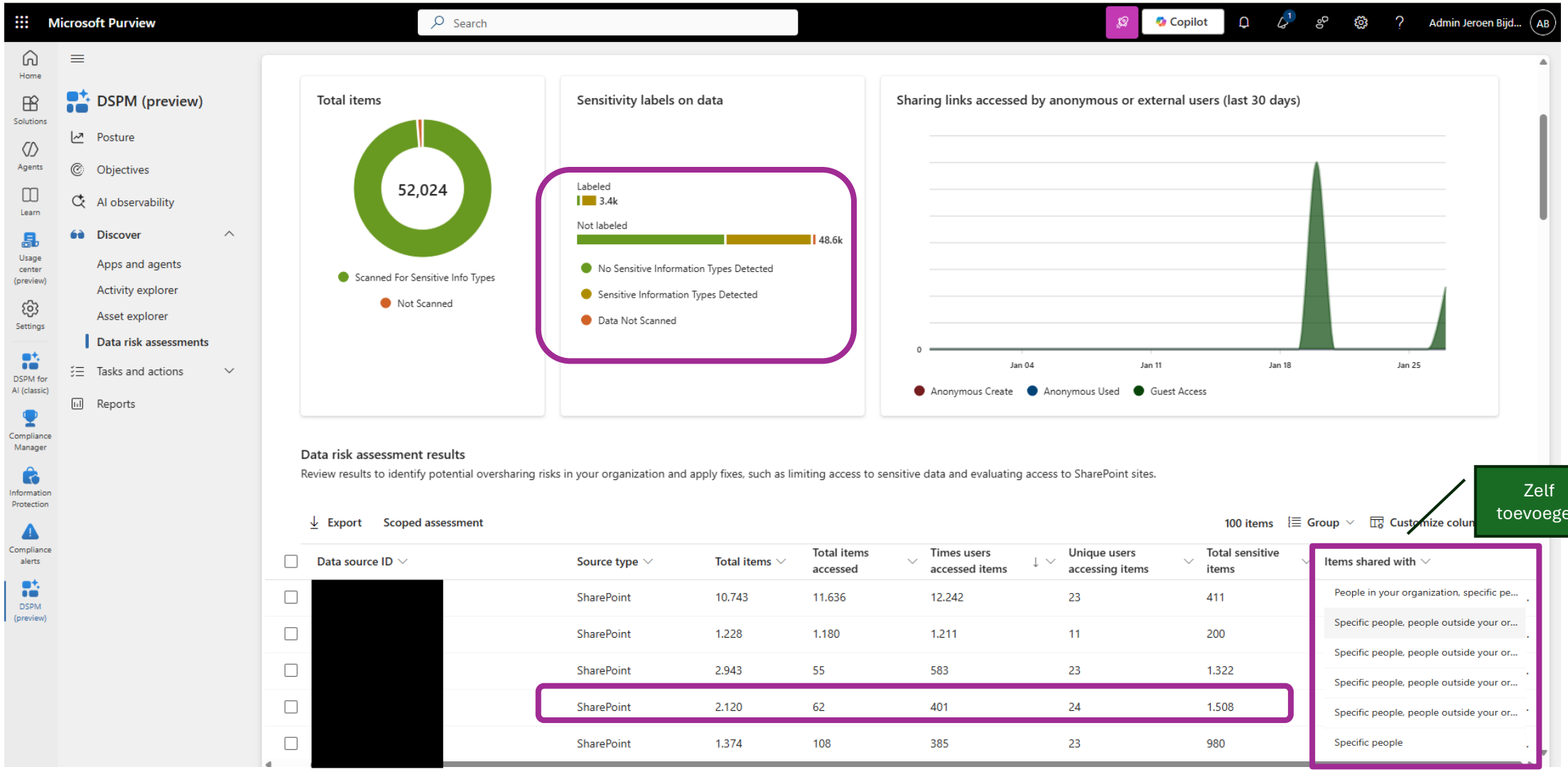
DSPM gereedmaken



DSPM (preview) standaard rapport



DSPM (preview) standaard rapport



DSPM (preview) inzicht per regel

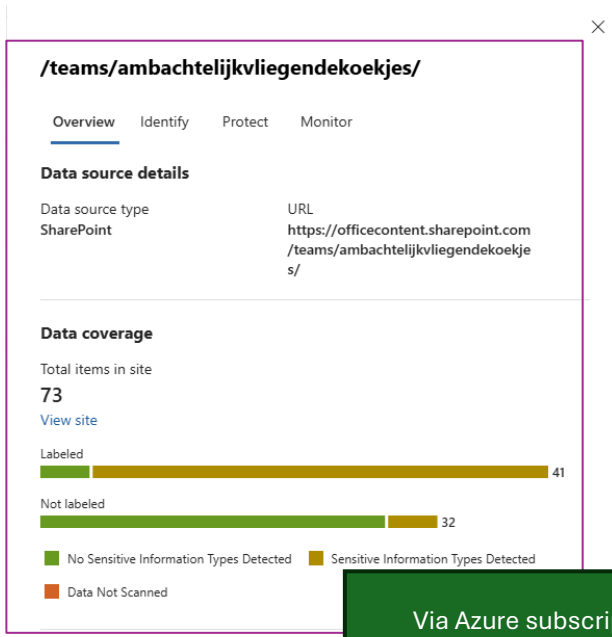
Classificatie

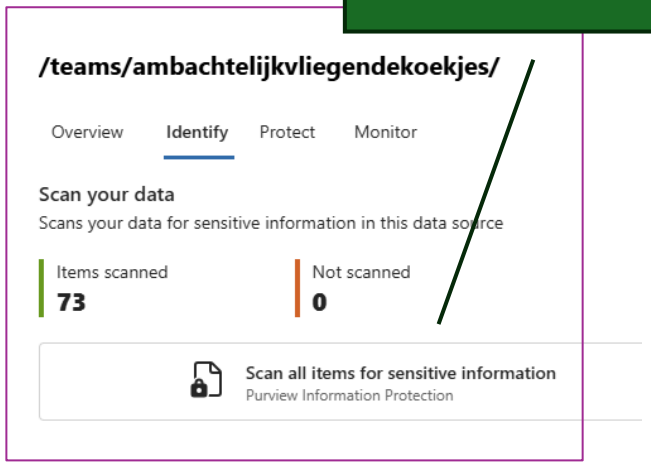
SAM

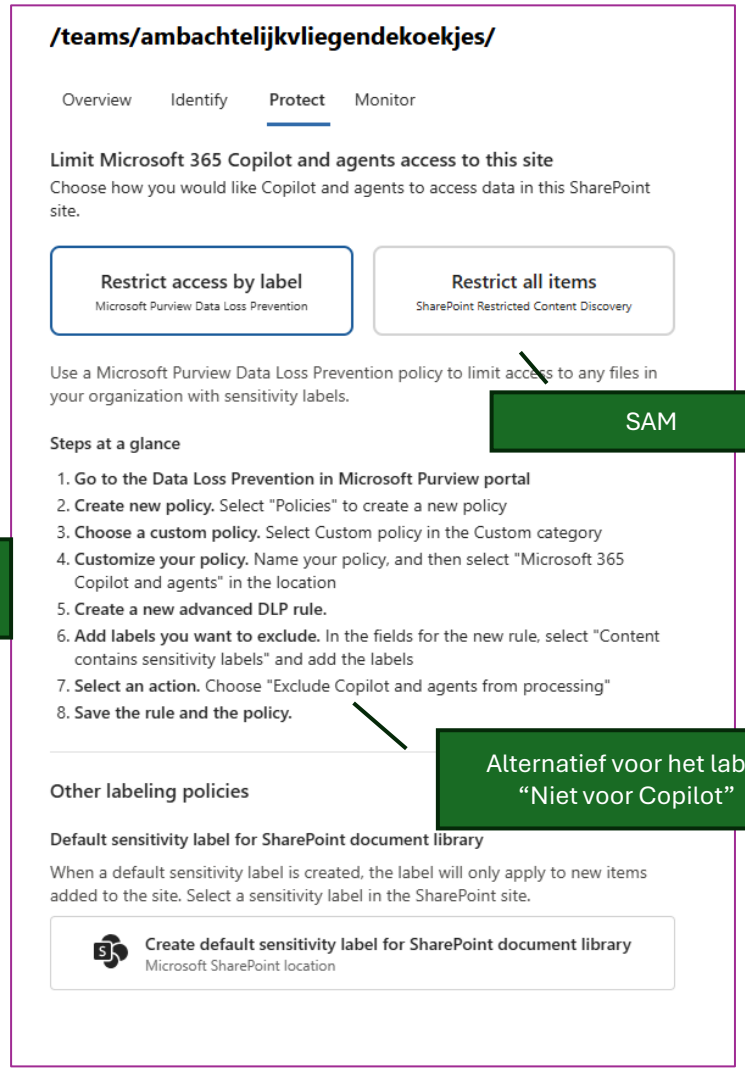
Via Azure subscriptie

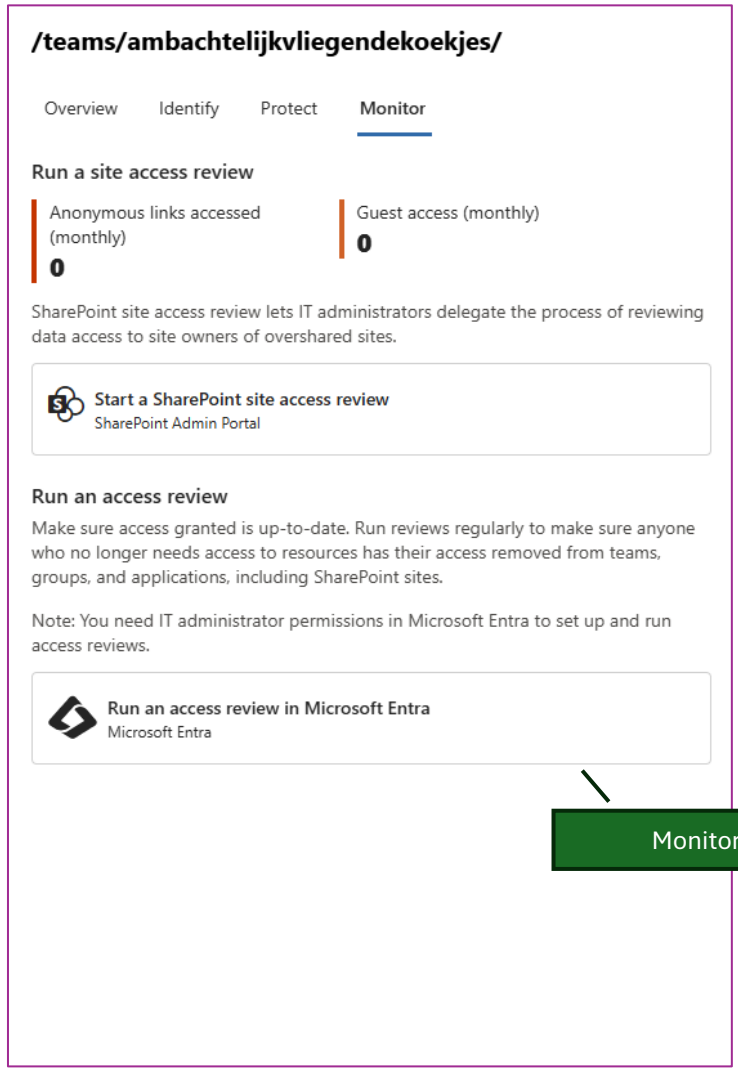
Alternatief voor het label “Niet voor Copilot”

Monitoring

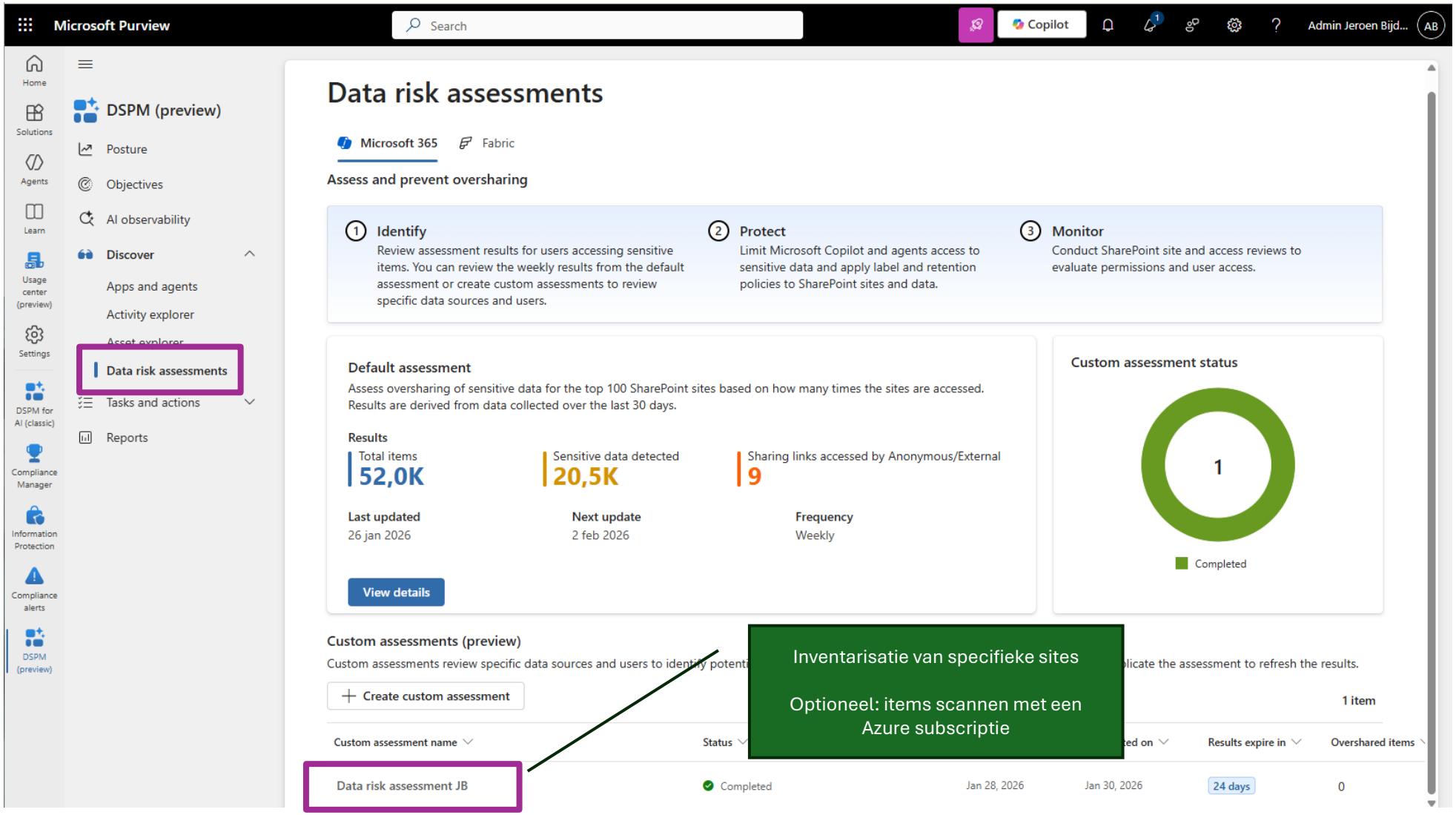








DSPM (preview) aangepast rapport



Gefaseerde Copilot uitrol

Adoptie & beleid

Dataveiligheid voor Copilot gebruik

Visie en beleid

- Sturing door FG en CISO/CIO
- Wat zijn de spelregels (beleid)
- Hoe is support geregeld, waar kan men melden (bijv. datalekken)

Corporate communicatie

- Wat verandert er voor de collega's
- De belangrijkste pijlers onder de aandacht brengen
- Wat is het effect / impact op het werk, whats in it for me

Inhoudelijk awareness programma

- Meetregelen implementeren
- Leren en ontwikkelen
- eLearning en of 2 minuten leren video's
- Webinars
- Klassikale training
- PupQuiz
- Datalek spel

Ambassadeur programma

- Kennis opdoen Klassikaal of online klassikaal (Live Leren)
- Feedback geven op een positieve manier
- Zichtbaar zijn als ambassadeur

Metingen

- Adoptionscore
- Securescore
- Kennis metingen
- Gedrags-metingen
- Test phishing mails

Verandermanagement (menskant)

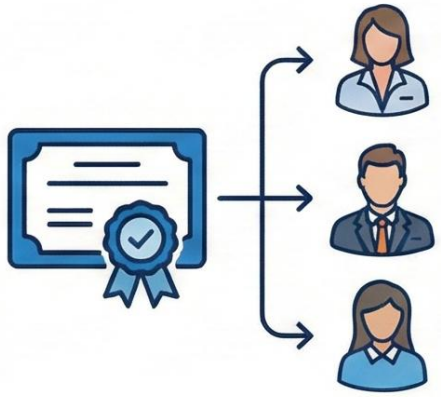
Optimale informatie inrichting

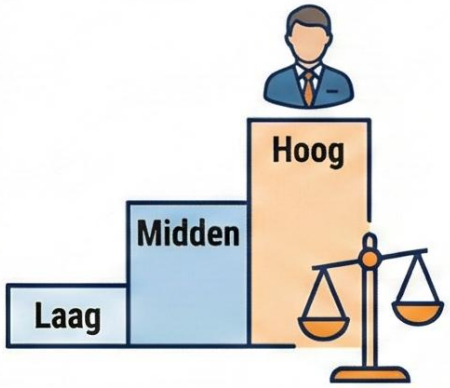
AI-Geletterdheid: Geen Optie, Maar Plicht

De Europese AI Act stelt strikte eisen aan organisaties: wie met AI werkt, moet aantoonbaar over de juiste kennis beschikken.

Verplichte AI-geletterdheid voor iedereen.

Of je nu beleidsmaker, beheerder of gebruiker bent: training is een wettelijke vereiste.



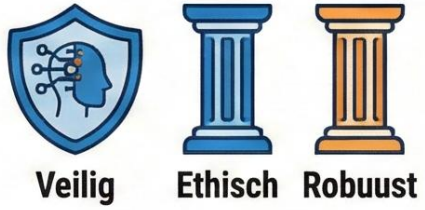


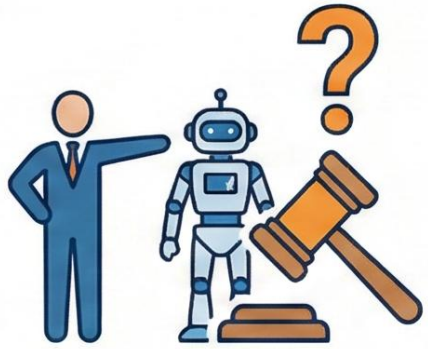
Training op ‘passend niveau’.

De diepgang van de training moet aansluiten bij jouw specifieke rol en de risico’s van het AI-systeem.

Focus op mensgerichte en veilige AI.

Het doel is dat iedereen begrijpt hoe AI veilig, ethisch en robuust ingezet kan worden volgens de EU-richtsnoeren.





Jij blijft eindverantwoordelijk.

Training helpt je kritisch te blijven; AI is de assistent, de mens neemt de beslissing.

Waarom een AI-Beleid Onmisbaar is voor Microsoft Copilot

DE NOODZAAK: WAAROM EEN BELEID?

Innovatie Versnellen, niet Remmen

Duidelijke kaders voorkomen onzekerheid bij medewerkers en dringen risicovolle "Shadow AI" terug.

Beheersing van Nieuwe Risico's

Voorkom dat gevoelige data in prompts belandt of dat onjuiste AI-hallucinaties als waarheid worden gecommuniceerd.

Betrouwbare AI als Kapstok

Beleid borgt dat AI-gebruik wettig (AVG), ethisch en technisch robuust blijft.

DE BELANGRIJKSTE BOUWSTENEN

De Gouden Vuistregel voor Data

Behandel Copilot als M365: deel alleen informatie die je ook via mail of OneDrive mag delen.

Menselijke Eindverantwoordelijkheid

AI is de conceptmaker; de mens controleert altijd de output op feiten en toon.

Drie Lenzen van Governance

Definieer rollen voor Managers, Implementers en Gebruikers.

Risicocategorieën voor Medewerkers

	Voorbeeld Gebruik	Actie
Laag	Samenvatten van eigen notities of brainstormen	Direct toegestaan
Verhoogd	Klantcommunicatie of juridische teksten	Menselijke review verplicht
Hoog	HR-selectie of beoordelingen van mensen	Altijd afstemmen met management

Jij bent verantwoordelijk voor het eindproduct

Auto sales rev up in October

Car, van, pickup and SUV sales surge 32pc year-on-year

By Aamir Shafaat Khan

KARACHI: Pakistan's automotive market showed strong growth in October, with sales of cars, vans, pickups and sport utility vehicles (SUVs) rising to 17,333 units, marking a 32 per cent year-on-year (YoY) increase and a modest 1pc month-on-month (MoM) rise.

According to Myesha Sohail of Topline Securities, the YoY growth reflects a stabilising macroeconomic environment, introduction of new variants, lower interest rates, easing inflation, and improving consumer sentiment.

MoM sales remained largely unchanged, mainly due to an 18pc decline in Pakistan Suzuki Motor Company (PSMC) volumes amid a company-wide reset. The discontinuation of models such as Ravi, Bolan, Every VX, and Wagon R led to MoM declines of 17pc, 84pc, and 28pc in Swift, Ravi, and Every, respectively. Bolan, meanwhile, has seen no sales since May 2025.

Cumulative sales in the first four months of FY26 rose 46pc to 59,600 units, compared to 40,693 units in the same period last year.

Indus Motor Company (IMC) posted the highest MoM growth, with sales climbing 44pc to 4,529 units. Corolla, Yaris, and Cross models collectively rose 41pc MoM and 78pc YoY to 3,742 units, while Fortuner and IMVs jumped 58pc MoM and 83pc YoY to 787 units. IMC's four-month sales stood at 14,418 units, up 66pc YoY.

Hyundai Nishat reported the highe... YoY growth among automakers, risi... 82pc to 1,086 units in October, led ... robust demand for Tucson and Elant... models. MoM sales, however, fell eigh... per cent. Total sales in July-October FY26 reached 4,698 units, up 81 per cent YoY.

Honda Atlas Cars Limited (HACL) recorded a 72pc YoY and 13pc MoM increase in October, with City and Civic models driving growth to 2,247 units. In 4MFY26, HACL sales surged 54 per cent to 7,487 units.

PSMC saw its October sales drop 18pc MoM to 7,403 units, primarily due to declines in Swift, Ravi, and Every. YoY sales increased slightly by 1pc. In 4MFY26, total Pak Suzuki sales rose 33pc YoY to 27,234 units.

Two- and three-wheeler sales surge

Sales of two- and three-wheelers increased 20pc YoY and 4pc MoM, reaching 165,500 units in October, nearing a four-year high. In 4MFY26, total sales climbed 30pc YoY to 597,000 units. Atlas Honda Limited (AHL) set a new record, selling 140,178 CD70 motorcycles in October, surpassing its September 2025 record.

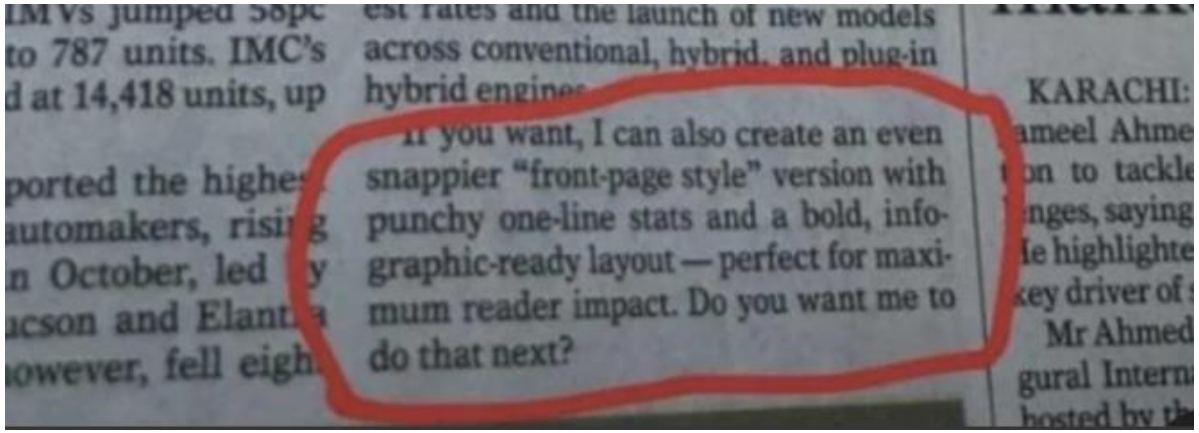
Tractor sales jumped 67pc YoY and 265pc MoM to 2,886 units in October, boosted by the Punjab Green Tractor Scheme. However, 4MFY26 sales fell 15pc to 5,867 units.

Truck and bus sales surged 118pc YoY in October, though they dipped seven per cent MoM to 766 units. In the first four months of FY26, sales had risen 106pc to 2,630 units.

Outlook for FY26

Myesha Sohail expects the positive momentum in Pakistan's auto sector to continue in FY26, driven by lower interest rates and the launch of new models across conventional, hybrid, and plug-in hybrid engines.

If you want, I can also create an even snappier "front-page style" version with punchy one-line stats and a bold, infographic-ready layout — perfect for maximum reader impact. Do you want me to do that next?



to 787 units. IMC's
d at 14,418 units, up
across conventional, hybrid, and plug-in
hybrid engines.
If you want, I can also create an even
snappier "front-page style" version with
punchy one-line stats and a bold, info-
graphic-ready layout — perfect for maxi-
mum reader impact. Do you want me to
do that next?

Vragen