



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**

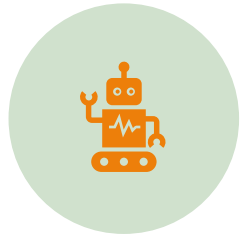


AI is gaaf



AI Act

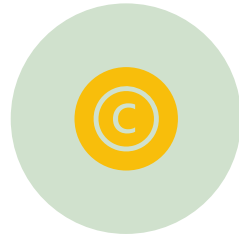
Juridische aspecten AI



AI Verordening



Privacy (AVG)



Auteursrecht



Security (BIO/NIS2)



Overheid? WoO,
Archiefwet, algoritme
kader ...

BIO: Baseline Informatiebeveiliging Overheid

NIS2: Europese 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:

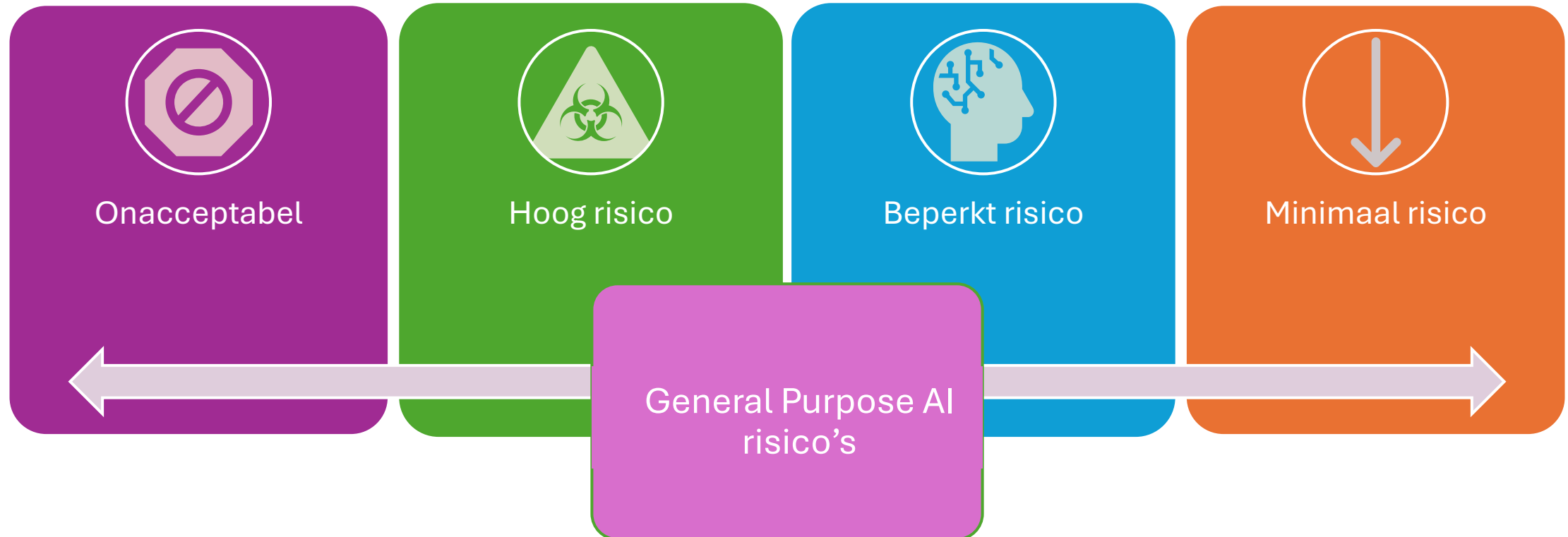
- AI in sollicitatieprocedures (CV-selectie)
- Medische AI (diagnoses)
- AI in kritieke infrastructuur (zoals energie)

Voorbeelden:

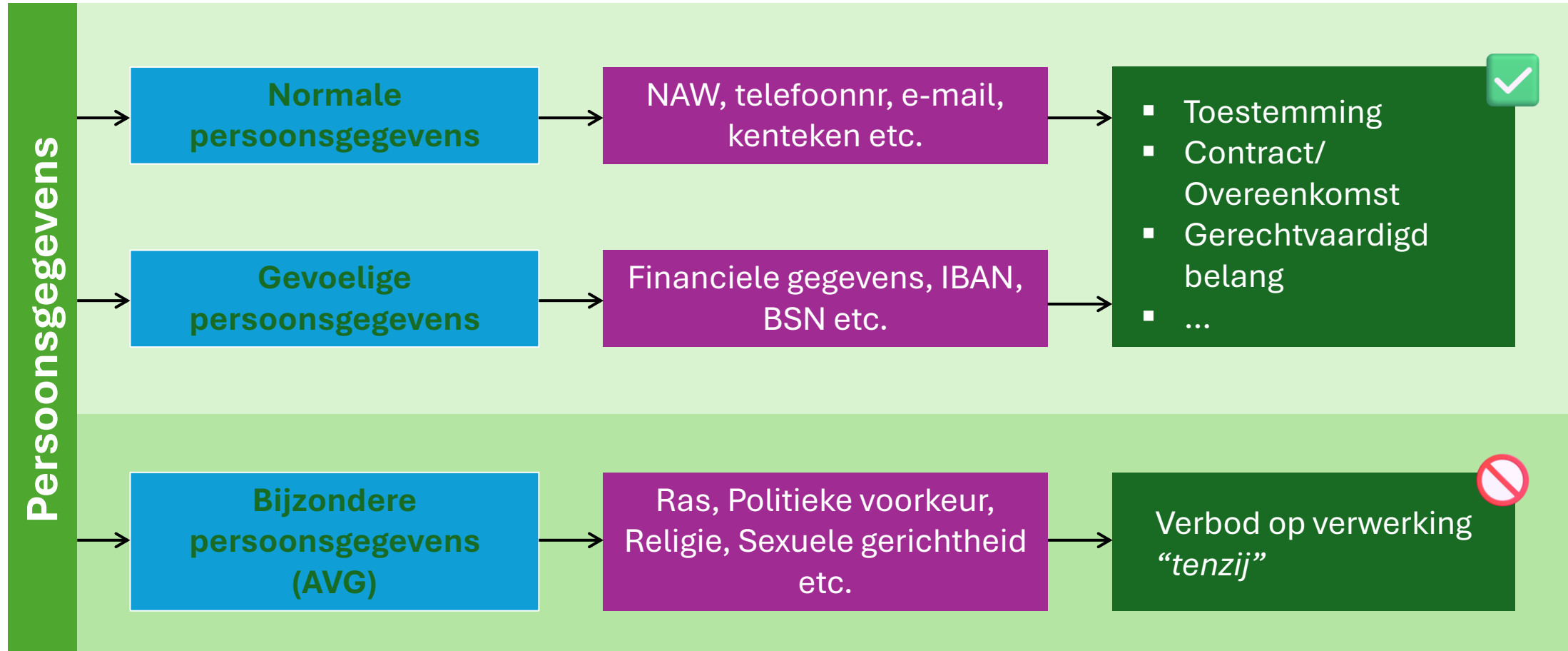
- Chatbots
- Deepfakes
- AI die tekst of beelden genereert

Voorbeelden:

- Spamfilters
- AI in videogames
- Aanbevelingsystemen (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

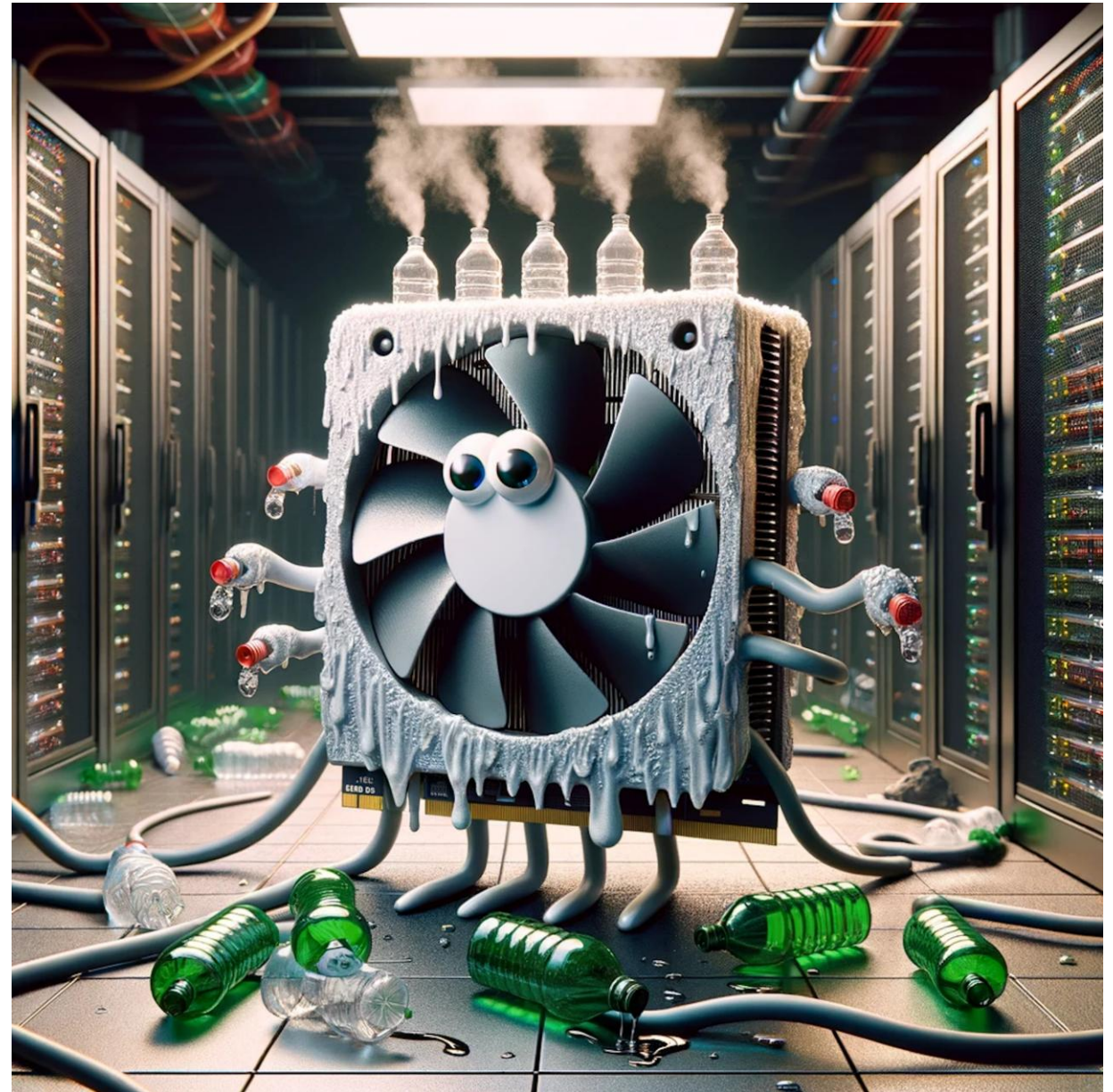
Milieu impact

AI servers

- 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)

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 instelling op publiek

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.

Standaard delen voor iedereen

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

Verbroken rechten sets

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

Gebruik van de groep iedereen behalve externe

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 en bestanden zonder vertrouwelijkheid labels

Digitale vervuiling (ROT)

Redundant

- Meerdere kopieën van hetzelfde document met deels verschillende informatie:
- ProjectPlanDefinitief.docx
- ProjectPlanDefinitief_V4.docx
- ProjectPlanDefinitief_review.docx

Obsolete

- Een strategie plan wat inmiddels achterhaald is
- Een oude HR handboek wat vervangen is door een nieuwe versie maar nog wel beschikbaar is

Trivial


- Persoonlijk aantekeningen op een algemene plek
- Foto's van feesten van verschillende jaren
- Informele notulen van vergaderingen

Digitale vervuiling (ROT)

Redundant	Obsolete	Trivial
<ul style="list-style-type: none">• Meerdere kopieën van hetzelfde document met deels verschillende informatie:• ProjectPlanDefinitief.docx• ProjectPlanDefinitief_V4.docx• ProjectPlanDefinitief_review.docx	<ul style="list-style-type: none">• Een strategie plan wat inmiddels achterhaald is• Een oude HR handboek wat vervangen is door een nieuwe versie maar nog wel beschikbaar is	<ul style="list-style-type: none">• Persoonlijk aantekeningen op een algemene plek• Foto's van feesten van verschillende jaren• Informele notulen van vergaderingen
<ul style="list-style-type: none">• Procedure: Enkelvoudig opslag meervoudig gebruik	<ul style="list-style-type: none">• Procedure: Archief stukken	<ul style="list-style-type: none">• 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









Home > Connectors

Connectors

Gallery Your Connections

Connect your organization's data to improve insights and information provided by Copilot, agents, and Microsoft Search.

[+ Add Connection](#) [Refresh](#)

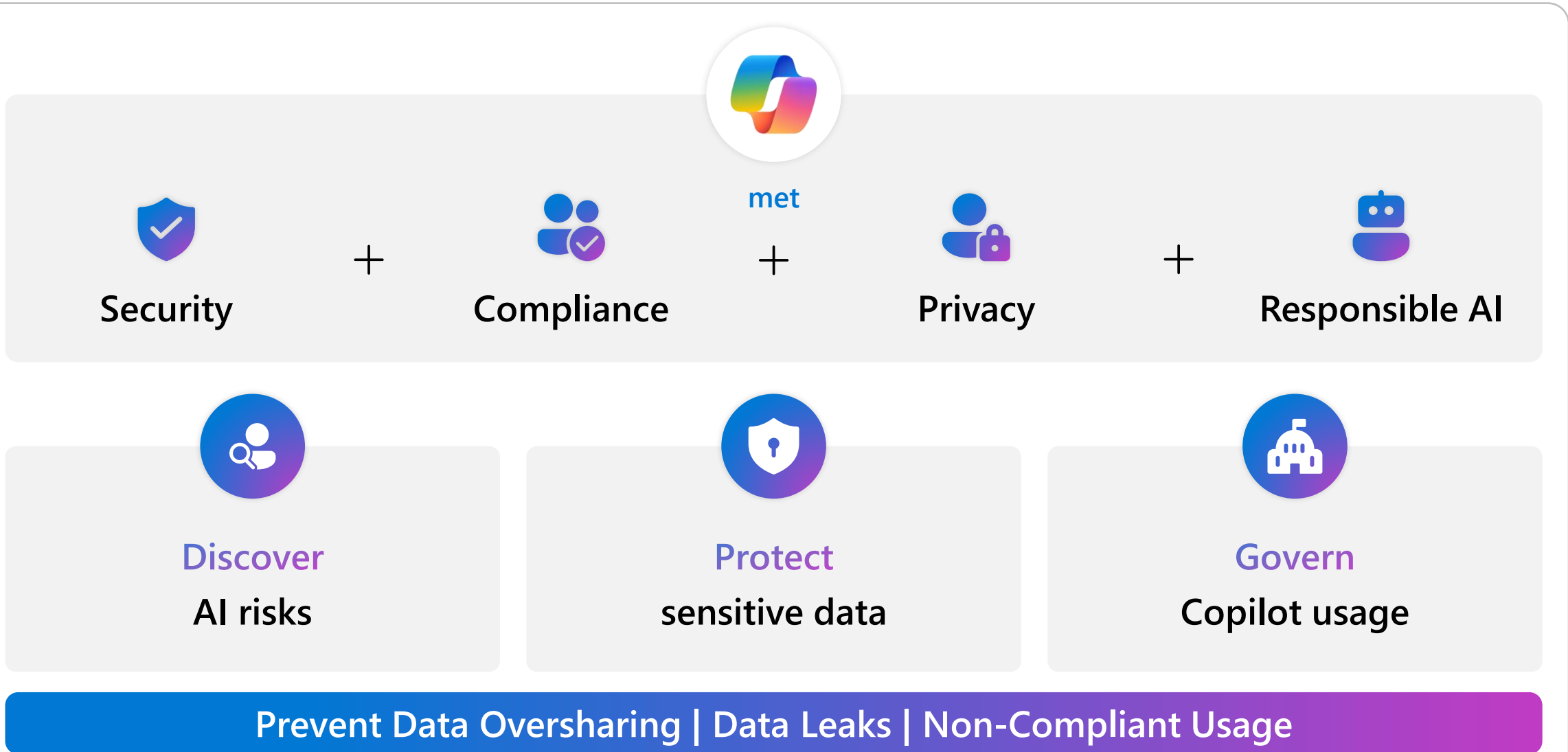
Connection Name	Display Name	Type	Staged Rollout
 Notion	Notion	MCP Enabled by Microsoft	Add staging
 HubSpot	HubSpot	MCP Enabled by Microsoft	Add staging
 Canva	Canva	MCP Enabled by Microsoft	Add staging
 Linear	Linear	MCP Enabled by Microsoft	Add staging
 GoogleContacts	Google Contacts	MCP Enabled by Microsoft	Add staging
 GoogleCalendar	Google Calendar	MCP Enabled by Microsoft	Add staging
 Intercom	Intercom	MCP Enabled by Microsoft	Add staging
 avk.nl Add description for Copilot	avk.nl	Synced	Add staging

Copilot Control System



Framework

Copilot Control System framework



Links

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

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	<ol style="list-style-type: none"> Identify the most popular sites & assess oversharing <ul style="list-style-type: none"> Export the top 100 most used sites from SPO admin center Run SAM permission state report¹ 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 types³ Grant Copilot access to popular, low risk sites <ul style="list-style-type: none"> 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 identified¹ Turn on proactive audit and protection <ul style="list-style-type: none"> Turn Off EEEU (everyone except external users) at the tenant level² 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 Compliance³ Turn on oversharing SPO Purview DLP policy in simulation mode to detect anyone sharing links for labeled and unlabeled data² 	<ol style="list-style-type: none"> Discover oversharing risks <ul style="list-style-type: none"> 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 actions¹ Create customized Purview DSPM for AI Data assessments to scale out data security actions, pivoted on labels and sensitive information types³ Restrict sensitive info from Copilot access and/or processing <ul style="list-style-type: none"> Initiate SAM Access Review for all sites that are overshared¹ Apply SAM restricted access control (RAC) on business-critical sites¹ 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 user² Exclude Copilot from summarizing sensitive content via sensitivity labels³ Increase site privacy <ul style="list-style-type: none"> Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members² Apply default site library sensitivity labels to protect new and modified unlabeled documents³ Turn on enforce-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & starting remediating them² Disable RSS (if enabled) to allow full Copilot experience¹ 	<ol style="list-style-type: none"> Further reduce risk and simplify oversight <ul style="list-style-type: none"> Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners¹ Automate SAM permission state report to maintain permissions hygiene¹ <ul style="list-style-type: none"> Automate permission reports and actions to maintain permission hygiene¹ 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 action¹ Control site provisioning by allowing creation for users that complete training¹ <ul style="list-style-type: none"> Use change history to identify site changes that may cause oversharing¹ Routinely run Purview DSPM for AI Data assessments to scale out data security actions, pivoted on labels and sensitive information types³ Continuously manage all your oversharing Purview DLP alerts via incidents with Microsoft Defender XDR incident queue² View risky user activity in context of oversharing Purview DLP incidents³ Further secure sensitive data <ul style="list-style-type: none"> 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 policies¹ Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access² Improve Copilot responses <ul style="list-style-type: none"> Setup Purview retention/deletion policies for SharePoint to reduce data surface² Identify inactive sites with SAM, then restrict access or delete¹

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**

Microsoft 365 Copilot

You own at least 1 subscription for this product. [Manage subscription details](#)

Microsoft 365 E5 EEA (no Teams)

You own at least 1 subscription for this product. [Manage subscription details](#)

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

The screenshot displays the SharePoint Admin Center interface. The top navigation bar includes the AVK logo, the text "SharePoint admin center", and user information for "Admin Jeroen Bijd...". The left-hand navigation pane lists various administrative areas, with "Data access governance" highlighted. The main content area is titled "Data access governance" and includes a "PRO" badge. It features a "Reports" section with a link to "All review requests" and an introductory paragraph about maintaining security and compliance. A "Get started" callout box recommends starting with a snapshot report. Below this, there are three report categories: "Snapshot reports" (with an information icon), "Site permissions across your organization" (marked as "RECOMMENDED"), and "Site permissions for users" (marked as "NEW"). Each category has a "View reports" button. The "Snapshot reports" section is highlighted with a purple border. At the bottom, there is a "Sensitivity labels applied to files" section with a "View reports" button. The URL at the bottom of the page is https://officecontent-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement.

Site permissions across your organization

Data access governance > Site permissions across your organization > SharePoint report

SharePoint report

This page lists the top 100 sites with the highest number of unique users who have access to the sites and their content. You can download a .csv report for up to 1 million sites.

[Download detailed report](#)

[+](#) Initiate site access review [View all reviews](#) [Restrict site access](#)

Showing top 100 of 135

Filters: [Template: All](#) [Site sensitivity: All](#) [External sharing: All](#) [Privacy: All](#)

<input type="checkbox"/>	Name	URL	Site access review status	Files	Items with unique...	Total permissi...	Guest user permissio...	External participa...	Entra groups	Count of 'People...	Count of 'Anyone' li.
<input type="checkbox"/>			-	22	1	47	0	0	3	0	0
<input type="checkbox"/>			-	3682	62	45	4	0	8	15	0
<input type="checkbox"/>			-	1581	45				10	3	0
<input type="checkbox"/>			-	23276	69				8	10	0
<input type="checkbox"/>			-	195	7	36	46	0	0	0	0
<input type="checkbox"/>			-	2493	81	35	8	0	6	13	0
<input type="checkbox"/>			-	692	11	30	3	0	6	0	0
<input type="checkbox"/>			-	77	0	28	0	0	2	0	0
<input type="checkbox"/>			-	82	5	27	0	0	6	0	0

Vooral inzage qua rechten niet de gevoeligheid van deze informatie

Verbroken rechten

Gasten toegevoegd

Iedereen toegevoegd

SharePoint Advanced Management



Rechten structuren

SharePoint Advanced Management

SharePoint admin center

Home > Advanced management

Advanced management

Easily manage your content with policies, reports, and settings that simplify your workflow, strengthen security, and help your organization work better together.

[Learn more about SharePoint Advanced Management](#)

Overview All features

What's included

Feature ↑	Location	Purpose
Block download policy for SharePoint and OneDrive	Microsoft PowerShell	Prevent download for both external and internal users
Change history	Reports > Change history	Find who made particular site or organization setting changes and when
Conditional access policies for SharePoint and OneDrive	Microsoft Entra conditional access	Control whether users can access sensitive sites based on conditions like location or operating system
Data access governance reports	Reports > Data access governance	Discover potential oversharing and keep track of sites that have sensitive files
OneDrive access restriction	Policies > Access control > OneDrive access restriction	Allow only particular groups of users to use OneDrive
Recent actions	Active sites > Recent actions	Review recent site changes you made
Site lifecycle management	Policies > Site lifecycle management	Automate tasks across the life cycle of your sites
Site-level access restriction	Policies > Access control > Site-level access restriction	Allow admins to restrict access to specific SharePoint sites and their content

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

Site lifecycle management

The screenshot shows the SharePoint admin center interface. The left sidebar contains navigation options: Home, Sites (Active sites, Deleted sites), Containers, Policies (Sharing, Access control, Site lifecycle management), Settings, Content services, Migration, Reports, Advanced, More features, Advanced management (PRO), and Customize navigation. The main content area is titled "Site lifecycle management" (PRO) and includes a description: "Use this page to create and manage policies that automate tasks across the lifecycle of your sites." and a link: "Learn more about managing the lifecycle of your sites".

Three policy categories are highlighted with a dashed box and annotated with green boxes:

- Inactive site policies** (Number of policies: 1):
 - Create and configure policies to:
 - Identify inactive sites
 - Send notifications to site owners or admins
 - Automatically archive or mark sites in read-only

Annotation: 6 maanden geen activiteiten
- Site ownership policies** (Number of policies: 1):
 - Create and configure policies to:
 - Identify sites that don't meet organization's ownership criteria
 - Send notifications to find new site owners or admins
 - Automatically mark sites in read-only

Annotation: Teams eigenaar rollen en verantwoordelijkheden
- Site attestation policies** (Number of policies: 1):
 - Create and configure policies to:
 - Identify sites due for attestation of their information
 - Send notifications to site owners or admins seeking attestation
 - Automatically archive or mark sites in read-only

Annotation: Her bevestiging noodzaak site

Each policy category has an "Open" button. The interface also shows "Copilot", "Admin Jeroen Bijd...", "Dark mode", and a "Show all" button in the bottom right corner.

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 ↓	Channels ↓
✓ 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



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

External file sharing ⓘ

New and existing guests

[More sharing settings](#)

Restrict content from Microsoft 365 Copilot ⓘ PRO

- On
- Off

Custom scripts ⓘ

Blocked
[Edit](#)

Privacy

- Private
- Public

Sensitivity label ⓘ

None

Restricted site access ⓘ PRO

Ambachtelijk Vliegende Koekjes, Jeroens Demo site
[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

<input checked="" type="checkbox"/>	Site name ↑ ⌵	URL ⌵	Teams ⌵	Channels
<input checked="" type="checkbox"/>	Jeroens Demo site	.../teams/JeroensDemosite	-	-



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

SharePoint admin center | Copilot | ? | Admin Jeroen Bijd... AB

Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive. [Learn more about managing sharing settings](#)

External sharing

Content can be shared with:

SharePoint | OneDrive

Most permissive | Least permissive

- Anyone**
Users can share files and folders using links that don't require sign-in.
- New and existing guests**
Guests must sign in or provide a verification code.
- Existing guests**
Only guests already in your organization's directory.
- Only people in your organization**
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings ▾

File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

- Specific people (only the people the user specifies)
- Only people in your organization
- Anyone with the link

Choose the permission that's selected by default for sharing links.

- View

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-mail 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 plaintext wordt verzonden. Door deze communicatie af te luisteren, kon Stacksmashing de sleutel achterhalen.

Stacksmashing maakte daarvoor een zogeheten TPM-sniiffer 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-sniiffer aan te sluiten op de LPC Bus en de sleutel te stelen. De benodigde hardware om de TPM-sniiffer 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) via the LPC bus.



Vertrouwelijkheidslabels

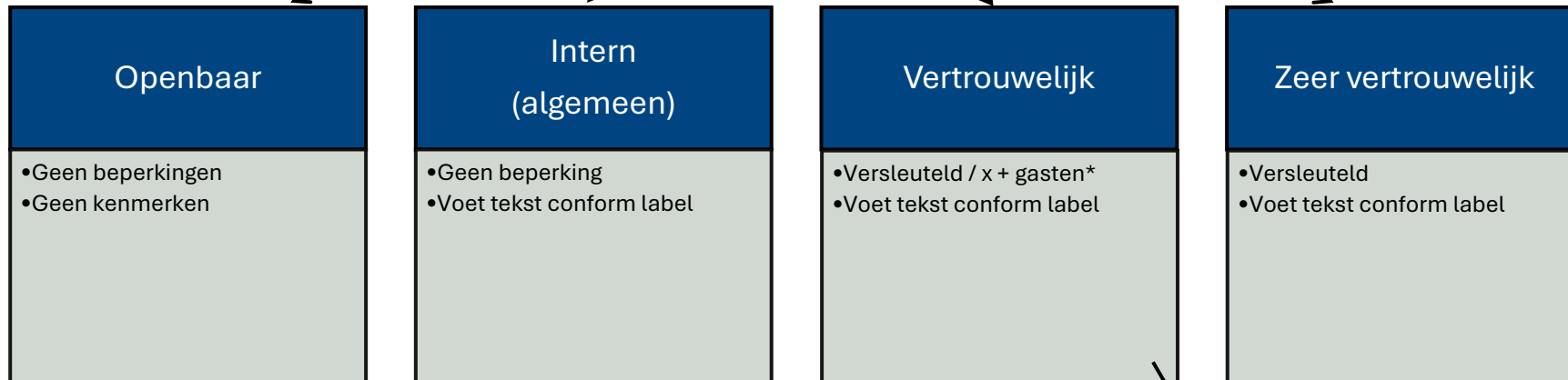
Autorisatie



Document

Er is 1 optie mogelijk per document

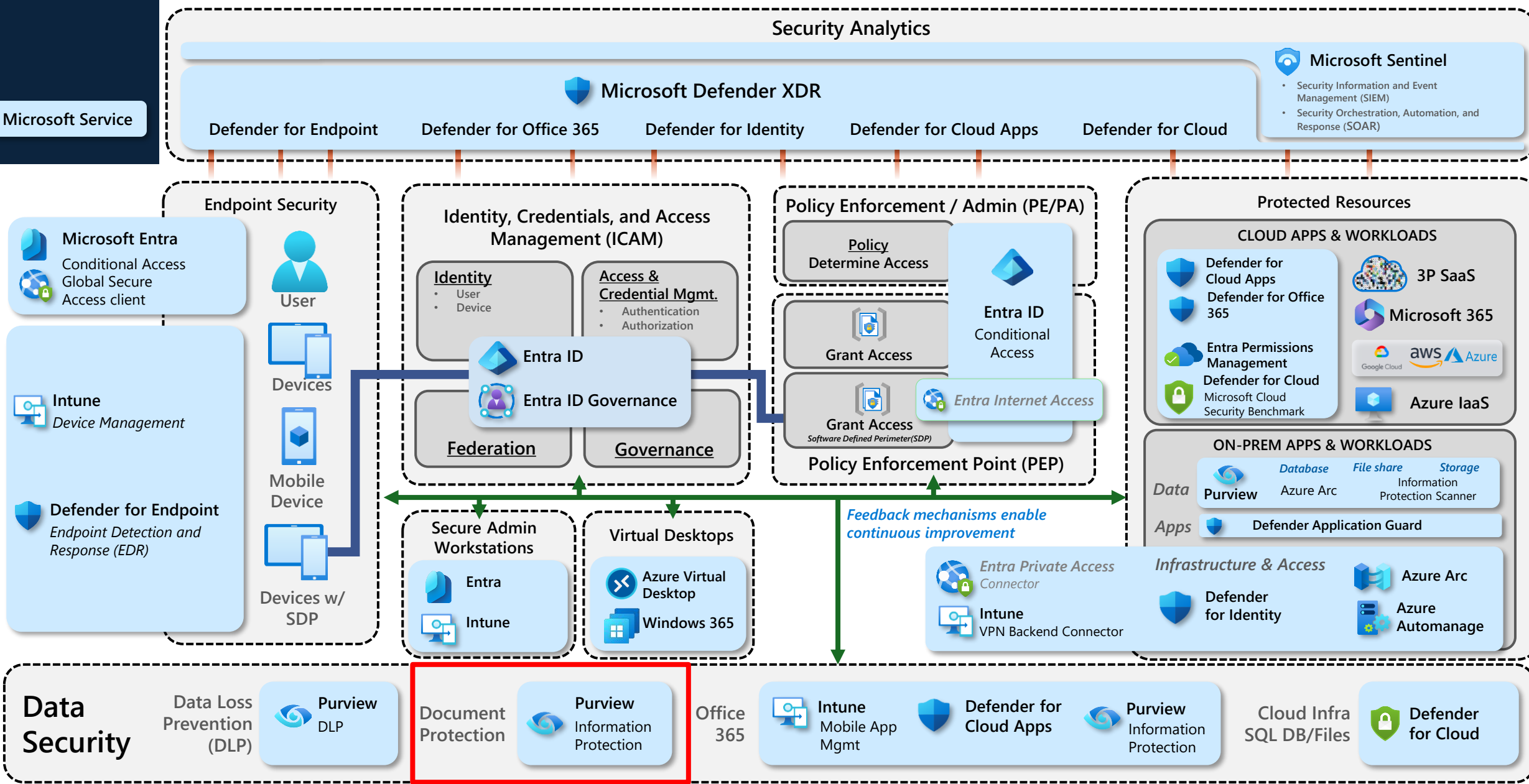
Classificatie



Keuze of (alle) gast gebruikers toegang hebben tot dit label

Microsoft Tools Mapping

Microsoft Service



Security Analytics

Microsoft Defender XDR

Microsoft Sentinel

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Defender for Endpoint Defender for Office 365 Defender for Identity Defender for Cloud Apps Defender for Cloud

Endpoint Security

Microsoft Entra
Conditional Access
Global Secure
Access client

Intune
Device Management

Defender for Endpoint
Endpoint Detection and Response (EDR)

User

Devices

Mobile Device

Devices w/ SDP

Identity, Credentials, and Access Management (ICAM)

Identity

- User
- Device

Access & Credential Mgmt.

- Authentication
- Authorization

Entra ID

Entra ID Governance

Federation **Governance**

Policy Enforcement / Admin (PE/PA)

Policy Determine Access

Grant Access

Grant Access
Software Defined Perimeter (SDP)

Entra ID Conditional Access

Entra Internet Access

Policy Enforcement Point (PEP)

Protected Resources

CLOUD APPS & WORKLOADS

Defender for Cloud Apps

Defender for Office 365

Entra Permissions Management

Defender for Cloud

Microsoft Cloud Security Benchmark

3P SaaS

Microsoft 365

Google Cloud AWS Azure

Azure IaaS

ON-PREM APPS & WORKLOADS

Data

Purview Database File share Storage

Azure Arc Information Protection Scanner

Apps

Defender Application Guard

Infrastructure & Access

Defender for Identity

Azure Arc

Azure Automanage

Secure Admin Workstations

Entra

Intune

Virtual Desktops

Azure Virtual Desktop

Windows 365

Feedback mechanisms enable continuous improvement

Entra Private Access Connector

Intune VPN Backend Connector

Data Security

Data Loss Prevention (DLP) Purview DLP

Document Protection Purview Information Protection

Office 365 Intune Mobile App Mgmt Defender for Cloud Apps Purview Information Protection

Cloud Infra SQL DB/Files Defender for Cloud

Sluit Co-Pilot uit

Vertrouwelijkheidslabel maken

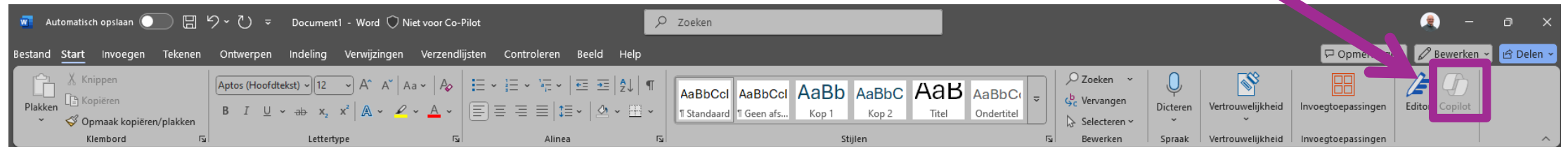
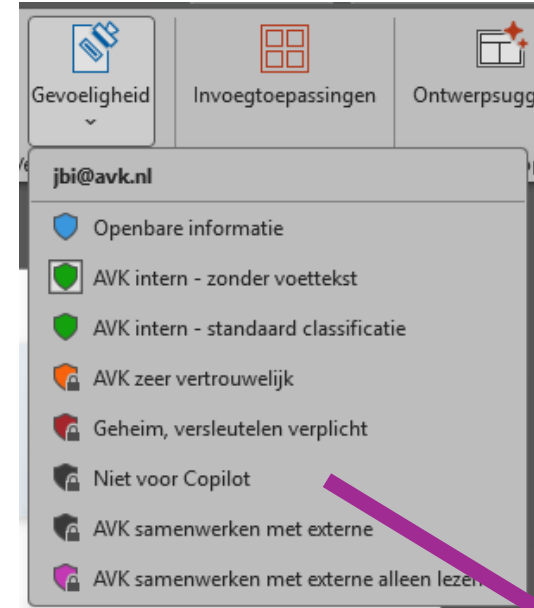
```
Set-Label -Identity "Niet voor Co-pilot" -AdvancedSettings @{Tooltip="Deze inhoud wordt niet gebruikt door Co-Pilot";BlockContentAnalysisServices="True"}
```

```
PS C:\Windows\system32> Set-Label -Identity "Niet voor Co-Pilot" -AdvancedSettings @{Tooltip="Deze inhoud wordt niet 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]
[blockcontentanalysiservices, True]
```

Sluit Co-Pilot uit



Dit is een test voor het label niet co-pilot...

Purview DSPM

Overzicht

Purview overzicht

Solutions [Explore all](#) →

- Audit
- Communication Compliance
- Compliance alerts
- Compliance Manager
- Data Catalog
- Data Lifecycle Management
- Data Loss Prevention
- Data Security Investigations
- Data Security Posture Management (classic)
- DSPM (preview)**
- DSPM for AI (classic)**
- eDiscovery
- Information Barriers
- Information Protection
- Insider Risk Management
- Records Management

agents are here
Automate security with AI.
[Learn more](#)

For solutions?
Items either have a new home or were retired. To find the ones that moved, try searching for them above. [Review list of relocated and retired features](#)

Information Protection | Data Loss Prevention | Insider Risk Management | [View all solutions](#) →

DSPM for AI

Microsoft Purview Search Copilot Admin Jeroen Bijd...

Microsoft Purview now secures Copilot in Fabric and Security Copilot interactions

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 Adaptive Protection

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 AI RMF. To ensure safe AI interactions, make

Interactions with sensitive data
Last 30 days

3.1K

DSPM (preview)

Microsoft Purview: New Microsoft Purview Data Security Posture Management Experience

Microsoft Purview

■ □ □ IN DEVELOPMENT

PREVIEW AVAILABLE ROLLOUT START
December 2025 April 2026

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
532728

Cloud instances(s)
Worldwide (Standard Multi-Tenant)

Platform(s)
Web

Release phases(s)
General Availability, Preview

DSPM gereedmaken

Microsoft Purview Search Copilot Admin Jeroen Bijd... AB

Setup tasks

These setup tasks provide visibility to sensitive data, including risks and security controls to mitigate those risks and safeguard sensitive data.

Not Started **4** Dismissed **0** Completed **5**

Refresh 9 items Search Group

Setup task	Type	Dur...	Completed by	Completed on
<input checked="" type="checkbox"/> Activate Microsoft Purview Audit Get insights into user interactions with Microsoft Copilot experiences and agents.	Required	7 minute		
<input type="checkbox"/> Extend insights into sensitive data in AI app interactions Detects sensitive information shared with AI apps in browsers, applications, APIs, and more.	Recommend	5 minute		
<input checked="" type="checkbox"/> Extend your insights for data discovery Discover sensitive data in user interactions with other AI apps.	Recommend	5 minute		
<input checked="" type="checkbox"/> Install Microsoft Purview browser extension Detect risky user activity and get insights into user interactions with other AI apps.	Recommend	1 hour		
<input checked="" type="checkbox"/> Onboard devices to Microsoft Purview Protect sensitive data from leaking to other AI apps.	Recommend	1 hour		
<input checked="" type="checkbox"/> Protect your data with sensitivity labels Sets up default sensitivity labels to enforce access rights and protect your sensitive data.	Recommend	5 minute		
<input type="checkbox"/> Secure interactions from enterprise AI apps Capture prompts and responses for regulatory compliance from enterprise AI apps.	Recommend	5 minute		

DSPM (preview) standaard rapport

Microsoft Purview Search Copilot Admin Jeroen Bijd... AB

Data risk assessments

Microsoft 365 Fabric

Assess and prevent oversharing

- 1 Identify**
Review assessment results for users accessing sensitive items. You can review the weekly results from the default assessment or create custom assessments to review specific data sources and users.
- 2 Protect**
Limit Microsoft Copilot and agents access to sensitive data and apply label and retention policies to SharePoint sites and data.
- 3 Monitor**
Conduct SharePoint site and access reviews to evaluate permissions and user access.

Default assessment

Assess oversharing of sensitive data for the top 100 SharePoint sites based on how many times the sites are accessed. Results are derived from data collected over the last 30 days.

Results

Total items	Sensitive data detected	Sharing links accessed by Anonymous/External
52,0K	20,5K	9

Last updated: 26 jan 2026 | Next update: 2 feb 2026 | Frequency: Weekly

[View details](#)

Custom assessment status

1

Completed

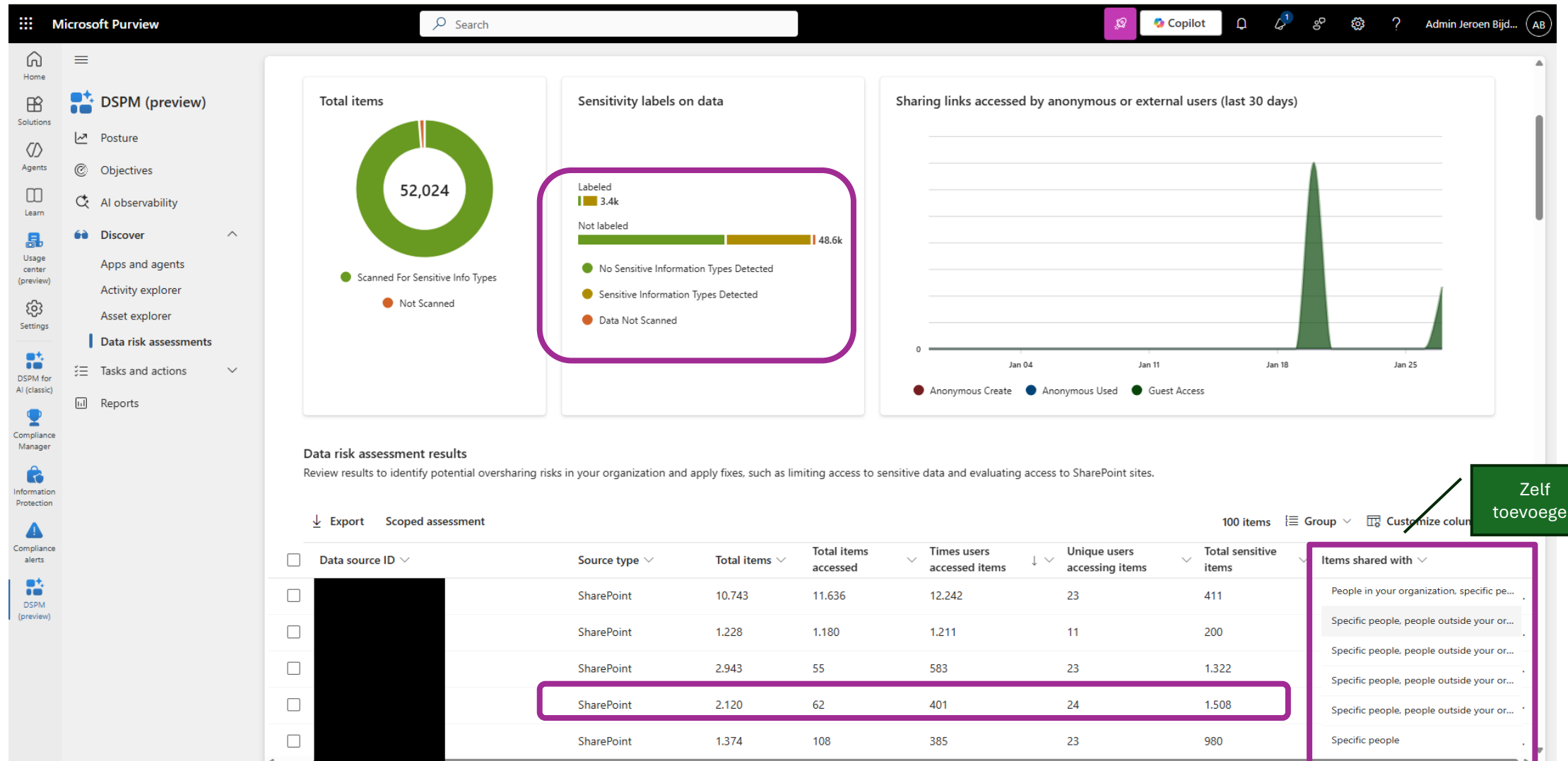
Custom assessments (preview)

Custom assessments review specific data sources and users to identify potential oversharing of sensitive data. If the results are expired, you can duplicate the assessment to refresh the results.

[+ Create custom assessment](#) 1 item

Custom assessment name	Status	Started on	Completed on	Results expire in	Overshared items
Data risk assessment JB	Completed	Jan 28, 2026	Jan 30, 2026	24 days	0

DSPM (preview) standaard rapport



DSPM (preview) inzicht per regel

Classificatie

/teams/ambachtelijkvliegendekoekjes/

Overview Identify Protect Monitor

Data source details

Data source type: SharePoint
URL: https://officecontent.sharepoint.com/teams/ambachtelijkvliegendekoekjes/

Data coverage

Total items in site: 73
View site

Labeled: 41
Not labeled: 32

Legend: No Sensitive Information Types Detected (green), Sensitive Information Types Detected (yellow), Data Not Scanned (orange)

Via Azure subscriptie

/teams/ambachtelijkvliegendekoekjes/

Overview Identify Protect Monitor

Scan your data

Scans your data for sensitive information in this data source

Items scanned: 73
Not scanned: 0

Scan all items for sensitive information
Purview Information Protection

/teams/ambachtelijkvliegendekoekjes/

Overview Identify Protect Monitor

Limit Microsoft 365 Copilot and agents access to this site

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

Restrict access by label (Microsoft Purview Data Loss Prevention)
Restrict all items (SharePoint Restricted Content Discovery)

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

Steps at a glance

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

Other labeling policies

Default sensitivity label for SharePoint document library

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

Create default sensitivity label for SharePoint document library (Microsoft SharePoint location)

SAM

Alternatief voor het label "Niet voor Copilot"

/teams/ambachtelijkvliegendekoekjes/

Overview Identify Protect Monitor

Run a site access review

Anonymous links accessed (monthly): 0
Guest access (monthly): 0

SharePoint site access review lets IT administrators delegate the process of reviewing data access to site owners of overshared sites.

Start a SharePoint site access review (SharePoint Admin Portal)

Run an access review (Microsoft Entra)

Note: You need IT administrator permissions in Microsoft Entra to set up and run access reviews.

Monitoring

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
- Gedragsmetingen
- Test phishing mails

Verandermanagement (menskant)



Optimale informatie inrichting

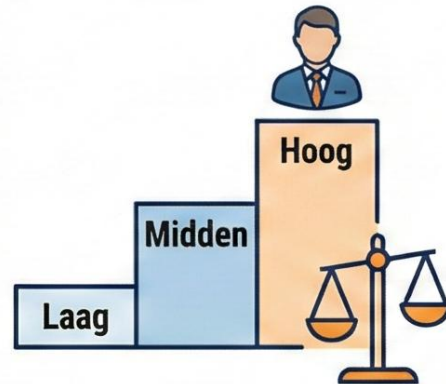


AI-Geletterdheid: Geen Optie, Maar Plicht

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.



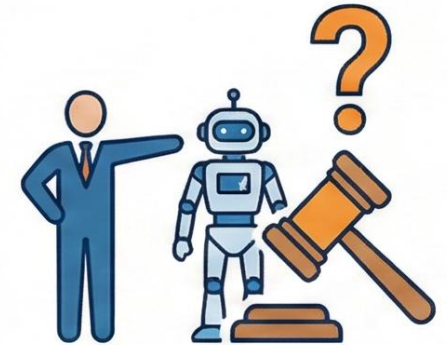
Veilig



Ethisch



Robuust



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



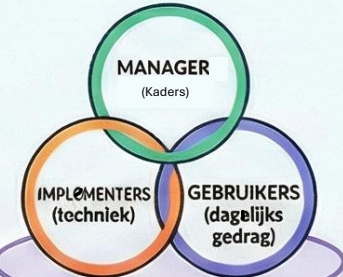
De Gouden Vuistregel voor Data

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 highest YoY growth among automakers, rising 82pc to 1,086 units in October, led by robust demand for Tucson and Elant models. MoM sales, however, fell eight

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?

SBP market

KARACHI: Ameer Ahmed Khan to tackle challenges, saying he highlighted key driver of... Mr Ahmed gural Intern hosted by the

IMVs jumped 58pc to 787 units. IMC's sales stood at 14,418 units, up 66pc YoY.

ported the highest YoY growth among automakers, rising 82pc in October, led by Tucson and Elanta models. MoM sales, however, fell eight

est 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?

KARACHI: Ameer Ahmed Khan to tackle challenges, saying he highlighted key driver of... Mr Ahmed gural Intern hosted by the

Vragen

