



Extending Power BI governance with Microsoft Purview

Erwin de Kreuk

Principal Consultant – Data & AI
InSpark



@ErwinDeKreuk



[linkedin.com/in/ErwinDeKreuk](https://www.linkedin.com/in/ErwinDeKreuk)



[ErwinDeKreuk.com](https://www.ErwinDeKreuk.com)





Marc Lelijveld

Solution Architect – Data & Analytics
Macaw Netherlands



@MarcLelijveld



linkedin.com/in/MarcLelijveld



Data-Marc.com



Data-Marc



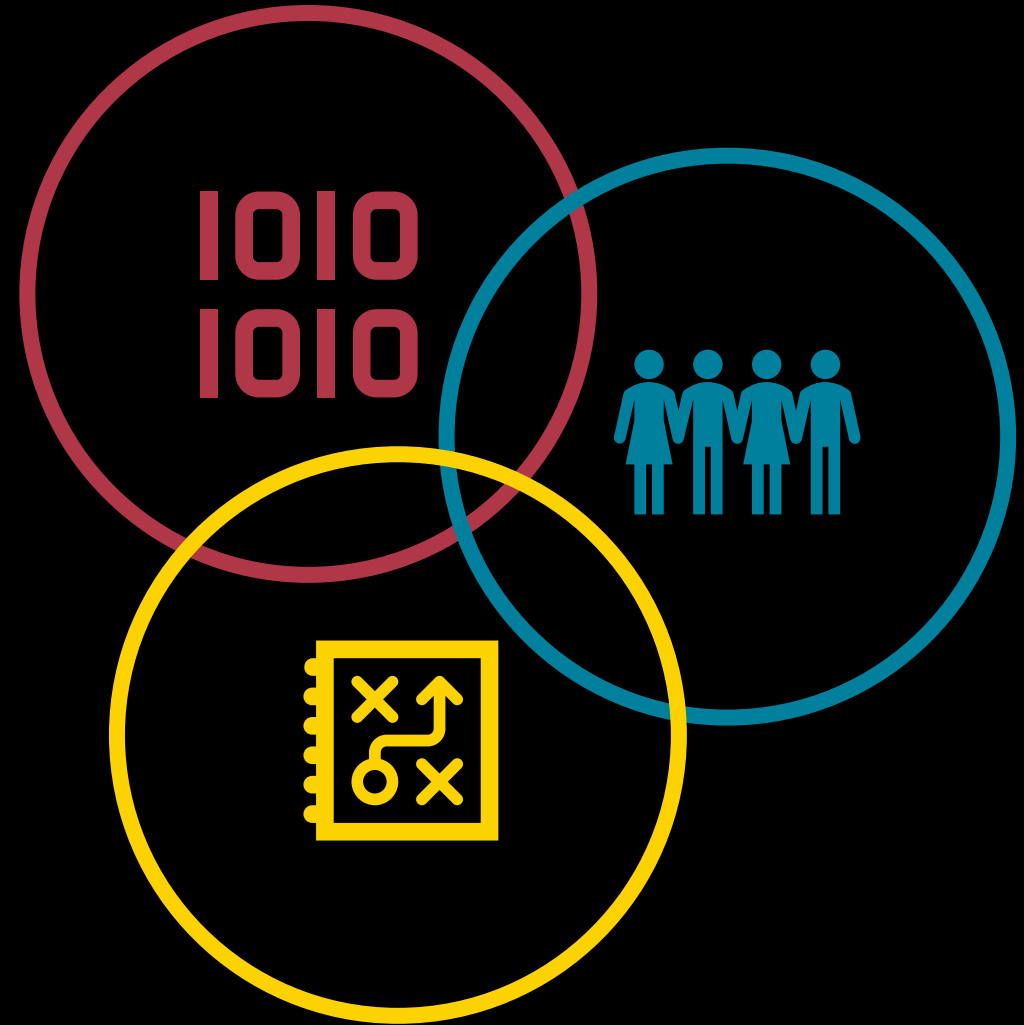
Objectives of today

- What do we understand as Governance
- Governance in Power BI
 - Data classification
 - Sensitivity labels
 - Endorsement
- What is Microsoft Purview
- Magic uncovered
- Strategy
- Findings & experiences



Combination of three components

- Data
- Analytics
- People



[data + analytics + people]

[data + analytics + people]

- Cloud
- On-prem
- Hybrid

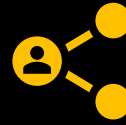


[data + analytics + people]



Discover

Search for data and combine different sources to one model



Share

Share insights and analytics across the organization



Analyze

Analyze tons of data in a few clicks and let it add value



Find & Explore

Find answers and explore data in visuals + Q&A capabilities



Visualize

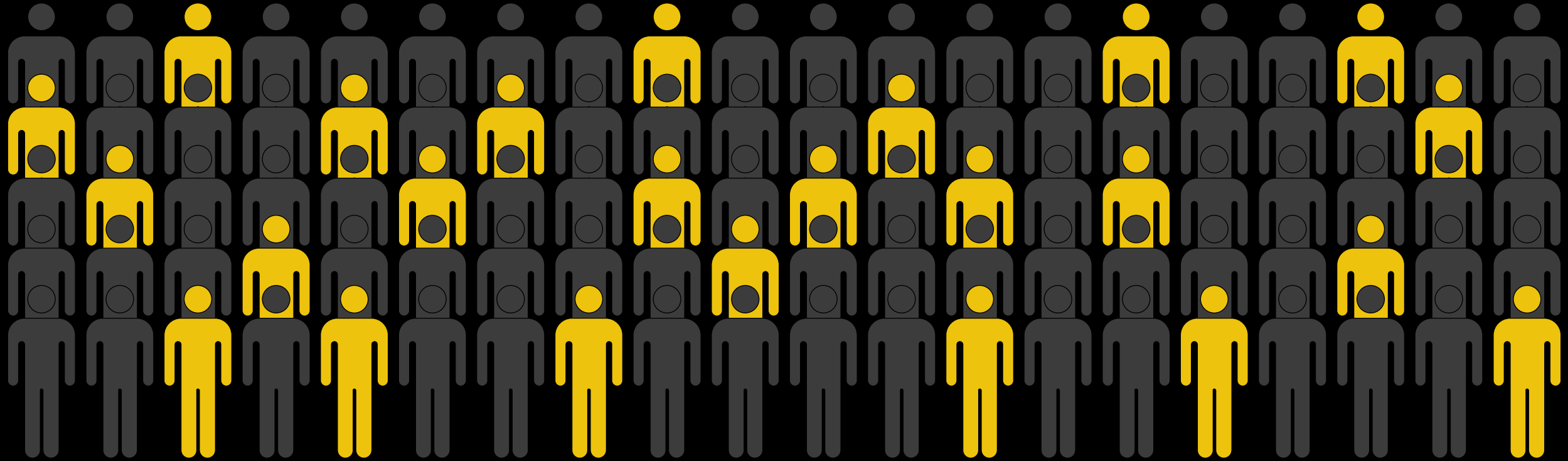
Transform millions of rows of data in stunning visuals



Anywhere

Your data on your fingertips on any device wherever you are.

[data + analytics + people]



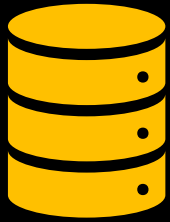
[data + analytics + people]

= competitive advantage

Data driven ambition



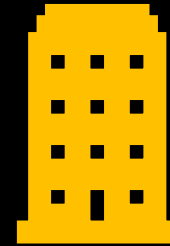
Open ends



Where does the data
come from?



How reliable is the
data?

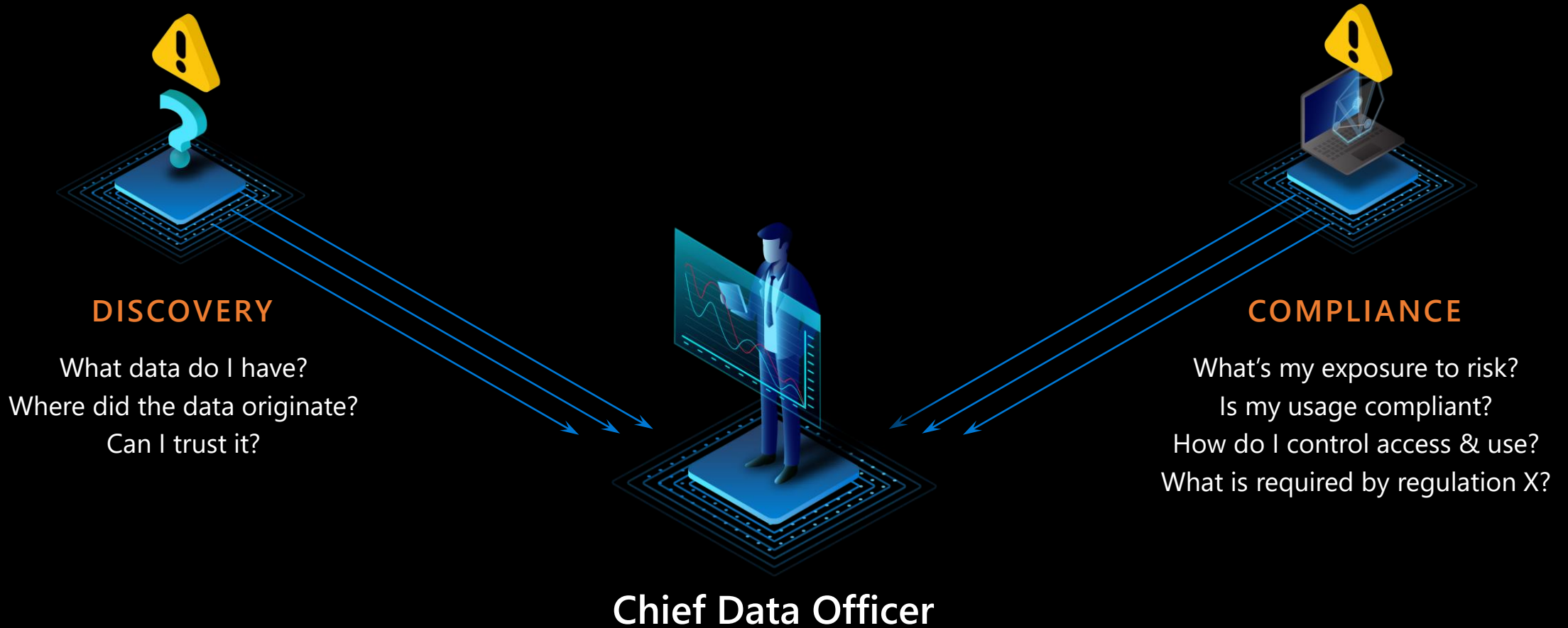


What do I already have
available?

Understanding of governance



Data governance is becoming increasingly interdisciplinary



Challenges for Data Consumers

- There's no central location to register data sources
- Data-consumption experiences require users to know the connection string or path.
- Data sources and documentation might live in several places
- There's no explicit connection between the data and the experts that understand the data's context.

Challenges for Data Producers

- Annotating data sources with descriptive metadata is often a lost effort. Client applications typically ignore descriptions that are stored in the data source.
- Creating documentation for data sources can be difficult and it's an ongoing responsibility to keep documentation in sync with data sources. Users might not trust documentation that's perceived as being out of date.
- Creating and maintaining documentation for data sources is complex and time-consuming.
- Restricting access to data sources and ensuring that data consumers know how to request access is an ongoing challenge.

Challenges for security administrators

- Everything just mentioned and:
- An organization's data is constantly growing and being stored and shared in new directions. The task of discovering, protecting, and governing sensitive data is one that never ends.
- How to ensure that the organization's content is being shared with the correct people, applications, and with the correct permissions.
- Understanding the risk levels in an organization's data requires diving deep into the content, looking for keywords, RegEx patterns, and sensitive data types.
- Constantly monitor all data sources for sensitive content, as even the smallest amount of data loss can be critical to your organization.
- Ensuring that an organization continues to comply with corporate security policies is a challenging task as the content grows and changes.

Governance in Power BI



Our scope for Power BI governance today

- Cataloguing of Power BI artifacts
- Ownership / contact information
- Data classification
- Content endorsement



Endorsement

Helps with:







- Reuse of content
 - Certified datasets
 - Promoted datasets
- Indicates a certain quality of the solution
- Works for dataflows, datasets, reports, dashboard and apps
- Makes datasets discoverable

Requires:

- Mail enabled security group, who can grant certified stamp
- Mail enabled security group, who can make datasets discoverable
- Process around certification

Select a dataset to create a report

All datasets

| Name | ENDORSEMENT ↓ | Owner | Workspace/App | Refreshed |
|------------------------|---|--------------|---------------|-------------|
| Retail Analysis |  Certified | Steve Myer | Retail | 4 days ago |
| Customer Profitability |  Certified | Susan Mailer | Customer | 6/23/17 |
| Ventage Global |  Promoted | Lane Barnes | Ventage | 3/3/18 |
| IT Spend Analytics |  Promoted | Ari Gold | IT | 3 hours ago |
| Team Analytics |  Promoted | Ana Smith | Analytics | 7/12/18 |
| Opportunity Analysis |  Promoted | Lane Barnes | My Workspace | 6/12/17 |
| Retail | | Lane Barnes | My Workspace | 2 days ago |
| Procurement Analysis | | Lane Barnes | My Workspace | 7/22/18 |
| Sales | | Lane Barnes | My Workspace | 1/24/17 |

OK Cancel



CERTIFIED



PROMOTED

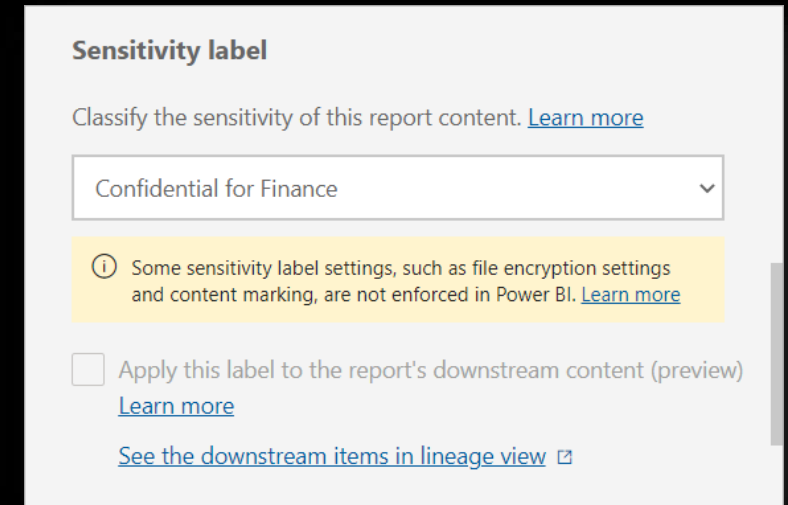
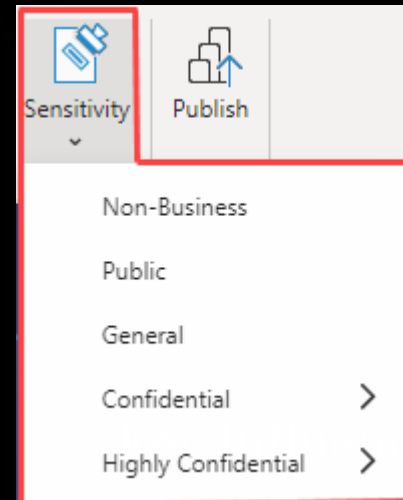
Sensitivity labeling in Power BI

Helps with:

- Data classification on type of data (like compliance of data etcetera)
- Have an idea of the sensitivity of the data (e.g., GDPR compliancy)
- Give an impression on where the data can be used / shared according to assigned policies and labels.
- Has policies assigned to which extend the content can be used.

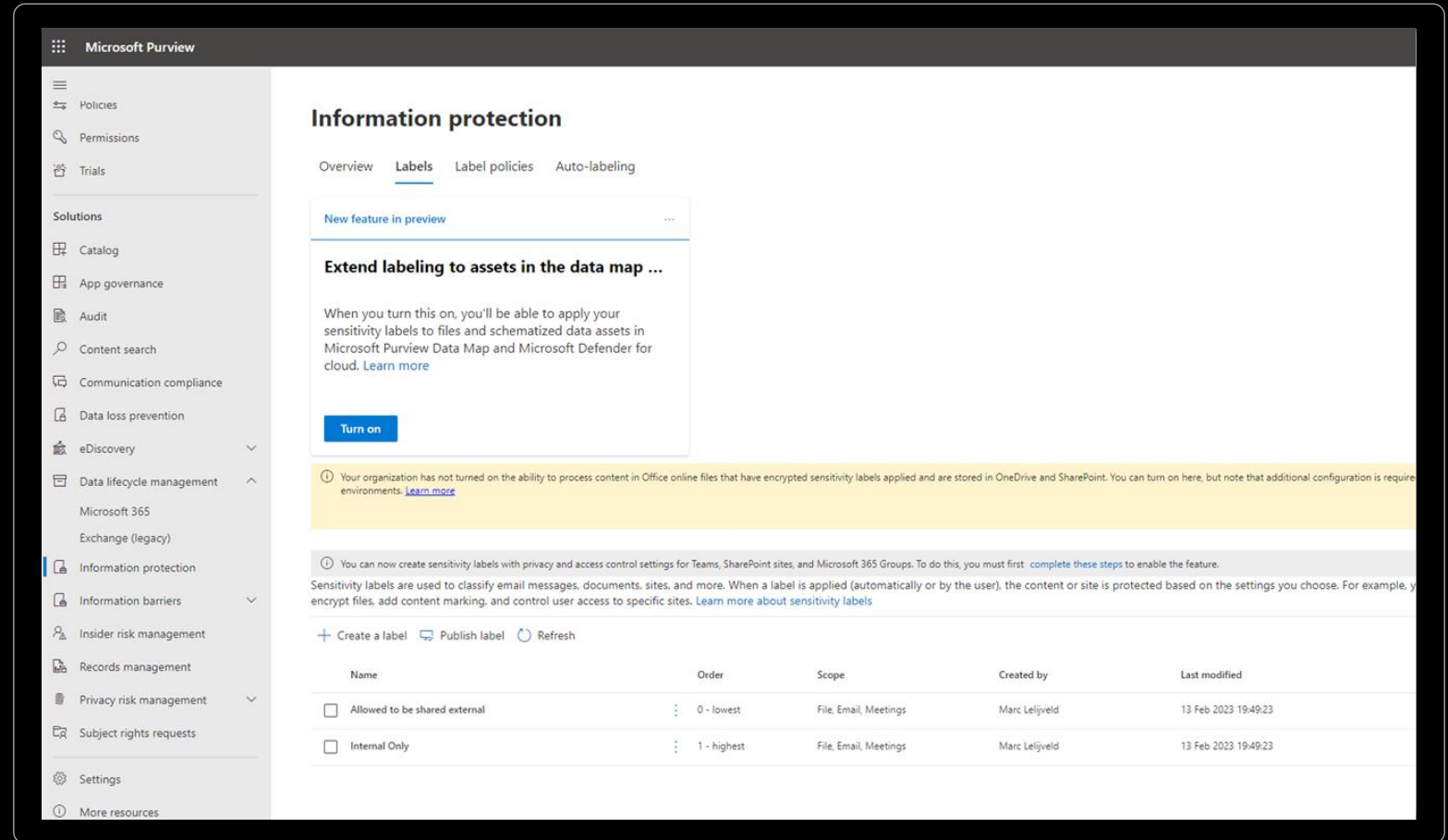
Requires:

- Right licensing (security and compliance as part of E5)
- Policies to be setup
- (Potentially) force labeling of all content through tenant configuration



Setting up sensitivity labels

- Navigate to the compliance & security center, recently rebranded to Microsoft Purview.
- This center is only accessible for compliance admins. Power BI Service admin permissions will not suffice.

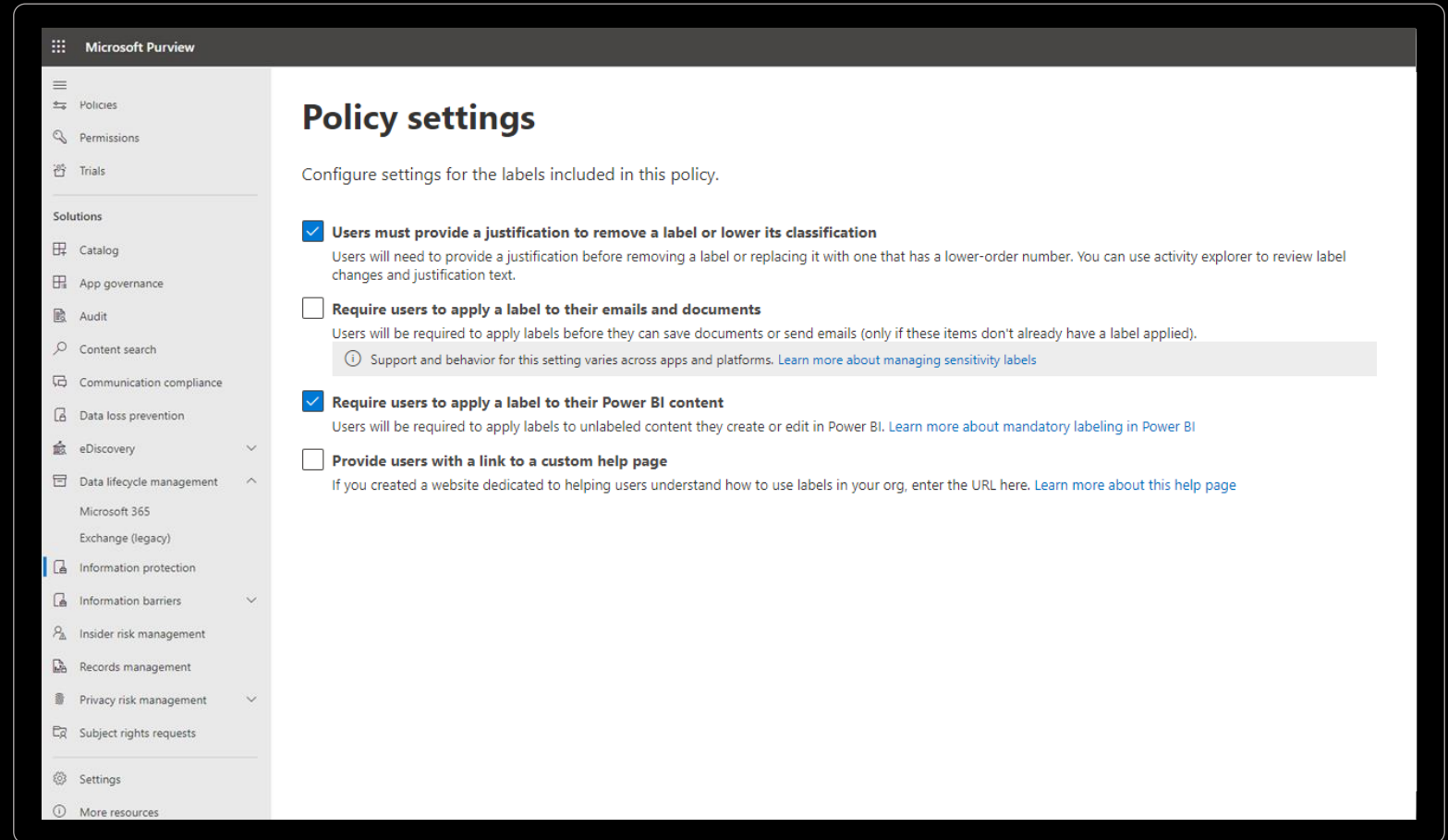


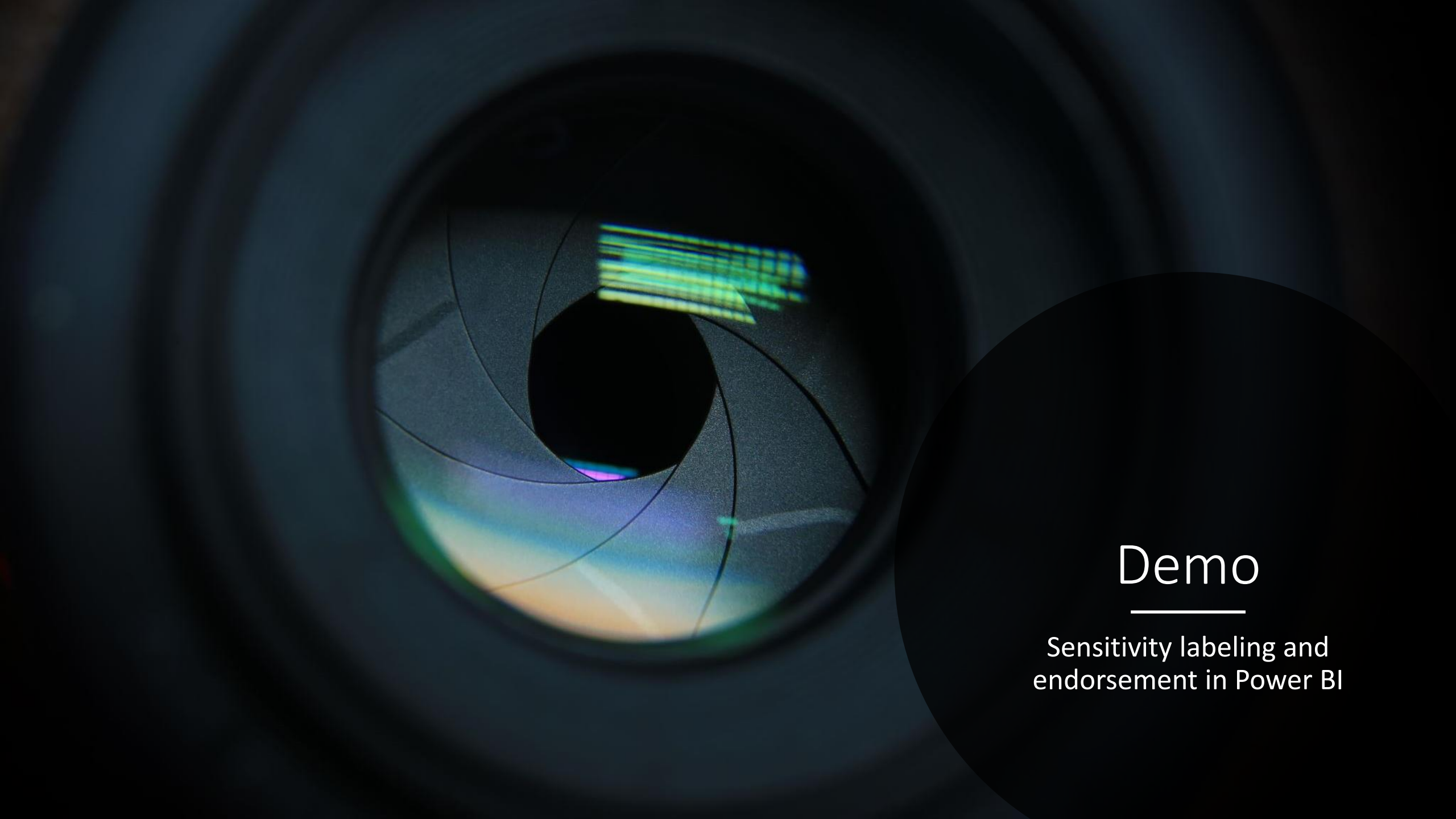
The screenshot displays the Microsoft Purview Information protection interface. The left sidebar contains a navigation menu with categories: Policies, Permissions, Trials, Solutions (Catalog, App governance, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery, Data lifecycle management, Microsoft 365, Exchange (legacy)), Information protection (selected), Information barriers, Insider risk management, Records management, Privacy risk management, Subject rights requests, Settings, and More resources. The main content area is titled 'Information protection' and has tabs for Overview, Labels (active), Label policies, and Auto-labeling. A 'New feature in preview' banner highlights the 'Extend labeling to assets in the data map ...' feature, which allows applying sensitivity labels to files and schematized data assets in Microsoft Purview Data Map and Microsoft Defender for cloud. A 'Turn on' button is present. Below this, a yellow warning message states: 'Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn on here, but note that additional configuration is required. [Learn more](#)'. A grey informational message follows: 'You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first [complete these steps](#) to enable the feature. Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)'. At the bottom, there are links for '+ Create a label', 'Publish label', and 'Refresh'. A table lists existing labels:

| Name | Order | Scope | Created by | Last modified |
|--|-------------|-----------------------|----------------|----------------------|
| <input type="checkbox"/> Allowed to be shared external | 0 - lowest | File, Email, Meetings | Marc Lelijveld | 13 Feb 2023 19:49:23 |
| <input type="checkbox"/> Internal Only | 1 - highest | File, Email, Meetings | Marc Lelijveld | 13 Feb 2023 19:49:23 |

Create policies

- After creating a label, you must set policies to labels.
- Labels can be setup for all Microsoft 365 content, as well as Power BI specific.
- Label enforcement can be configured for all Power BI content.





Demo

Sensitivity labeling and
endorsement in Power BI

Overview of Purview



History



• Microsoft Purview april 2022



• Azure Purview sept 2021



• ADC Gen 2



• BlueTalon Acquisition june 2019



• ADC Gen 1

Azure Purview is now Microsoft Purview

Microsoft Purview brings together trusted products for governance and compliance under one umbrella so it's easier to manage all of your data.

Microsoft Purview

The future of compliance and data governance

Risk & compliance

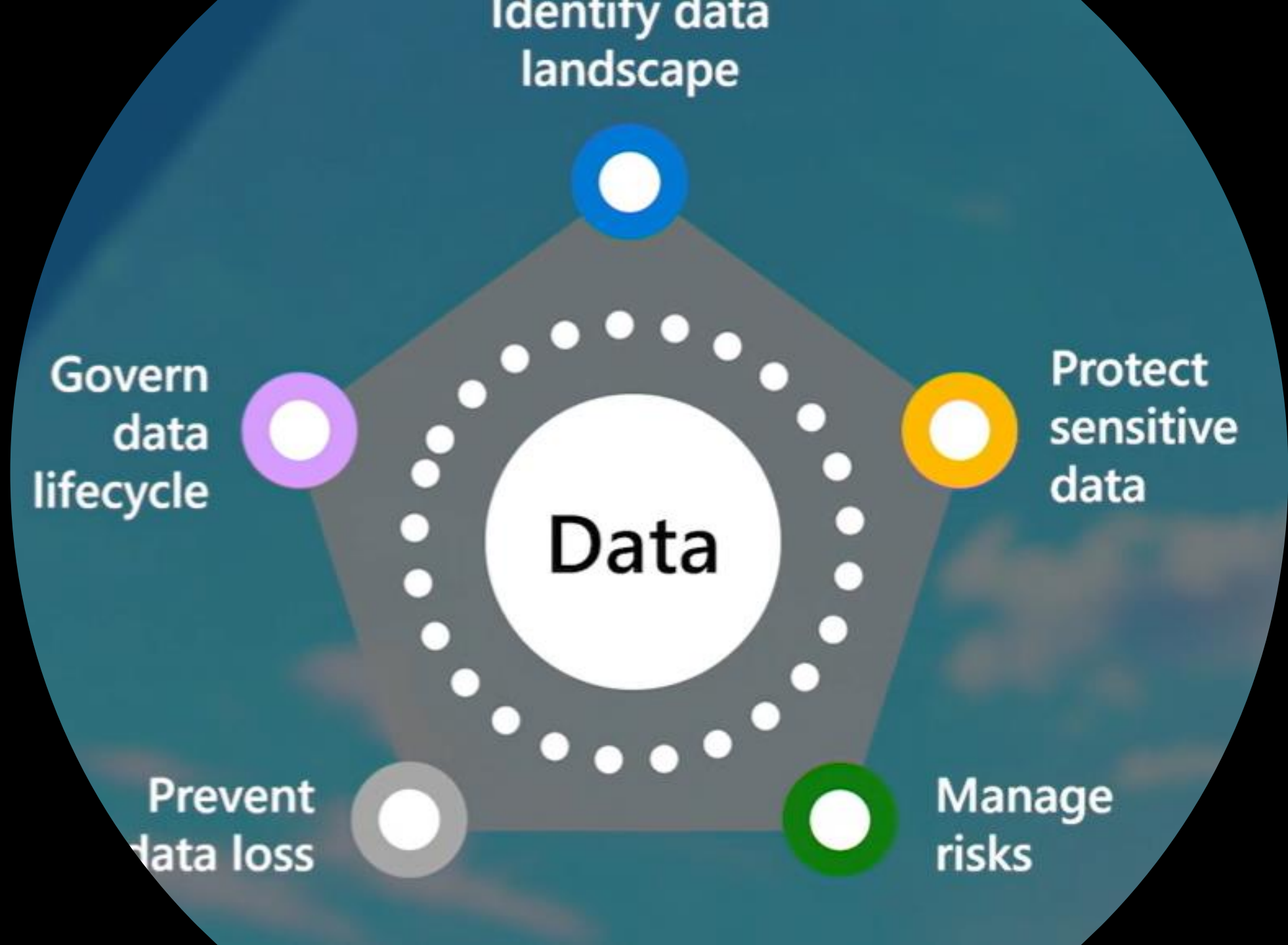
For risk, compliance, and legal teams

| Former Name | New Name |
|--|--|
| Microsoft 365 Advanced Audit | Microsoft Purview Audit (Premium) |
| Microsoft 365 Basic Audit | Microsoft Purview Audit (Standard) |
| Microsoft 365 Communication Compliance | Microsoft Purview Communication Compliance |
| Microsoft Compliance Manager | Microsoft Purview Compliance Manager |

Microsoft Purview

Unified data governance

For data consumers, data engineers, data officers

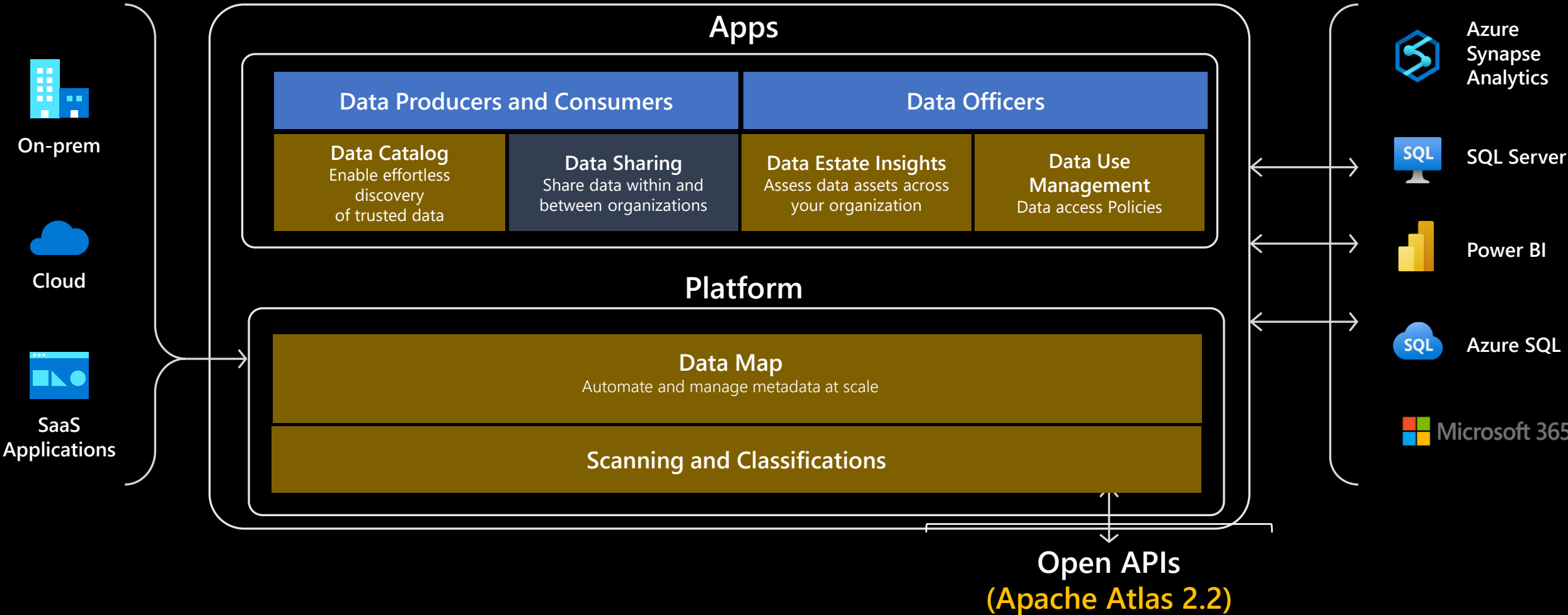


Generally Available

Preview

Microsoft Purview

Unified Data Governance



Microsoft Purview Overview

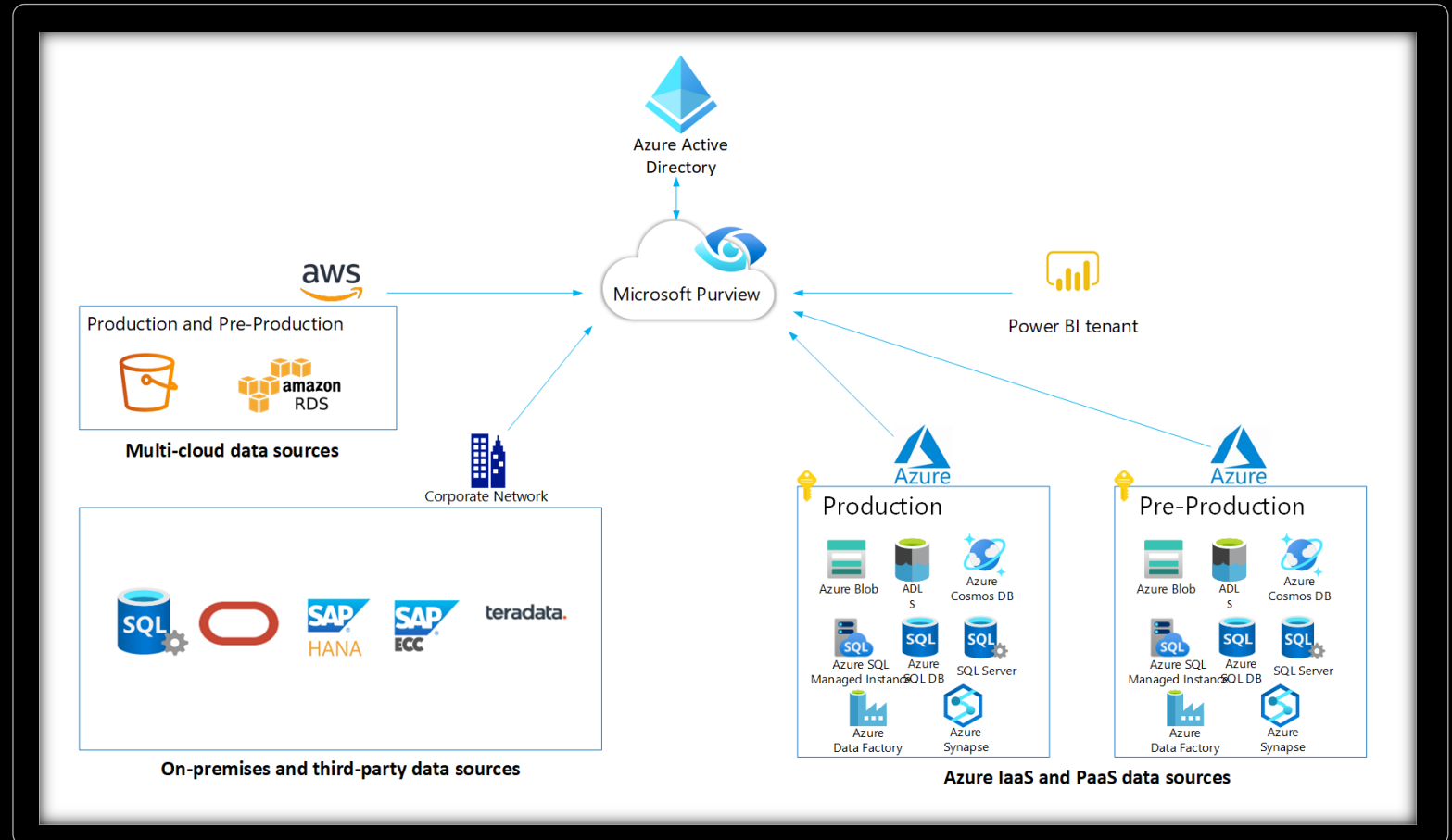
Power BI

Azure IaaS and PaaS Data sources

AWS

On-Premise data sources

Third-Party datasource



Connect Power BI To Microsoft Purview



Same Tenant



Cross Tenant

Scan Power BI

Admin Portal

- Allow Service Principal
- Detailed Metadata
- Dax and Mashup Expressions

Enhance admin APIs responses with DAX and mashup expressions

Enabled for the entire organization

Users and service principals eligible to call Power BI admin APIs will get detailed metadata about queries and expressions comprising Power BI items. For example, responses from GetScanResult API will contain DAX and mashup expressions. [Learn more](#)

Note: For this setting to apply to service principals, make sure the tenant setting allowing service principals to use read-only admin APIs is enabled. [Learn more](#)

☒ Enabled

Apply to:

☒ The entire organization

☐ Specific security groups

☐ Except specific security groups

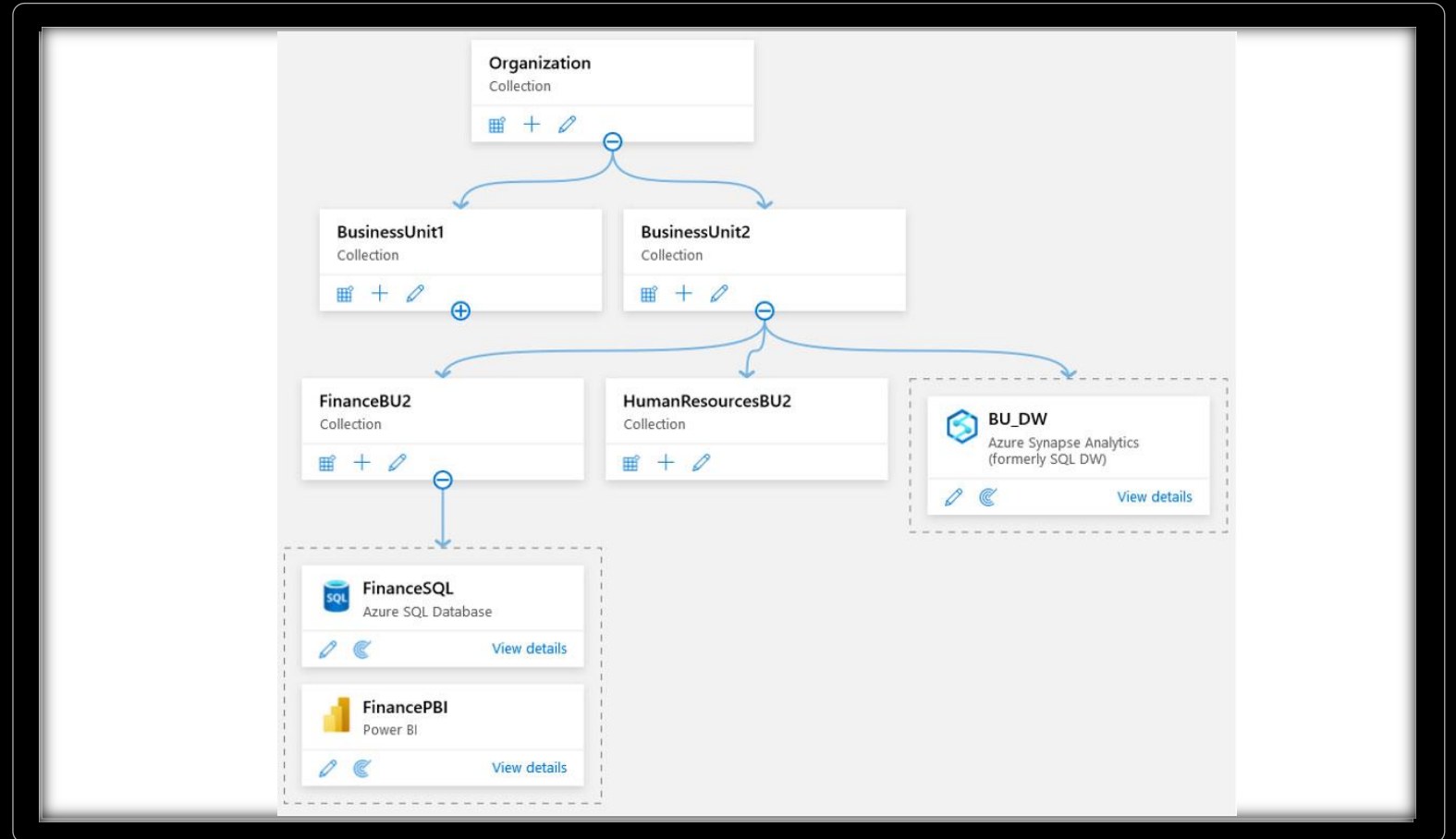
Scan Power BI

Admin Portal

- Allow Service Principal
- Detailed Metadata
- Dax and Mashup Expressions

Register Power BI as a Source

- Tenant ID
- Collections



Scan Power BI

Admin Portal

- Allow Service Principal
- Detailed Metadata
- Dax and Mashup Expressions

Register Power BI as a Source

- Tenant ID
- Collections

Setup Scan

- Personal Workspace (in- / excluded)

Set a scan trigger

Set a scan trigger to run the scan at specific dates and times. If once, the scan will start after set up is completed. If recurring, the scan will start at a date and time you choose. The initial scan is a full scan and every subsequent scan is incremental.

☒ Recurring ☐ Once

Time zone * ⓘ

(UTC) Coordinated Universal Time

Recurrence *

Every 1 Month(s)

☒ Month days ☐ Week days

Select day of the month to scan

| | | | | | | |
|----|----|----|------|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | Last | | | |

Schedule scan time (UTC)

h:mm:ss AM

Supported capabilities

- | | | | |
|---|-----------------------|---|---|
| ✓ | • Metadata Extraction | → | • Workspaces |
| ✓ | • Full Scan | | • Dashboards |
| ✓ | • Incremental Scan | | • Reports |
| ✓ | • Lineage | | • Datasets including tables and columns |
| ✗ | • Scoped Scan | | • Dataflows |
| ✗ | • Classification | | • Datamarts |
| ✗ | • Access Policy | | |
| ✗ | • Data Sharing | | |

Supported Scenarios (security wise)



public access allowed



public access allowed



public access allowed/**Denied**



public access allowed/**Denied**

- Disabled from all networks
Public network access will be disabled for Purview account, portal, and ingestion.

- ▶ Azure Private Link
Enabled for the entire organization
- ▶ Block Public Internet Access
Enabled for the entire organization

Scan Power BI Cross-Tenant

Setup Scan

- Create Credential
- Connect via SHIR
- Add Credential

Scan "LS_POWERBI_DATA-MARC"

Name *

Personal workspaces *

☐ Include ☒ Exclude

i Changes to the scan configuration will reset the upcoming scan to be a full scan for this data source. [Learn more](#) ×

Connect via integration runtime * *i*

Credential *

Select a collection

i All assets scanned will be included in the collection you select.

Observations

- When scanning **without** SHIR, user account with PBI Service Admin permissions + App Registration is required.
- Scanning **with** SHIR an App Registration will suffice.



- Demo Microsoft Purview

Magic
uncovered?




Scanner API

Set of 4 APIs to get all Admin Insights

- | | |
|---------------------------|-------------------------------------|
| • GET Modified Workspaces | To list all workspaces with changes |
| • POST Workspace Info | To start a scan |
| • GET Scan Status | To start polling till scan is ready |
| • GET Scan Results | To get the results of the scan |

HTTP

 Copy

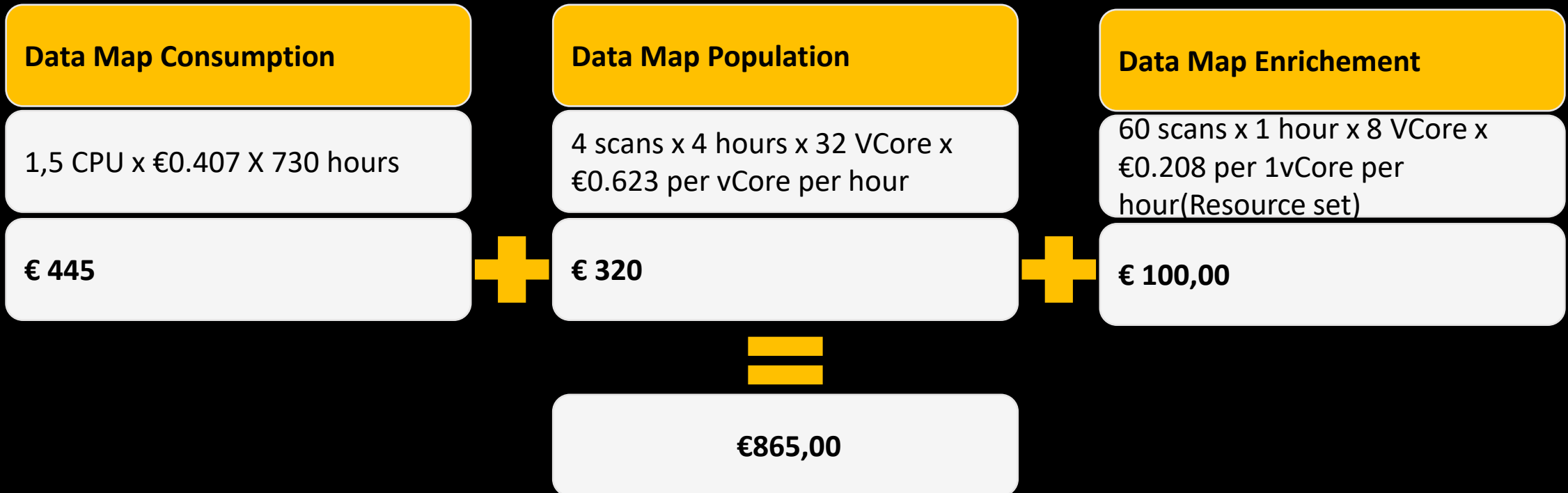
 Try It

```
GET https://api.powerbi.com/v1.0/myorg/admin/workspaces/modified
```

Cost

- Purview cost
 - Incremental scans
 - Full scans
- Creating your own solution
 - Development effort

Pricing - Example



Findings and experiences



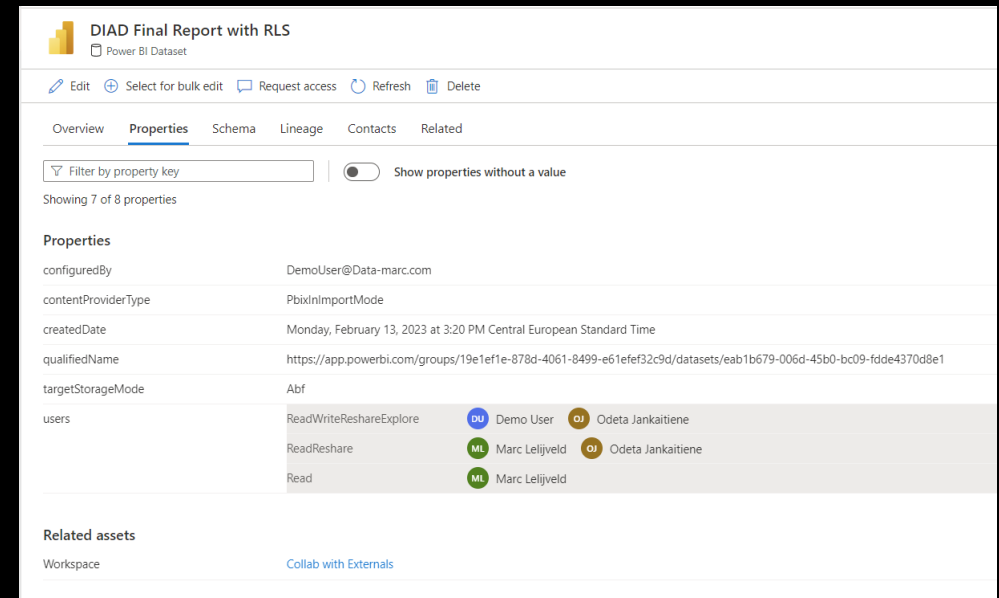
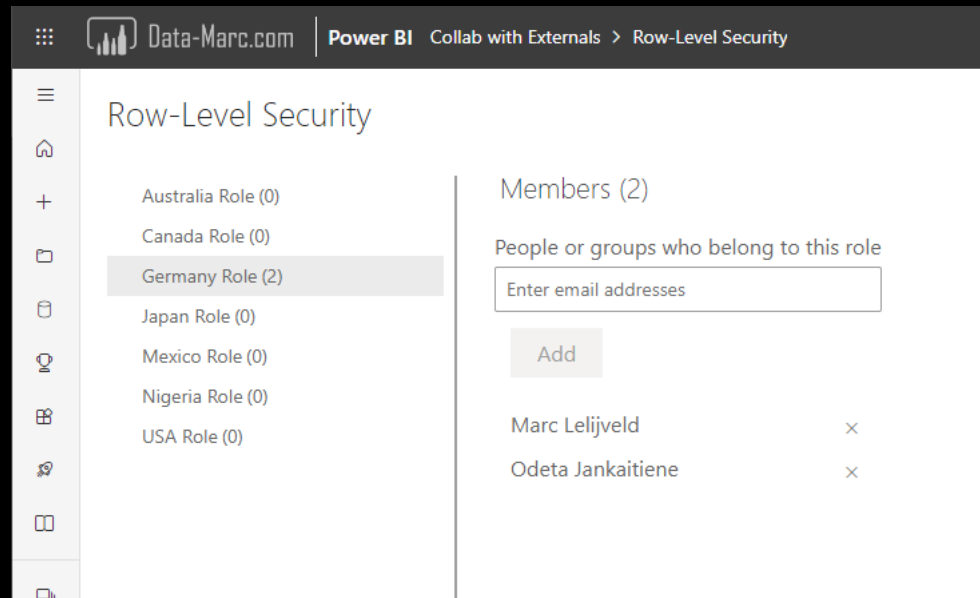
Endorsement

- None / Promoted / Certified
- Purview has its own version of certified for non-Power BI artifacts.
- Power BI artifacts cannot be endorsed within Purview
- Policies in Power BI tenant settings define who can certify.



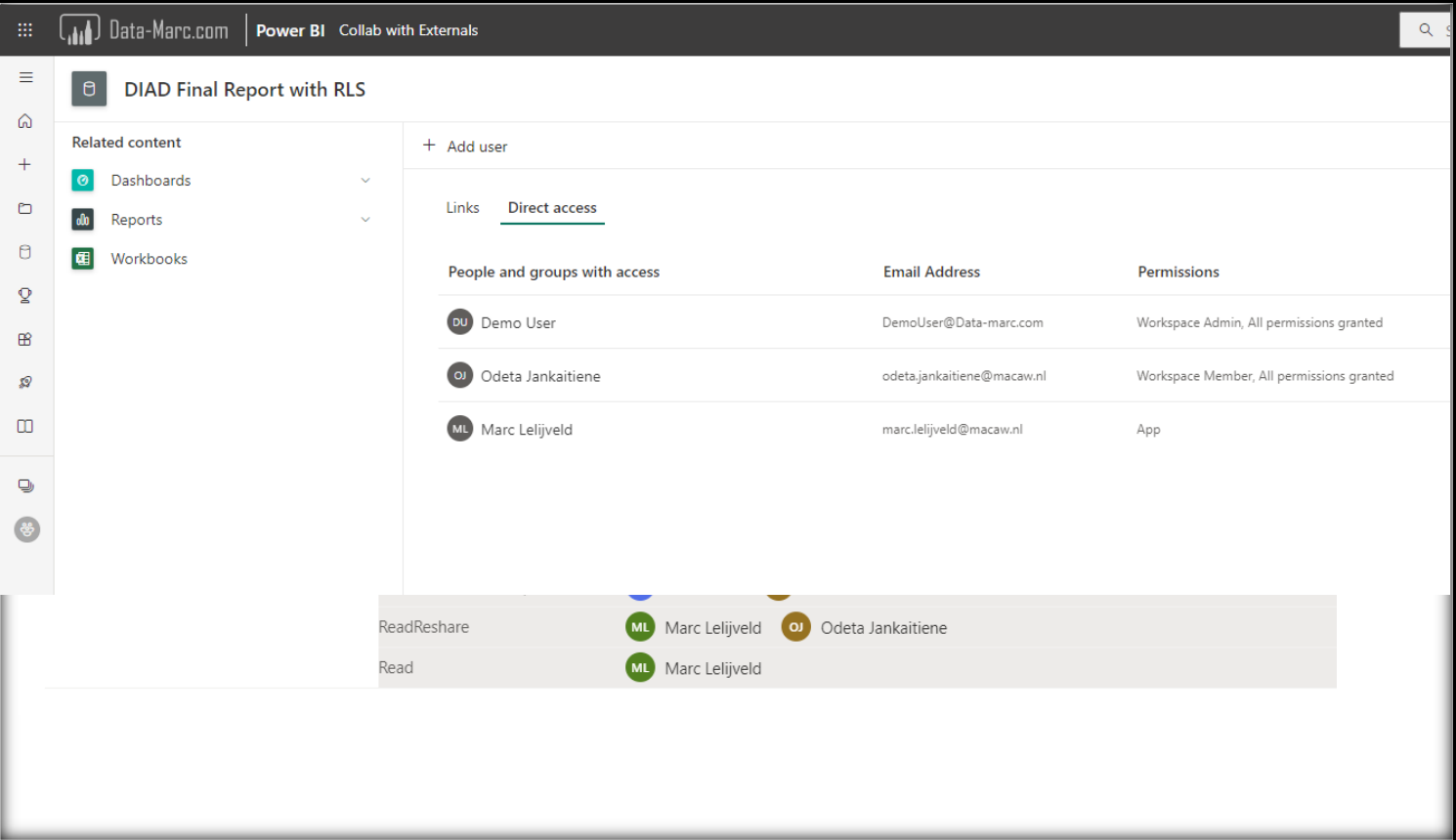
Power BI dataset security

- Roles (RLS/OLS) are not visible within Purview.



Some unclear aspects

Ownership and permissions on dataset cannot be matched with what we see in Power BI.



The screenshot shows the Power BI interface for a workspace named "DIAD Final Report with RLS". The left sidebar lists "Related content" with categories: Dashboards, Reports, and Workbooks. The main area displays the "Direct access" link settings. A table lists the users with access:

| People and groups with access | Email Address | Permissions |
|-------------------------------|----------------------------|---|
| DU Demo User | DemoUser@Data-marc.com | Workspace Admin, All permissions granted |
| OJ Odeta Jankaitiene | odeta.jankaitiene@macaw.nl | Workspace Member, All permissions granted |
| ML Marc Lelijveld | marc.lelijveld@macaw.nl | App |

Below the table, a list of permissions is shown:

- ReadReshare: ML Marc Lelijveld, OJ Odeta Jankaitiene
- Read: ML Marc Lelijveld

Some unclear aspects

Contact information from Power BI reports and solutions is not shared to Purview.

Edit "Power BI Wide World Importers"

[Overview](#) [Schema](#) [Lineage](#) [Contacts](#)

Select contacts to add to this asset.

Experts

Experts are often business process or subject matter experts in different business areas or departments.

Select user or group

Owners

Owners are often senior executives or business area owners that define governance or business processes over certain data areas.

Select user or group

Impact on Power BI

- Purview gives a glossary of Power BI artifacts
- Might decrease duplication of solutions
- Most valuable when enriched with
 - Sensitivity Labels (requires E5)
 - Endorsement
 - Additional information like contact information
- Purview primarily focusses on meta data – leaves out usage & adoption aspects.

Any questions left?



Thank you for attending!



Marc Lelijveld

Solution Architect – Data & Analytics
Macaw Netherlands



@MarcLelijveld



linkedin.com/in/MarcLelijveld



Data-Marc.com



Data-Marc



Erwin de Kreuk

Principal Consultant – Data & AI
InSpark



@ErwinDeKreuk



linkedin.com/in/ErwinDeKreuk



ErwinDeKreuk.com

