Protect, Discover & Understand data with Microsoft Fabric & Microsoft Purview

Let’s connect

@erwindekreuk.bsky.social

linkedin.com/in/erwindekreuk

erwindekreuk.com

github.com/edkreuk

https://sessionize.com/erwin-de-kreuk/

Dutchfabricusergroup.com

Microsoft® Most Valuable Professional



Let’s connect

https://www.linkedin.com/in/marco-oesterlin/

https://medium.com/@marcoOesterlin

https://github.com/MarcoOesterlin

https://sessionize.com/marco-osterlin/

Microsoft® MVP Most Valuable Professional



Premium sponsors

VENZO_

INSPARI

valantic companies

itm8®

Eddytor™

dataon

Power your data

Standard sponsors

Backstage

Columbus

TheVIT

DATA - ANALYTICS - AI

twoday

Raffle Prizes

EUROPEAN MICROSOFT FABRIC Community Conference










AI is transforming the world


Data is the fuel
that *powers* AI

Today's data realities

What data do I have?

Is it trustworthy?

Can people access the data needed to make the right decisions?

How can I enable faster business insights?

What's my compliance exposure?



Problem statement

Modern organizations generate valuable insights from data, but lack the oversight needed to ensure that data is trustworthy, secure, and compliant at scale.

Without integrated governance and security across the analytics lifecycle, data-driven decisions become risky, compliance exposure increases and AI innovation cannot be safely accelerated.

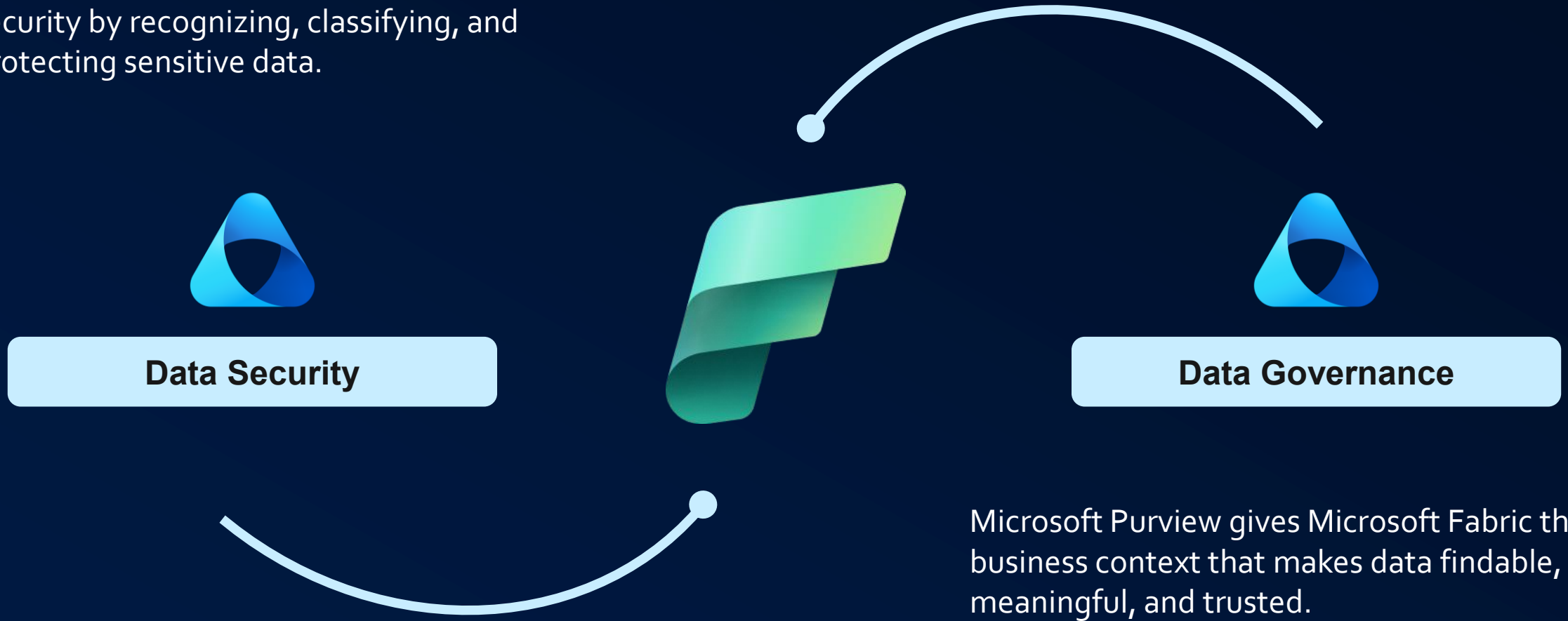
Agenda



- Intro: why trust matters
- Security foundations in Fabric
- Microsoft Purview Overview
- Purview & Fabric in Action

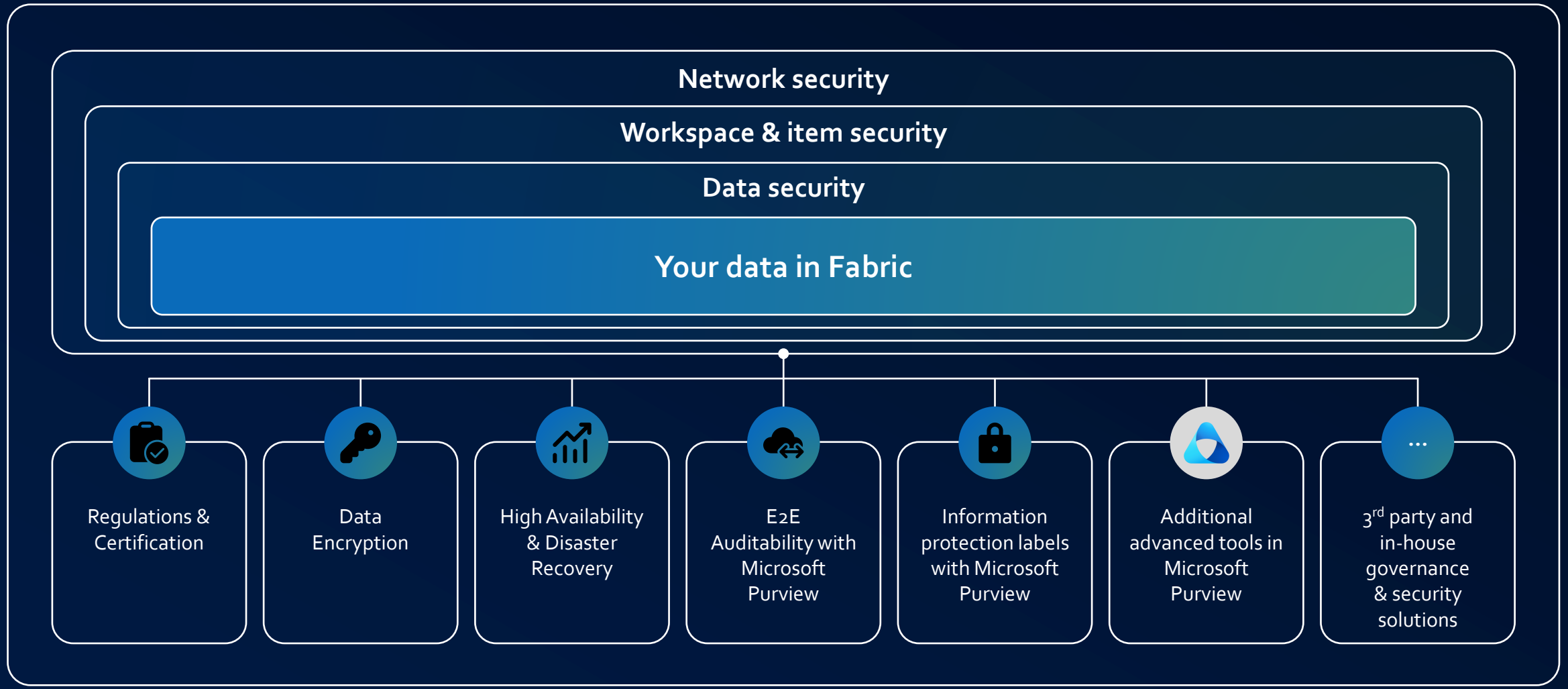
Microsoft Fabric & Microsoft Purview better together

Microsoft Purview strengthens Microsoft Fabric's security by recognizing, classifying, and protecting sensitive data.



Microsoft Purview gives Microsoft Fabric the business context that makes data findable, meaningful, and trusted.

Security layers in Microsoft Fabric



Building trust in your Data Platform



Data Governance and Stewardship

- Data Ownership
- Access Control
- Audit Trails
- Data Catalog



Data Quality Rules

- Accuracy
- Completeness
- Consistency
- Timeliness
- Uniqueness



Data Integration and Transformation Rules

- ETL/ELT
- Validation
- Schema Evolution
- Data Lineage



Monitoring and Alerting

- Data Quality Dashboards
- Anomaly Detection
- Automated Alerts



Policy and Compliance Rules

- Data Retention Policies
- Privacy Compliance
- Data Classification

Microsoft **Purview**

Integrated solutions to secure & govern the world's data

Data **Security**

Secure data across its lifecycle, wherever it lives

Data Loss Prevention
Insider Risk Management
Information Protection

Data Governance

Confidently activate your data & accelerate time to insights

Unified Catalog

Data Discovery
Curation
Data Quality
Data Health
Master Data Management[1]

Data Compliance

Manage critical risks and regulatory requirements

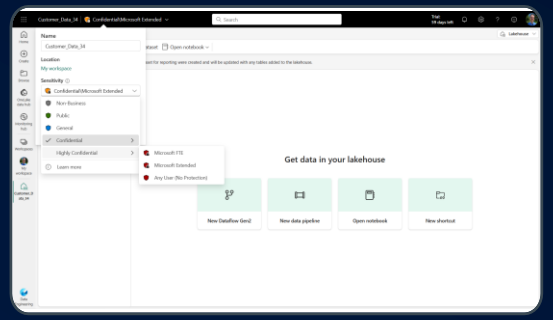
Compliance Manager
eDiscovery and Audit
Communication Compliance
Data Lifecycle Management
Records Management

Unstructured & Structured data | Traditional and AI generated data | Microsoft and Multi-cloud

Shared platform capabilities

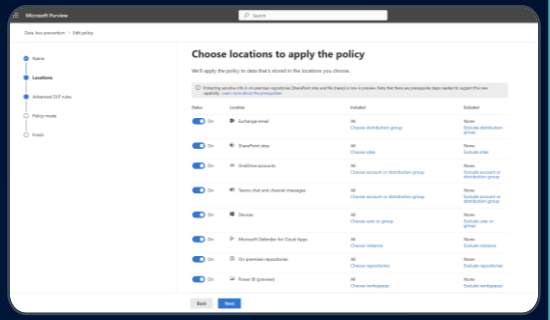
AI-based efficiency, Data Map, Classification, Labels, Audit Logs, Policies, Data Connectors

Microsoft Purview Data Security & Compliance integration with Fabric



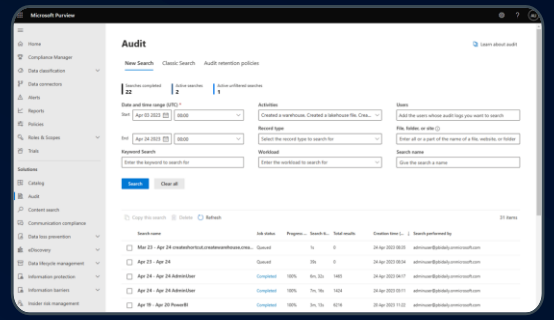
Information protection sensitivity labels and protection policies

Classify sensitive Fabric data using the same sensitivity labels that are used in Microsoft 365—the label and protection travels with the data within Fabric, and enforced even when the data is exported to Office.



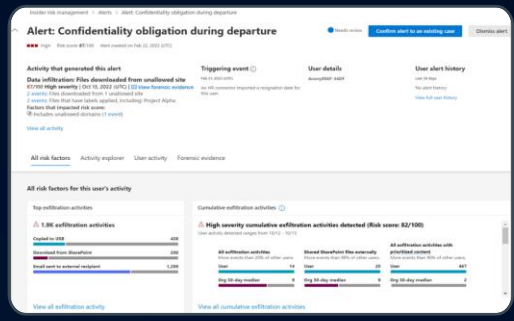
Data loss prevention policies

Automatically detect sensitive data such as PII or SSN in Lakehouse or Semantic Models and trigger automatic risk remediation actions such as alerts or restrict access.



Audit

Log user activities from Microsoft Fabric in MS Purview Audit to support security, forensic, and internal investigations.



Insider Risk Management

Ingest audit logs from Fabric in addition to other millions of signals to identify potential malicious or inadvertent insider risk.

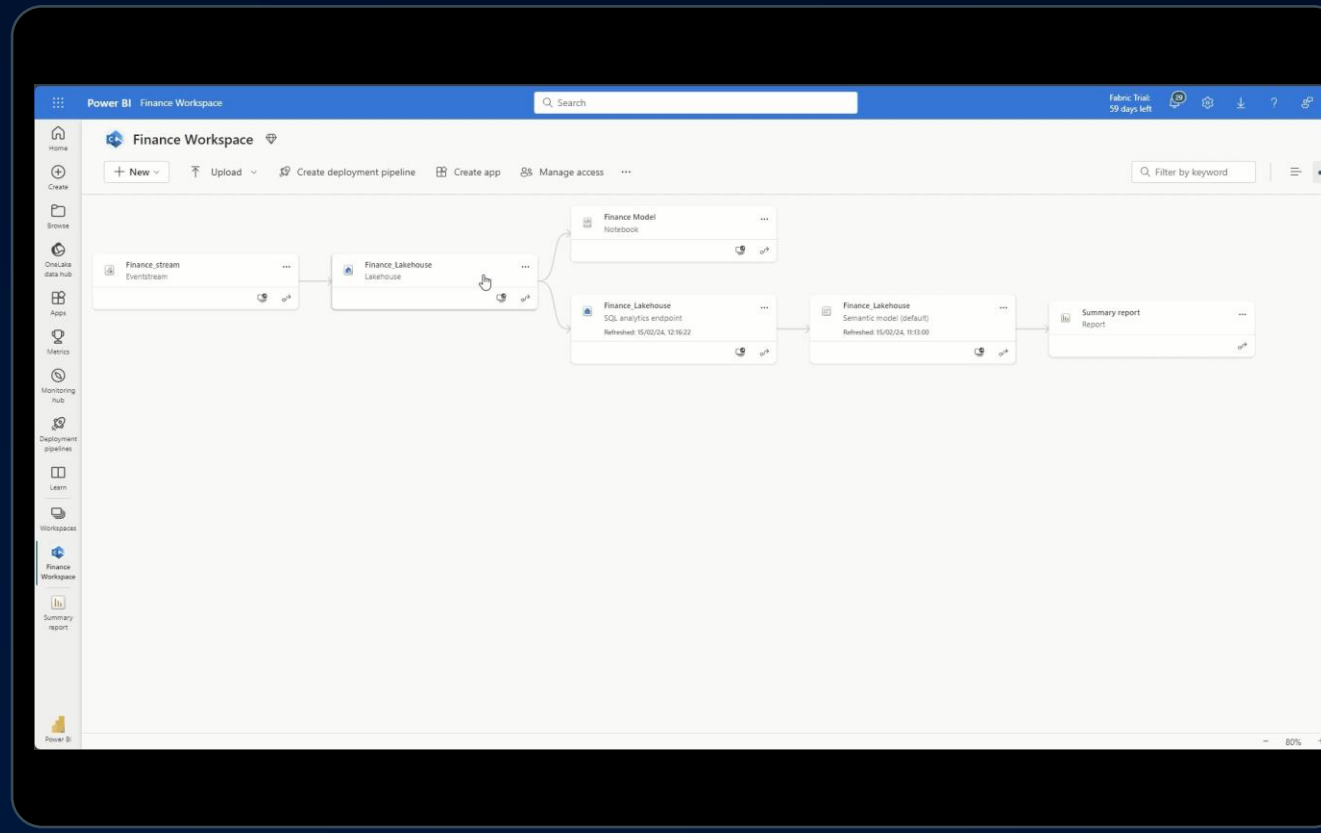
Additional Microsoft Purview purchase required

Microsoft Purview Information Protection Labels

Microsoft Purview Information Protection

Classify and protect sensitive data as it travels across Azure, Microsoft Fabric and Office

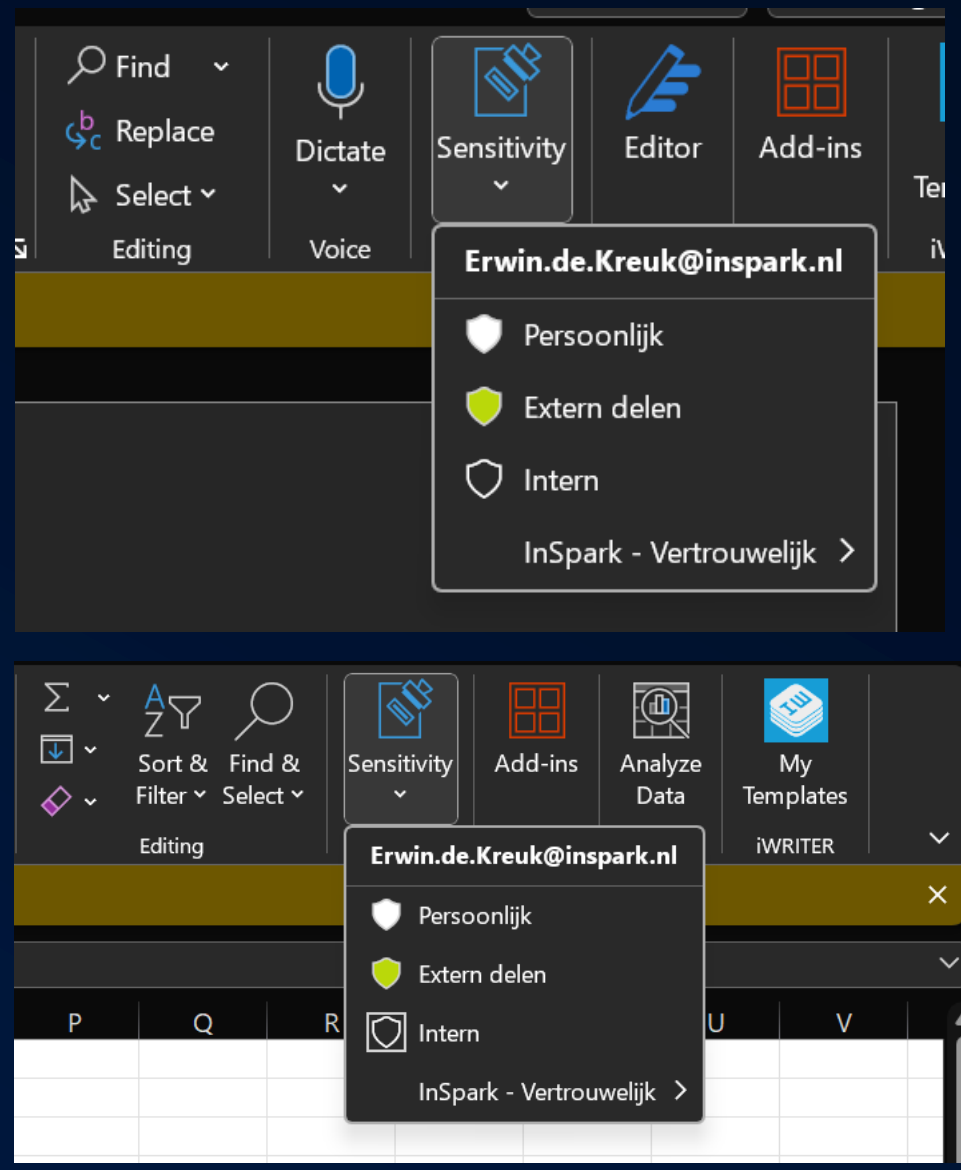
- Label data using the same sensitivity labels used in Office, SharePoint and Azure
- Label based data protection providing dynamic access controls
- Label and protection follow the data within Fabric and to Office, Power BI and PDF files
- Enforce labeling with mandatory and default label policies
- Track labeling activities via Purview Audit



Additional Microsoft Purview purchase required

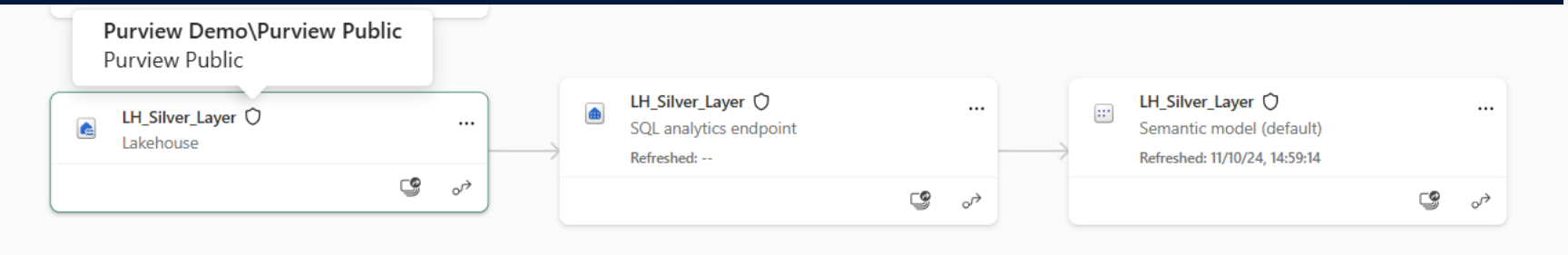
Microsoft Purview Information Protection

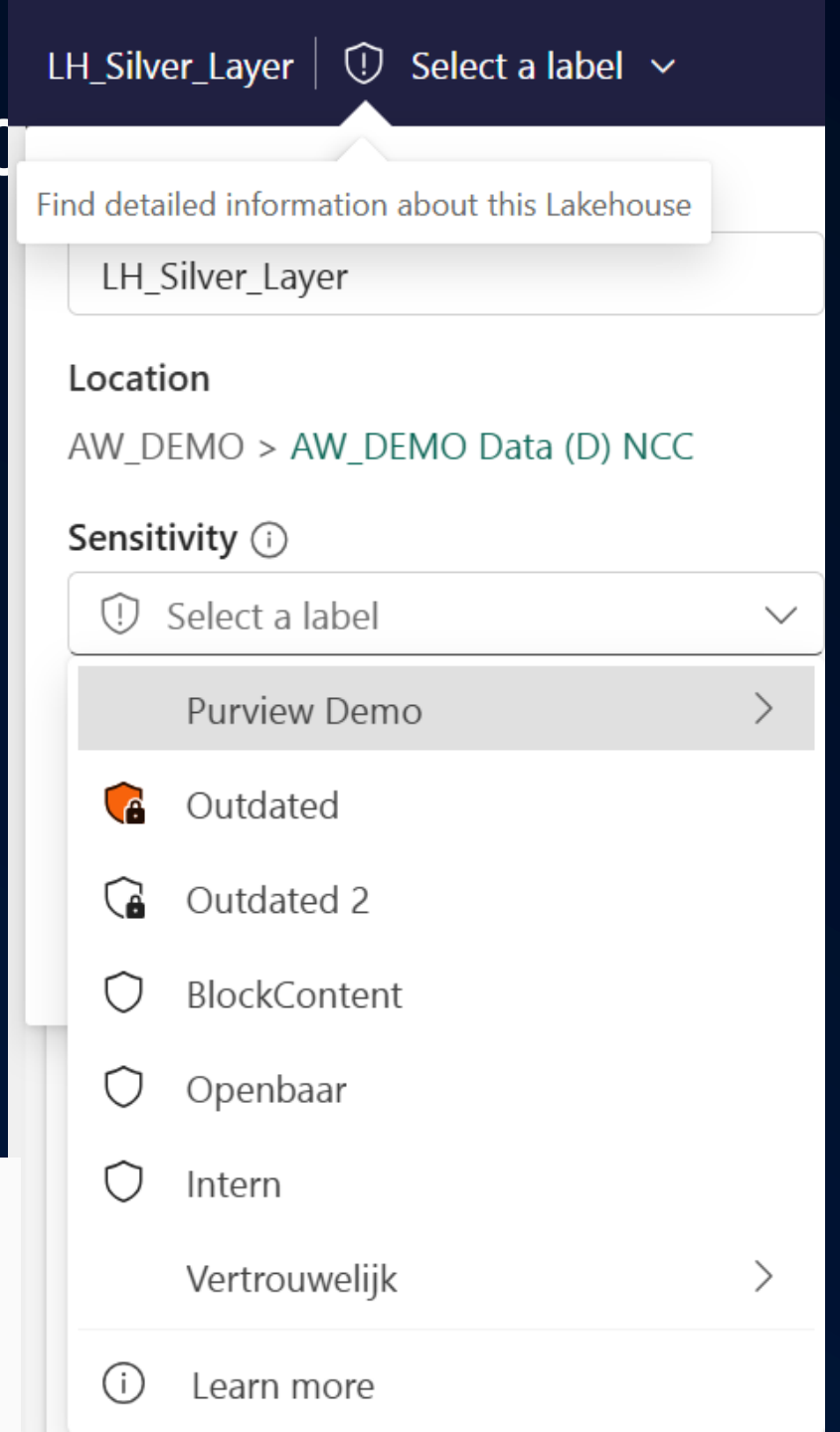
- MIP Labels in Office



Microsoft Purview Information Pro

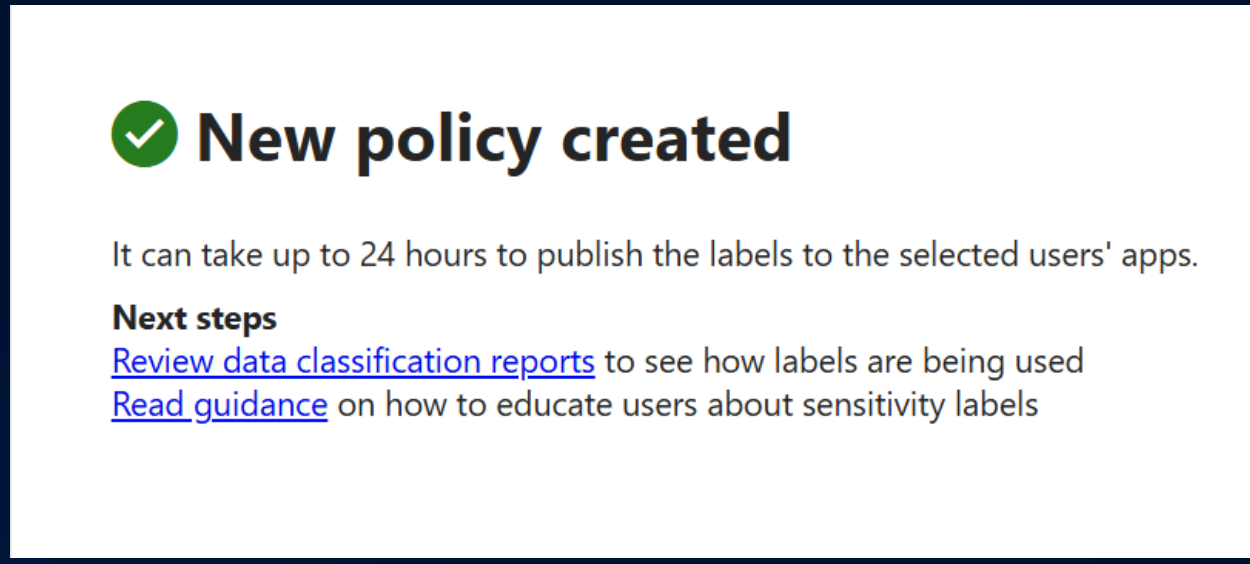
- MIP Labels in Office
- MIP Labels in Fabric
  - Inheritance of MIP labels in Fabric





Microsoft Purview Information Protection

- Create labels
- Publish labels
- Make sure you use 3-5 labels
  (people get confused with more)
- Use clear names:
  - Confidential1 >>>Confidential – Internal Employees only
- Prioritize labels appropriately
  - Start with the least restrictive (e.g., “Public”) at the top and most restrictive labels (e.g., “Highly Confidential”) at the bottom of the list



Fabric settings

Automatically apply sensitivity **label**s to downstream content

Enabled for the entire organization

With this setting enabled, whenever a sensitivity **label** is changed or applied to Fabric content, the **label** will also be applied to its eligible downstream content. Learn More

Enabled

Restrict content with protected **label**s from being shared via link with everyone in your organization

Enabled for the entire organization

This setting will prevent content with protection settings in the sensitivity **label** from being shared via link with everyone in your organization. Learn More

Enabled

To enable you need to allow users to apply sensitivity labels for Fabric content and allow shareable links to grant access to everyone in your organization

This setting applies to the entire organization

Domain admins can set default sensitivity **label**s for their domains (preview)

Disabled for the entire organization

Domain admins can set a default sensitivity **label** for their domains. The **label** they set will override your organization's default **label**s in Microsoft Purview, as long as it has a higher priority than the existing default **label**s set for your tenant. A domain's default **label** will automatically apply to new Fabric items created within the domain. Reports, semantic models, dataflows, dashboards, scorecards, and some additional item types aren't currently supported. Learn More

Allow users to apply sensitivity **label**s for content

Enabled for the entire organization

With this setting enabled, Microsoft Purview Information Protection sensitivity **label**s published to users by your organization can be applied. All prerequisite steps must be completed before enabling this setting.

Important: Sensitivity-**label**-based access control for Fabric and Power BI data and content is only enforced in the tenant where the **label**s were applied, in Power BI Desktop (.pbix) files, and in Excel, PowerPoint, and PDF files generated via supported export paths. Sensitivity-**label**-based access control is not supported in cross-tenant scenarios, such as external data sharing, or in any other export scenario, such as export to .csv or .txt formats. For more information, see Information protection in Microsoft Fabric: Access control.

Note: Sensitivity **label** settings, such as encryption and content marking for files and emails, are not applied to content in Fabric. Learn More. Encryption is applied to content in supported export paths.

Visit the Microsoft Purview portal to view sensitivity **label** settings for your organization.

Enabled

The setting below determines which users in the organization can apply and change sensitivity labels. All other users in the organization can only view the labels.

Apply sensitivity **label**s from data sources to their data in Power BI

Enabled for the entire organization

Only sensitivity **label**s from supported data sources will be applied. Please see the documentation for details about supported data sources and how their sensitivity **label**s are applied in Power BI. Learn about supported data sources

Enabled

Additional data sources may be supported in the future. With this feature enabled, the sensitivity labels from these data sources will also be applied in Power BI.

Home
Solutions
Learn
Settings
Insider Risk Managem...
Communi... Compliance
Unified Catalog
DSPM for AI
Information Protection

Information Protection
Overview
Reports
Recommendations
Sensitivity labels
Policies
Label publishing policies
Auto-labeling policies
Protection policies (previe...
Classifiers
Explorers
Diagnostics

Related solutions
Data Lifecycle Management
Data Loss Prevention

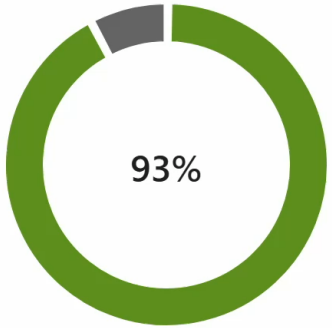
Reports

Microsoft 365 | Azure | On premises | AWS | Microsoft Fabric | Snowflake

Coverage

Protection coverage

Access control can be applied to items in Microsoft 365 and multicloud data sources, but encryption can be applied only to items in Microsoft 365. Learn how protection is applied to items.



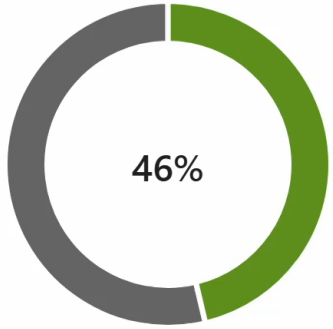
Microsoft 365 177

4 more

Explore protection policies

Sensitivity label coverage

Labeled and unlabeled items containing sensitive data across your data sources.



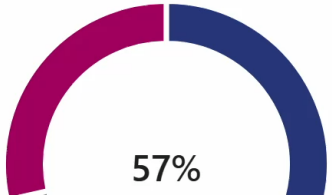
Labeled Not Labeled

Azure 301
Microsoft 365 177
Microsoft Fabric 128
Snowflake 25
Other cloud platforms 15

Explore labeled items

Data scanning summary

Snapshot of data source scans across your cloud platforms.



Azure 5
Microsoft 365 4
On premises

Microsoft Purview Information Protection Policies

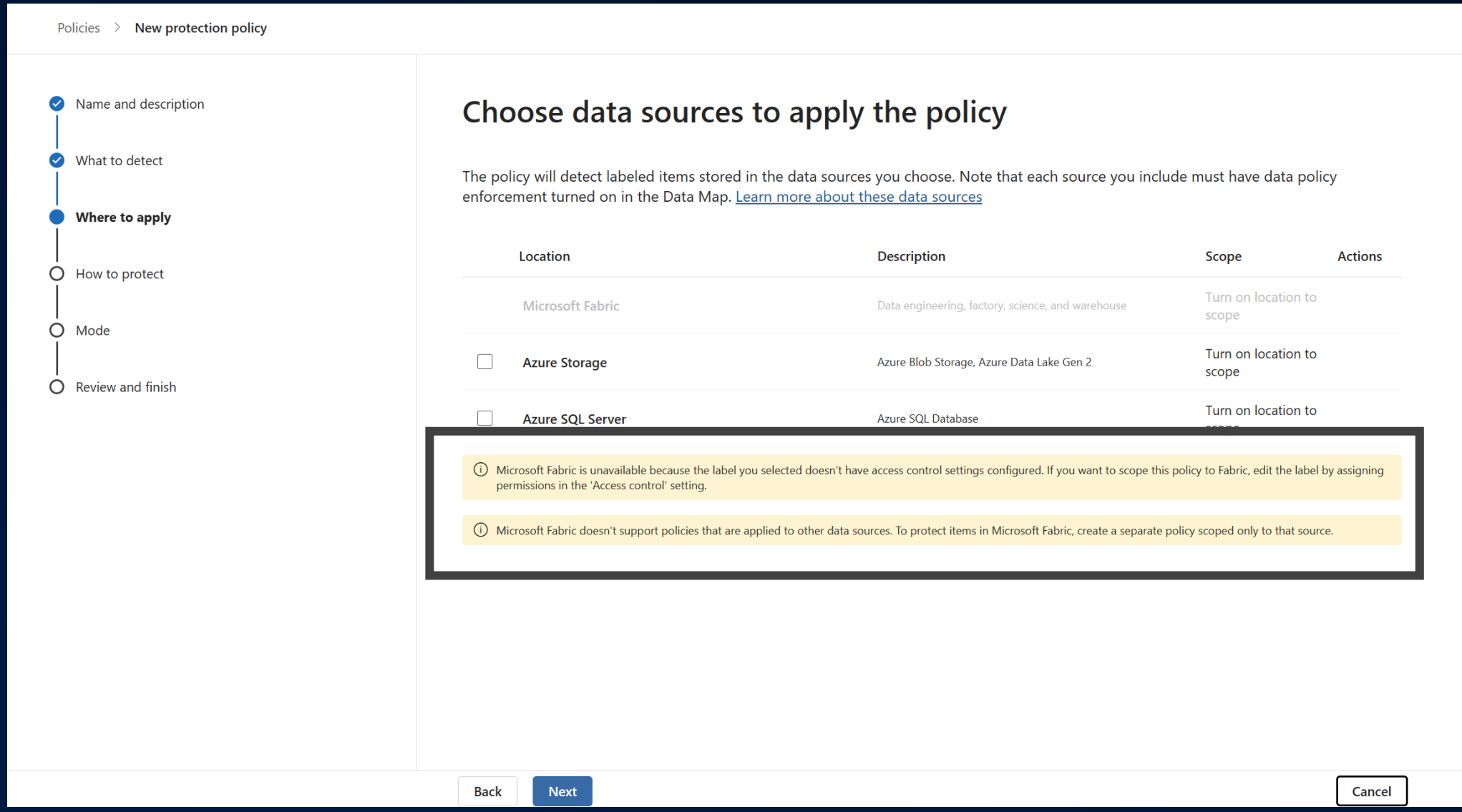
Information Protection in Fabric ensures your data is classified, protected, and governed consistently, wherever it flows

Microsoft Purview Information Protection Policies

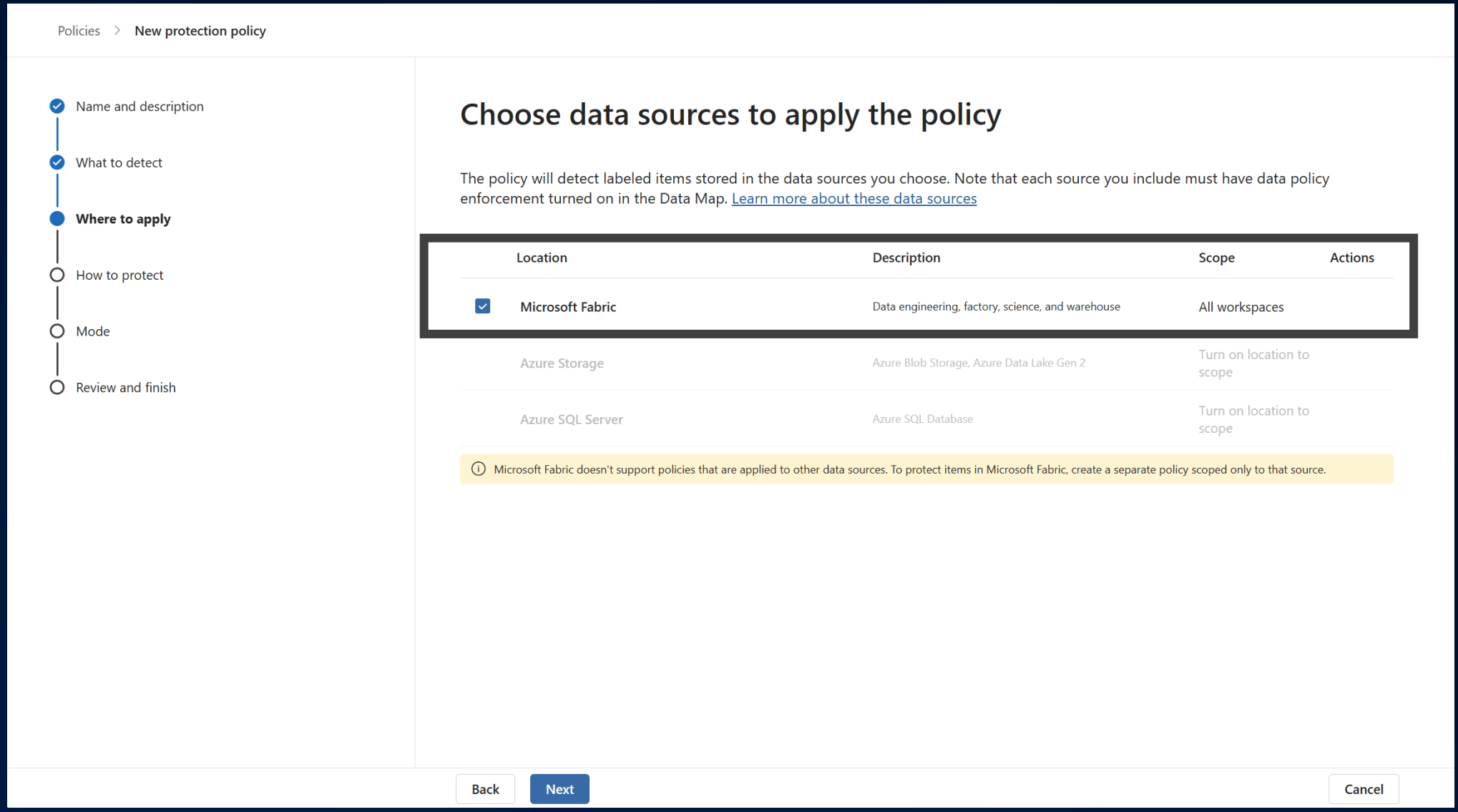
- **Apply sensitivity labels to data assets**
  - Classify data as:
    - Public / Internal / Confidential / Highly Confidential
  - Labels can be applied to:
    - Lakehouse tables / Semantic models / Reports
- **Automatic label inheritance**
  - Labels propagate through data lineage
  - Example:
    - Source = "Highly Confidential"
    - Downstream datasets/reports inherit same label
  - Ensures consistent classification across Fabric
- **Enforce access restrictions based on labels**
  - Restrict access to sensitive data:
    - Only specific users/groups allowed
  - Example:
    - "Highly Confidential" → only Finance team
  - Supports label-based access control
- **Protect data when exported**
  - Labels persist when data leaves Fabric
    - Export to Excel → file remains "Confidential"
    - Protection (e.g., restrictions) still enforced
  - Extends protection beyond the platform



Microsoft Purview Protection Policies



Microsoft Purview Protection Policies

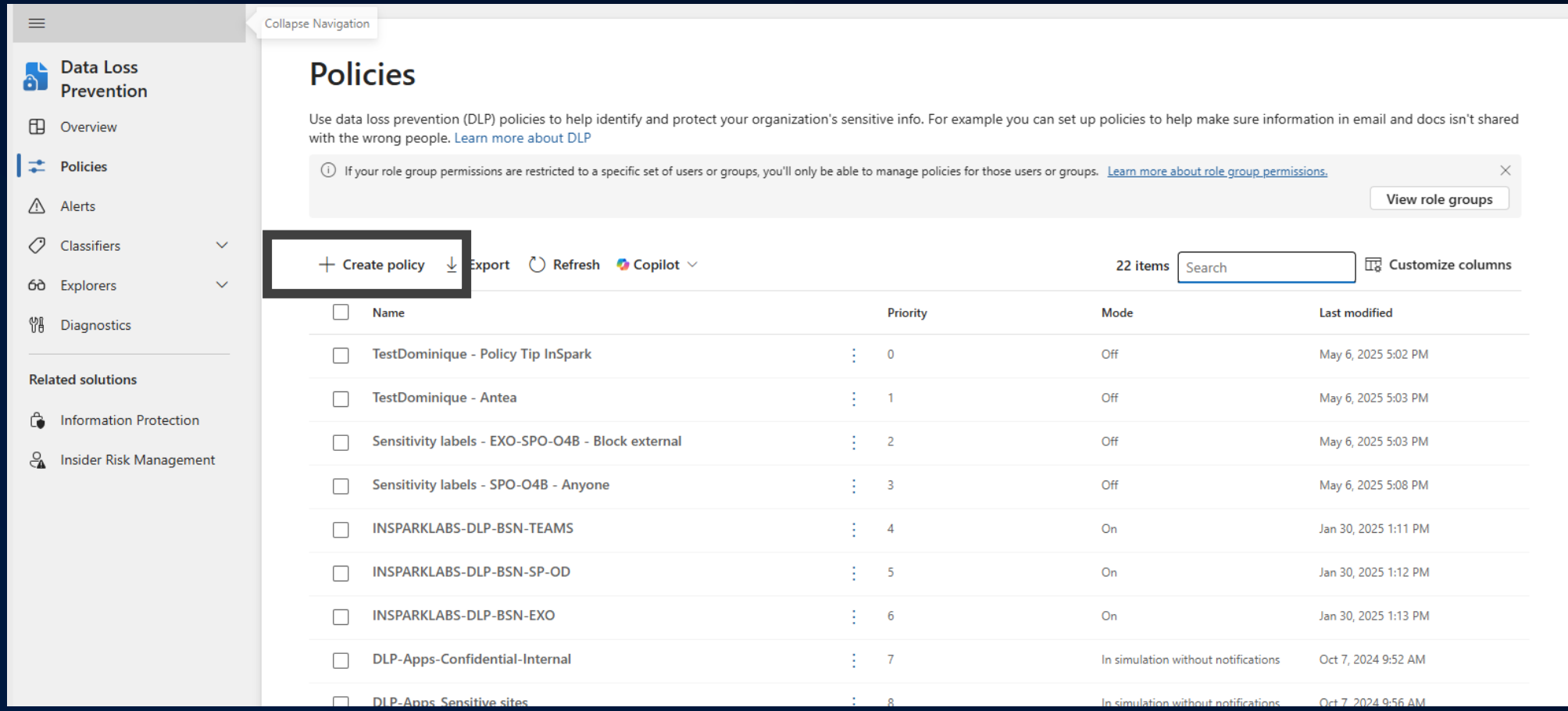


Demo

Microsoft Purview Data Loss Prevention

DLP in Fabric ensures sensitive data is automatically protected, governed, and controlled, without slowing down innovation.

Microsoft Purview Data Loss Prevention

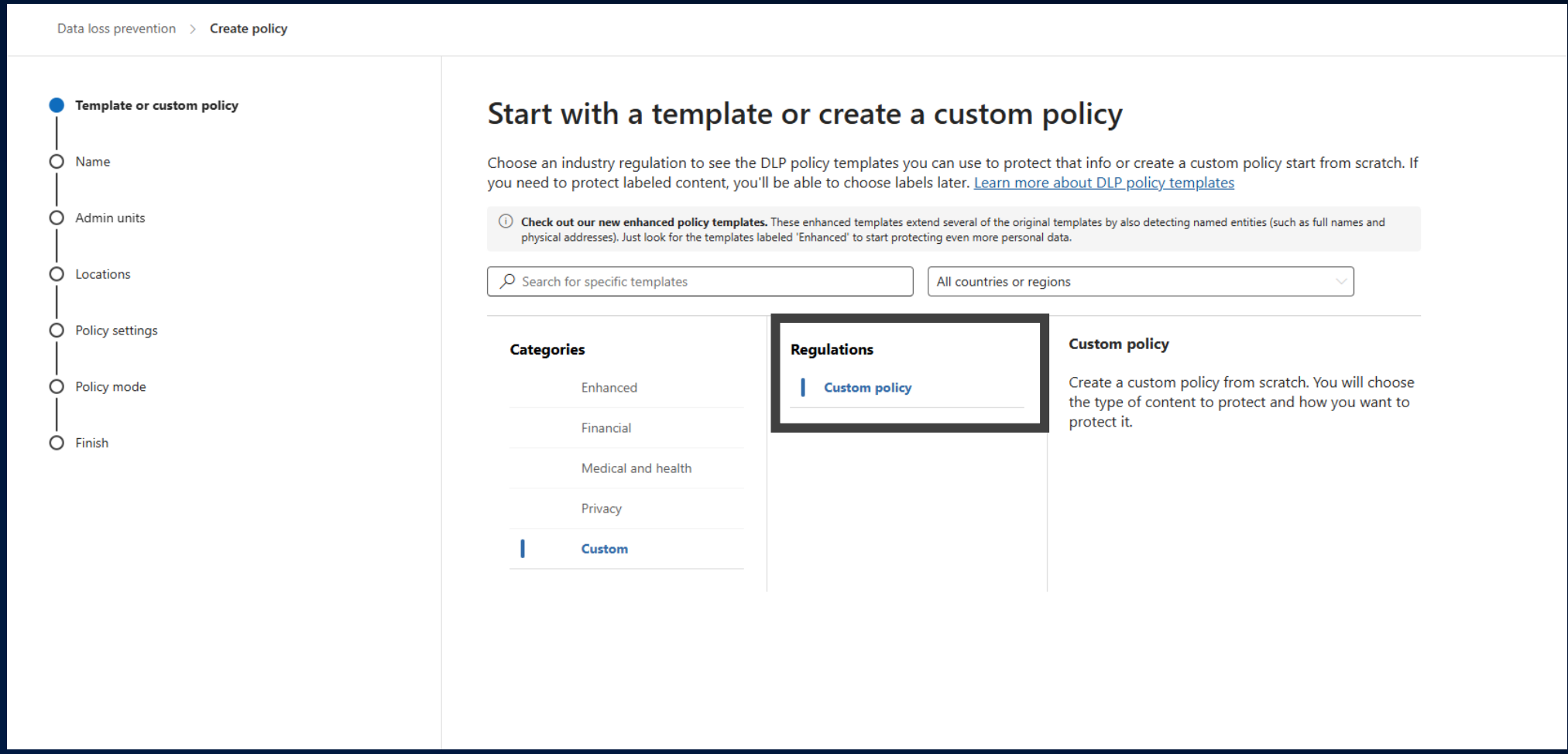


Microsoft Purview Data Loss Prevention

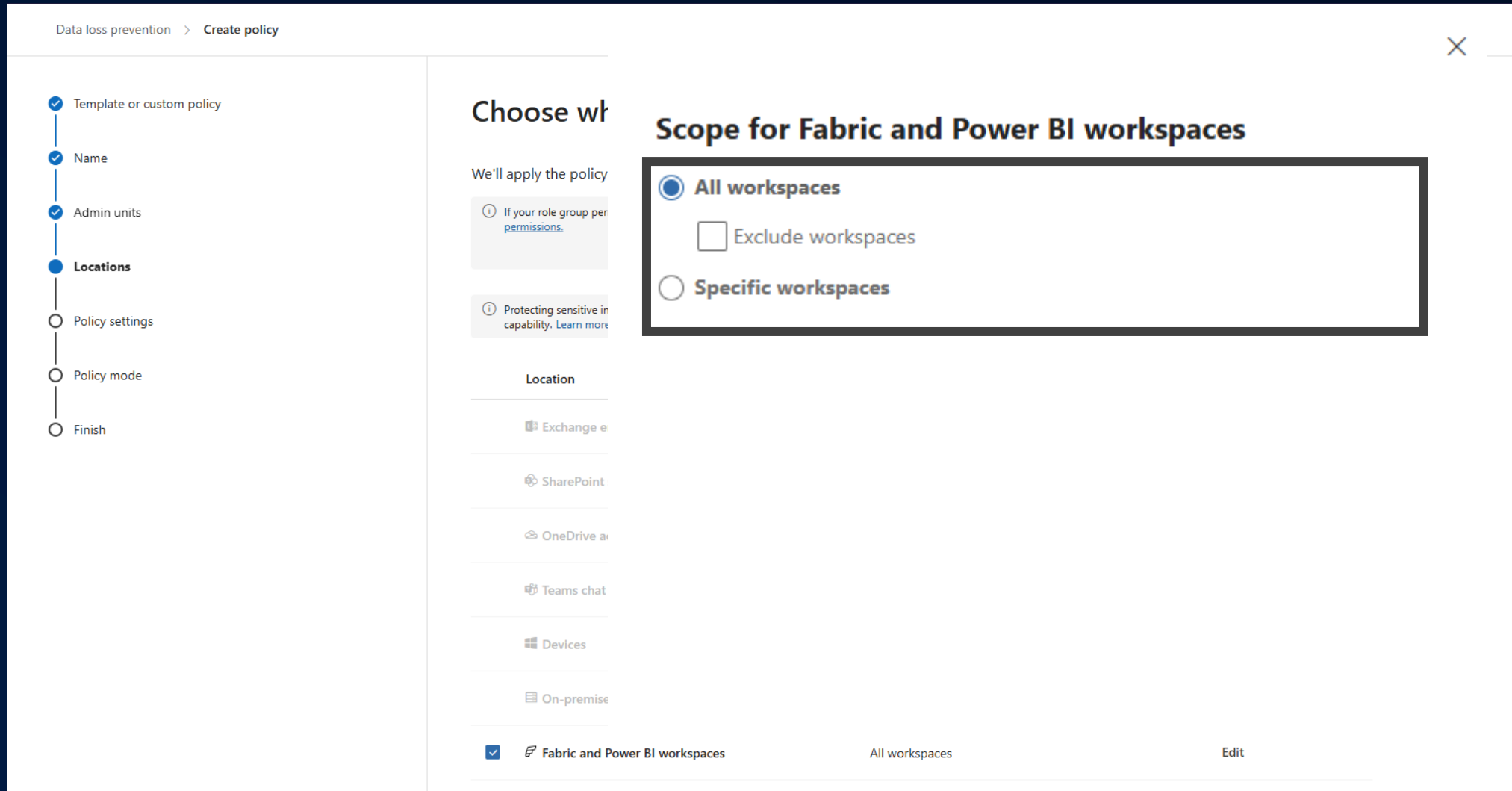
- **Protect sensitive data everywhere**
  - Automatically detects and protects sensitive data across Fabric (Lakehouse, Power BI, etc.)
- **Automatic data discovery**
  - Identifies PII and other sensitive information without manual intervention
- **Policy-driven protection**
  - Enforce consistent security policies (alerts, restrictions, blocking access) across the platform
- **Prevent data leakage & oversharing**
  - Stops accidental or intentional exposure of sensitive data to unauthorized users
- **Enables secure AI & analytics**
  - Ensures data is governed and protected, critical for AI, Copilot, and self-service analytics scenarios

DLP SETUP

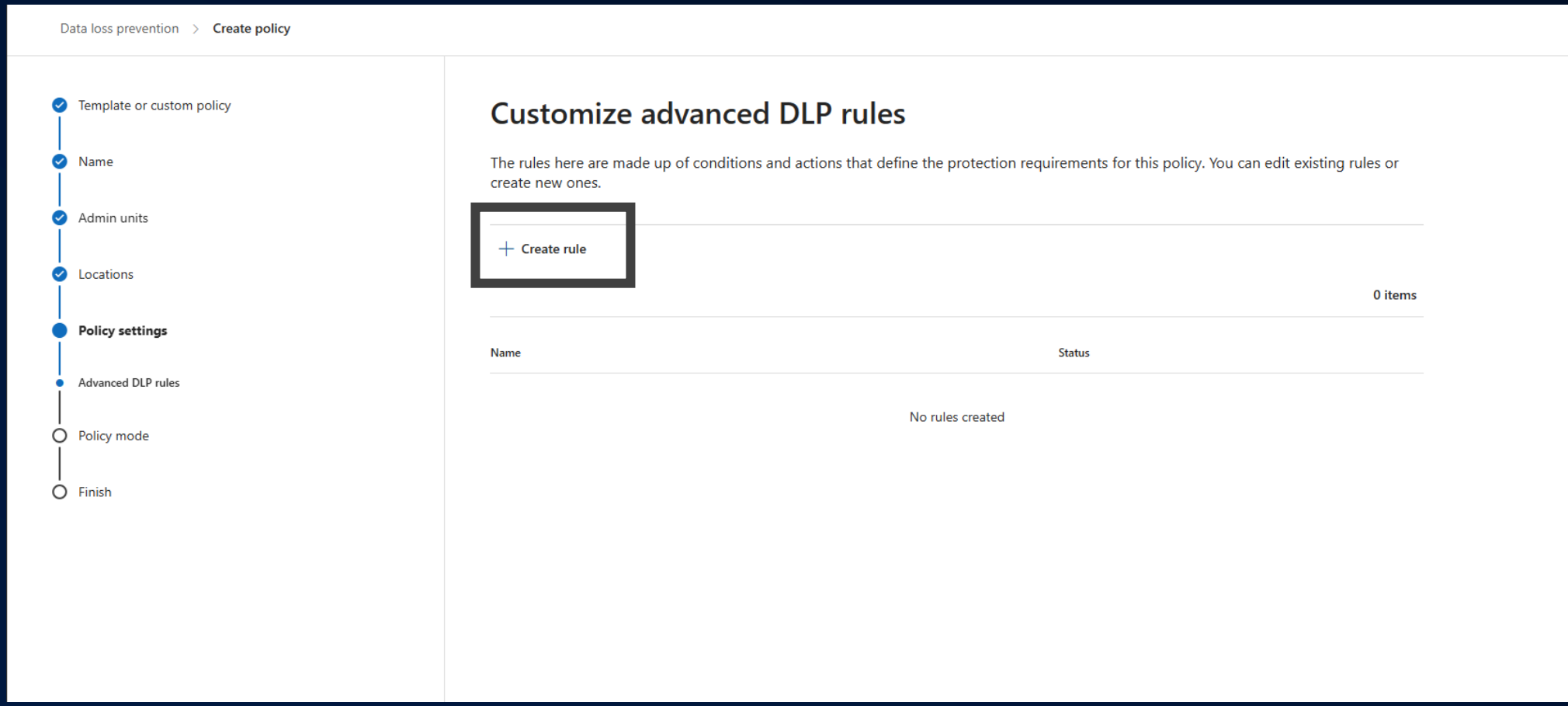
Microsoft Purview Data Loss Prevention



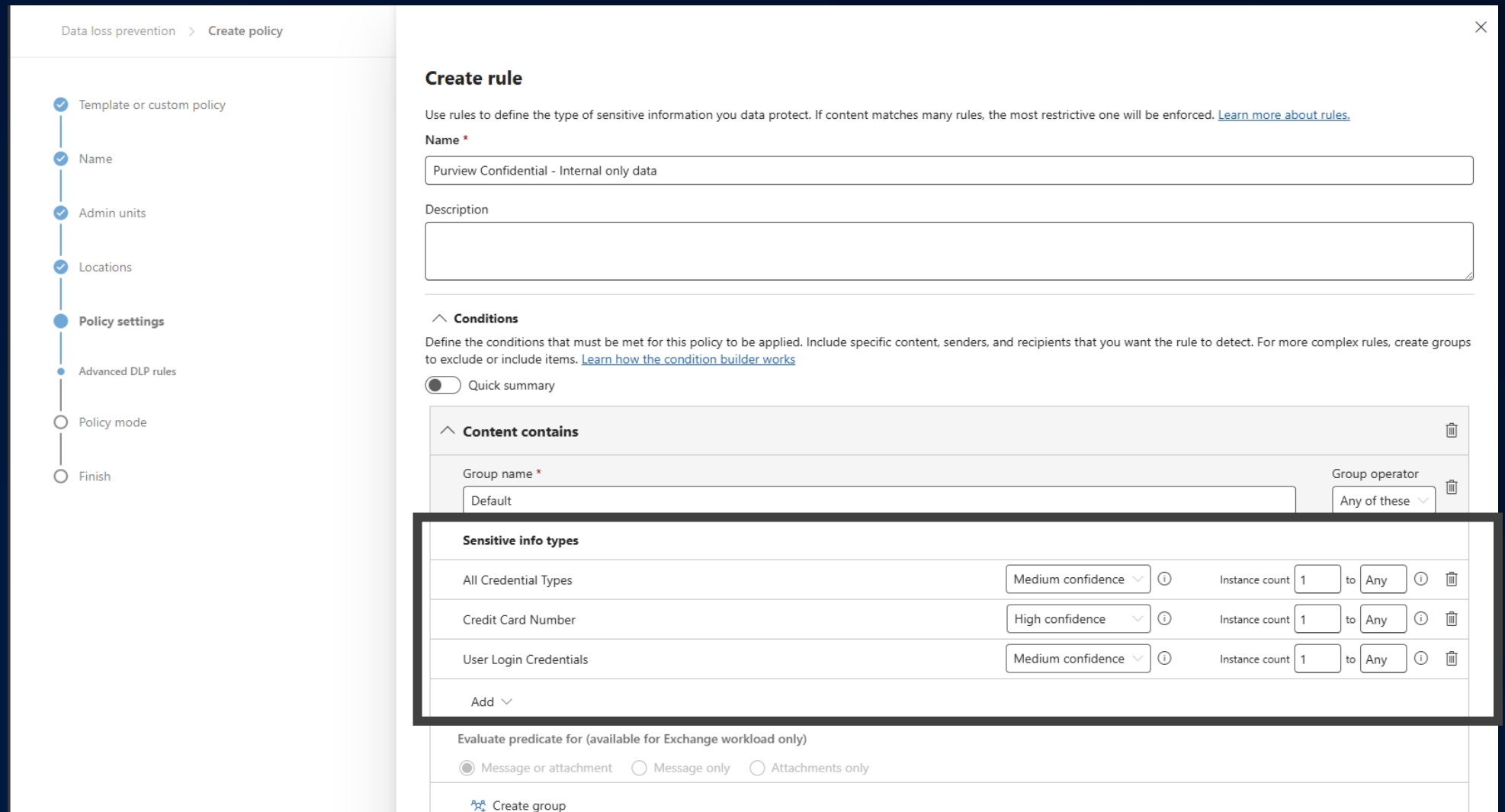
Microsoft Purview Data Loss Prevention



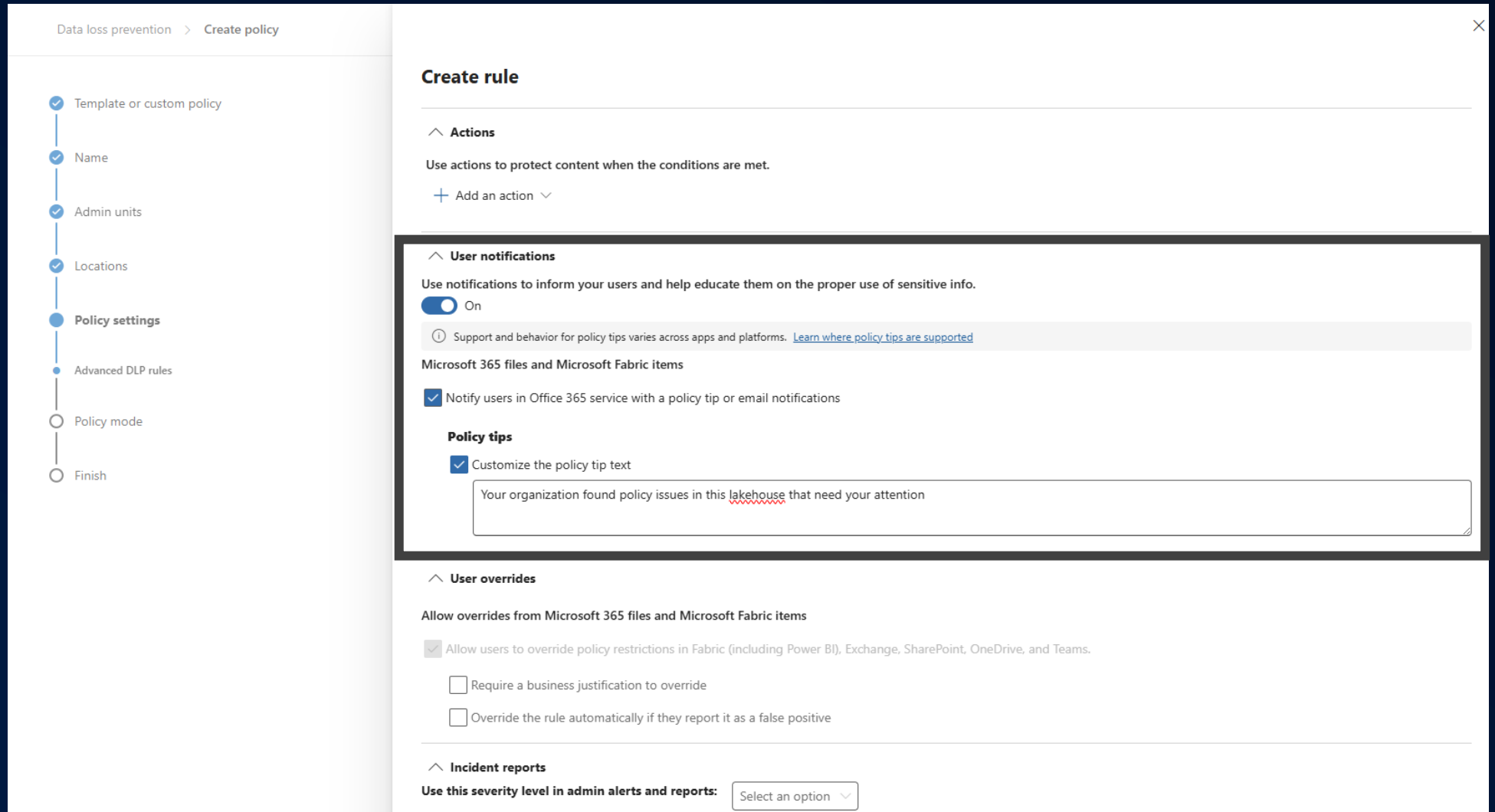
Microsoft Purview Data Loss Prevention



Microsoft Purview Data Loss Prevention



Microsoft Purview Data Loss Prevention



Demo

Microsoft Purview Data Loss Prevention

- Limitations
- Only workspaces hosted in Fabric or Premium capacities are supported.
- DLP policy templates aren't yet supported for Fabric DLP policies. When creating a DLP policy for Fabric, choose the "custom policy" option.
- DLP policies for Fabric aren't supported for sample semantic models, streaming datasets, or semantic models that connect to their data source via DirectQuery or live connection.
- DLP policies for Fabric apply only on data in Lakehouse Tables/ folder stored in Delta format.
- DLP policies for Fabric support all the primitive Delta types except *timestamp_ntz*.

Get started with DLP for Fabric and Power BI | Microsoft Learn

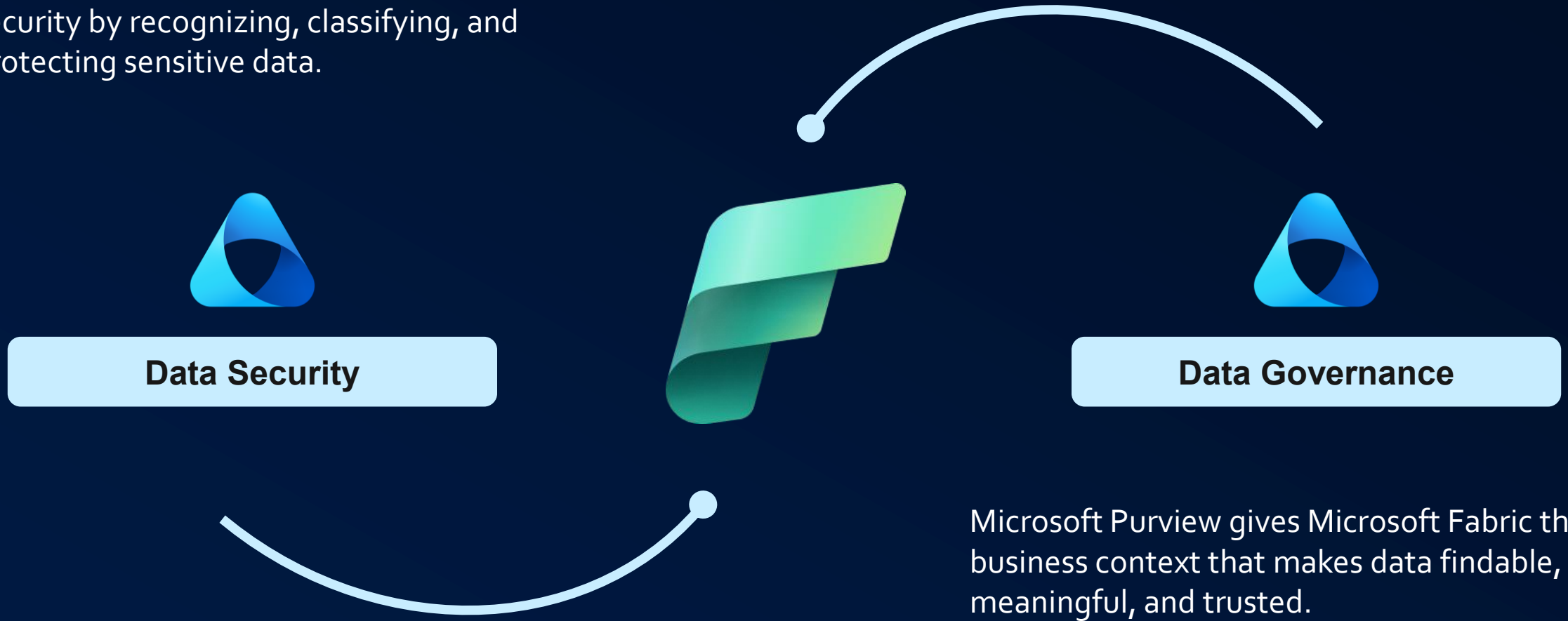
SKU/ Subscriptions Licensing

- The admin account that sets up the DLP rules must be assigned one of the following licenses:
  - Microsoft 365 E5
  - Microsoft 365 E5 Compliance
  - Microsoft 365 E5 Information Protection & Governance
  - Purview capacities

Discover & Understand your data

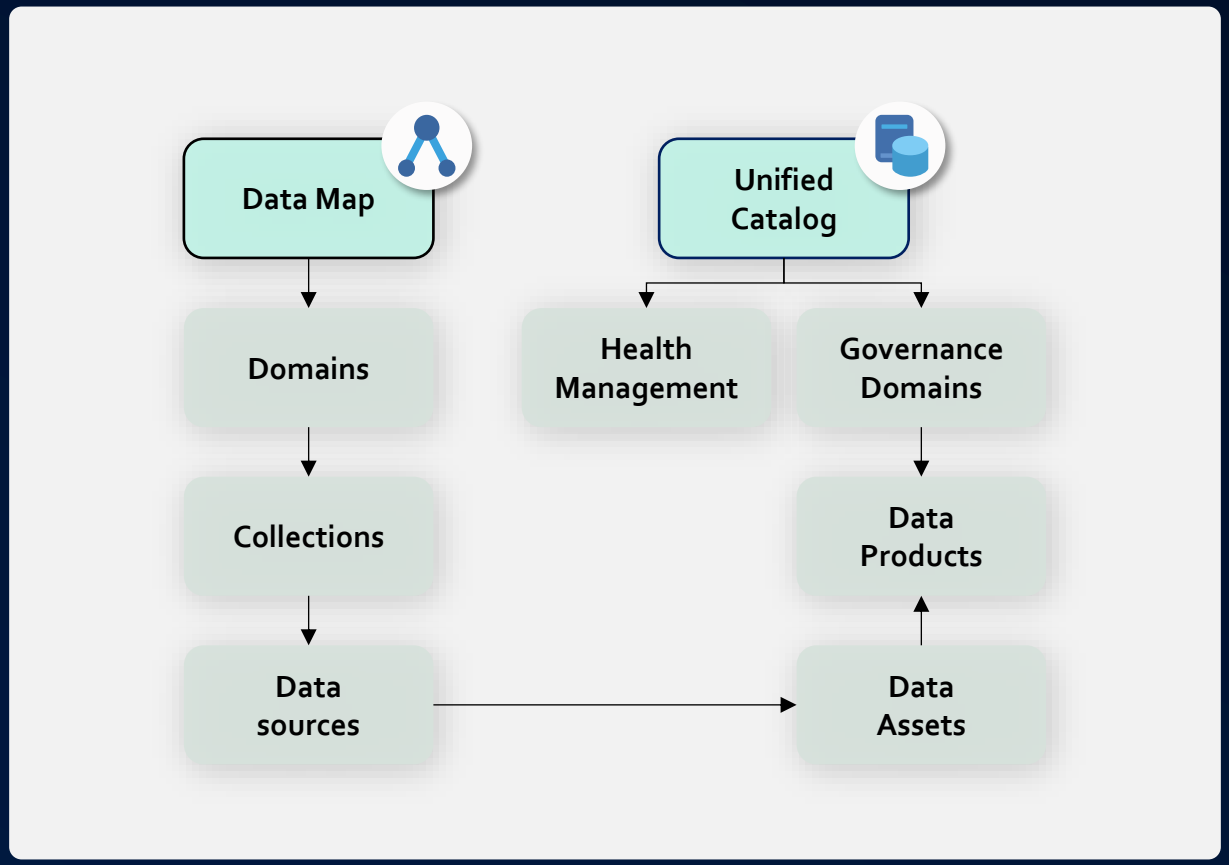
Microsoft Fabric & Microsoft Purview better together

Microsoft Purview strengthens Microsoft Fabric's security by recognizing, classifying, and protecting sensitive data.

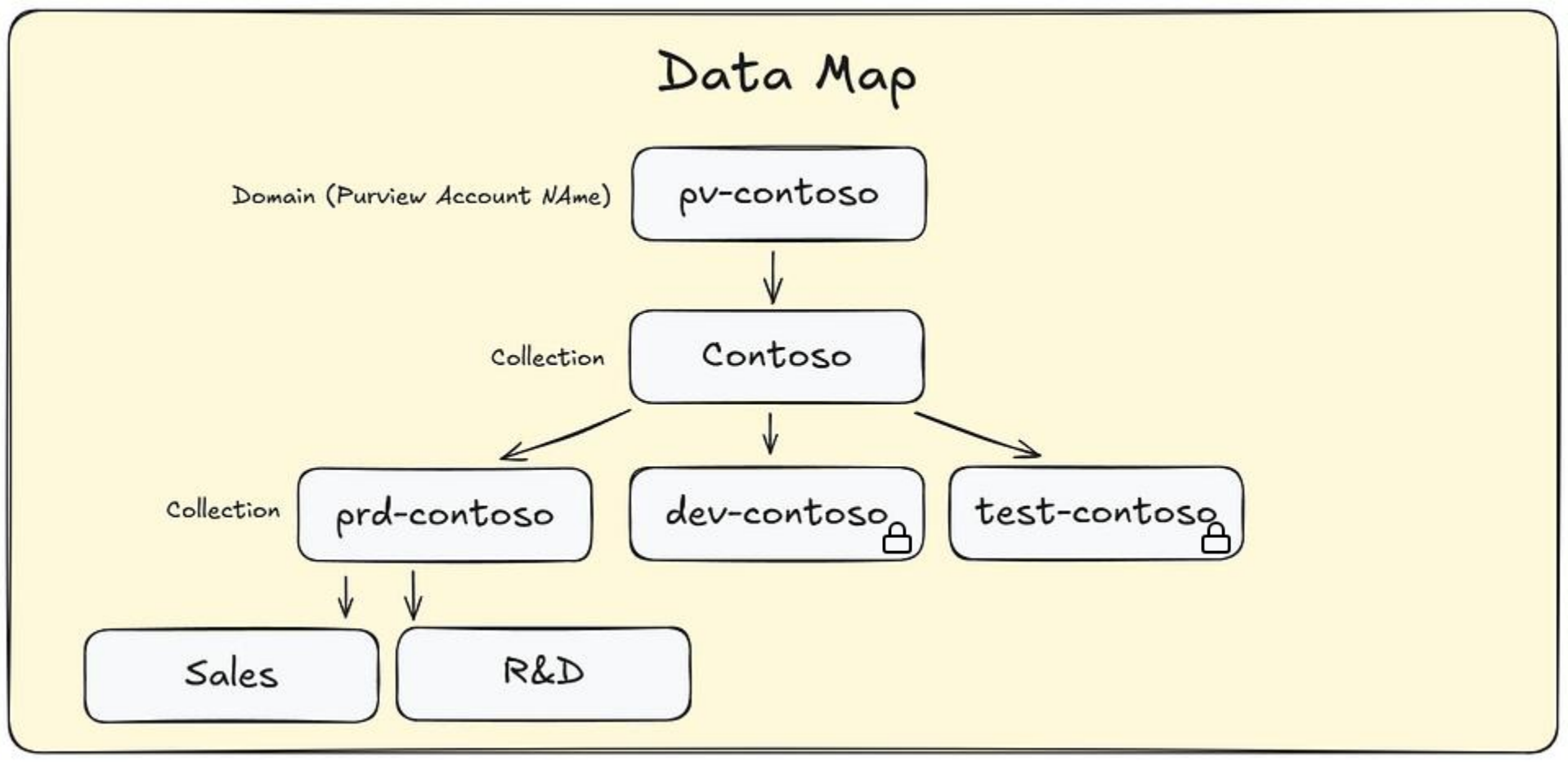


Microsoft Purview gives Microsoft Fabric the business context that makes data findable, meaningful, and trusted.

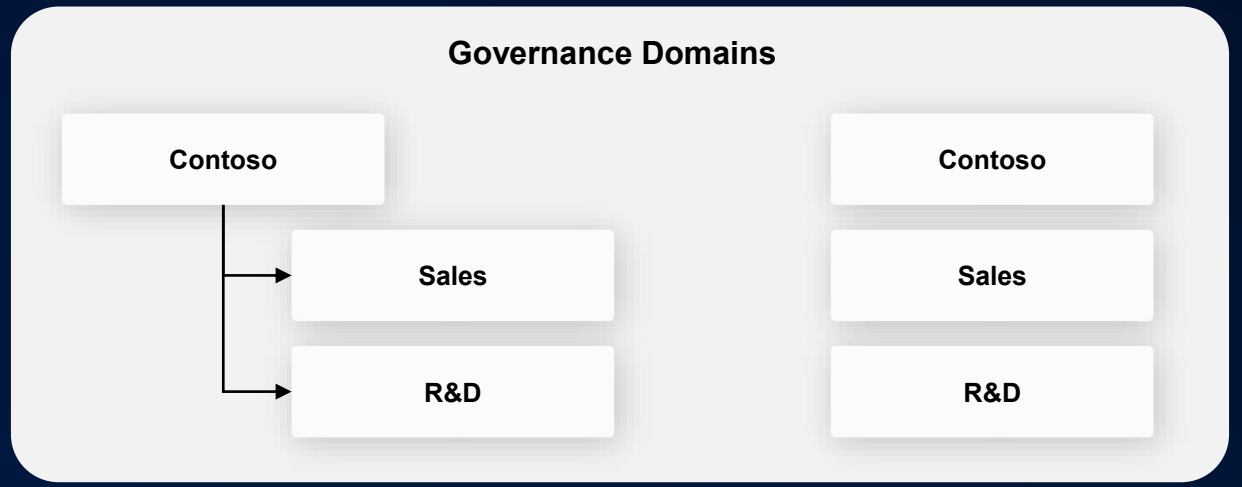
Microsoft Purview Unified Catalog Structure



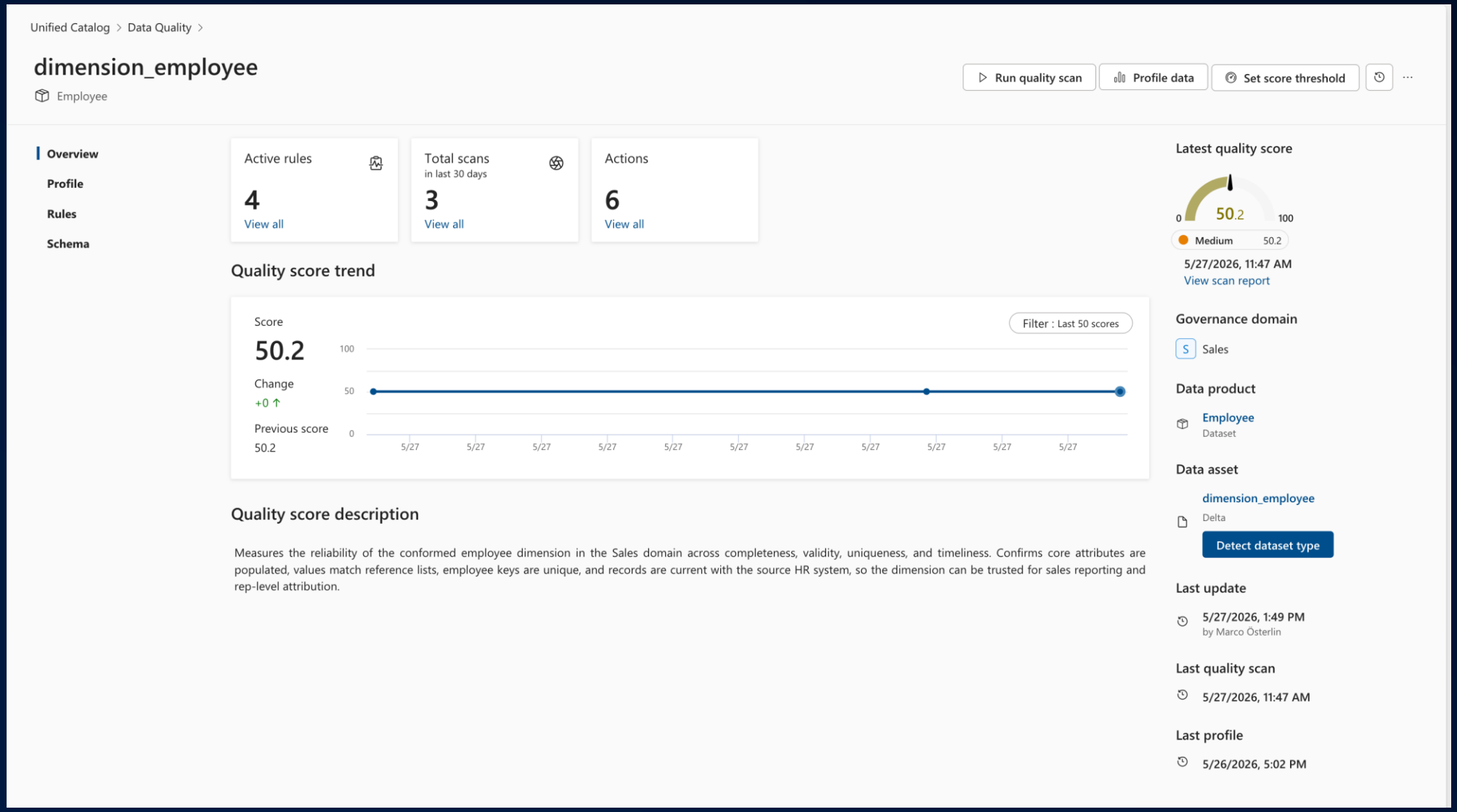
Microsoft Purview Unified Catalog
Data Map Design with Microsoft Fabric in mind



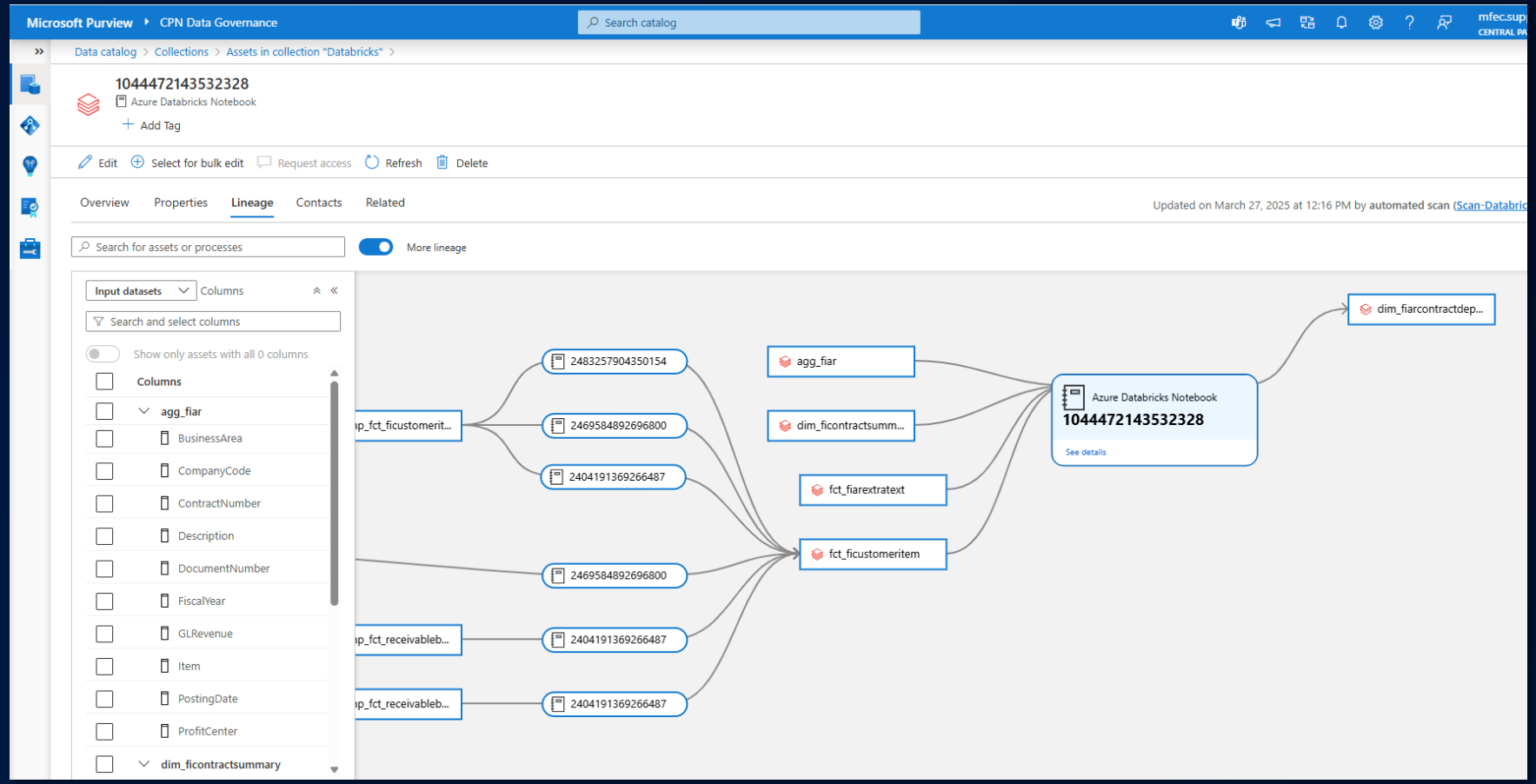
Microsoft Purview Unified Catalog
Unified Catalog – Governance Domain Design



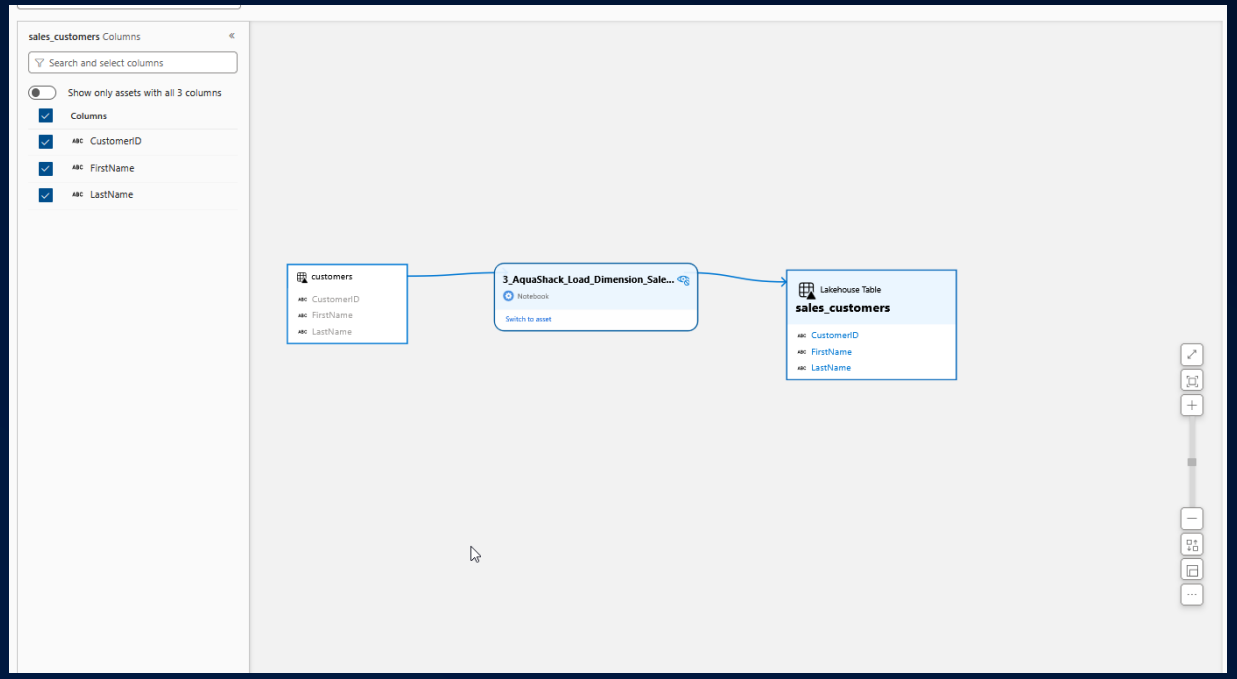
Microsoft Purview Unified Catalog
Data Quality

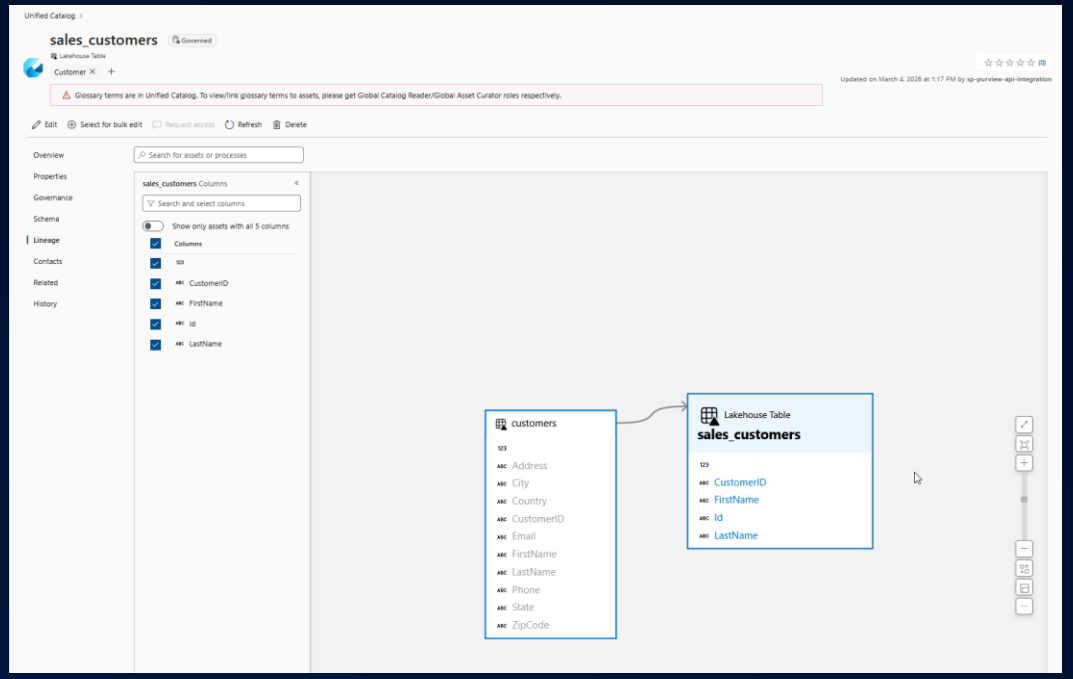


Microsoft Purview Unified Catalog Data Lineage



Microsoft Purview Unified Catalog
Data Lineage for Microsoft Fabric





Microsoft Purview Unified Catalog Context/Metadata Policy

Policy	Principle	Process
What	**Why**	**How**
Expected outcome	Explain the metadata policy value	Design, execute, and measure
Policies define the high-level objectives for metadata management, setting overall goals much like corporate governance. They establish what you aim to achieve and ensure alignment with the broader data governance strategy.	Principles are the foundational ideas that support and elaborate on policies, providing clarity and direction for consistent application. Multiple principles often support a single policy, driving the processes that implement the policy's intent.	Processes outline the specific actions required to implement policies and principles, ensuring strategic goals are executed effectively at the operational level. One or more processes typically support each principle.
Example	Example	Example
*All Data Products in the Unified Catalog **must** have an assigned Data Owner*	*Establishes clear accountability and responsibility.*	*Document Ownership in Unified Catalog after scanning the Data Assets and creating the Data Product*

Data Product / Data Asset Template

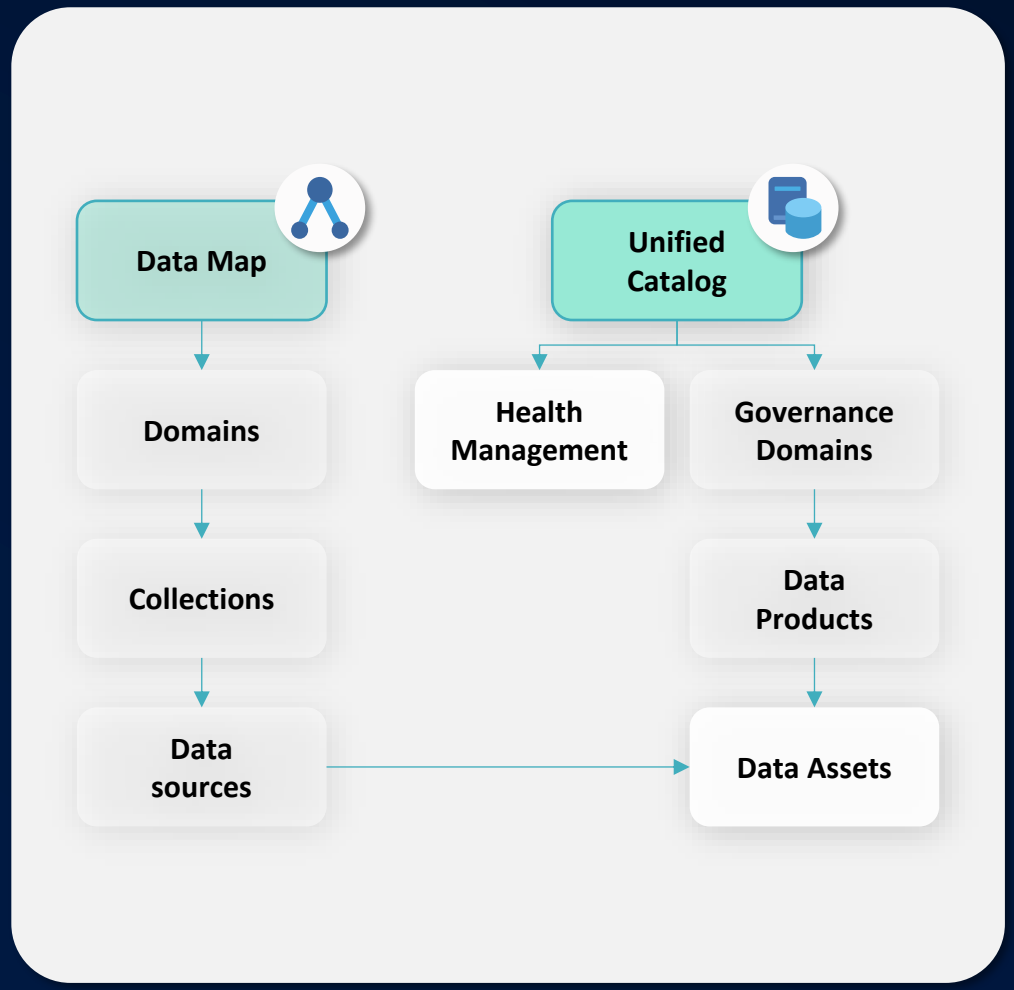
Data Asset Description Template

- **Data Asset Overview**: Begin with a brief overview summarizing the data source's purpose, origin, intended use & audience and primary use within the organization i.e., Business Function or Process.
- **Legal and Compliance Considerations**: briefly address any legal or compliance considerations related to the data, including privacy regulations, data usage restrictions, third-party agreements, terms of use for data aggregation, PII, FDA guidelines, external regulations, or relevant contractual obligations.
- **Access Permissions and Security**: Information about any restrictions or compliance requirements related to data access.

Data Asset Field Descriptions

- **Asset Description –** See description template above
- **Classification –** Custom Classification “No Classification needed”
    - **Awaiting decision from Privacy**
- **Business Glossary (Classic types) –** If applicable, Connect Terms to Data Assets
- **Assign Owners & Experts –** Minimum of 2 People min. 1 owner
- **Mandatory Managed Attributes (Classic types) –** Confidentiality & Sensitivity
    - **TBD – Other attributes if applicable, i.e., “GxP”**
- **Tags –** If Applicable

Microsoft Purview Pricing Model



Data Map Costs

All activities performed in the Microsoft Purview Data Map are subsumed by costs in the Unified Catalog. Effectively the processing power required such as scanning or classifying assets does not bear an upfront cost.

Unified Catalog Costs

There are two solutions in the Unified Catalog that incurs pricing, the **Health Management** & **Data Assets**.

Curated Data Assets in Microsoft Purview for consumer discovery incurs a price of $0.50 USD per governed asset.
In detail, a data assets is considered curated when they are attached to data products, critical data elements or annotated with metadata i.e., appointing ownership, or adding asset descriptions.

Health Management (or Data Management) solution require Data Management Processing Units to run health controls and data quality rules. The costs are calculated based on:

- The total amount of processing units needed based on the volume, complexity & physical topology of the data management utilization.
- One of three types of processing unit increasing in speed and parallelism:
  - Basic: $15 dollars per hour
  - Standard: $60 dollars per hour
  - Advanced: $240 dollars per hour

Note: The costs incurred as part of the Unified Catalog includes any future capabilities that may overlap with the existing pricing model such as additional data quality features requiring additional computing.

Microsoft Purview Unified Catalog

- Limitations
  - Data Map design is critical to get right as any decision will impact further impact scaling
  - Currently for all Fabric items besides Power BI, only item level metadata and lineage can be scanned.
  - For Lakehouse tables and files, sub-item level metadata scanning is available but sub-item level lineage isn't supported.
  - No out of box Column Level Lineage for Microsoft Fabric*
  - Data Lineage created by the API can’t be deleted manually, needs to be done by API.*
  - No automatic data classifications on Microsoft fabric assets*
  - You can only run Data Quality table by table, no cross referencing

Demo



Protect, Discover & Understand data with Microsoft Fabric & Microsoft Purview