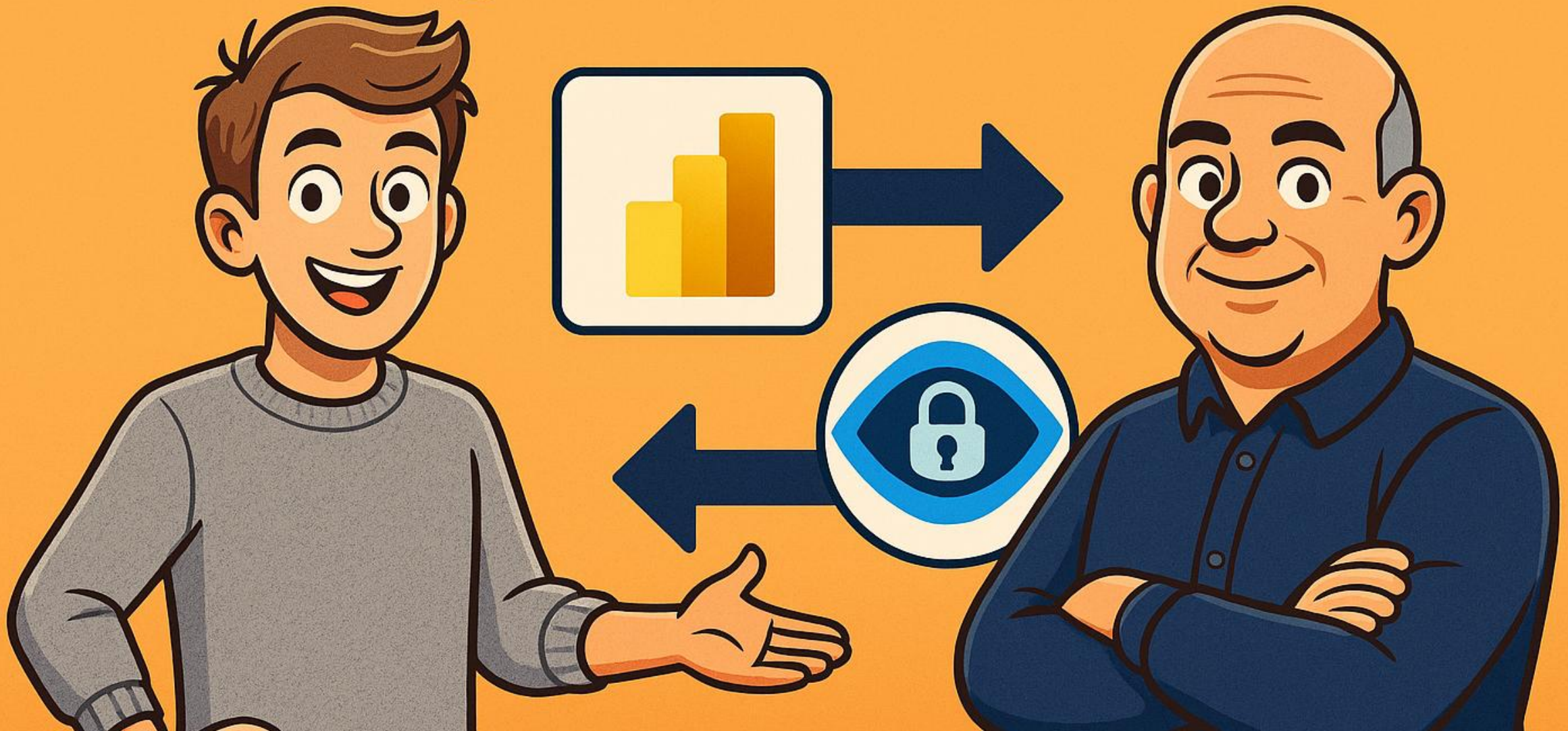
From Insight to Oversight: Securing Power BI with Purview



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

https://www.linkedin.com/in/jan-sparnaaij/

https://github.com/JanSparnaaij

https://sessionize.com/jan-sparnaaij

AI is transforming the world

Data is the fuel
that *powers* AI

Data-driven transformations yield significant benefits

54%

Increase in revenue performance

44%

Faster time to market

62%

Improvement in customer satisfaction

54%

Increased profit results

Source: How to lead a data-driven digital transformation by Harvard Business Review

But achieving these benefits comes with challenges

Over

91%

of leaders report their organizations have increased investment in data and analytics

Only

32%

of organizations report being able to realize tangible value from data and analytics

Source: Accenture, Closing the Data Value Gap
Source: Gartner, Modernize Data and Analytics Capabilities

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?

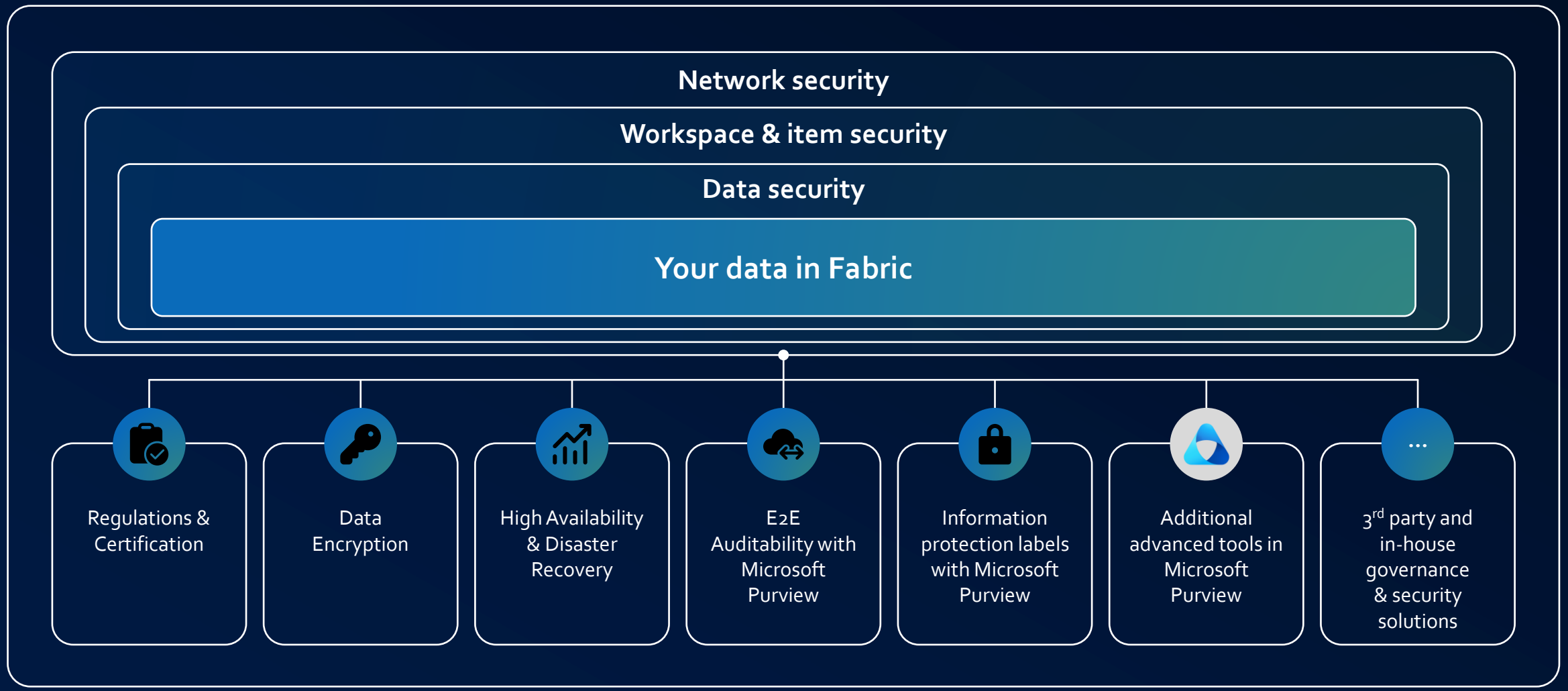
Problem statement

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

Security layers in Microsoft Fabric



Building trust in your Data Platform

Data Governance and Stewardship	Data Quality Rules	Data Integration and Transformation Rules	Monitoring and Alerting	Policy and Compliance Rules
Data Ownership Access Control Audit Trails Data Catalog	Accuracy Completeness Consistency Timeliness Uniqueness	ETL/ELT Validation Schema Evolution Data Lineage	Data Quality Dashboards Anomaly Detection Automated Alerts	Data Retention Policies Privacy Compliance Data Classification

The goal—Integrated solutions are better equipped to address customer needs to safely drive business value and AI innovation

Challenges	What customers want
Fragmentation	An integrated data platform with security and governance solutions
Evolving regulatory landscape	Sophisticated security and governance solutions that adapt to regulations as they are released
Growing data estates	Governance and security solutions that integrate across your entire, cross-cloud data estate
Safeguarding for AI	Trustworthy measures that provide assurance for AI innovation

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

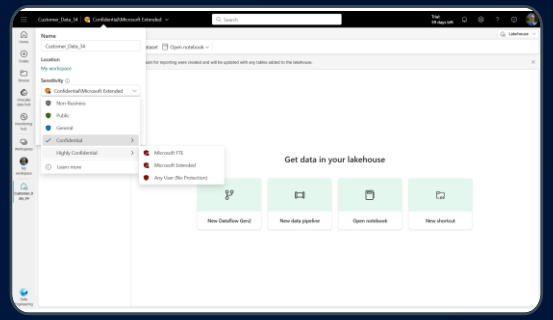
Compliance Manager
eDiscovery and Audit
Communication Compliance
Data Lifecycle Management
Records Management

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

Shared platform capabilities

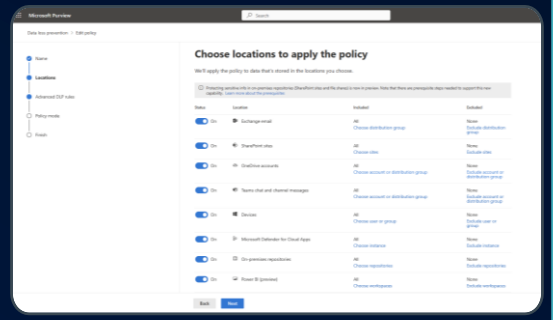
AI-based efficiency, Data Map, Classification, Labels, Audit Logs, Policies, Data Connectors

Purview Data Security & Compliance integration with Fabric



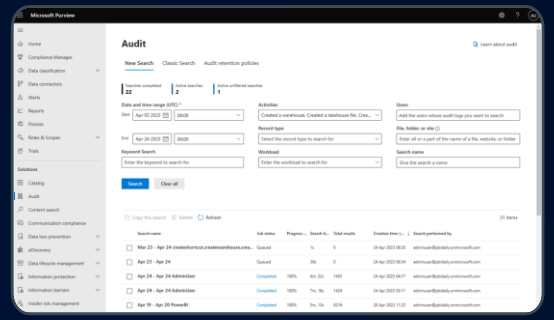
Information protection sensitivity labels and protection policies

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.



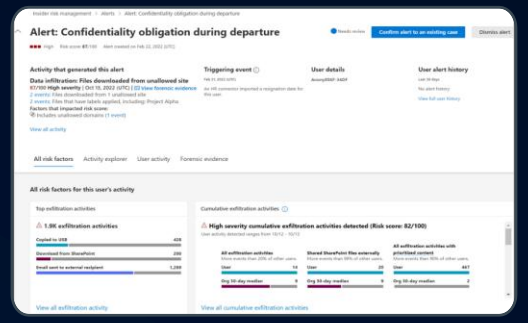
Data loss prevention policies

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

Purview Information Protection

Purview Information Protection for Fabric

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

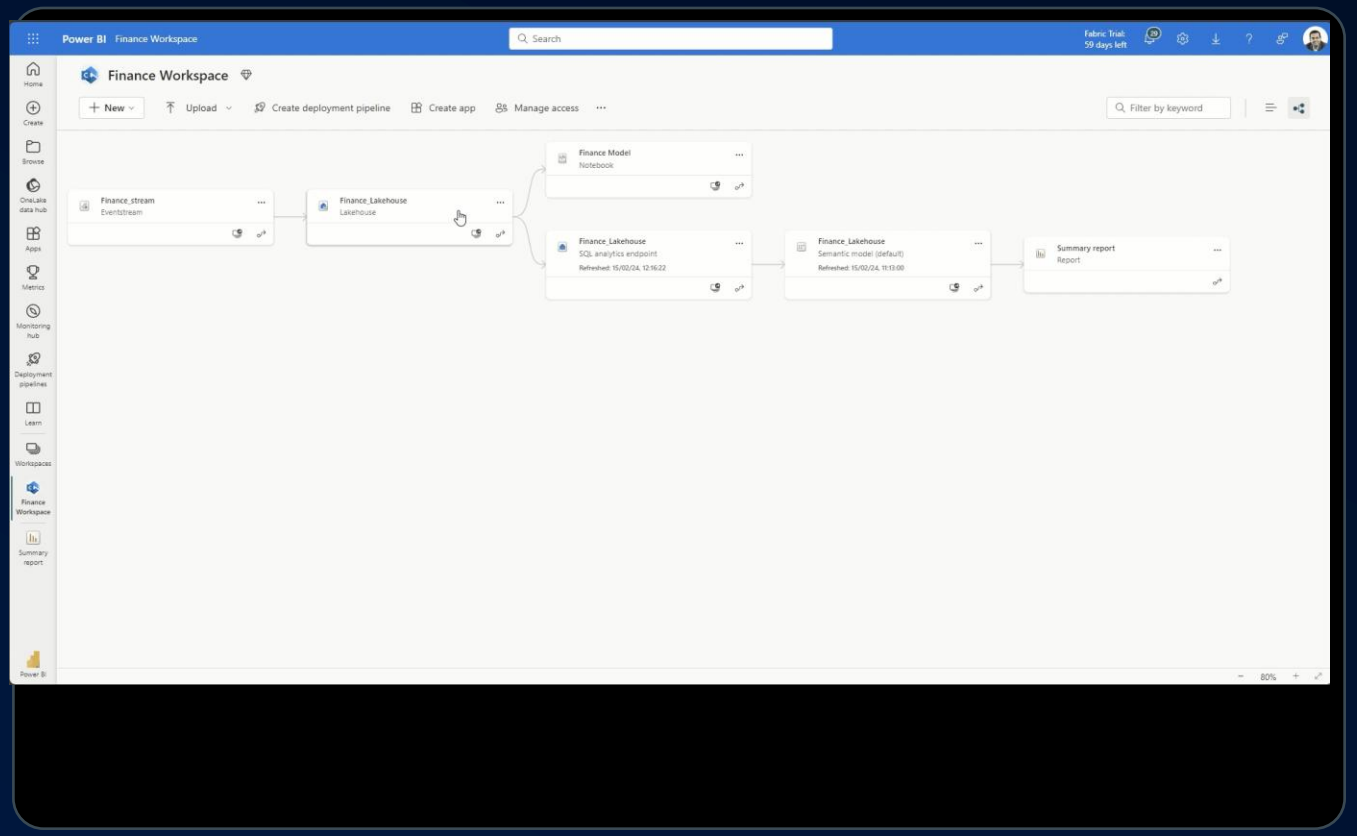
Label data using the same sensitivity labels used in Office, SharePoint, and Azure (GA)

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



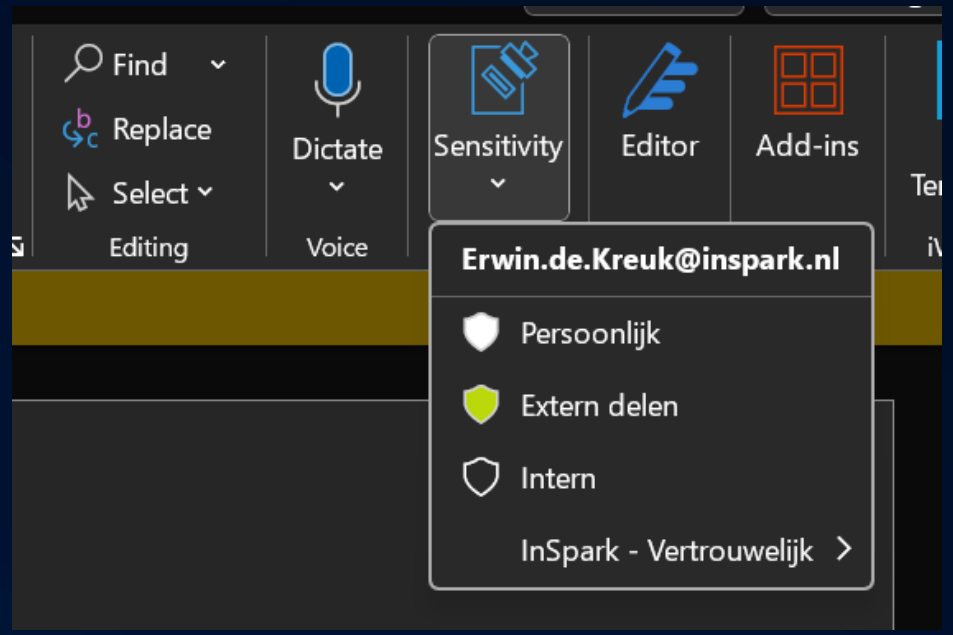
Roadmap : GA protection policies, auto-labeling, expend to table, column level granularity

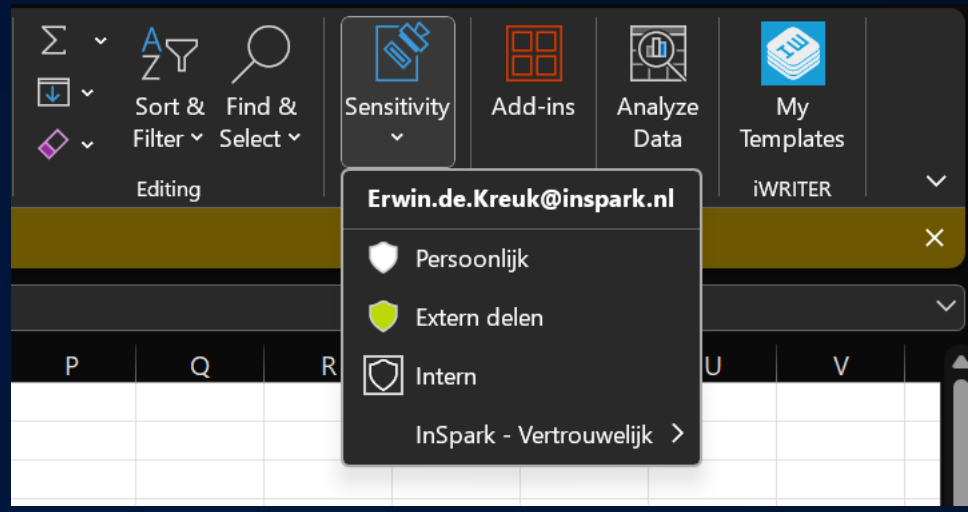
Additional Microsoft Purview purchase required

*Protection policies don't support PowerBI reports, dashboards and datamarts - planned

Purview Information Protection

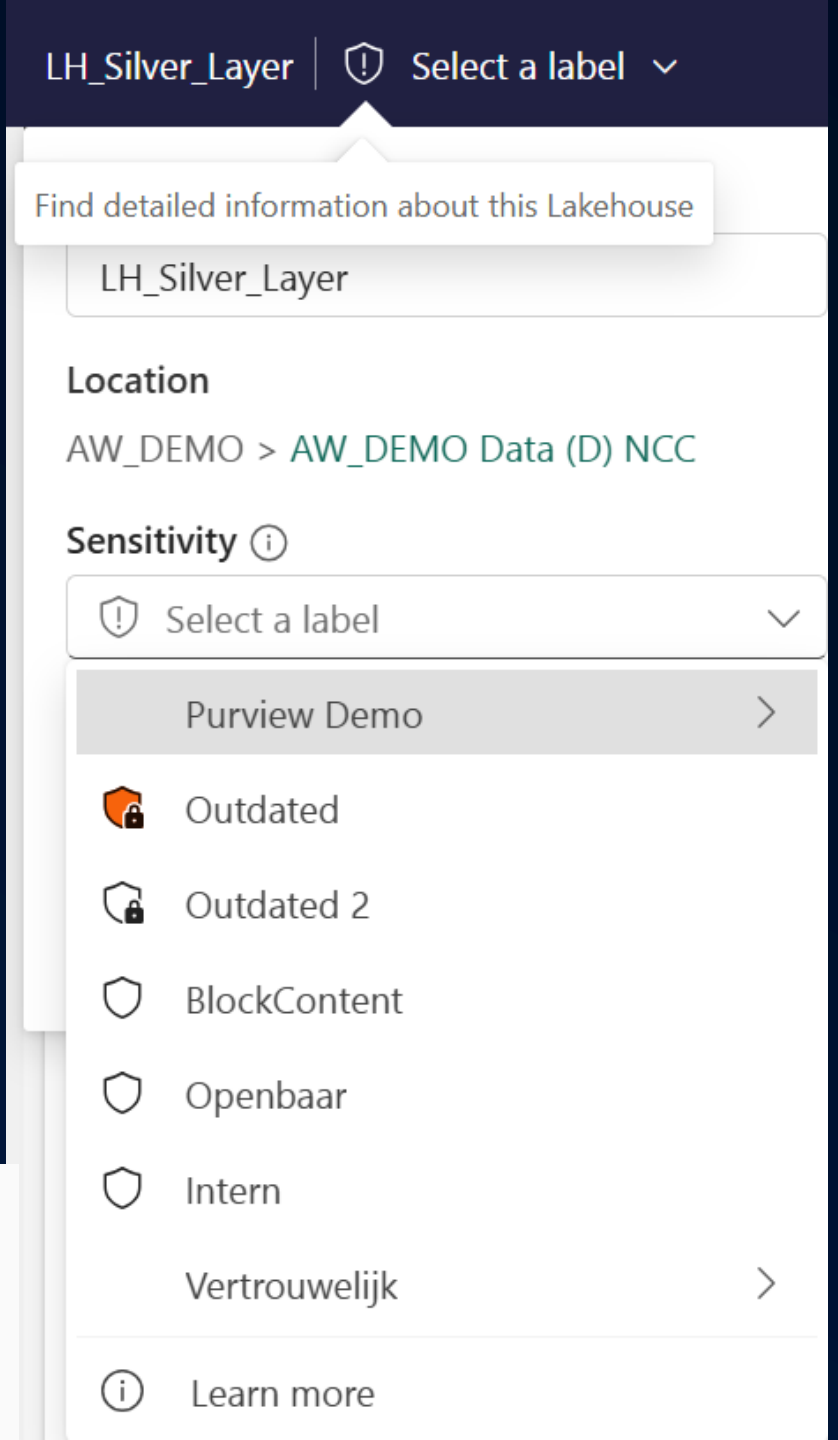
- MIP Labels in Office

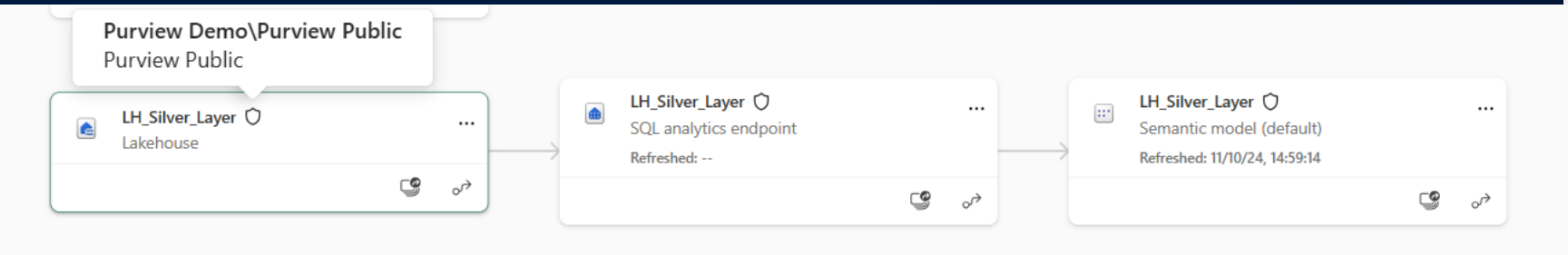




Purview Information Protection

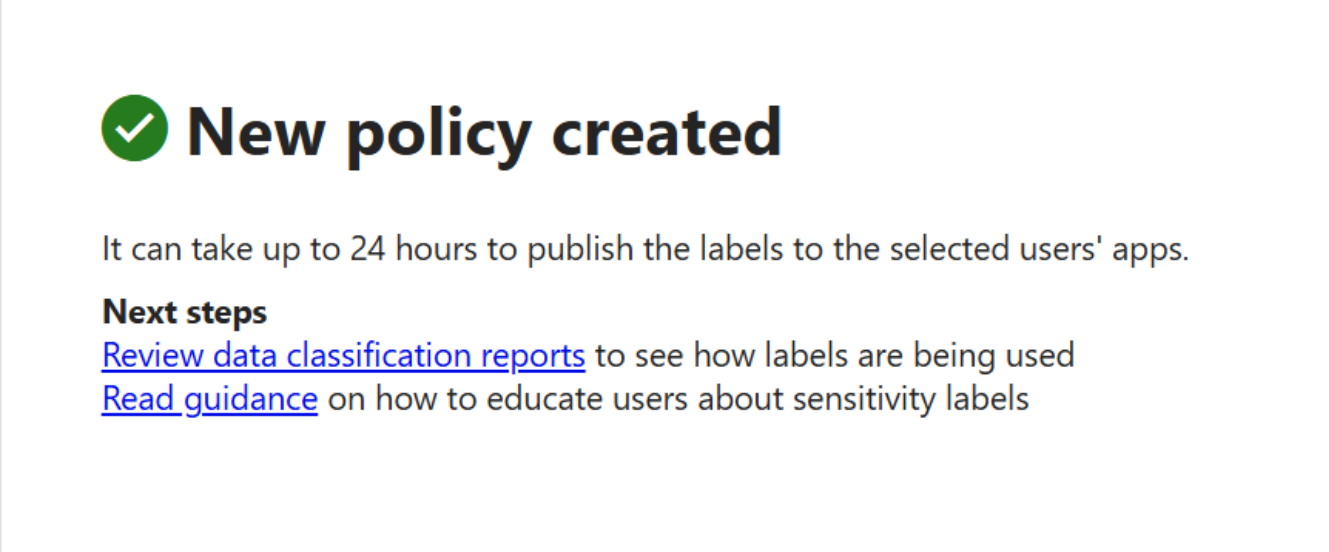
- MIP Labels in Office
- MIP Labels in Fabric
  - Inheritance of MIP labels in Fabric





Purview Information Protection

- Create labels
- Publish labels
- Make sure you use 3-5 labels(peopl
- Use clear names:
  - Confidential1 >>>Confidential – Inter
- 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 **labe**ls to downstream content
Enabled for the entire organization

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

Enabled

Restrict content with protected **labe**ls 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 **labe**l 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 **labe**ls for their domains (preview)
Disabled for the entire organization

Domain admins can set a default sensitivity **labe**l for their domains. The **labe**l they set will override your organization's default **labe**ls in Microsoft Purview, as long as it has a higher priority than the existing default **labe**ls set for your tenant. A domain's default **labe**l 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 **labe**ls for content
Enabled for the entire organization

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

Important: Sensitivity-**labe**l-based access control for Fabric and Power BI data and content is only enforced in the tenant where the **labe**ls were applied, in Power BI Desktop (.pbix) files, and in Excel, PowerPoint, and PDF files generated via supported export paths. Sensitivity-**labe**l-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 **labe**l 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 **labe**l 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 **labe**ls from data sources to their data in Power BI
Enabled for the entire organization

Only sensitivity **labe**ls from supported data sources will be applied. Please see the documentation for details about supported data sources and how their sensitivity **labe**ls 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.

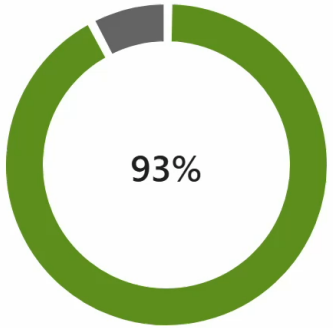
Reports

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.



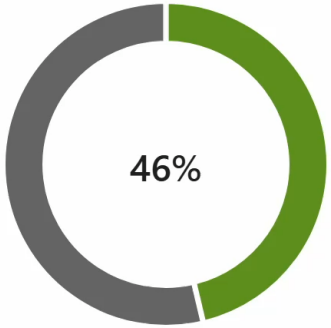
Microsoft 365 177

4 more

Explore protection policies

Sensitivity label coverage

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



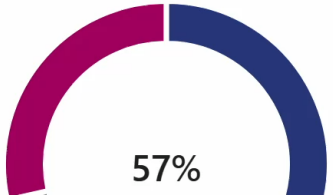
Labeled Not Labeled

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.



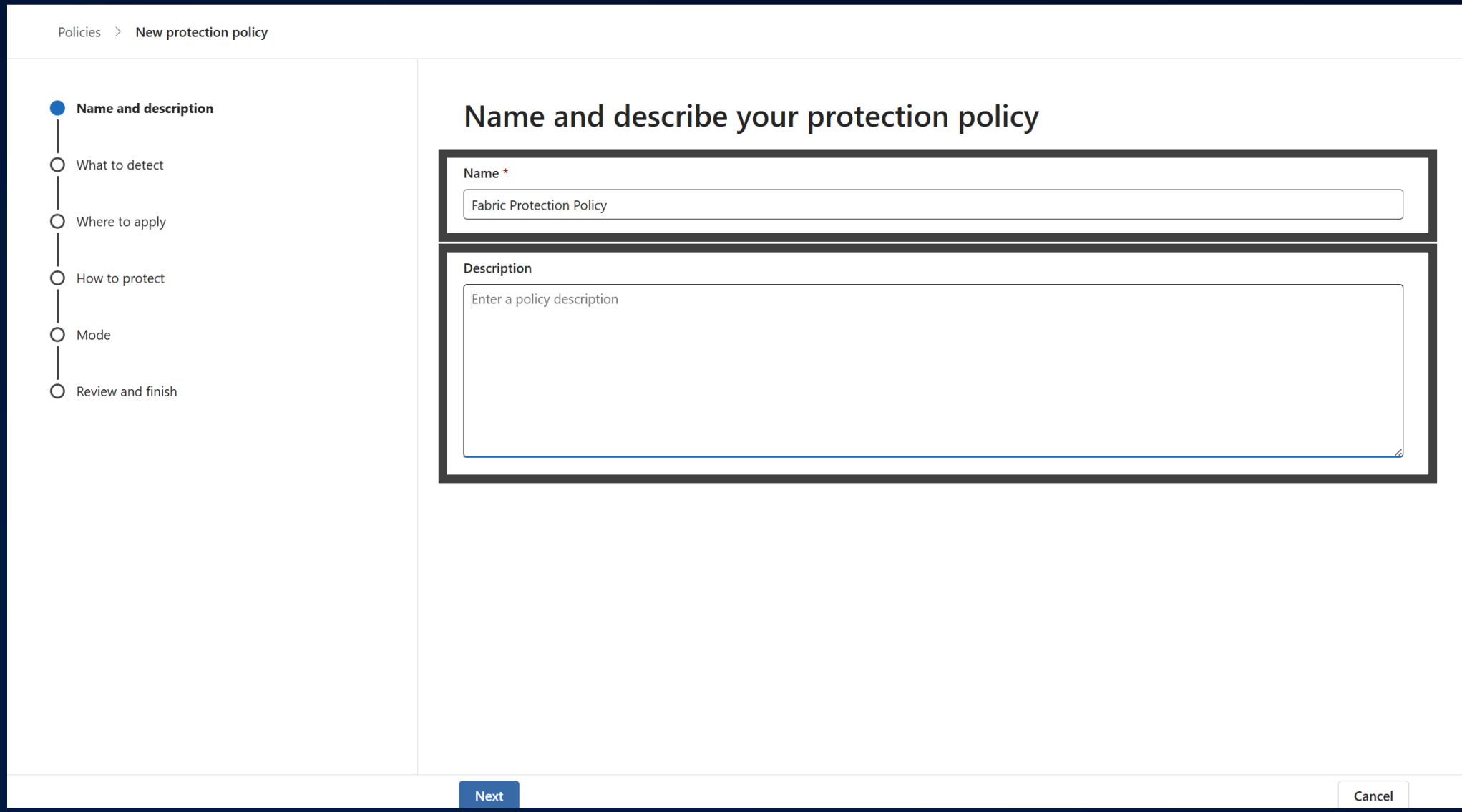
Azure 5
Microsoft 365 4
On premises

Demo

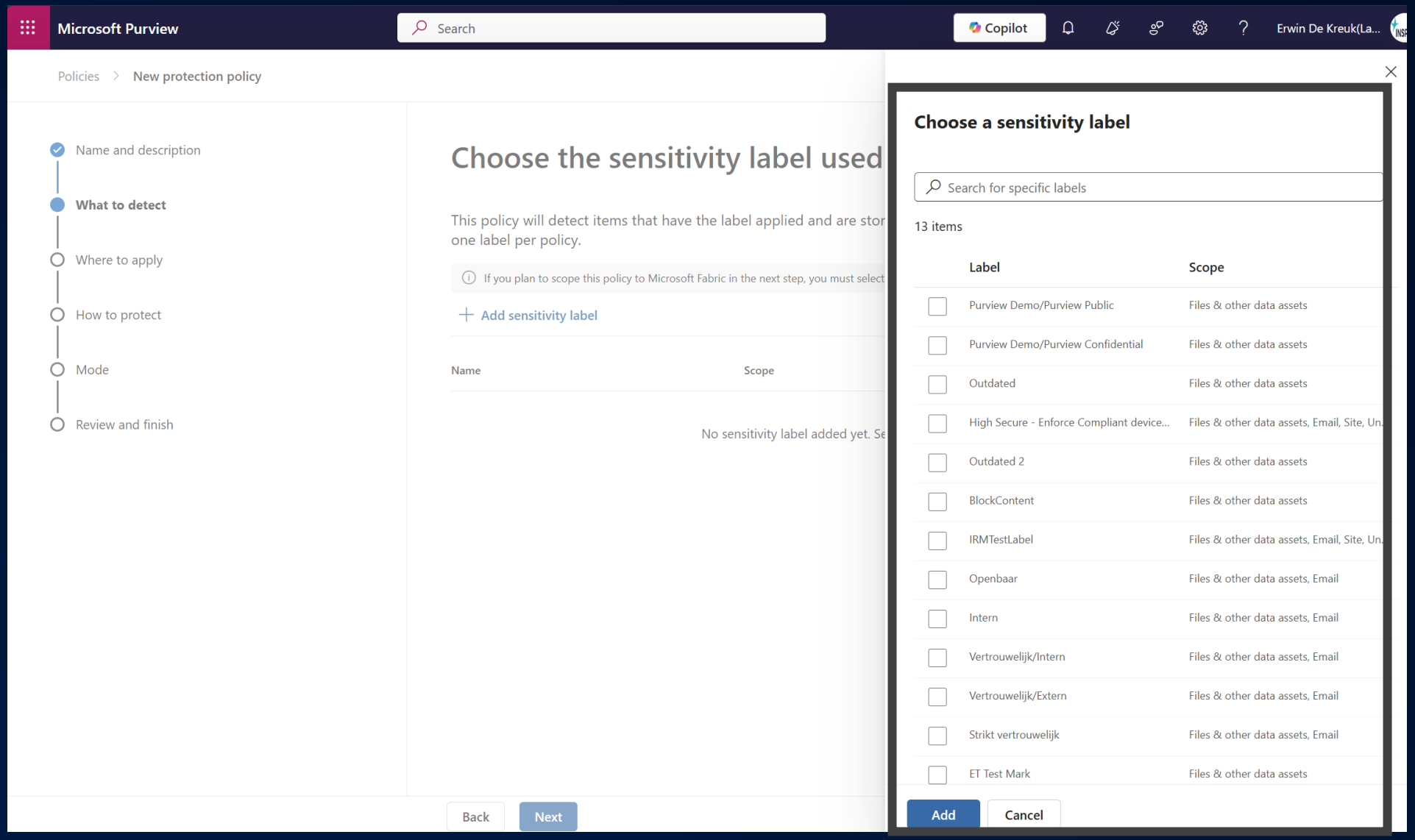
Labels

Purview Protection Policies

Purview Protection Policies



Purview Protection Policies



Purview Protection Policies

Policies > New protection policy

- Name and description
- What to detect
- **Where to apply**
- How to protect
- Mode
- Review and finish

Choose data sources to apply the policy

The policy will detect labeled items stored in the data sources you choose. Note that each source you include must have data policy enforcement turned on in the Data Map. Learn more about these data sources

	Location	Description	Scope	Actions
	Microsoft Fabric	Data engineering, factory, science, and warehouse	Turn on location to scope	
☐	Azure Storage	Azure Blob Storage, Azure Data Lake Gen 2	Turn on location to scope	
☐	Azure SQL Server	Azure SQL Database	Turn on location to	

Microsoft Fabric is unavailable because the label you selected doesn't have access control settings configured. If you want to scope this policy to Fabric, edit the label by assigning permissions in the 'Access control' setting.

Microsoft Fabric doesn't support policies that are applied to other data sources. To protect items in Microsoft Fabric, create a separate policy scoped only to that source.

Back | Next | Cancel

Purview Protection Policies

Policies > New protection policy

- Name and description
- What to detect
- **Where to apply**
- How to protect
- Mode
- Review and finish

Choose data sources to apply the policy

The policy will detect labeled items stored in the data sources you choose. Note that each source you include must have data policy enforcement turned on in the Data Map. Learn more about these data sources

	Location	Description	Scope	Actions
☑	Microsoft Fabric	Data engineering, factory, science, and warehouse	All workspaces	
	Azure Storage	Azure Blob Storage, Azure Data Lake Gen 2	Turn on location to scope	
	Azure SQL Server	Azure SQL Database	Turn on location to scope	

ⓘ Microsoft Fabric doesn't support policies that are applied to other data sources. To protect items in Microsoft Fabric, create a separate policy scoped only to that source.

Back | Next | Cancel

Purview Protection Policies

Policies > New protection policy

- Name and description
- What to detect
- Where to apply
- **How to protect**
- Mode
- Review and finish

Define access control settings

Except for the users and groups you add below, this policy will prevent everyone from accessing existing and future assets that have the label applied in data sources you specified. Learn more about these settings

Important: Ensure that any service principal accounts running Data Governance Scans for the scoped sources are included in a Security Group. Add this Security Group to the allowed list of your protection policies. This will prevent future scans from being blocked by access restrictions on labeled files.

Important. Allowing users and groups to retain specific access rights doesn't explicitly grant those rights to them. It simply means that they'll retain those rights if they already have them. In addition, these access control settins may be applied differently across Fabric items. Learn more about how access control is applied in Fabric

☐ Allow users to retain read access

Users and groups you add here won't be prevented from having read access to the labeled assets, provided they already have read permissions.

☐ Allow users to retain full control

Users and groups you add here won't be prevented from having full control of the labeled assets, provided they already have full control permissions. If they don't already have full control, they'll retain the current permissions they have.

Back | Next | Cancel

Purview Protection Policies

Policies > New protection policy

- Name and description
- What to detect
- Where to apply
- **How to protect**
- Mode
- Review and finish

Define access control settings

Except for the users and groups you add below, this policy will prevent everyone from accessing existing and future assets that have the label applied in data sources you specified. Learn more about these settings

Important: Ensure that any service principal accounts running Data Governance Scans for the scoped sources are included in a Security Group. Add this Security Group to the allowed list of your protection policies. This will prevent future scans from being blocked by access restrictions on labeled files.

Important. Allowing users and groups to retain specific access rights doesn't explicitly grant those rights to them. It simply means that they'll retain those rights if they already have them. In addition, these access control settins may be applied differently across Fabric items. Learn more about how access control is applied in Fabric

☑ **Allow users to retain read access**

Users and groups you add here won't be prevented from having read access to the labeled assets, provided they already have read permissions.

+ Add users and groups ✕ Remove all **2 users**

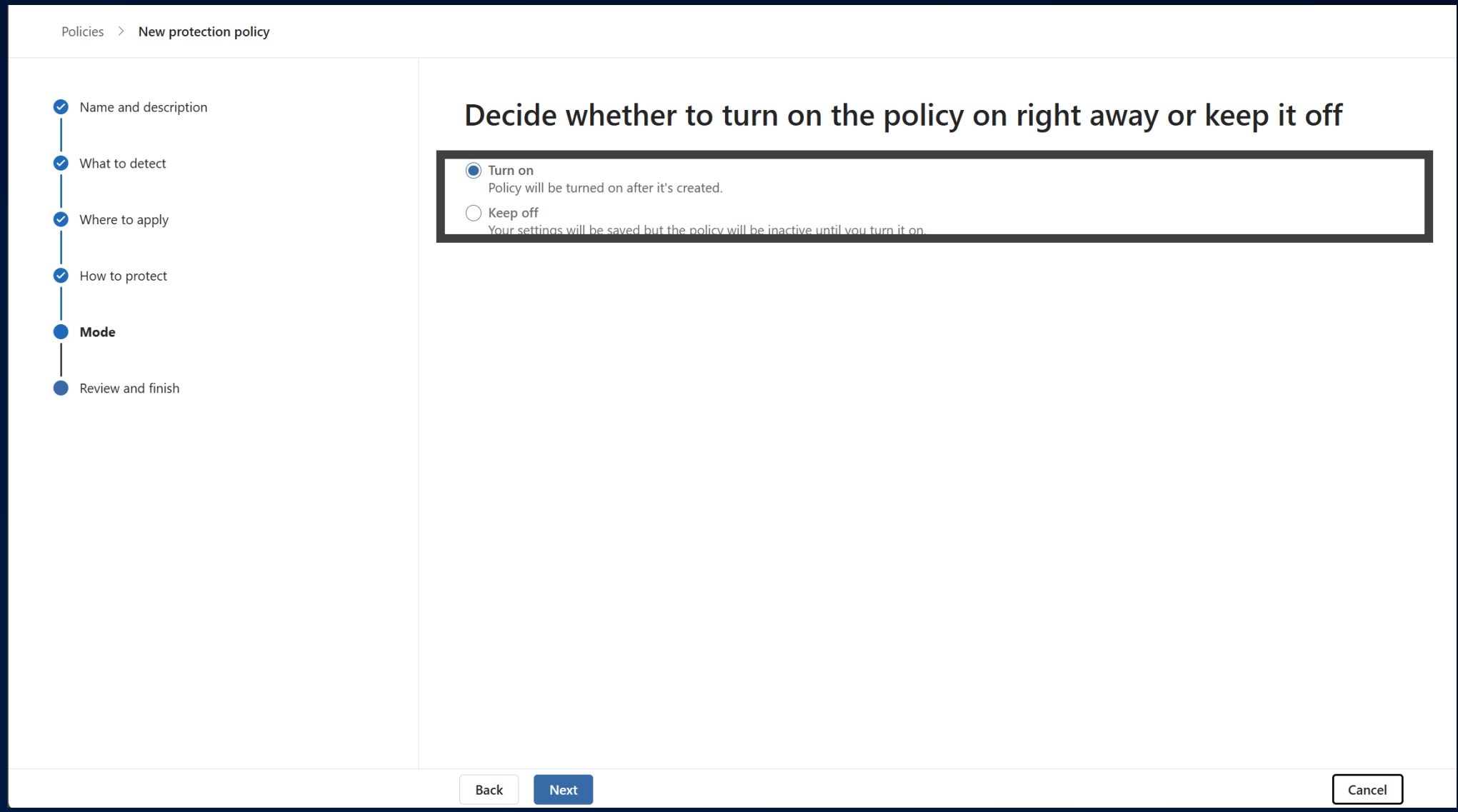
Name	Email address	
SG-FABRIC-ADMIN	ac0b3347-f637-4c58-8412-0155281c695b	✕
SG-FABRIC-CONTRIBUTOR	fec7309a-a272-43c2-8286-c828e27fd28c	✕

☐ Allow users to retain full control

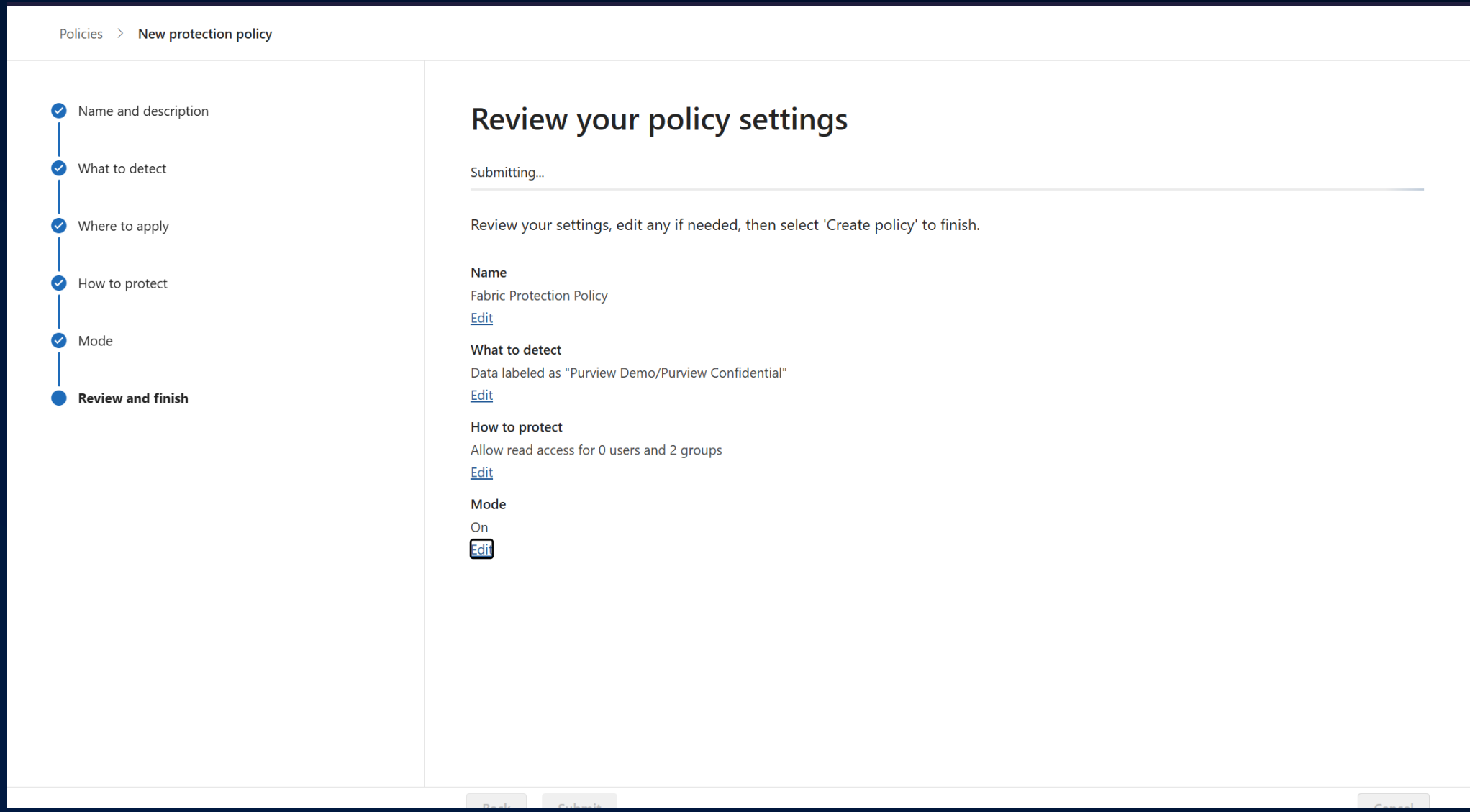
Users and groups you add here won't be prevented from having full control of the labeled assets, provided they already have full control permissions. If they don't already have full control, they'll retain the current permissions they have.

Back Next Cancel

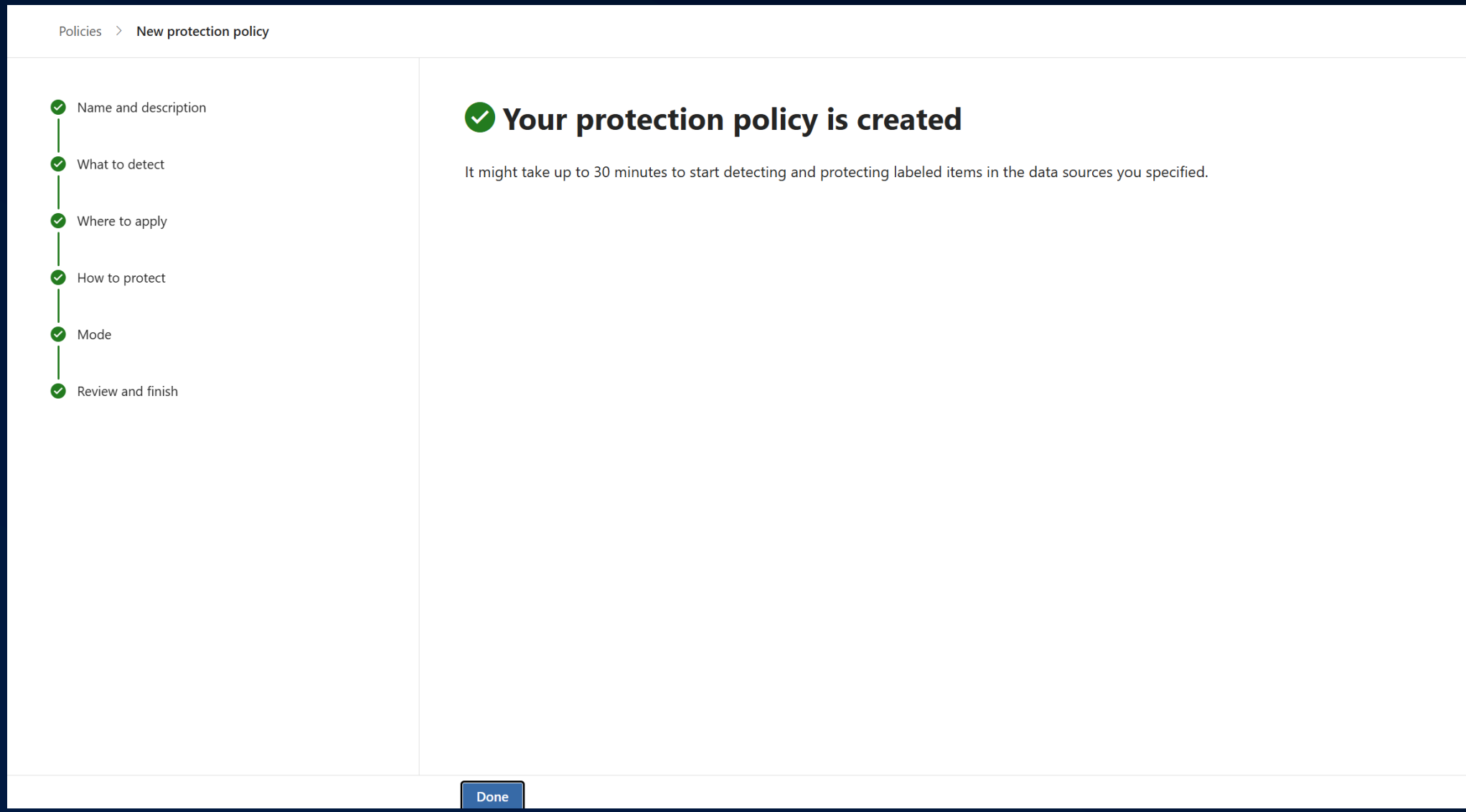
Purview Protection Policies



Purview Protection Policies



Purview Protection Policies

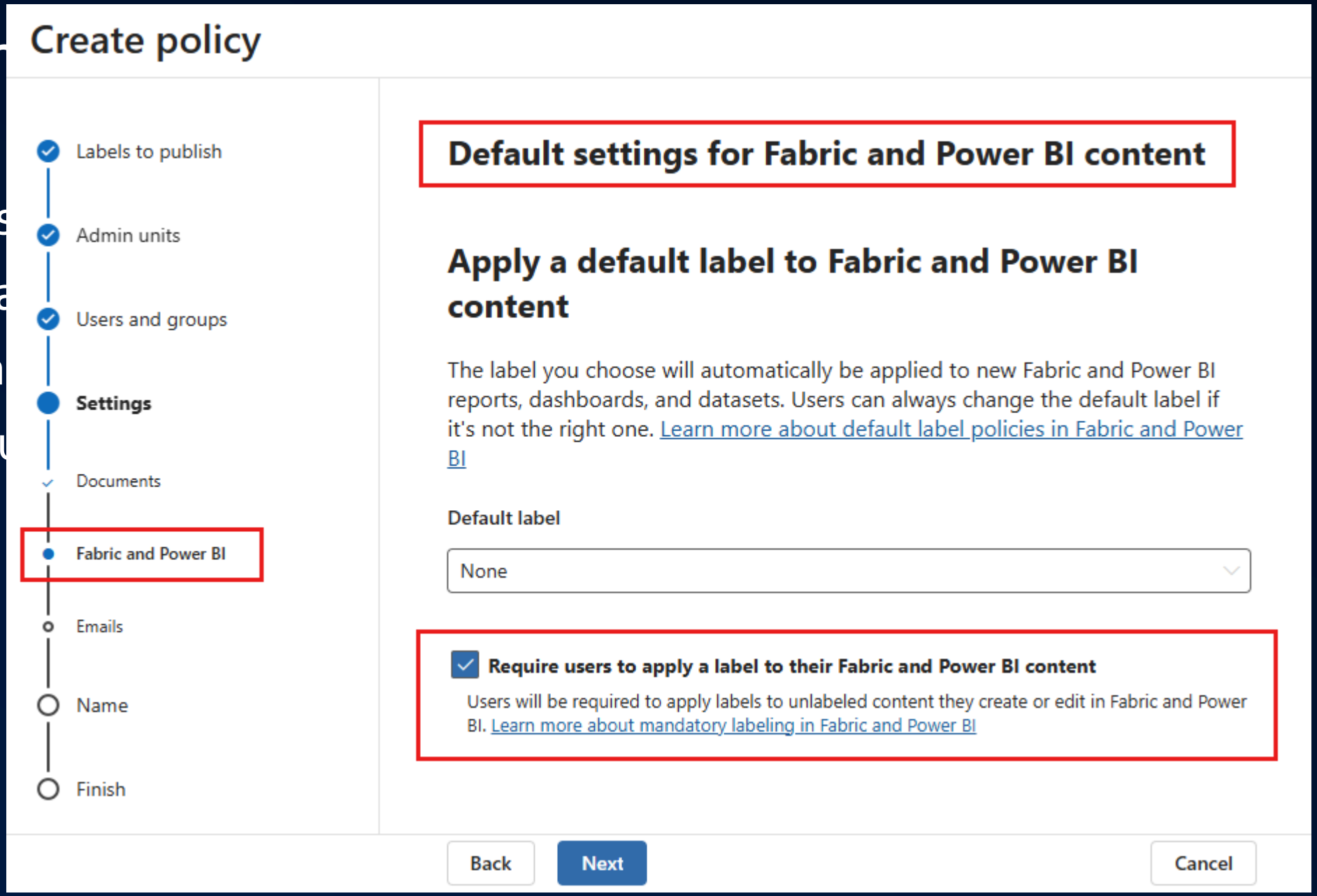


Purview Protection Policies

- Protection policies are useful in scenarios where organizations need to restrict access to sensitive items. For example, an organization might want to ensure that only specific internal users can access items labeled as "Confidential," while blocking access for everyone else.

Purview ar

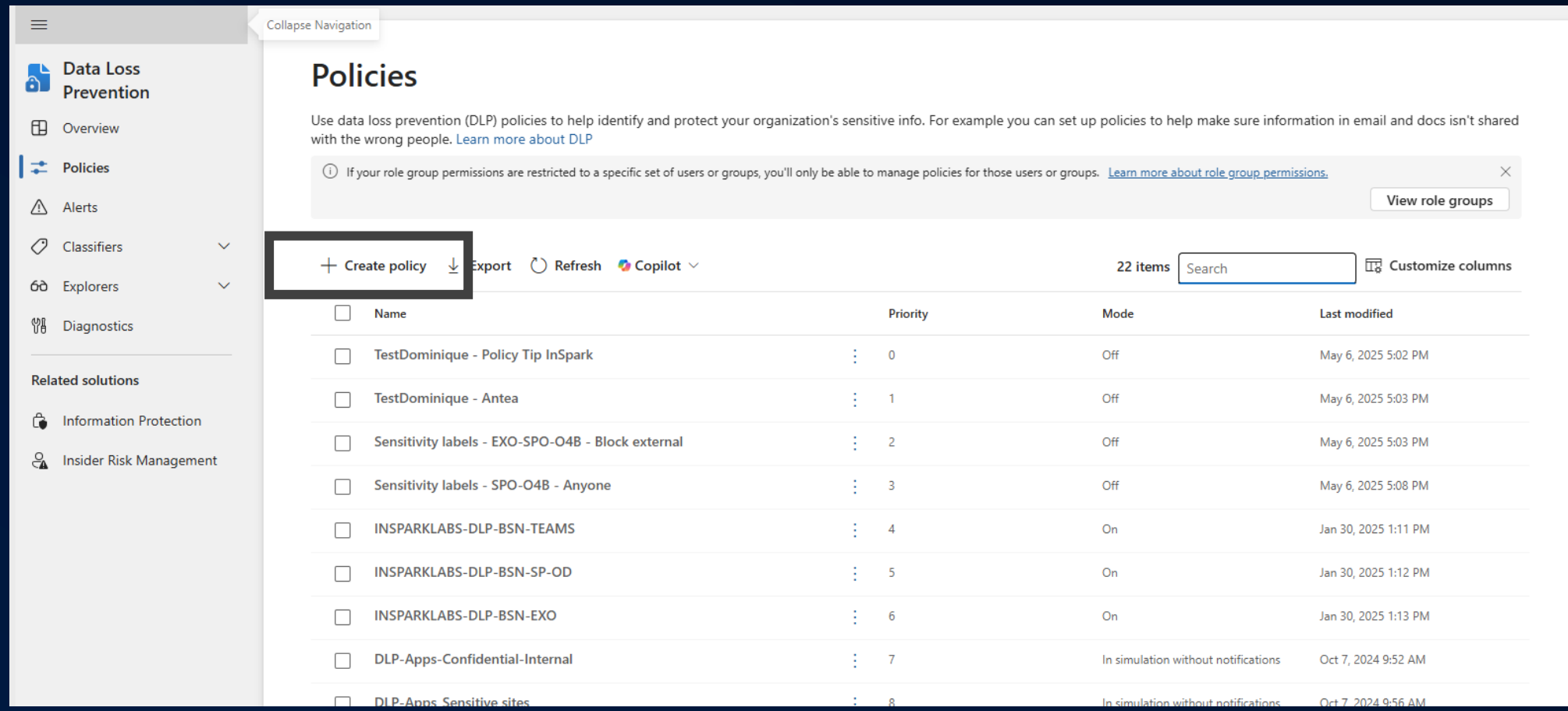
- Users **must** as
- DLP + automa
- API enforcem
- Domain-defau



Demo

Purview Data Loss Prevention

Purview Data Loss Prevention



Purview Data Loss Prevention

Data loss prevention > **Create policy**

- **Template or custom policy**
- Name
- Admin units
- Locations
- Policy settings
- Policy mode
- Finish

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

Enhanced templates currently aren't supported for following location(s): On-premises file repositories, Power BI, Azure Storage, Azure Sql Server, Aws S3, OpenAI ChatGPT, Google Gemini, Microsoft Copilot, DeepSeek

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates | All countries or regions

Categories

- Enhanced
- Financial
- Medical and health
- **Privacy**
- Custom

Regulations

- Australia Privacy Act Enhanced
- Australia Personally Identifiable Information (PII) Data
- Canada Personally Identifiable Information (PII) Data
- Canada Personal Information Protection Act (PIPA)
- Canada Personal Information Protection Act (PIPEDA)
- France Data Protection Act
- France Personally Identifiable Information (PII) Data
- **GDPR Enhanced**

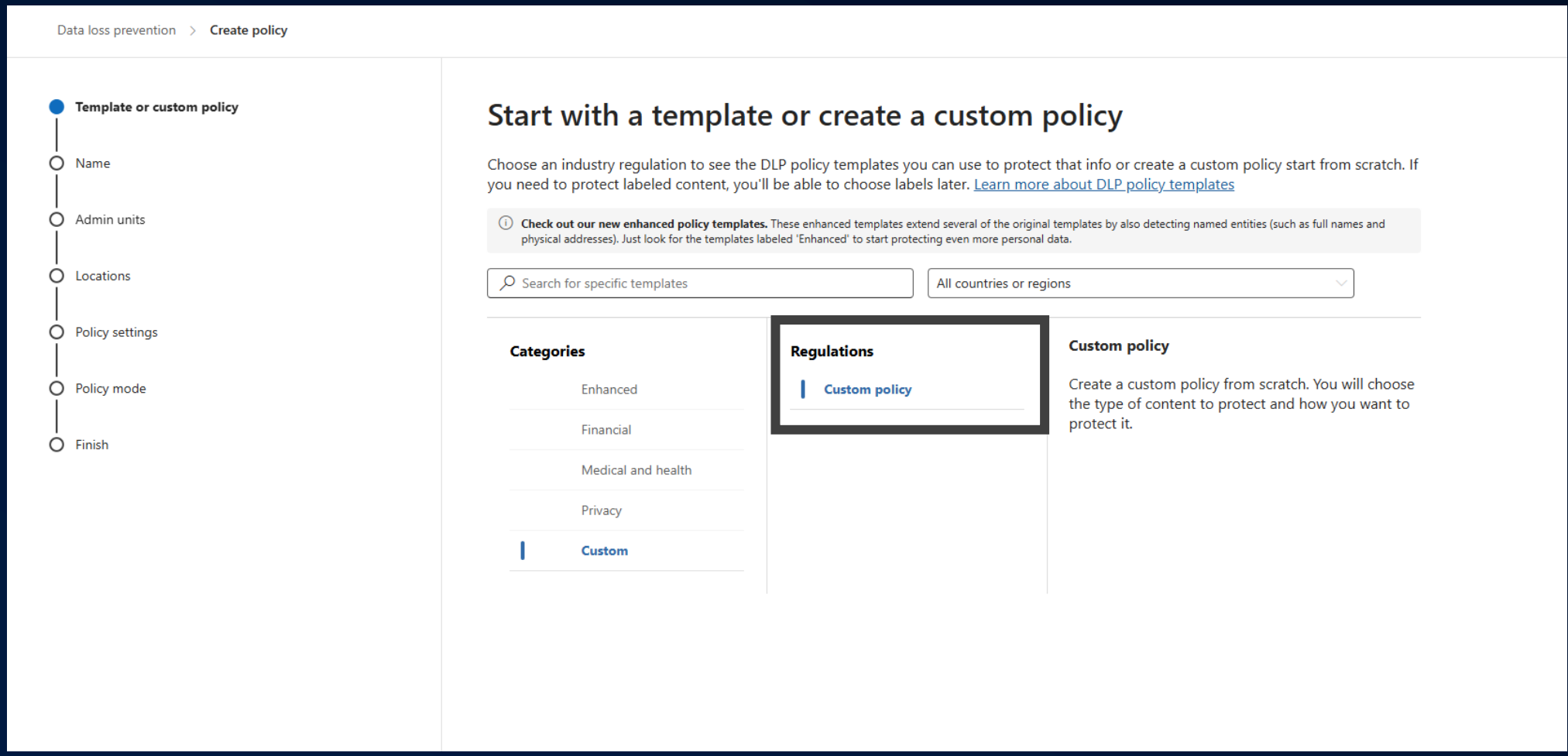
GDPR Enhanced

Helps detect the presence of personal information for individuals inside the European Union (EU) to assist in meeting GDPR privacy obligations. This enhanced template extends the original by also detecting people's full names and physical addresses for countries in the EU. We have enhanced it with Trainable Classifiers HR, Tax, Healthcare, and Legal Affairs to detect documents containing healthcare, tax fillings, legal terminology and HR records.

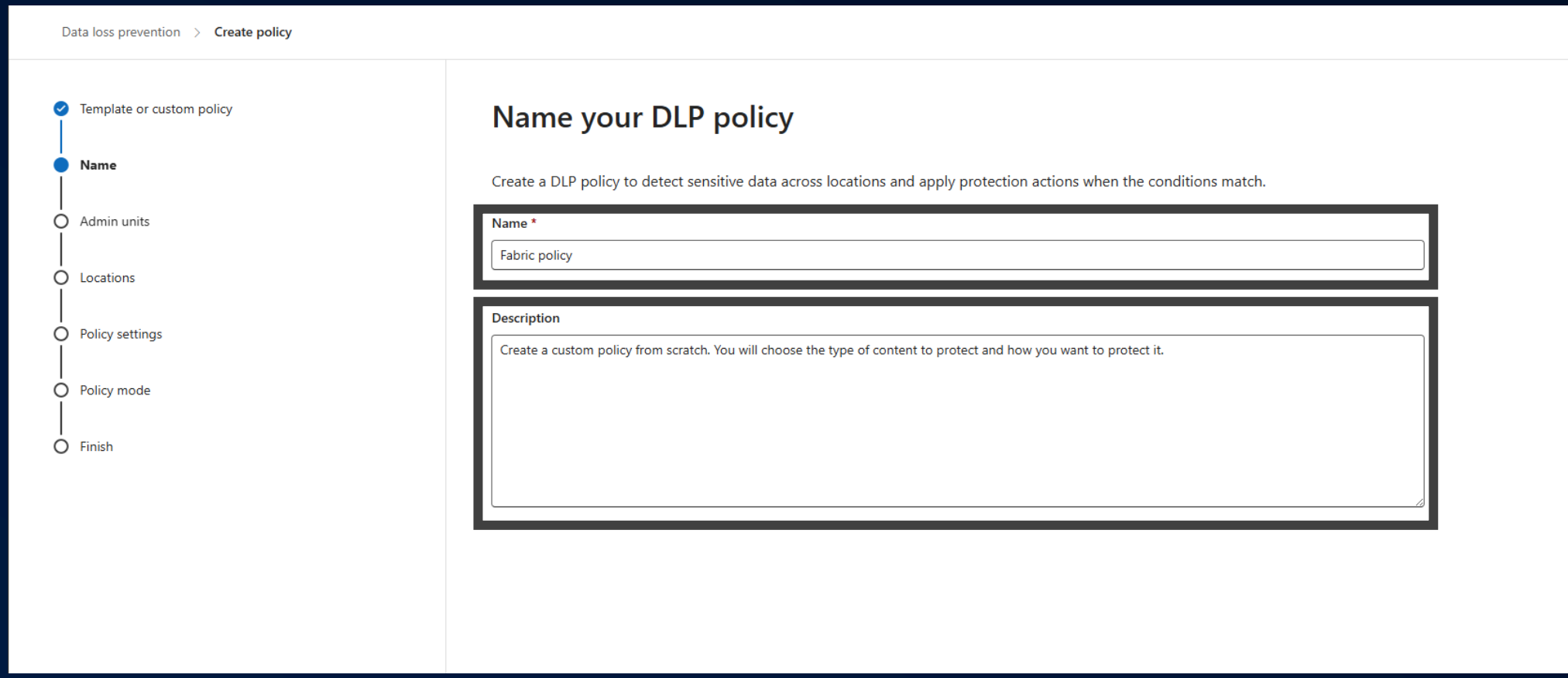
Protect this information:

- Business - HR
- Business - Tax
- Health/Medical Forms
- Employee disciplinary action files
- Invoice
- Business - Healthcare
- Legal Affairs
- Agreements

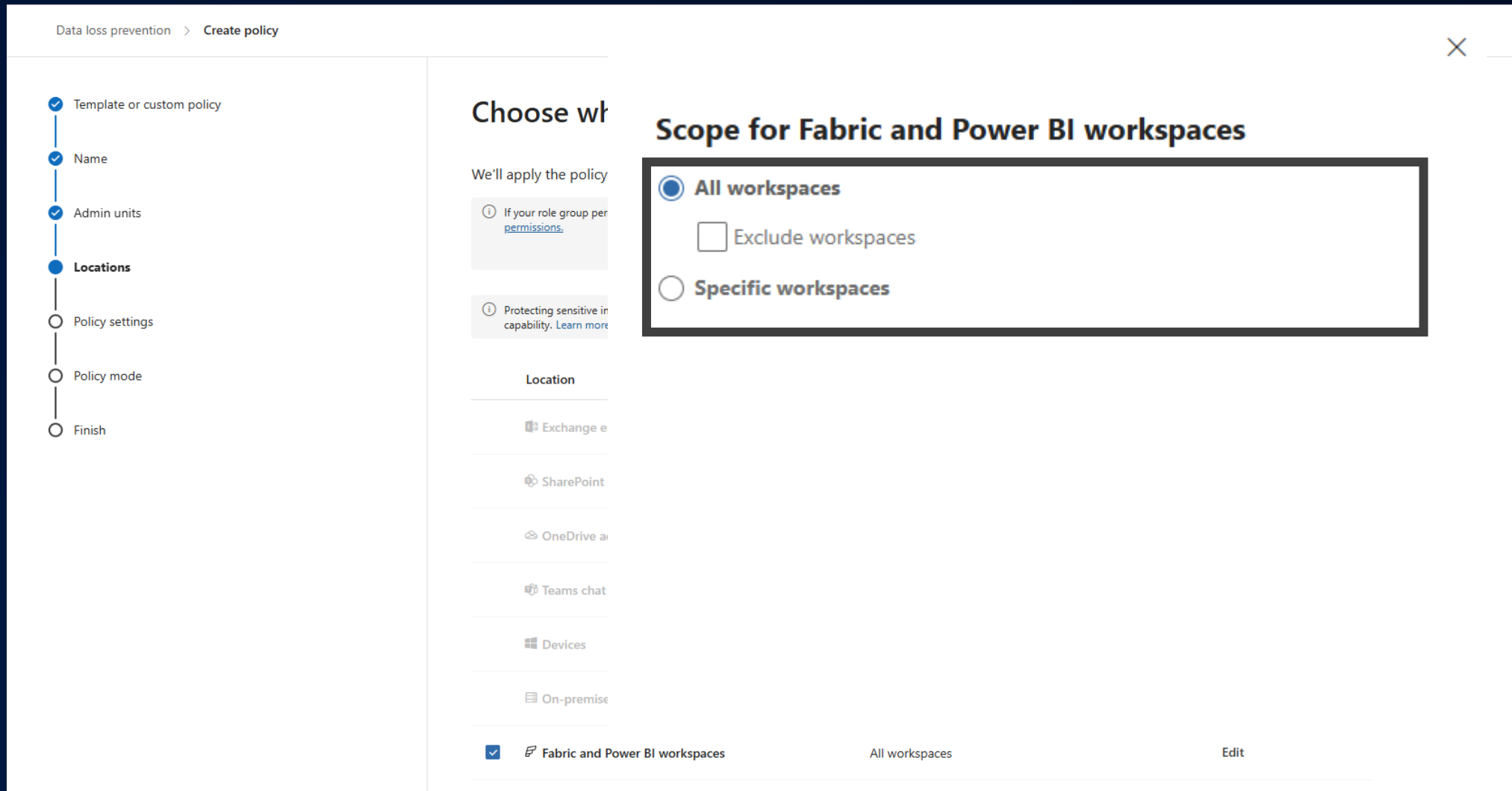
Purview Data Loss Prevention



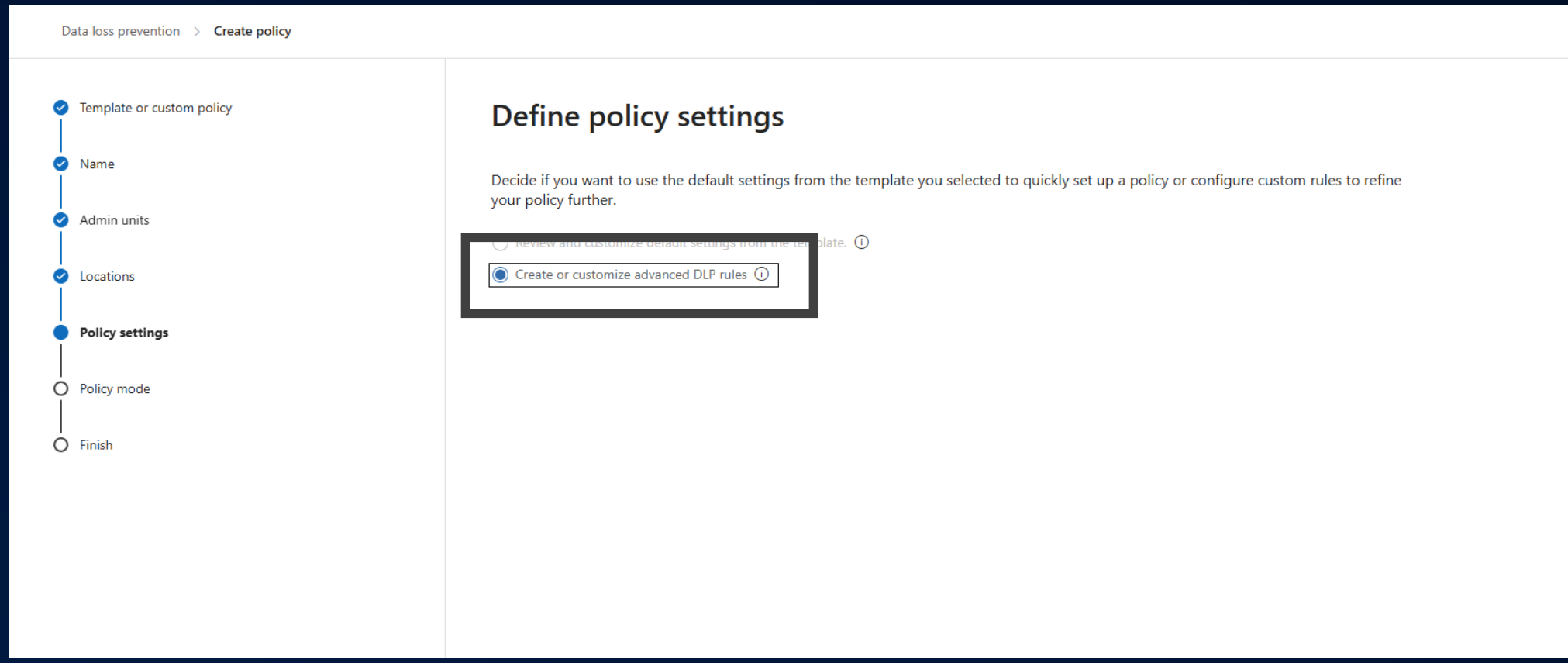
Purview Data Loss Prevention



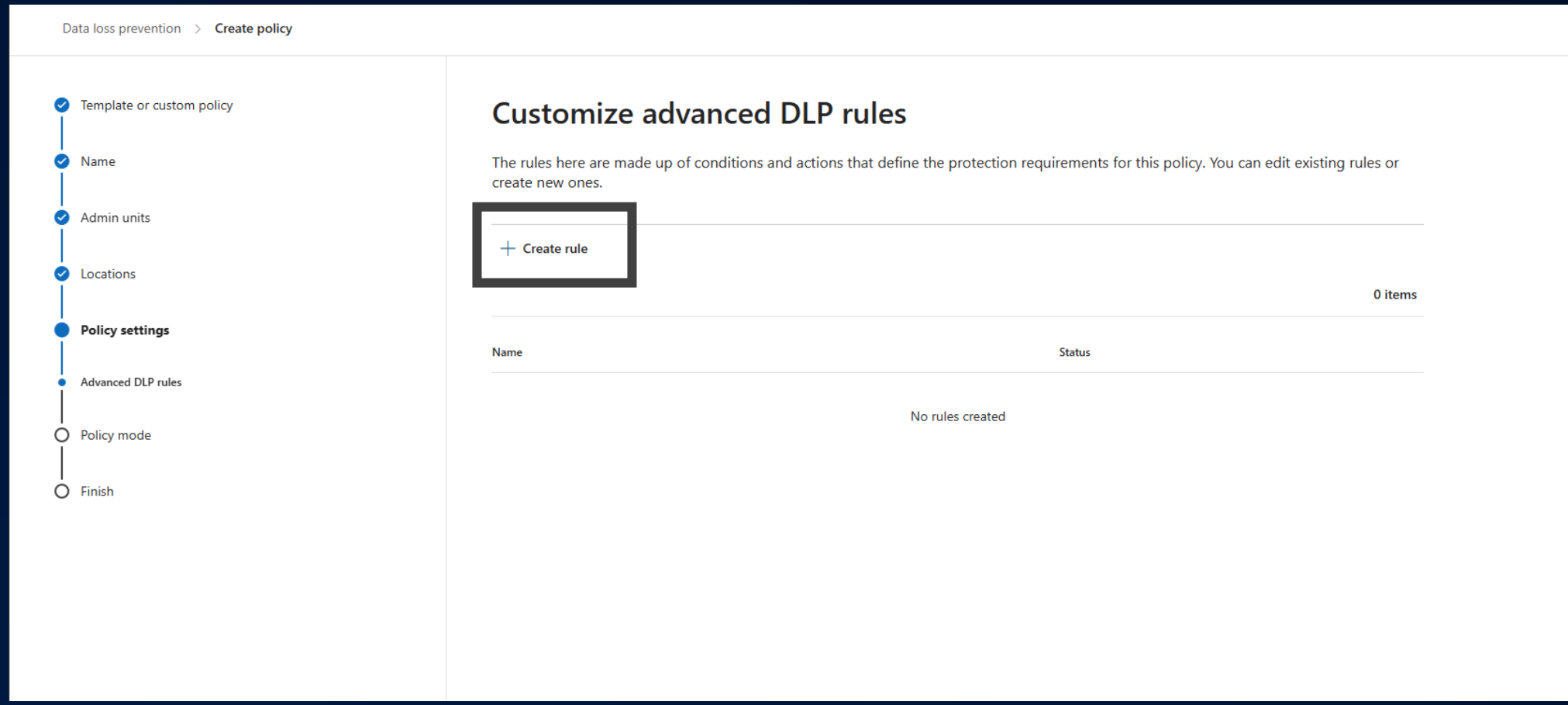
Purview Data Loss Prevention



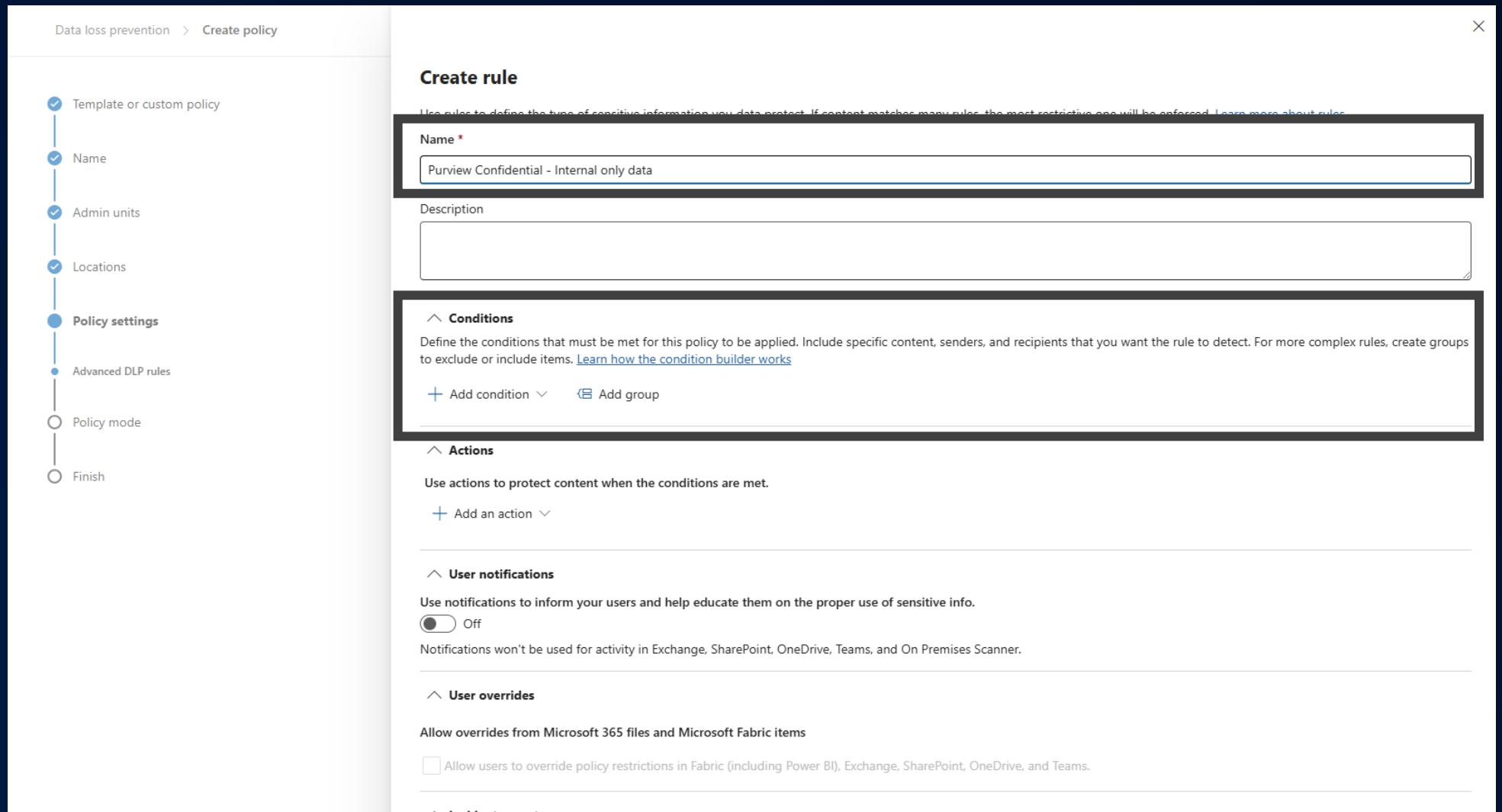
Purview Data Loss Prevention



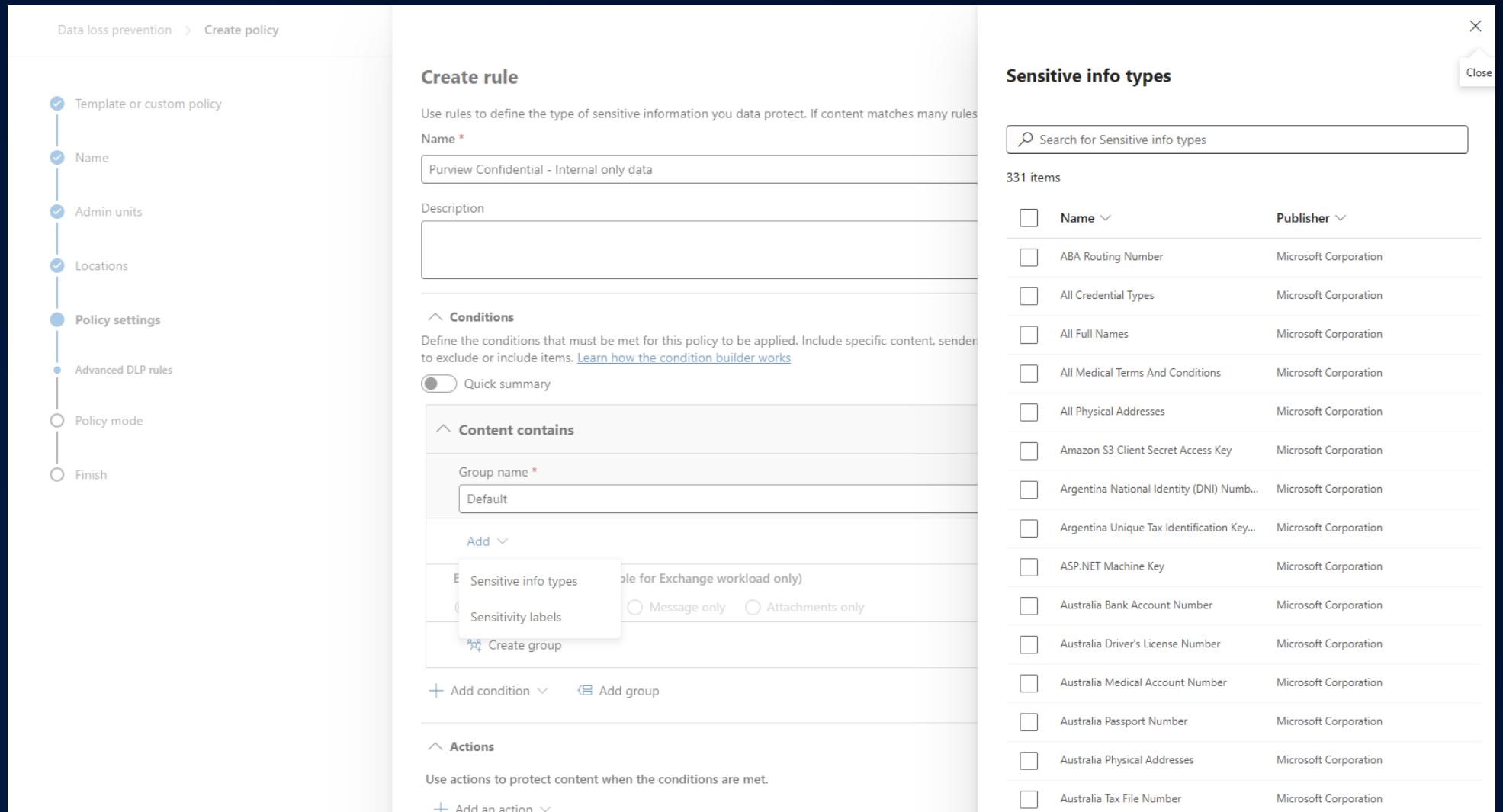
Purview Data Loss Prevention



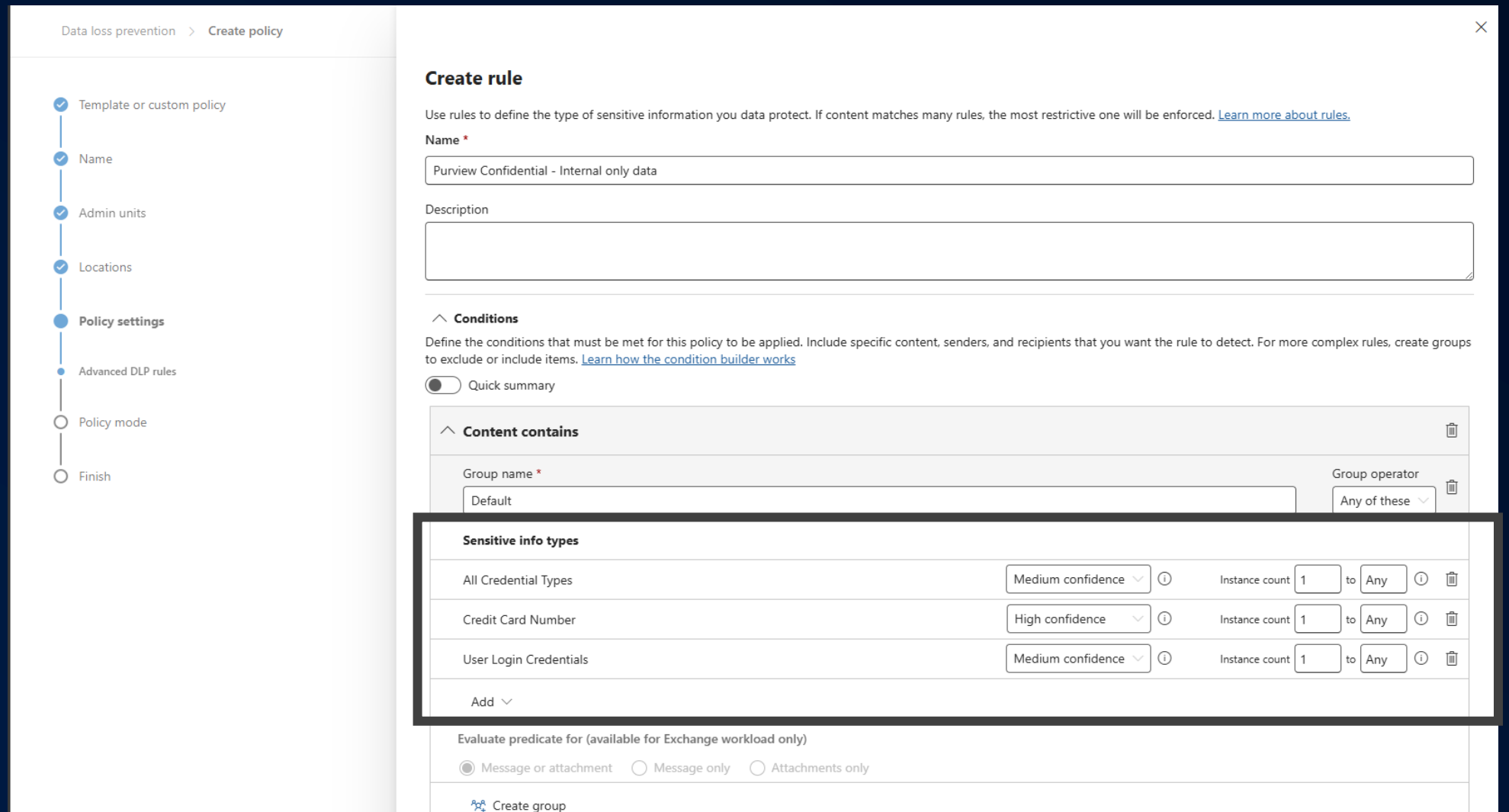
Purview Data Loss Prevention



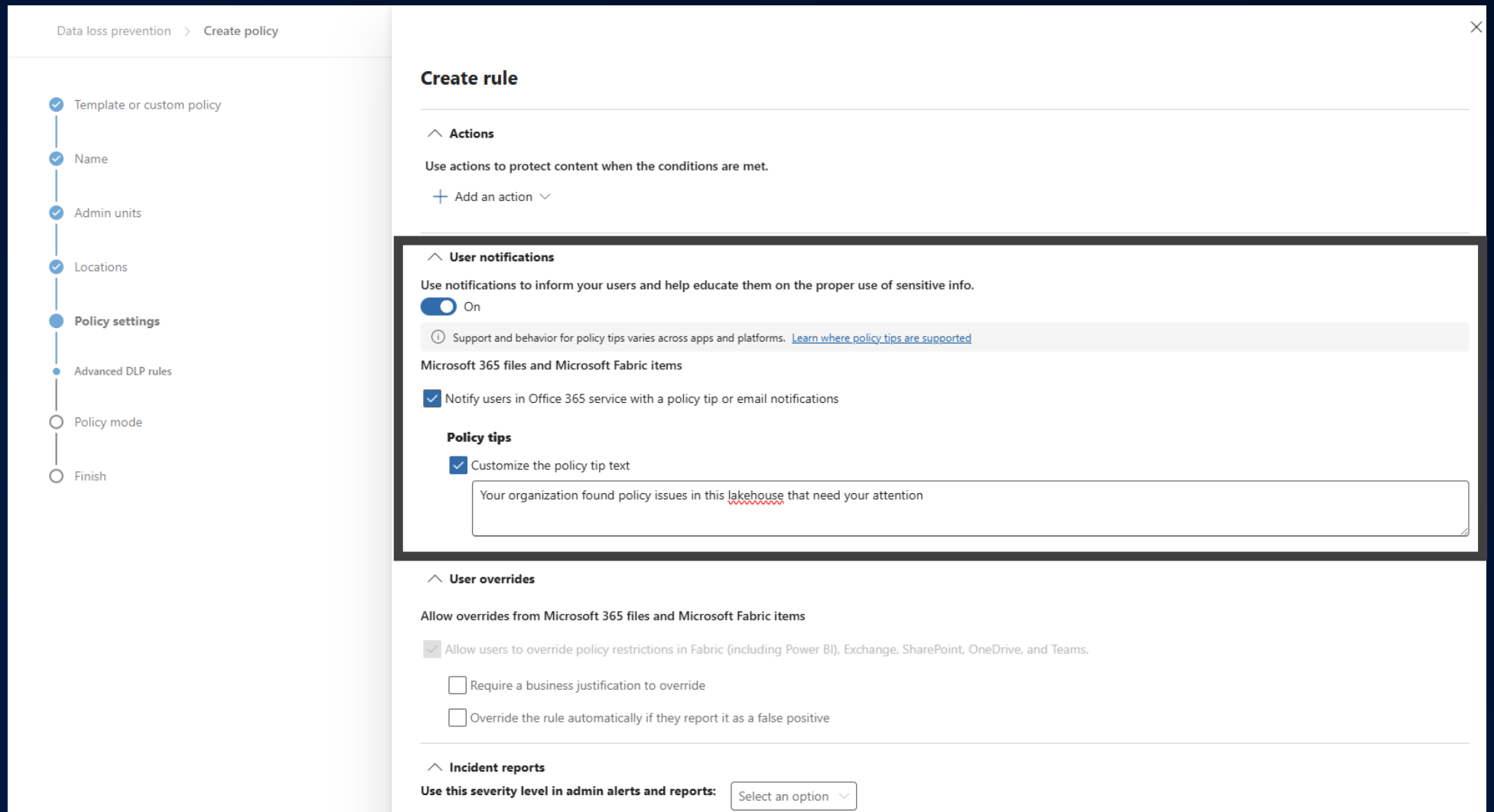
Purview Data Loss Prevention



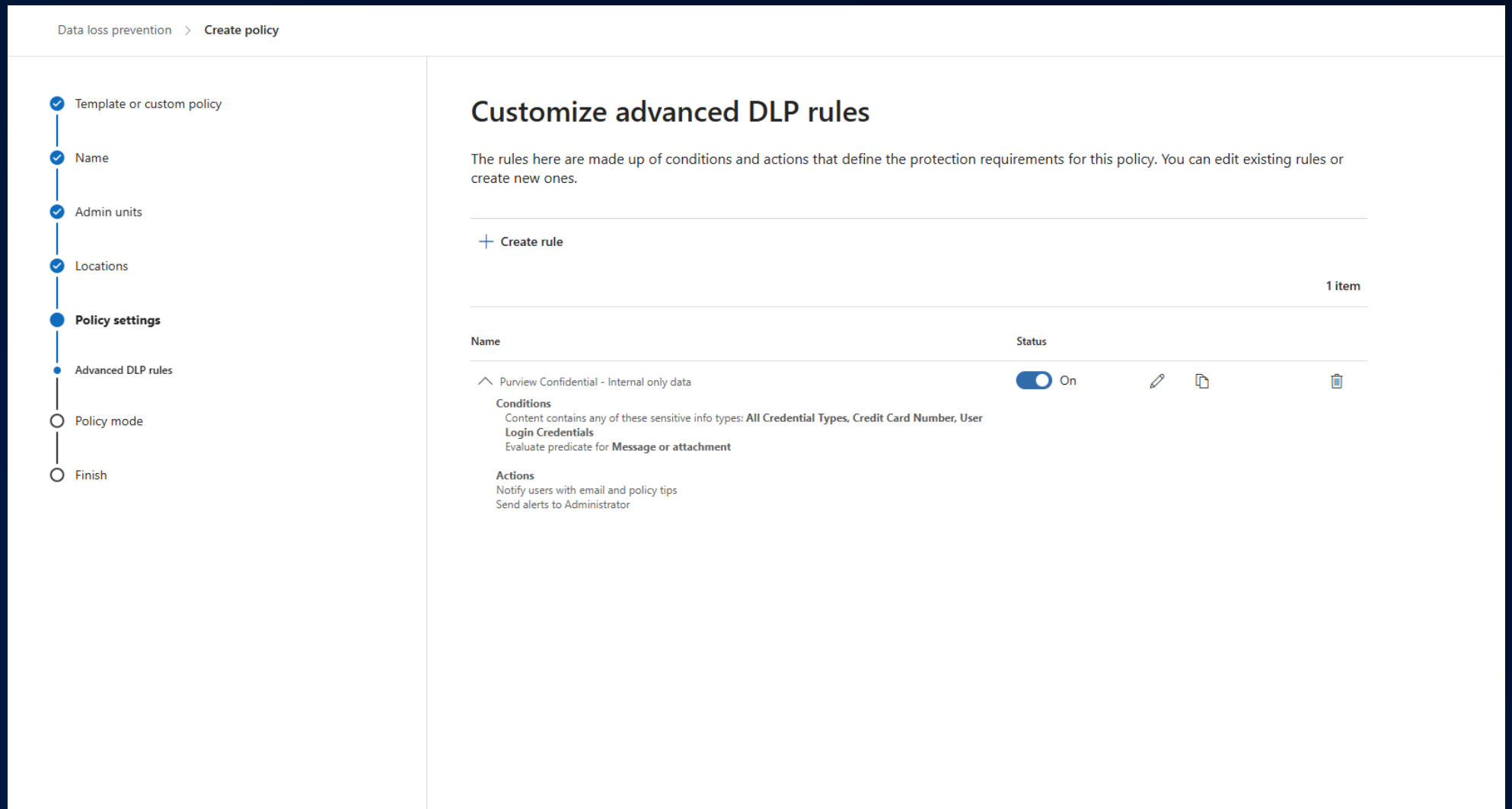
Purview Data Loss Prevention



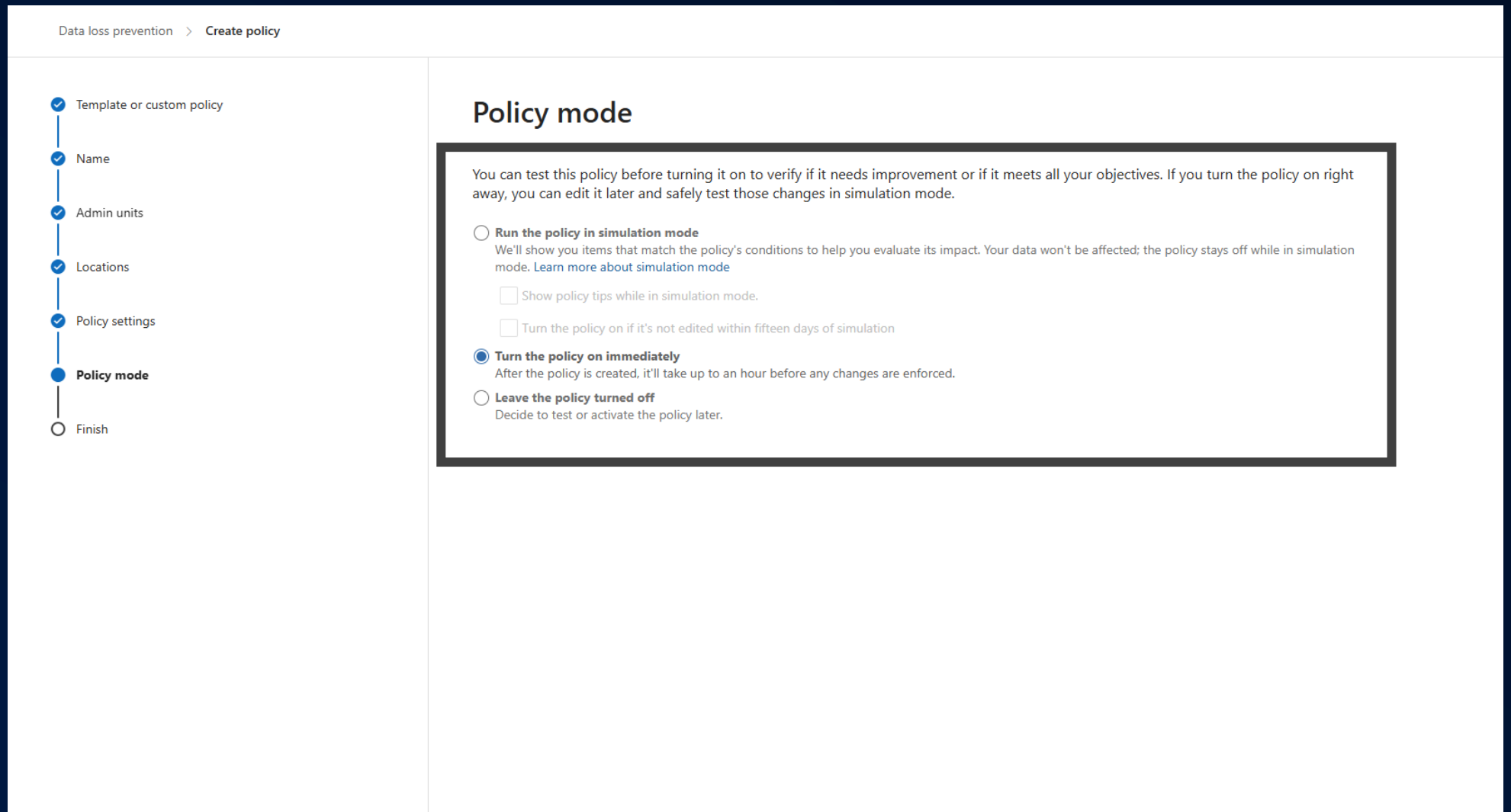
Purview Data Loss Prevention



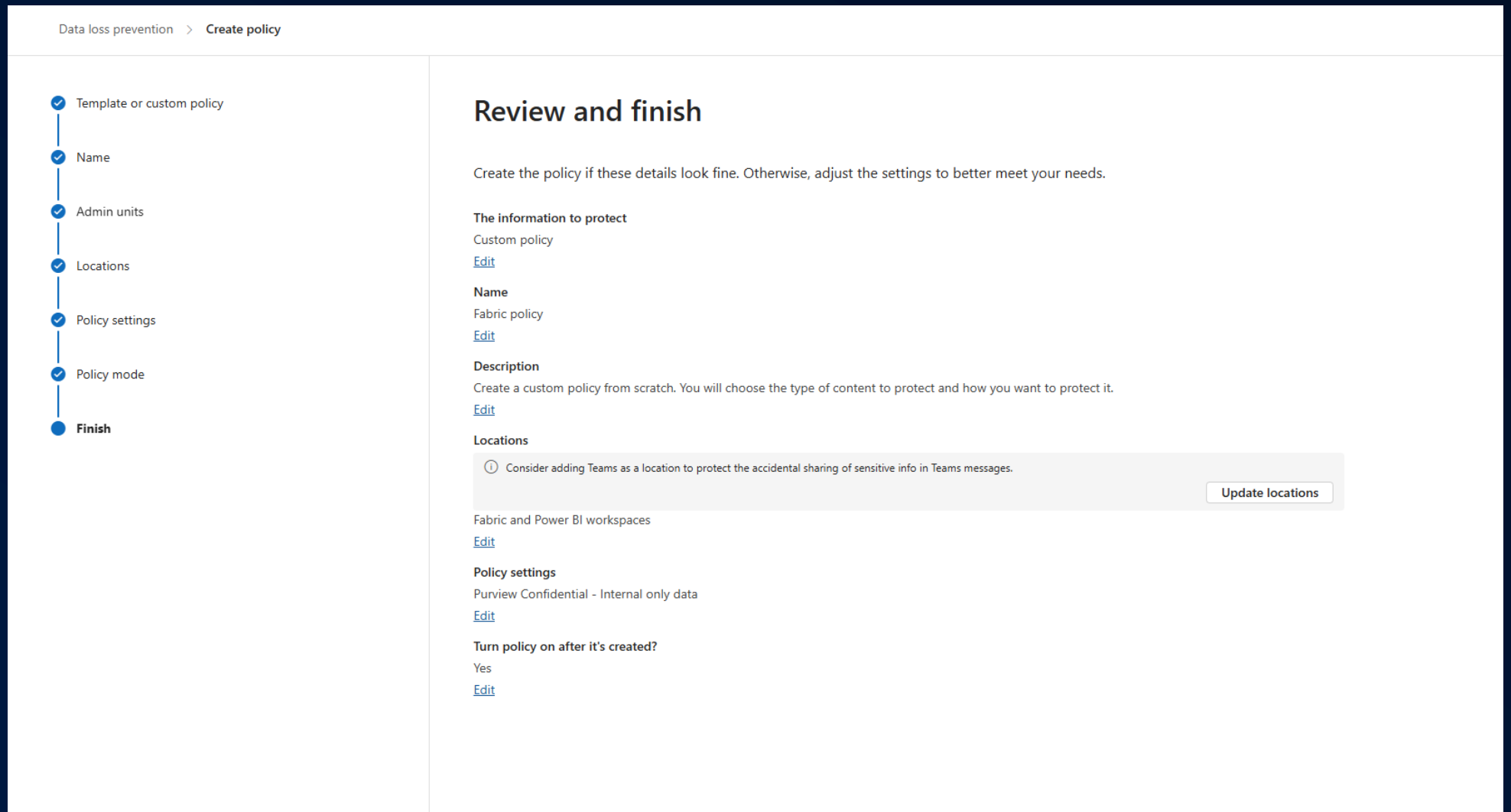
Purview Data Loss Prevention



Purview Data Loss Prevention



Purview Data Loss Prevention



Purview Data Loss Prevention

Data loss prevention > **Edit policy**

- Name
- Admin units
- Locations
- Advanced DLP rules
- Policy mode
- Finish

Policy updated

Data loss prevention policy has been updated.

Next steps

Monitor alerts to review policy matches. Learn about reviewing alerts

RECOMMENDATION

You're protecting this sensitive data, now make sure it's deleted when no longer relevant to your organization.

Removing unnecessary or obsolete data can reduce your risk during a security incident. Use auto-labeling policies in Data Lifecycle Management to help minimize your attack surface.

Secure Now

Related tasks

Create an insider risk policy to investigate and take action on insider risks and threats.	Get started
Create a records management policy to automatically retain or delete sensitive content	Get started
Create a communication compliance policy to detect inappropriate content in messages Permission required	Learn more

Demo

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

From Insight to Oversight: Securing Power BI with Purview

From Insight to Oversight: Securing Power BI with Purview