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




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.

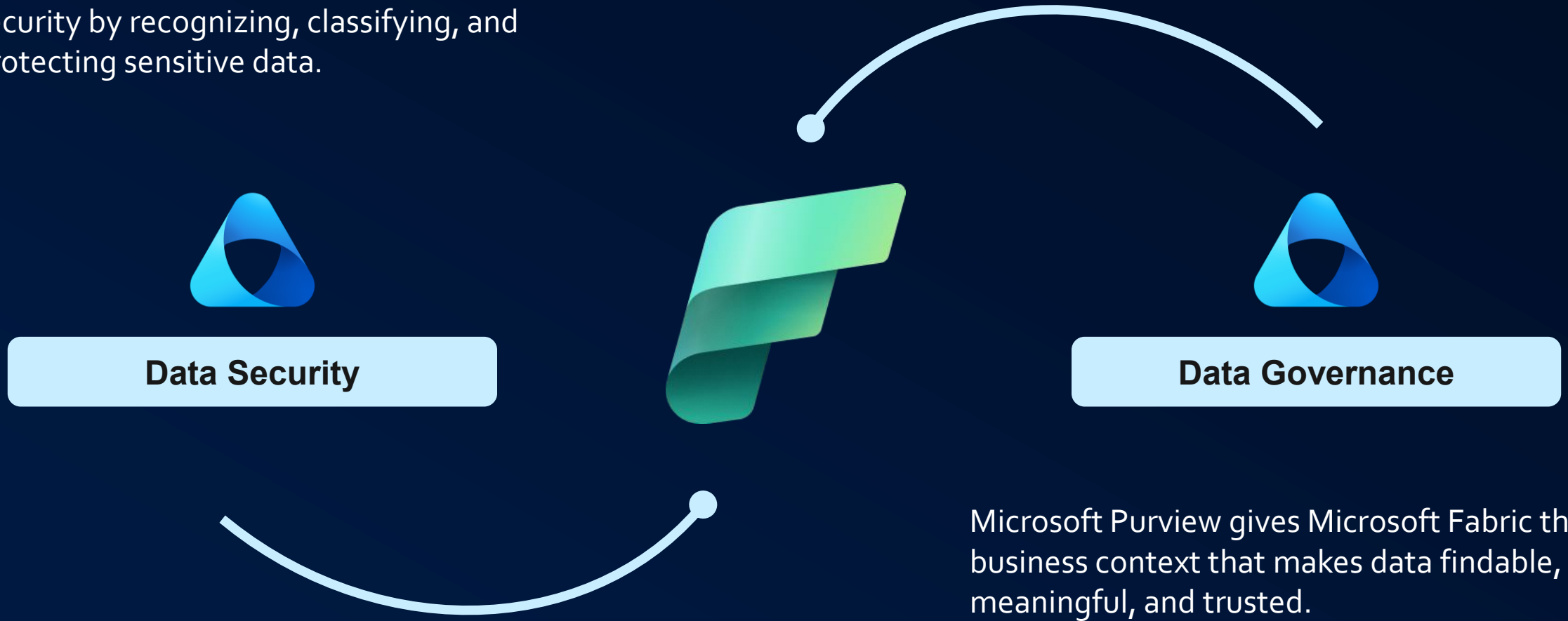
Agenda



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

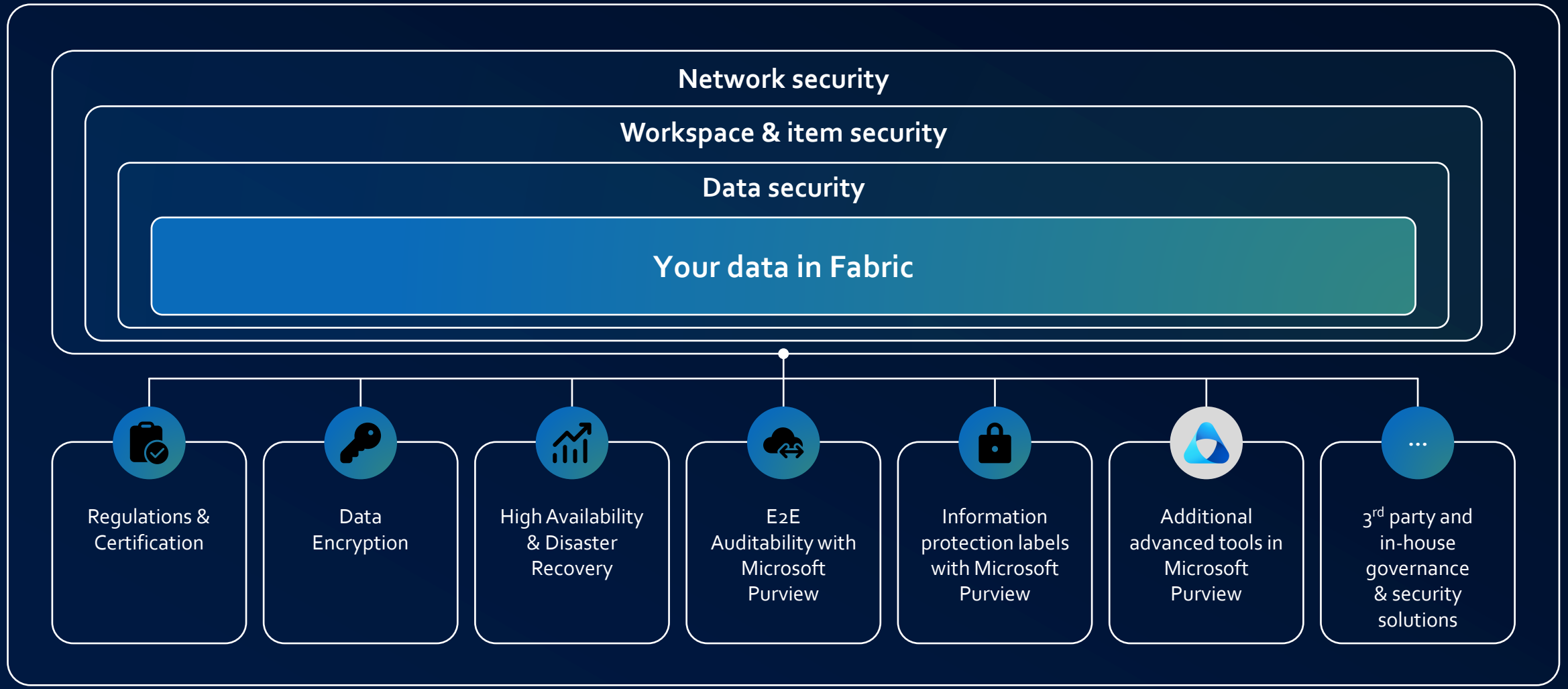
Microsoft Fabric & Microsoft better together

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

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

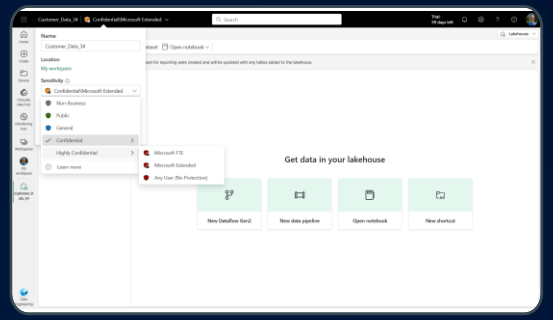
- Compliance Manager
- eDiscovery and Audit
- Communication Compliance
- Data Lifecycle Management
- Records Management

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

Shared platform capabilities

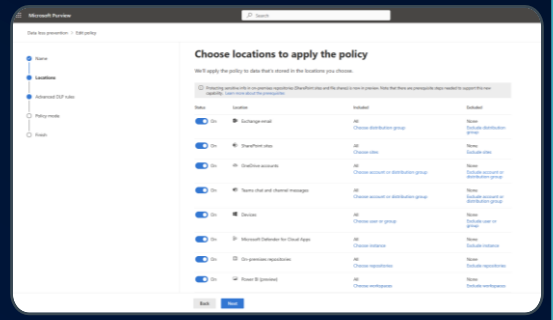
AI-based efficiency, Data Map, Classification, Labels, Audit Logs, Policies, Data Connectors

Purview Data Security & Compliance integration with Fabric



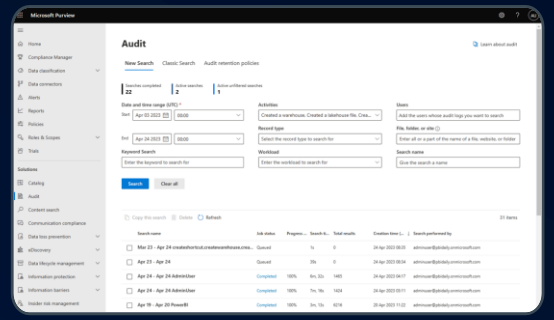
Information protection sensitivity labels and protection policies

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.



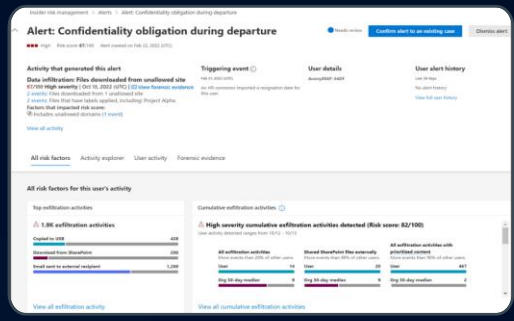
Data loss prevention policies

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

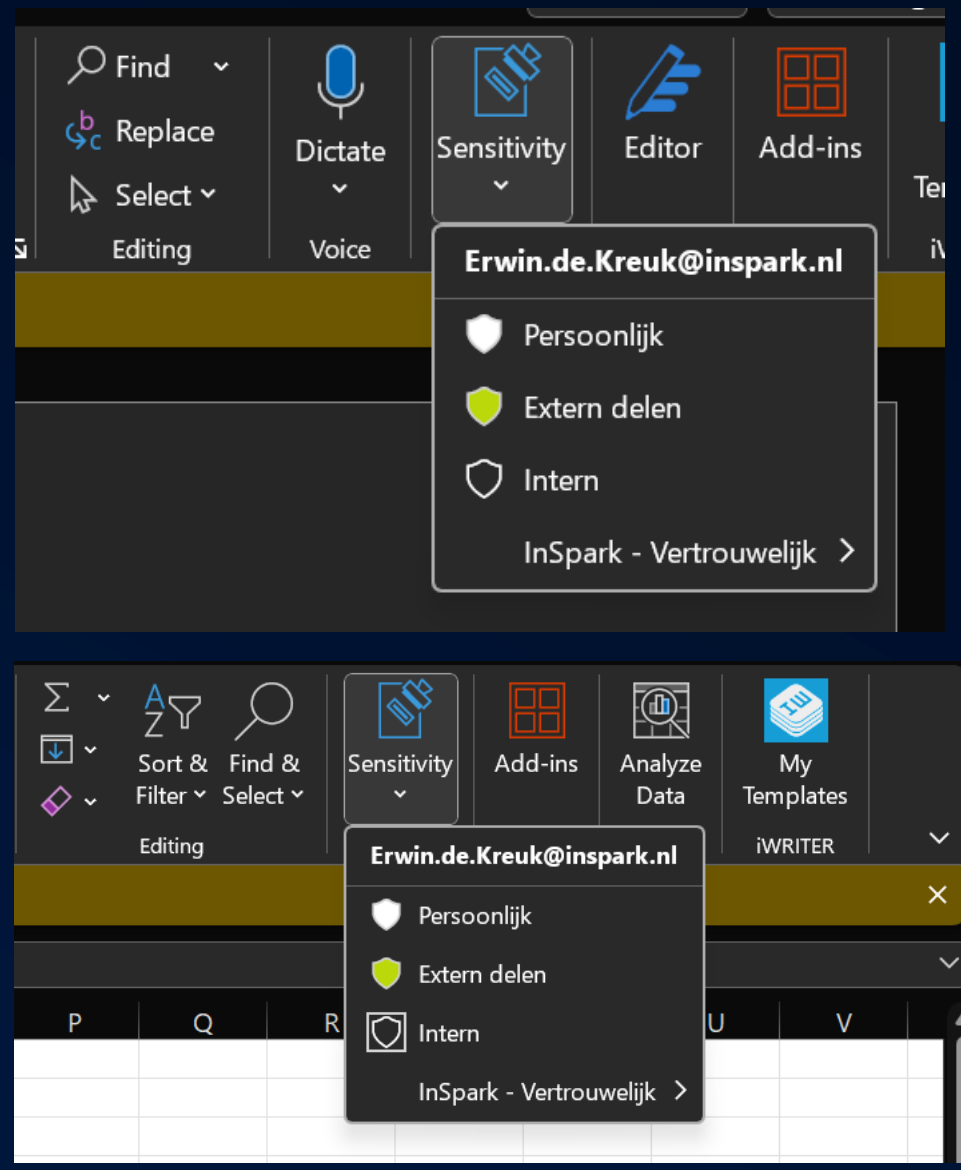
Ingest audit logs from Fabric in addition to other millions of signals to identify potential malicious or inadvertent insider risk.

Additional Microsoft Purview purchase required

Purview Information Protection

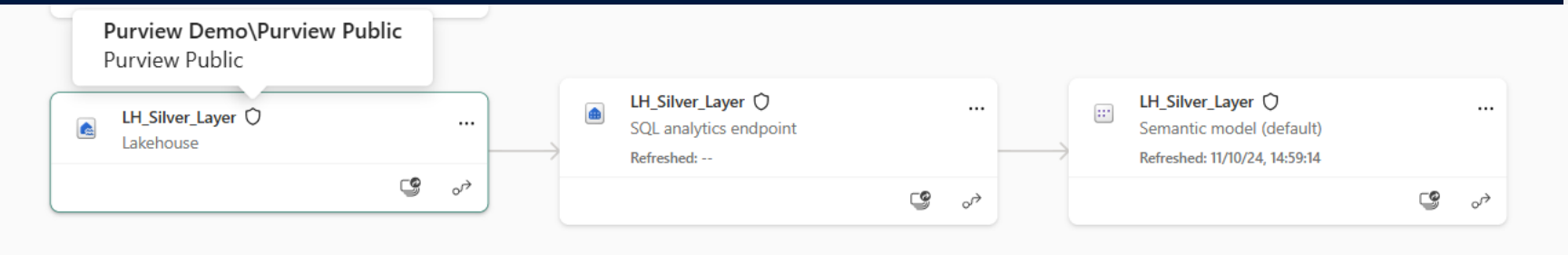
Purview Information Protection

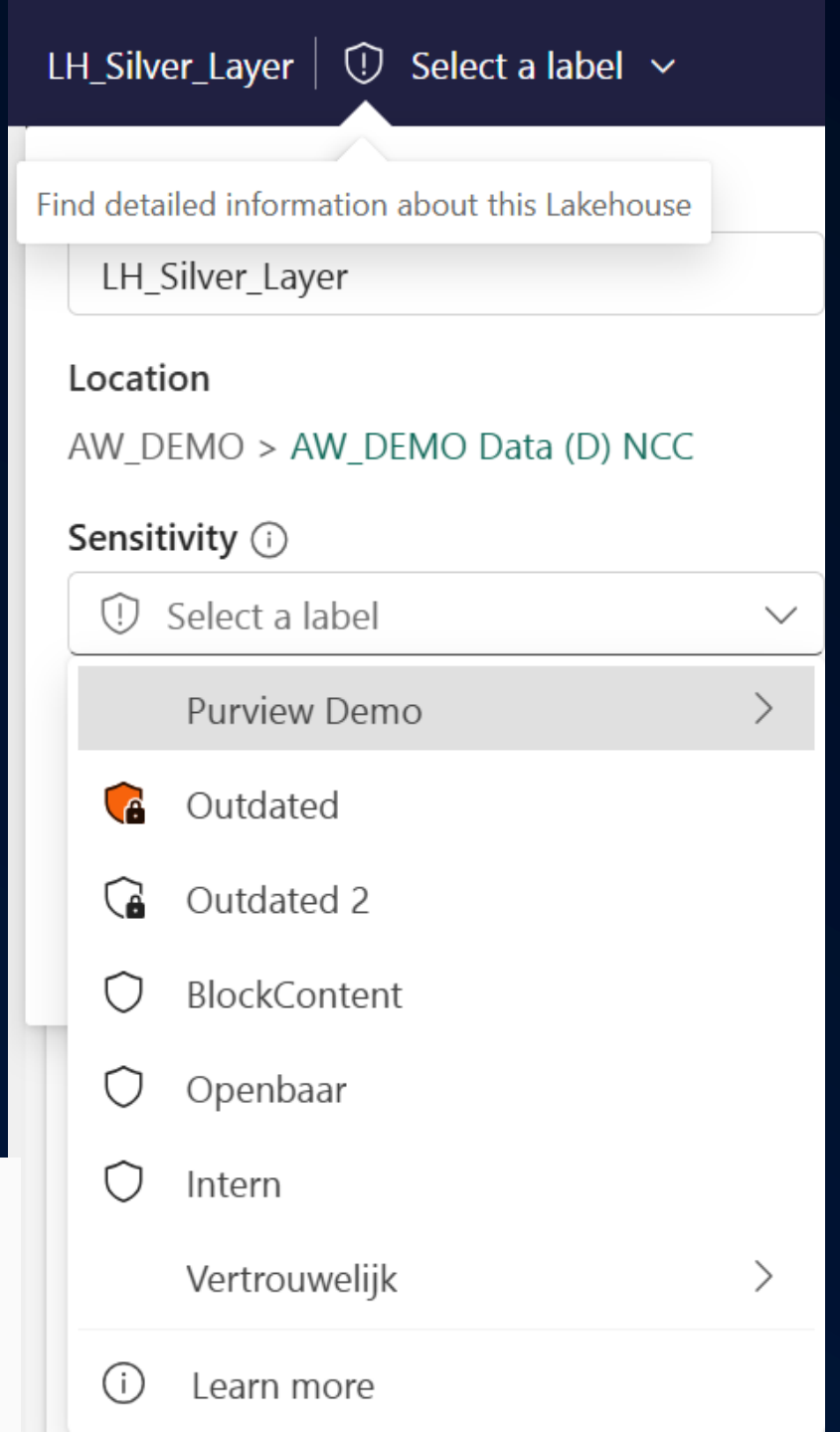
- MIP Labels in Office



Purview Information Protection

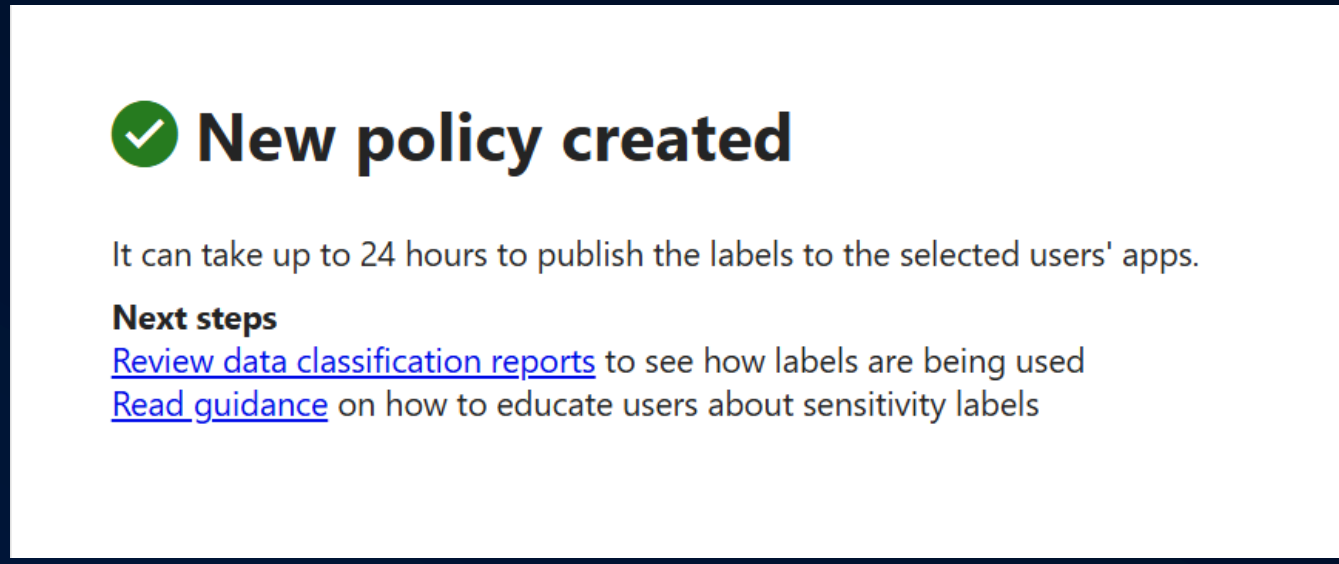
- MIP Labels in Office
- MIP Labels in Fabric
  - Inheritance of MIP labels in Fabric





Purview Information Protection

- Create labels
- Publish labels
- Make sure you use 3-5 labels(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

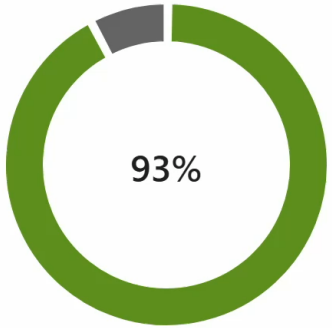
Reports

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.



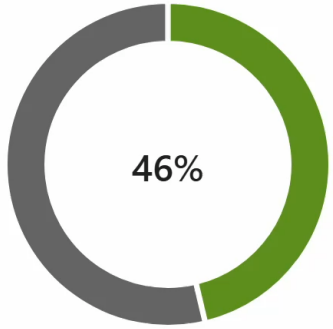
Microsoft 365 177

4 more

Explore protection policies

Sensitivity label coverage

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



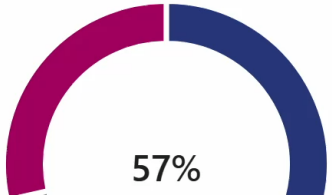
Labeled Not Labeled

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.



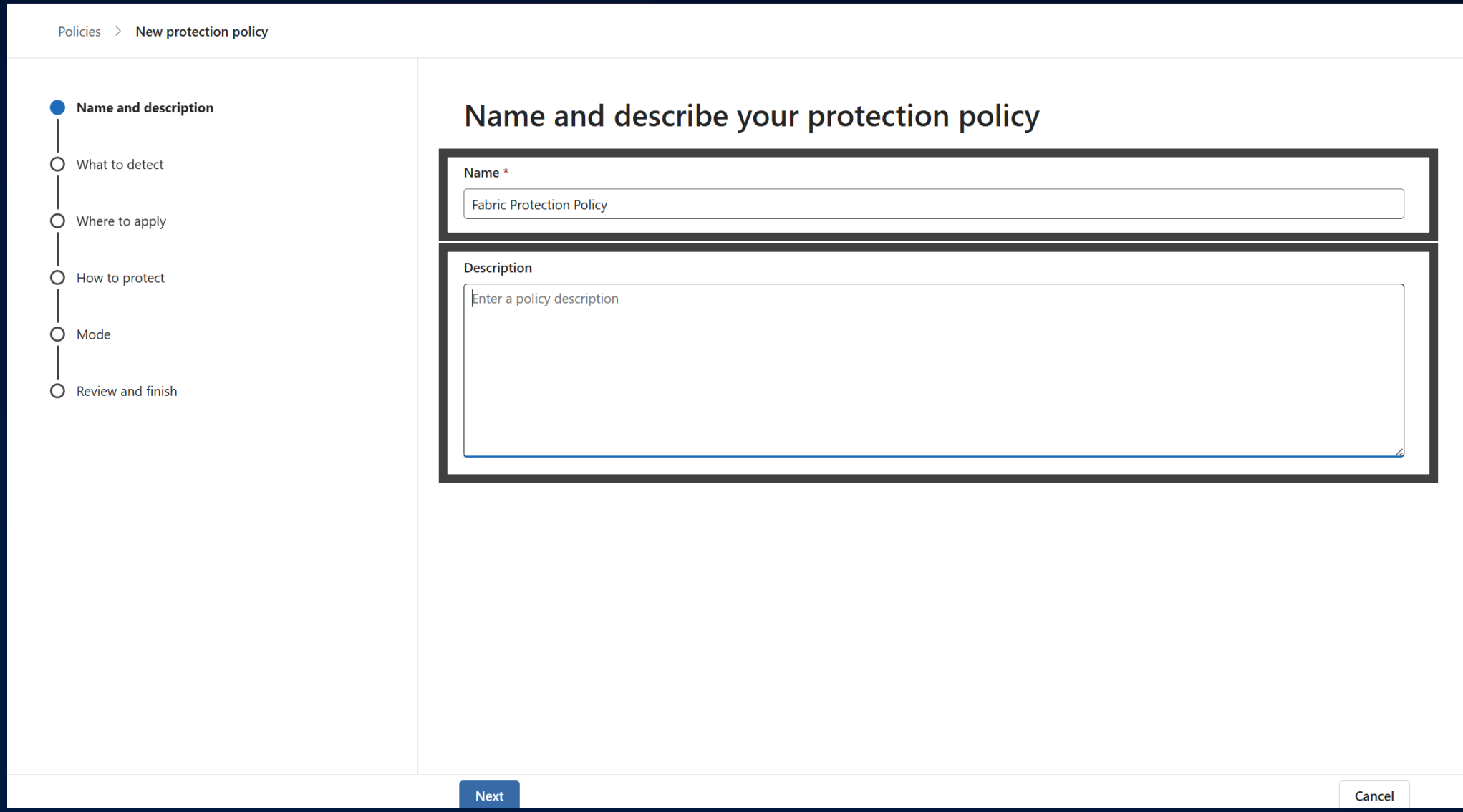
Azure 5
Microsoft 365 4
On premises

Demo

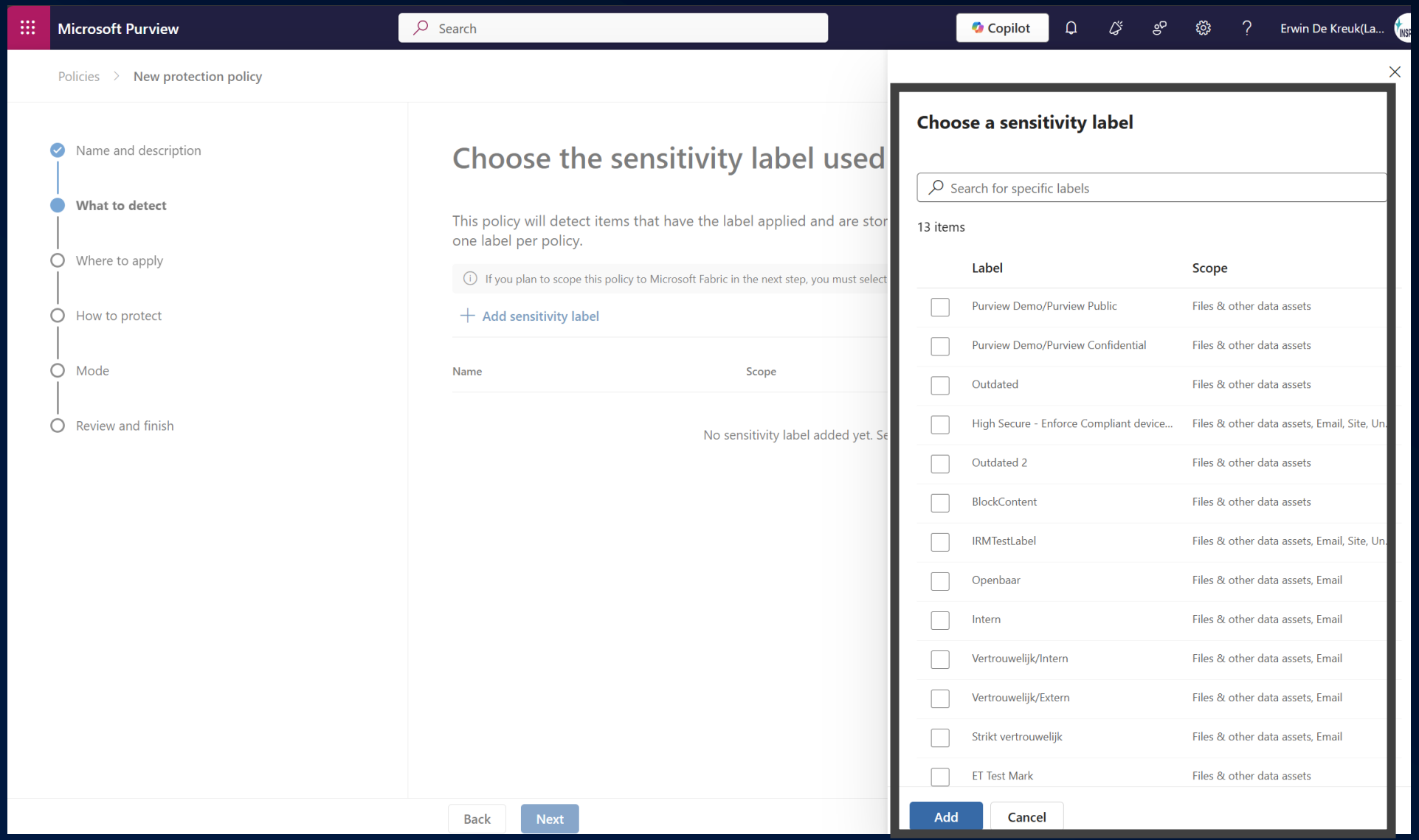
Labels

Purview Protection Policies

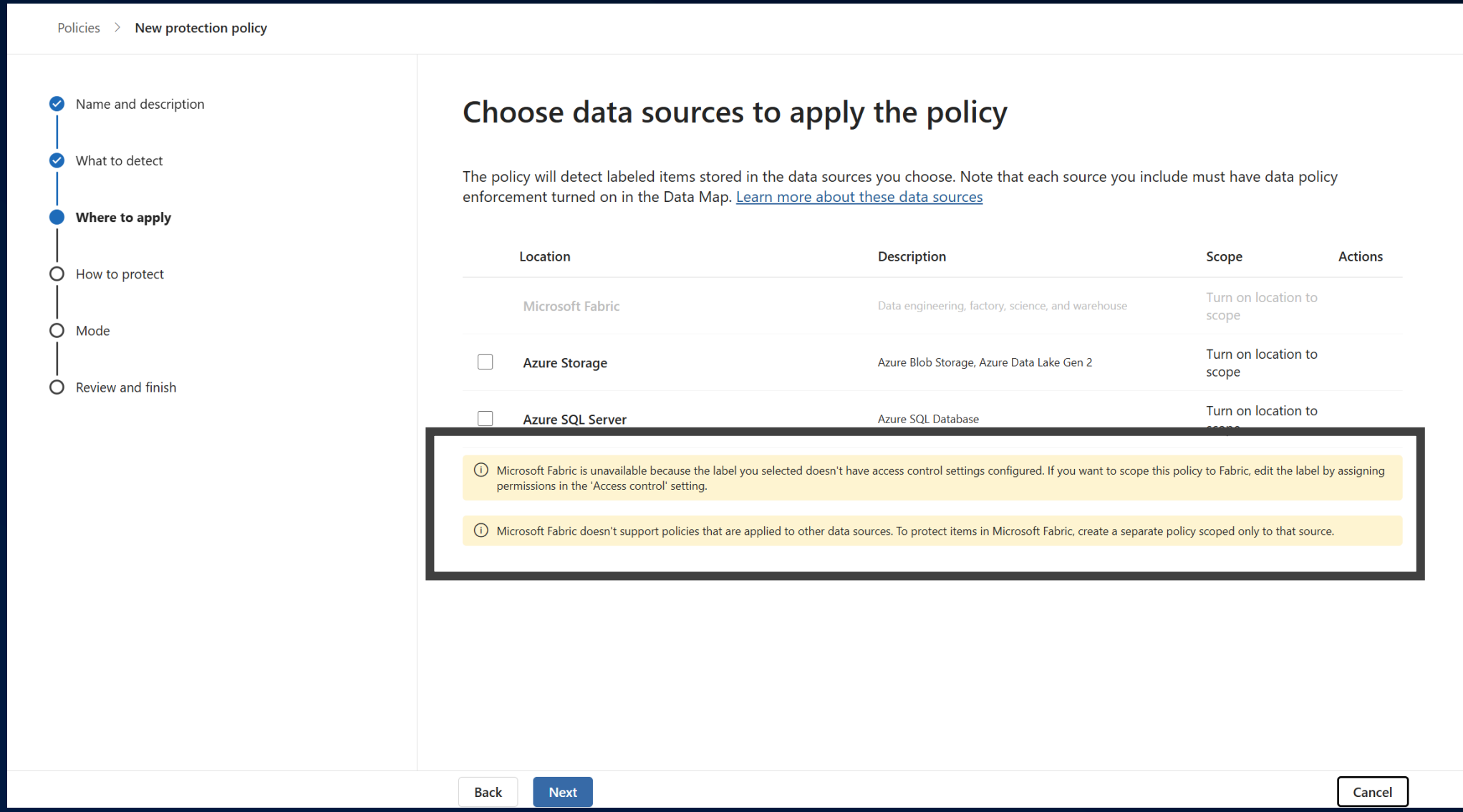
Purview Protection Policies



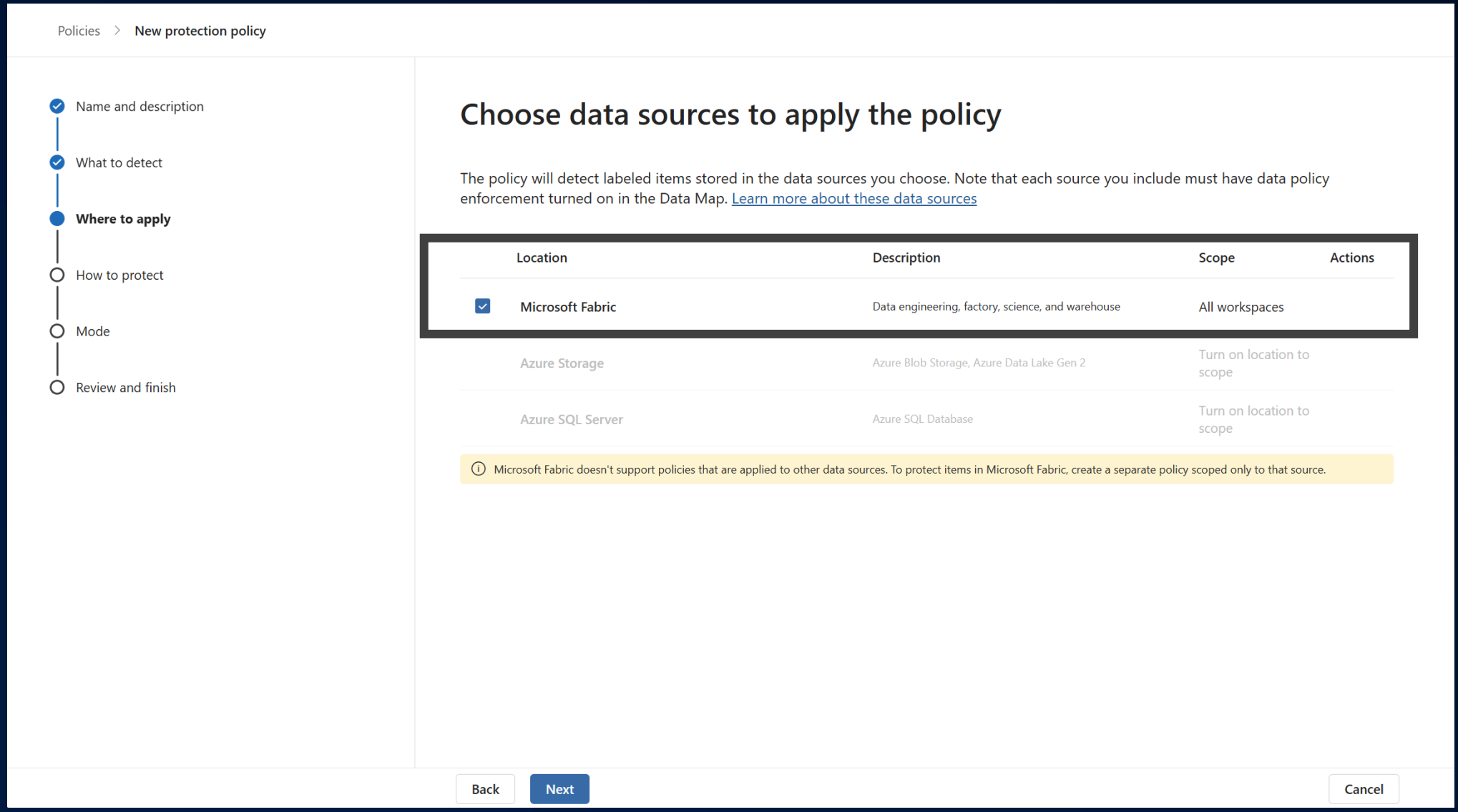
Purview Protection Policies



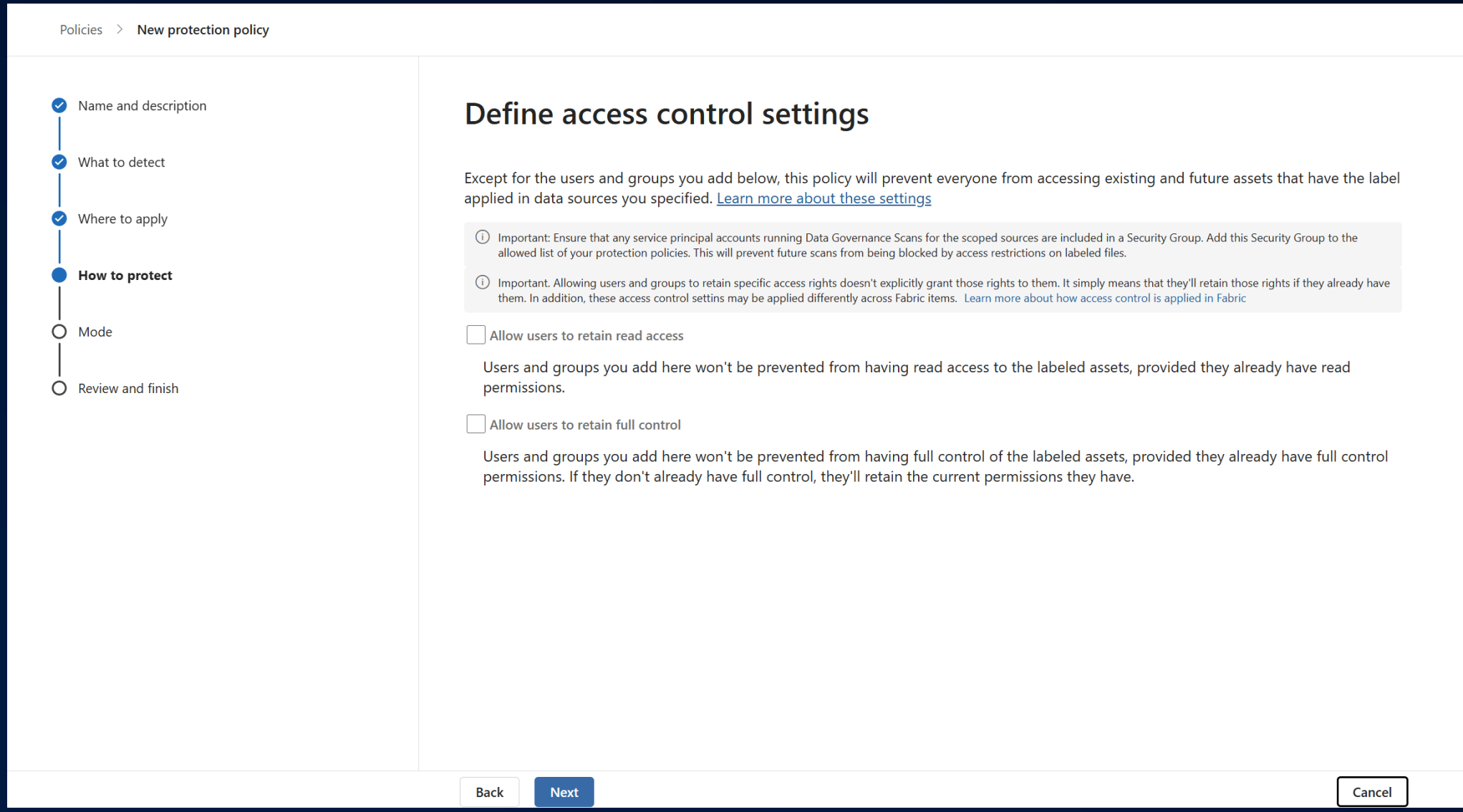
Purview Protection Policies



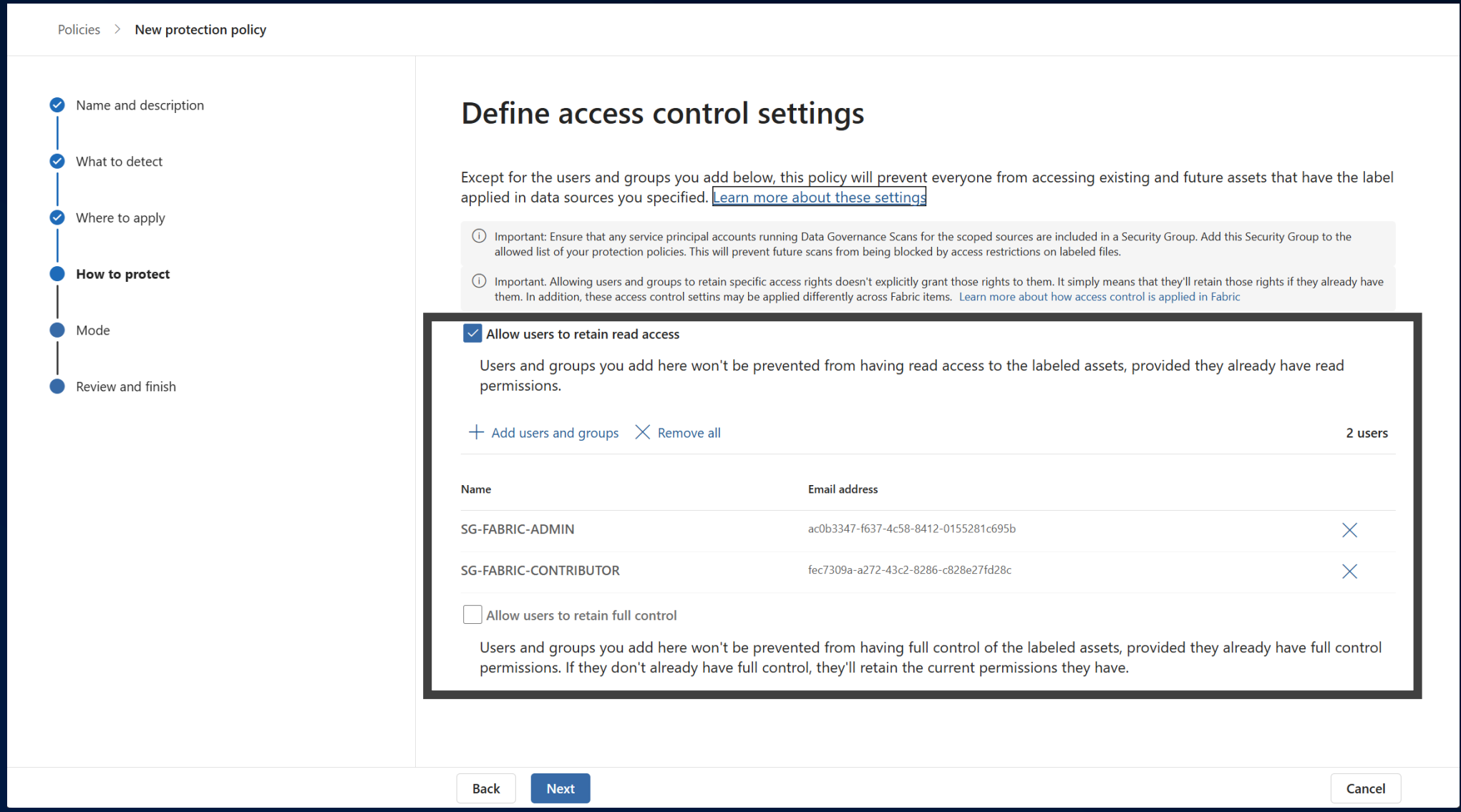
Purview Protection Policies



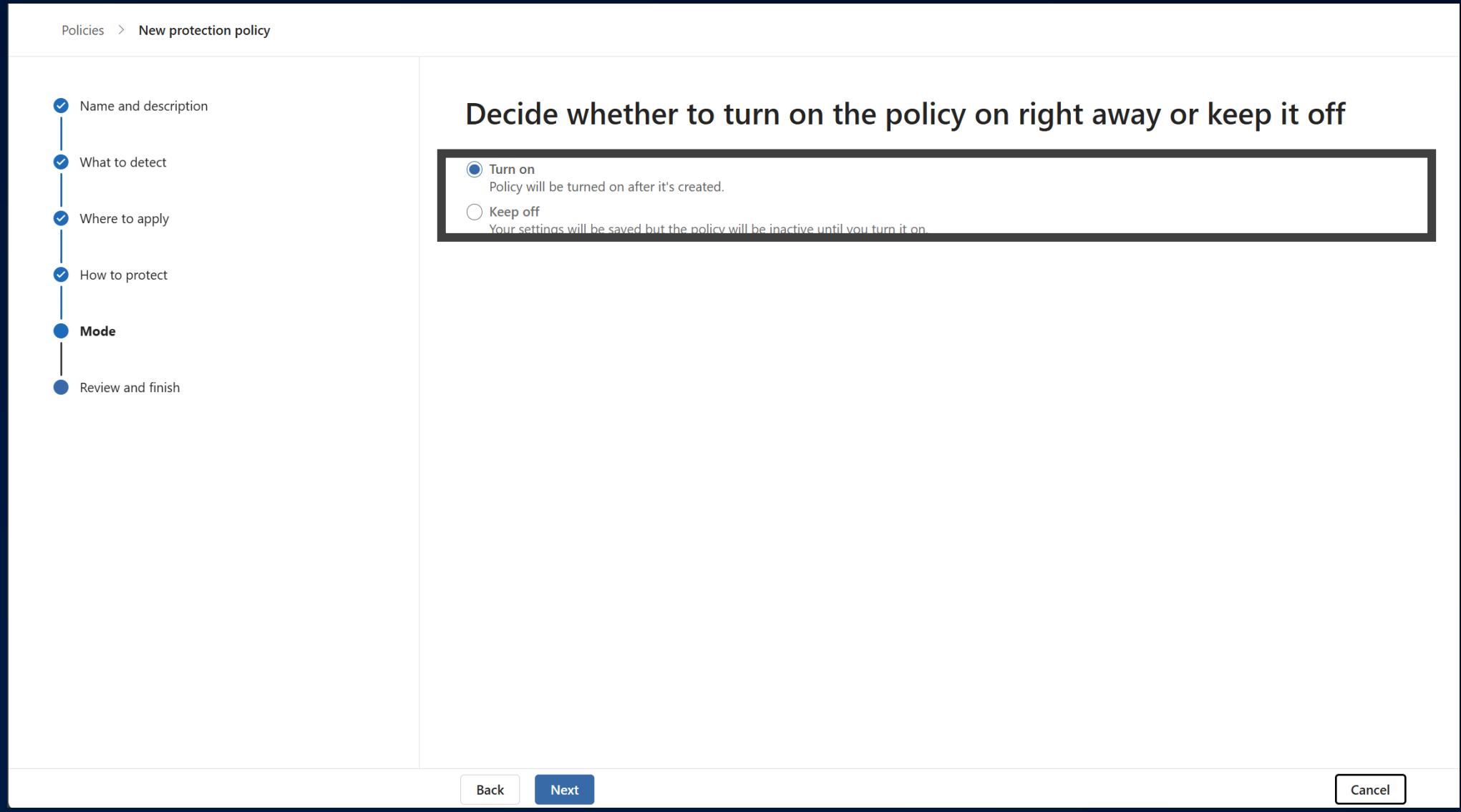
Purview Protection Policies



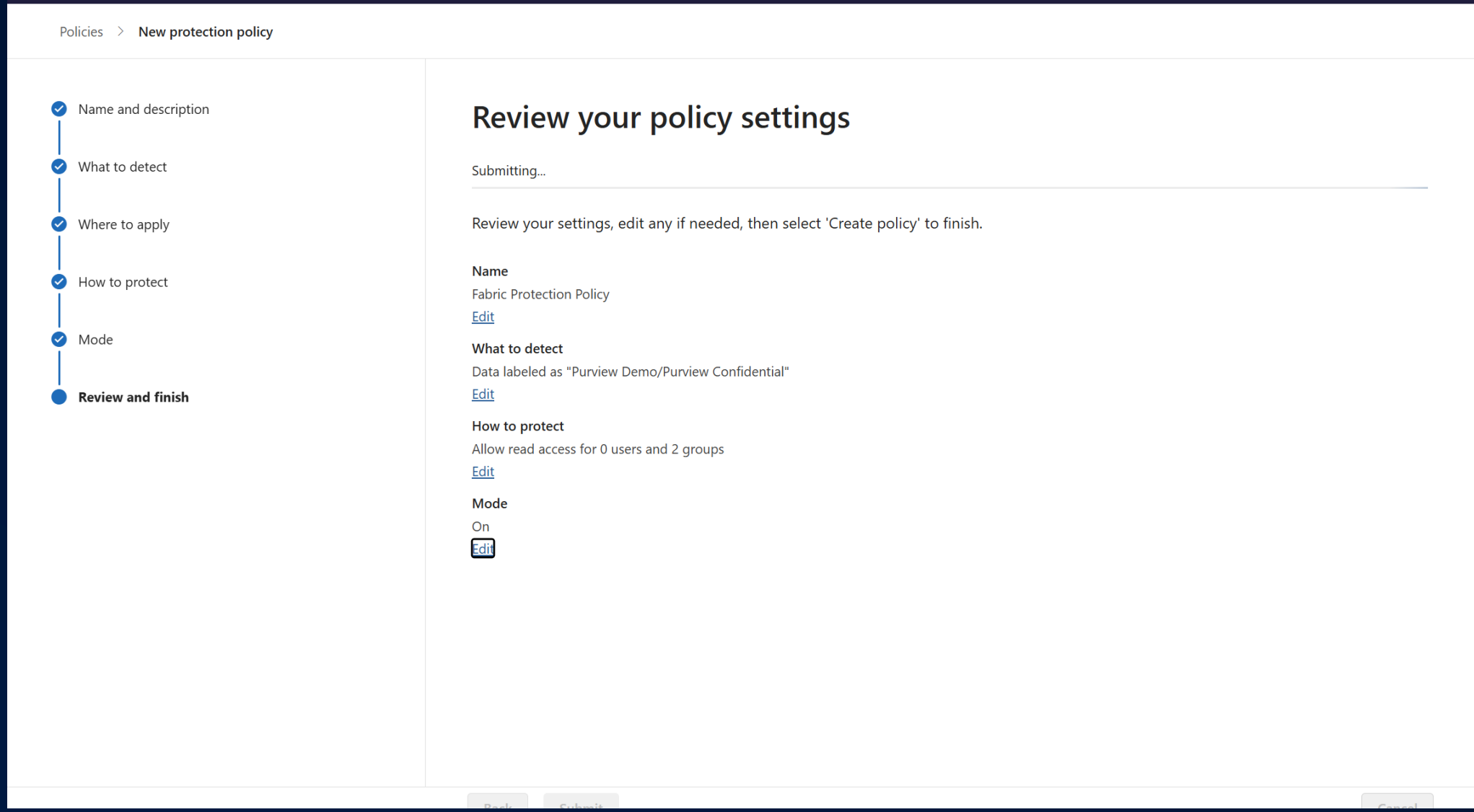
Purview Protection Policies



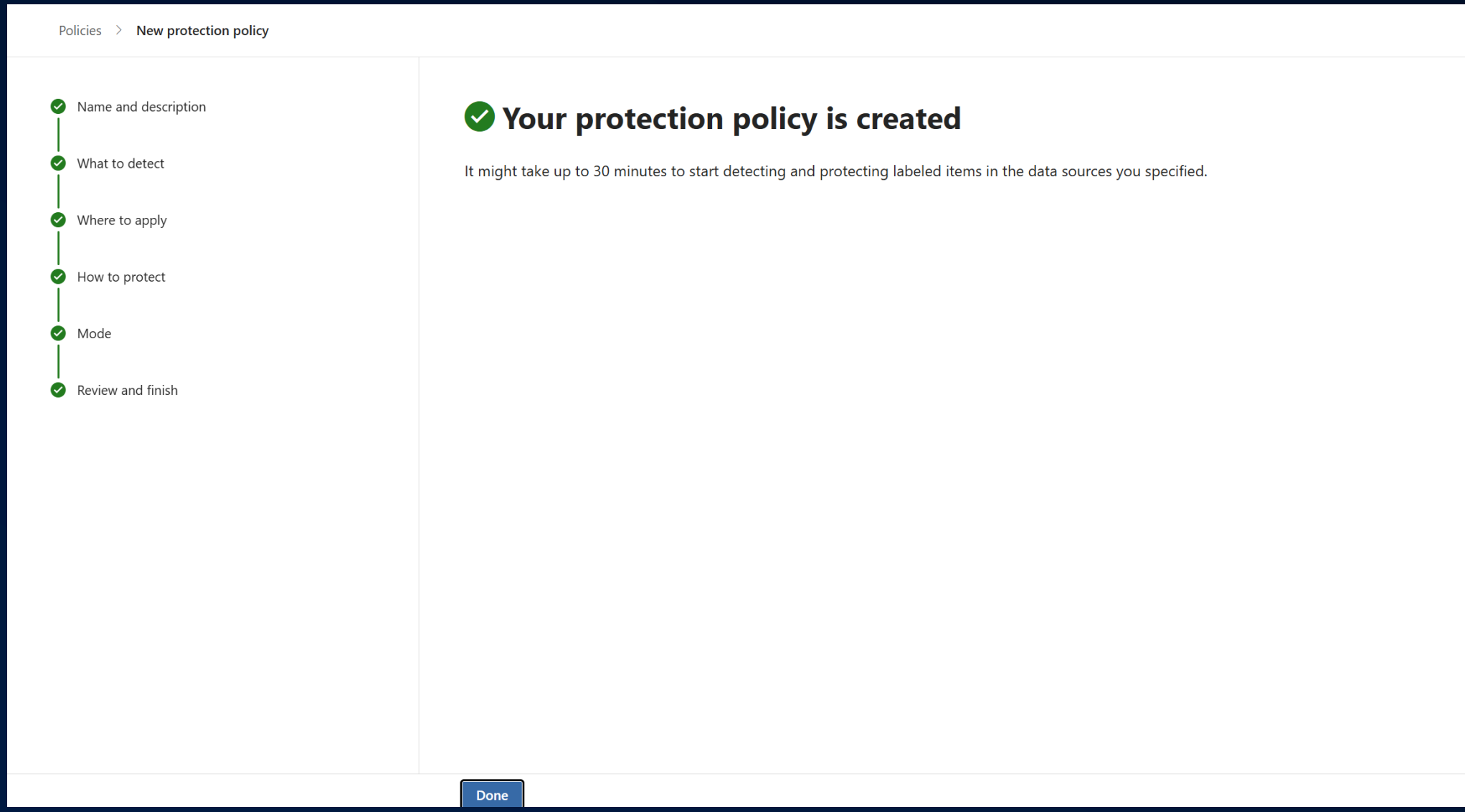
Purview Protection Policies



Purview Protection Policies



Purview Protection Policies

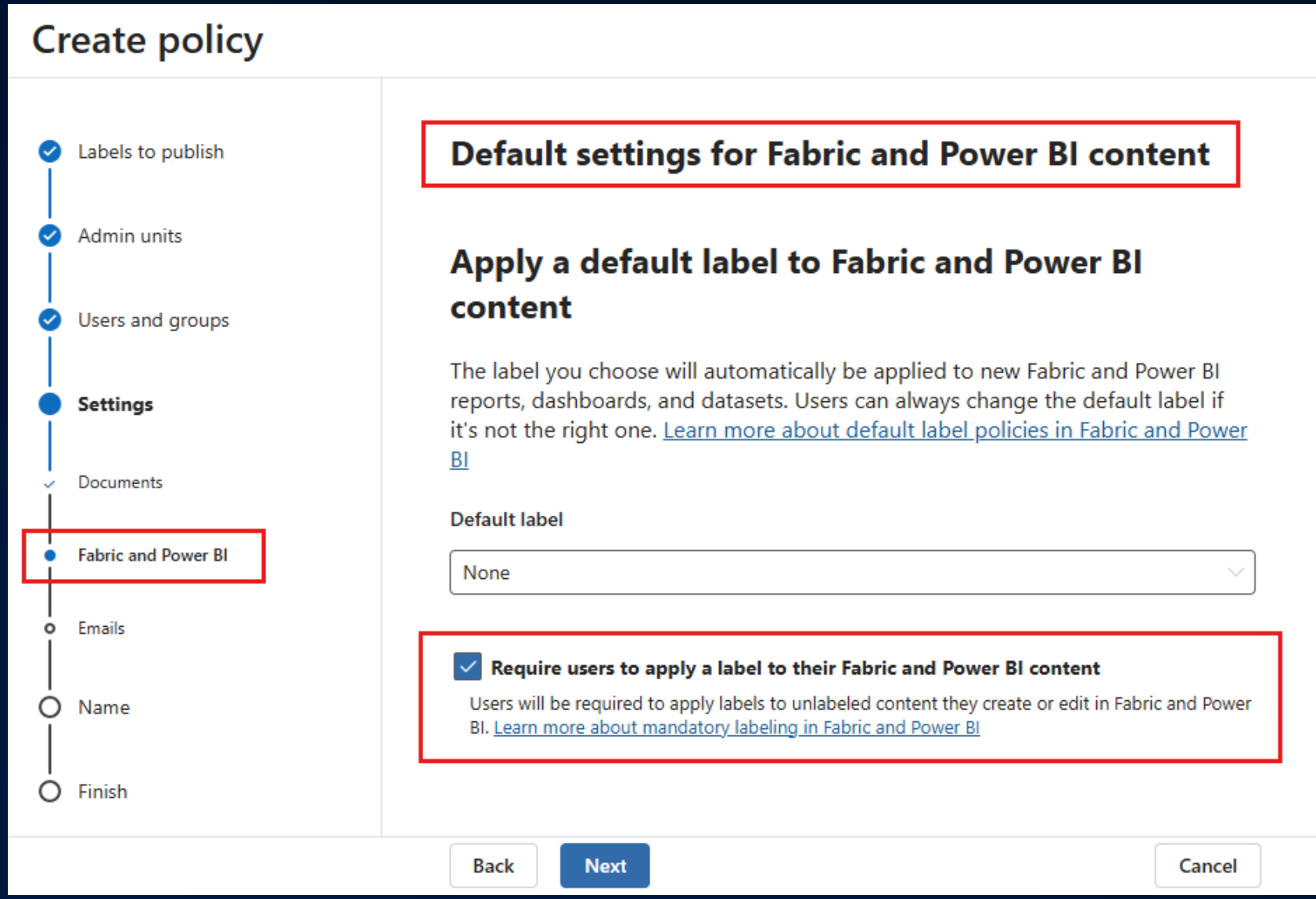


Purview Protection Policies

- 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 and Power BI

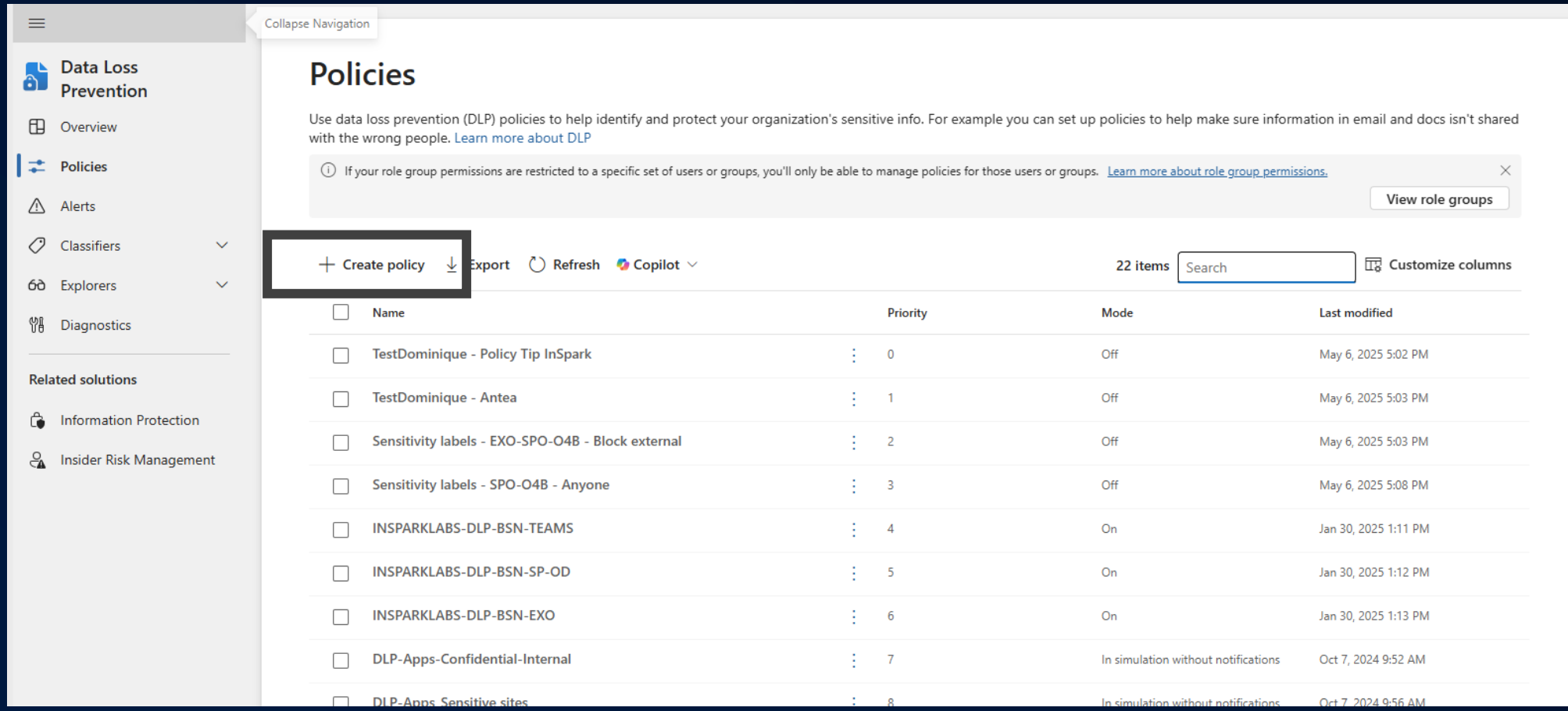
- Users **must** assign a label. Enforce through CI/CD
- DLP + automatic actions
- API enforcement
- Domain-default labels (preview)



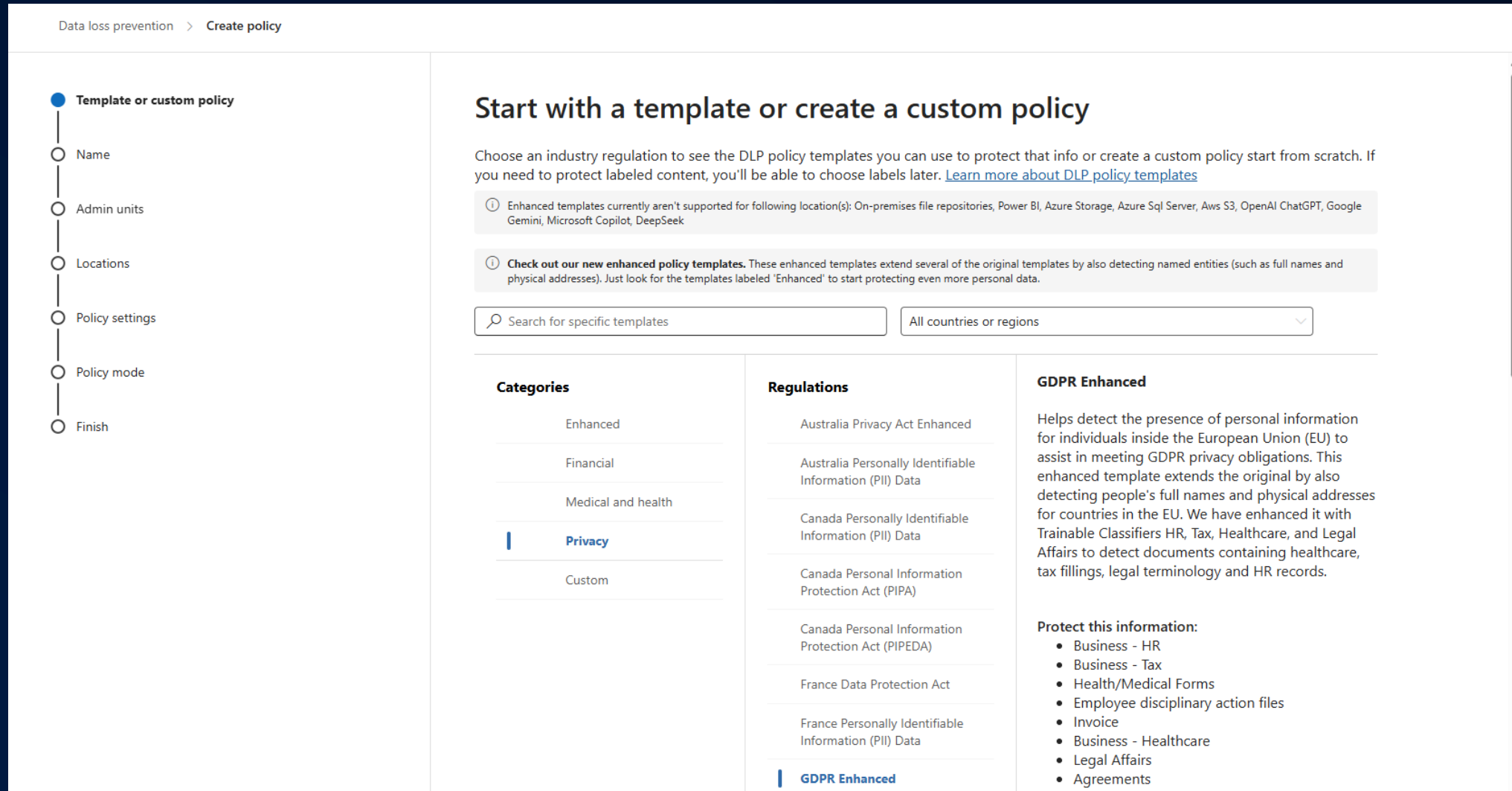
Demo

Purview Data Loss Prevention

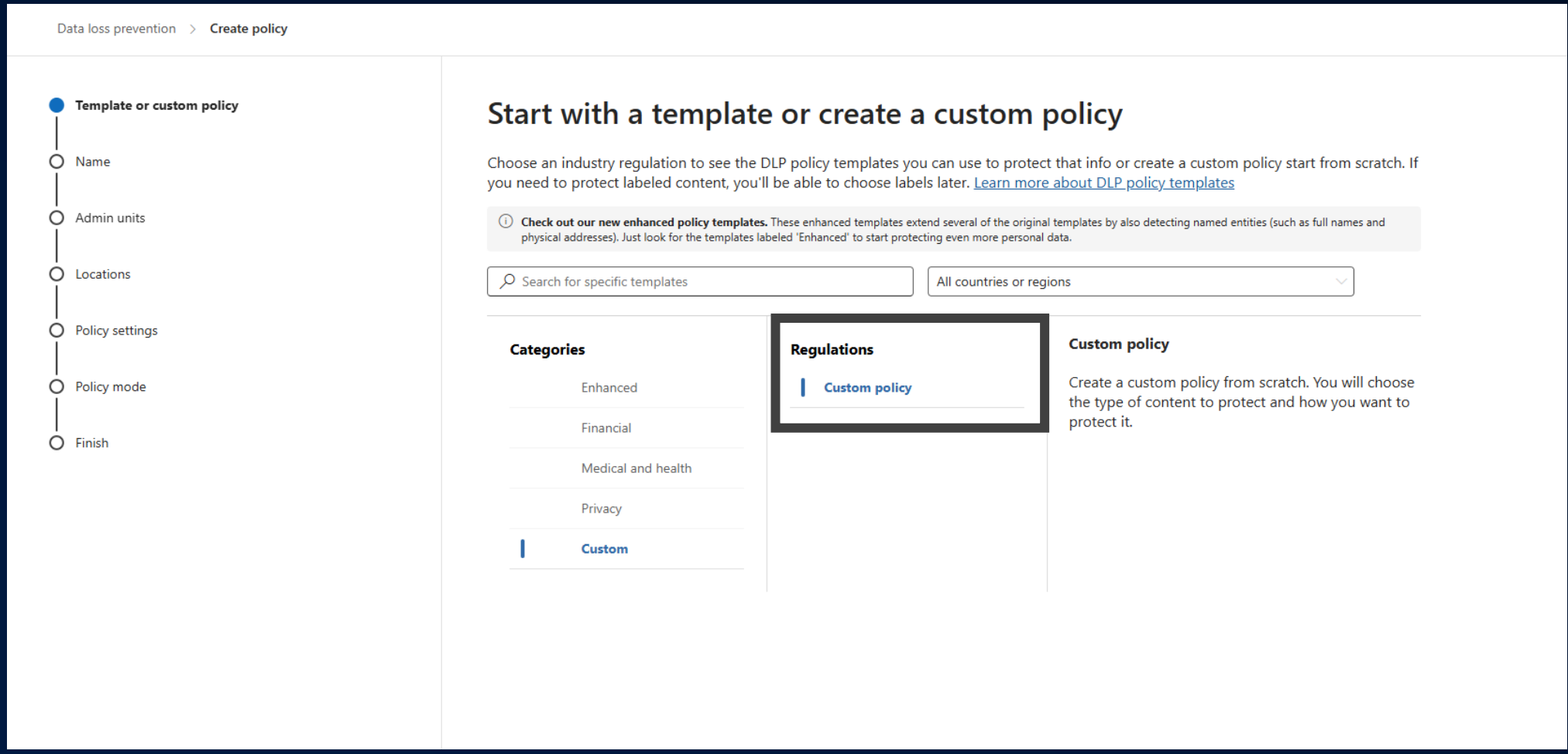
Purview Data Loss Prevention



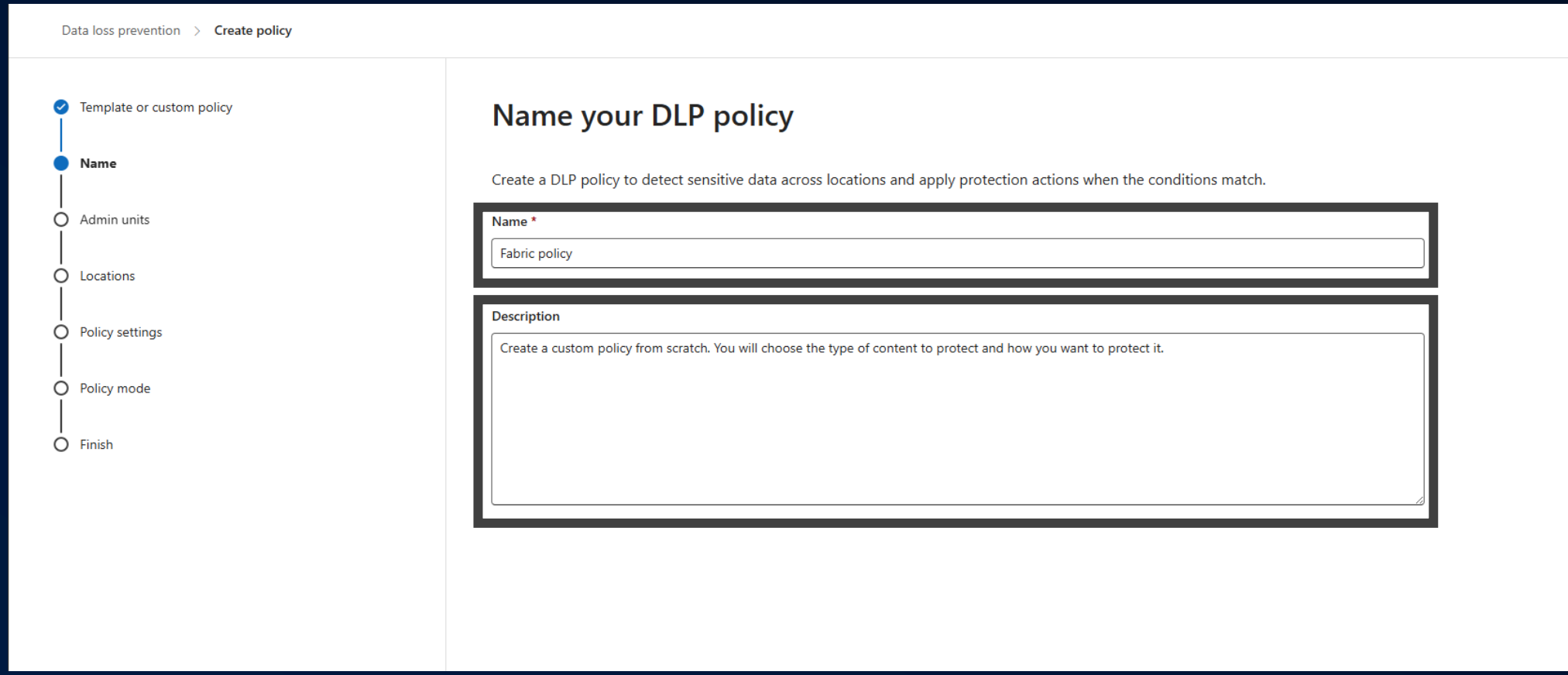
Purview Data Loss Prevention



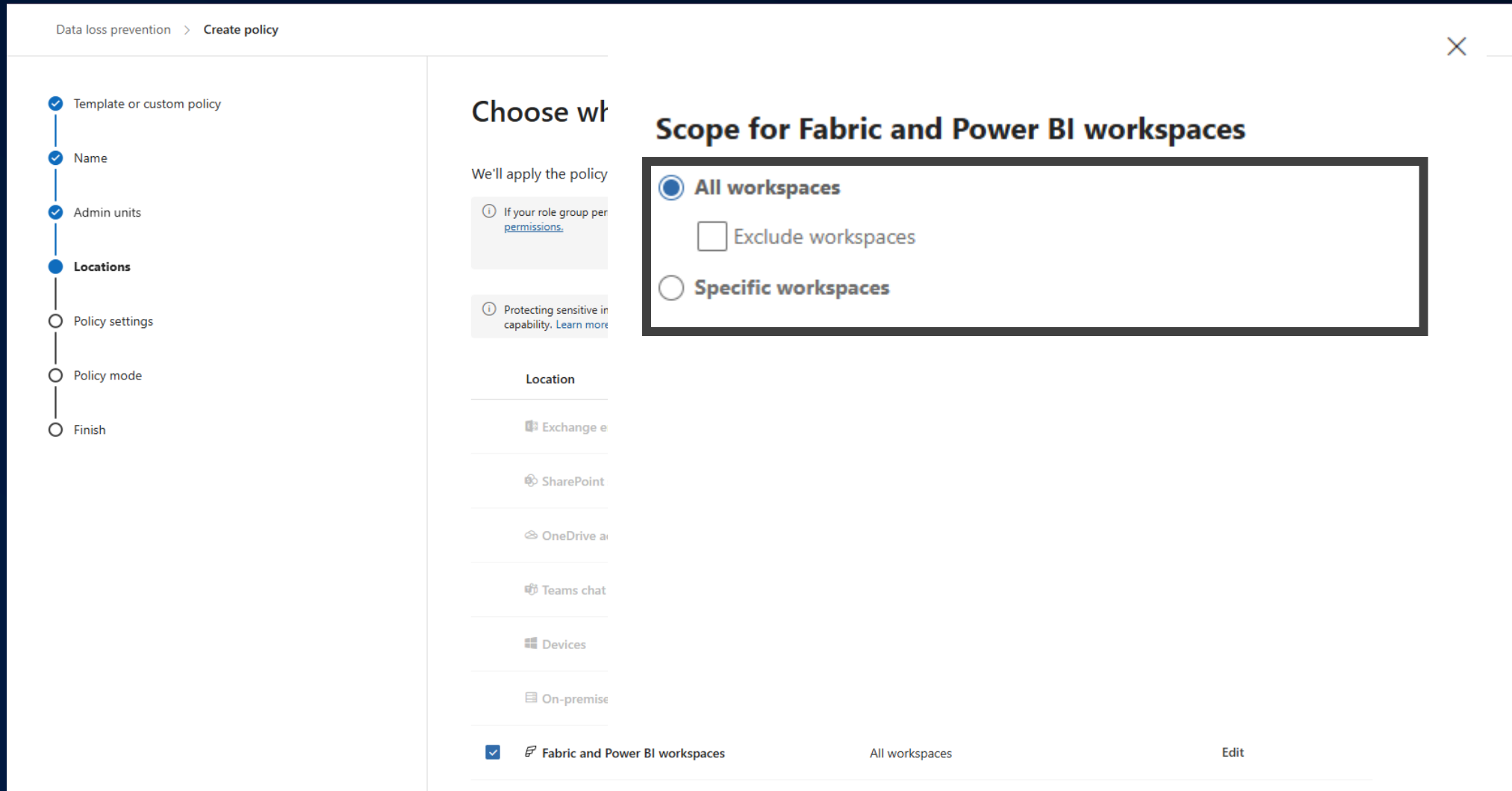
Purview Data Loss Prevention



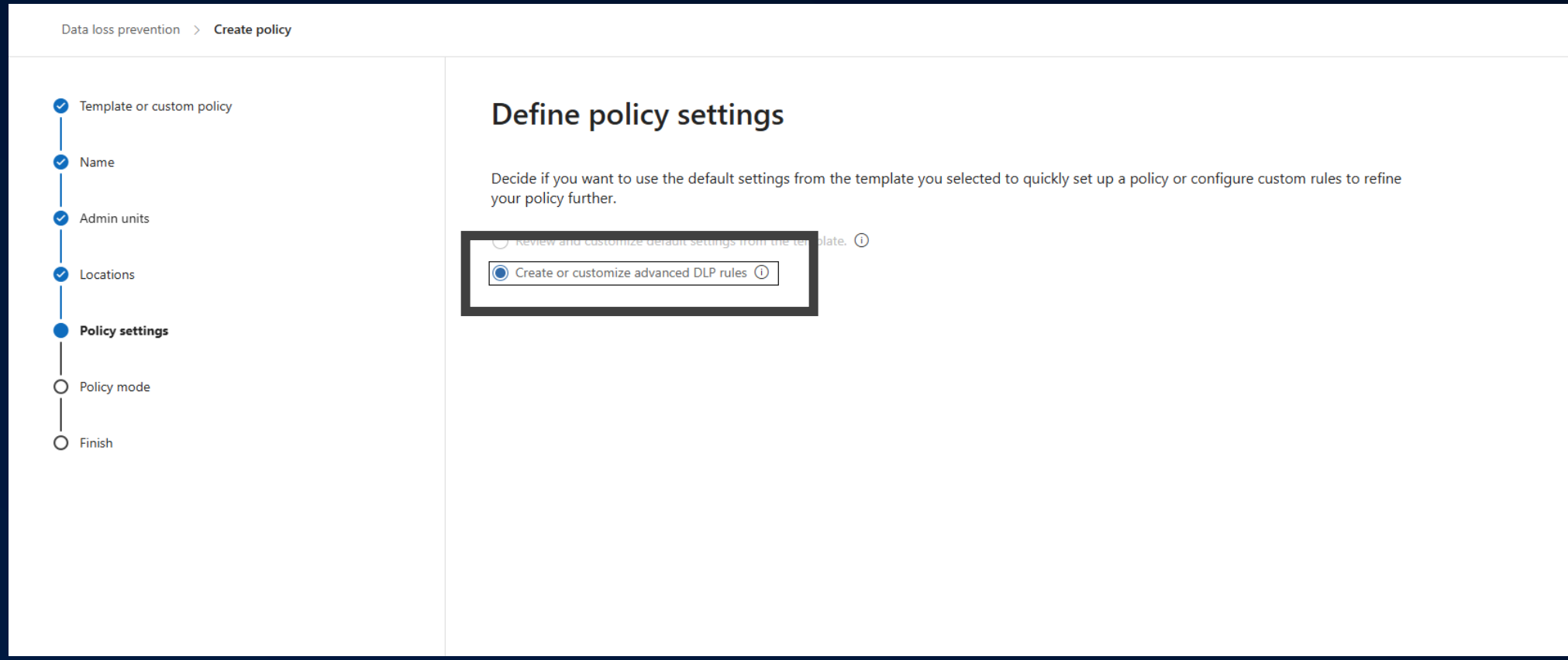
Purview Data Loss Prevention



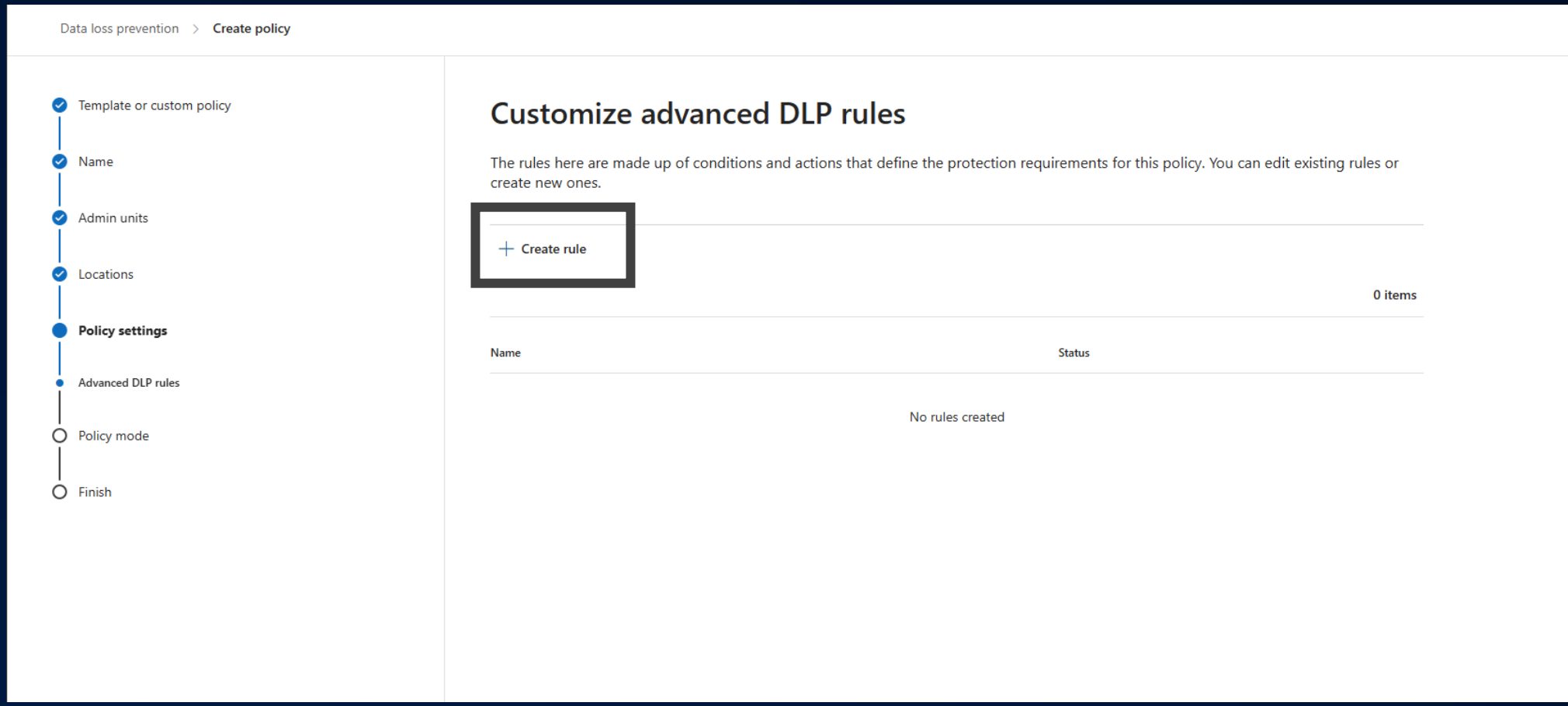
Purview Data Loss Prevention



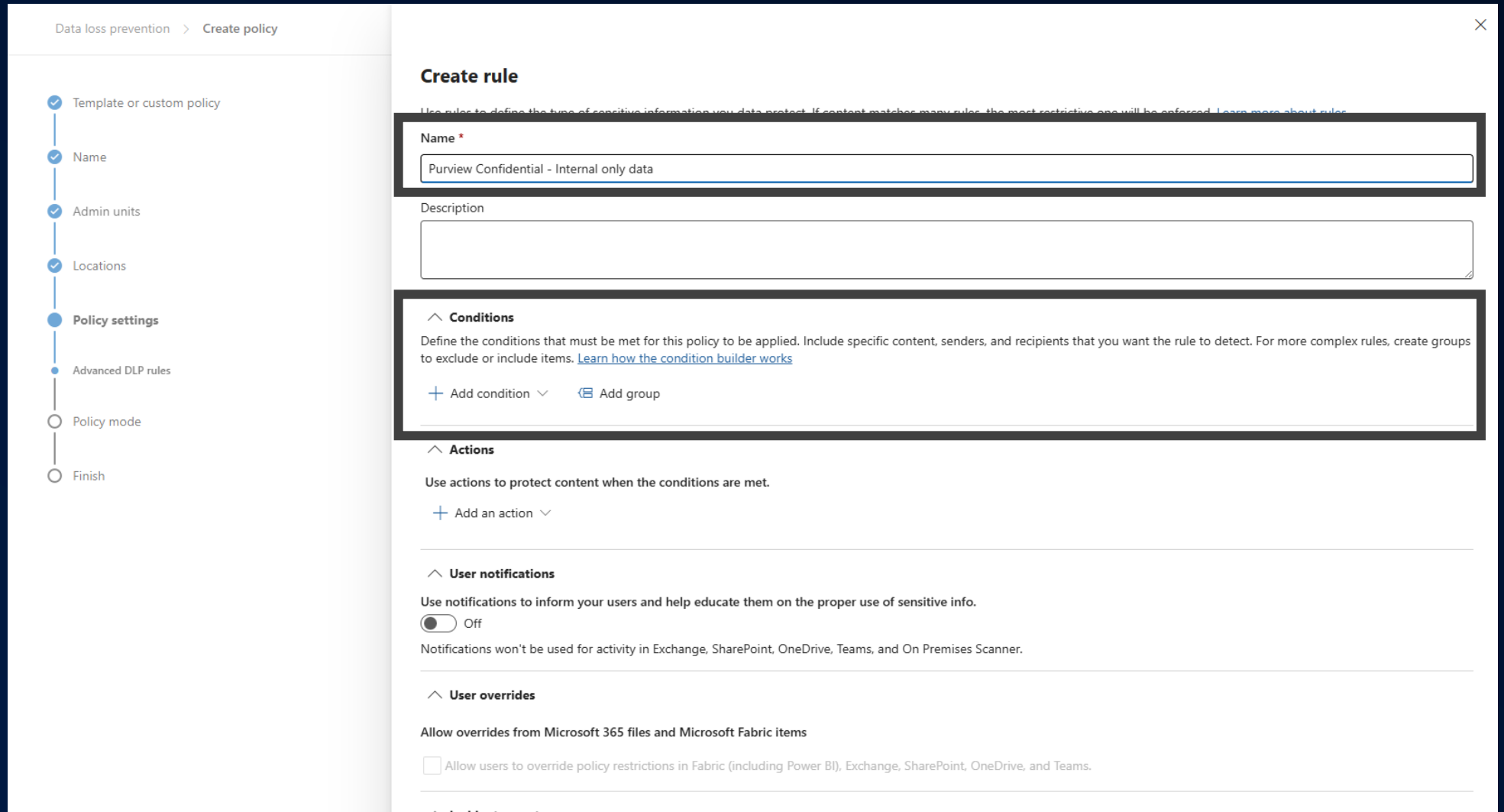
Purview Data Loss Prevention



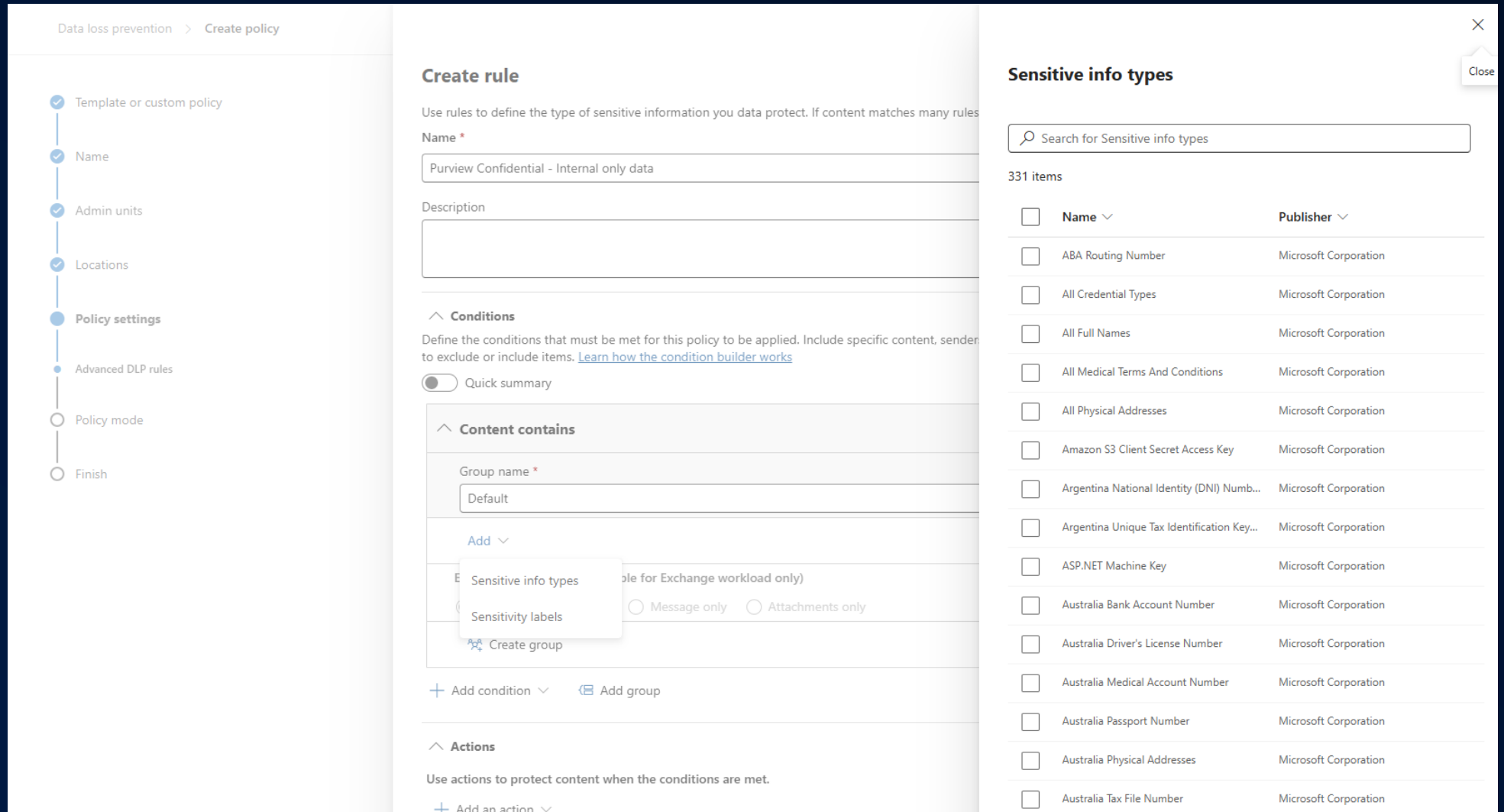
Purview Data Loss Prevention



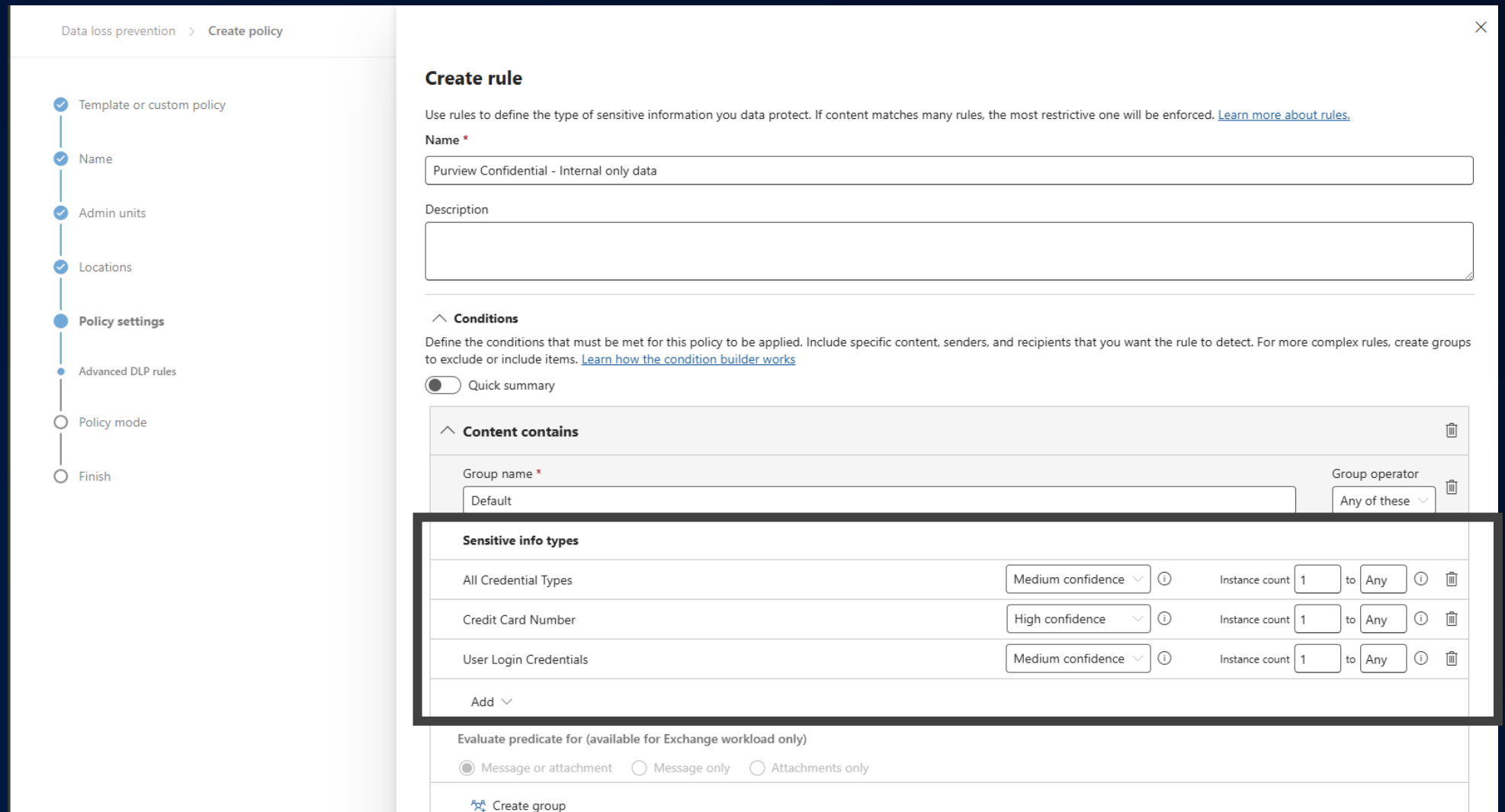
Purview Data Loss Prevention



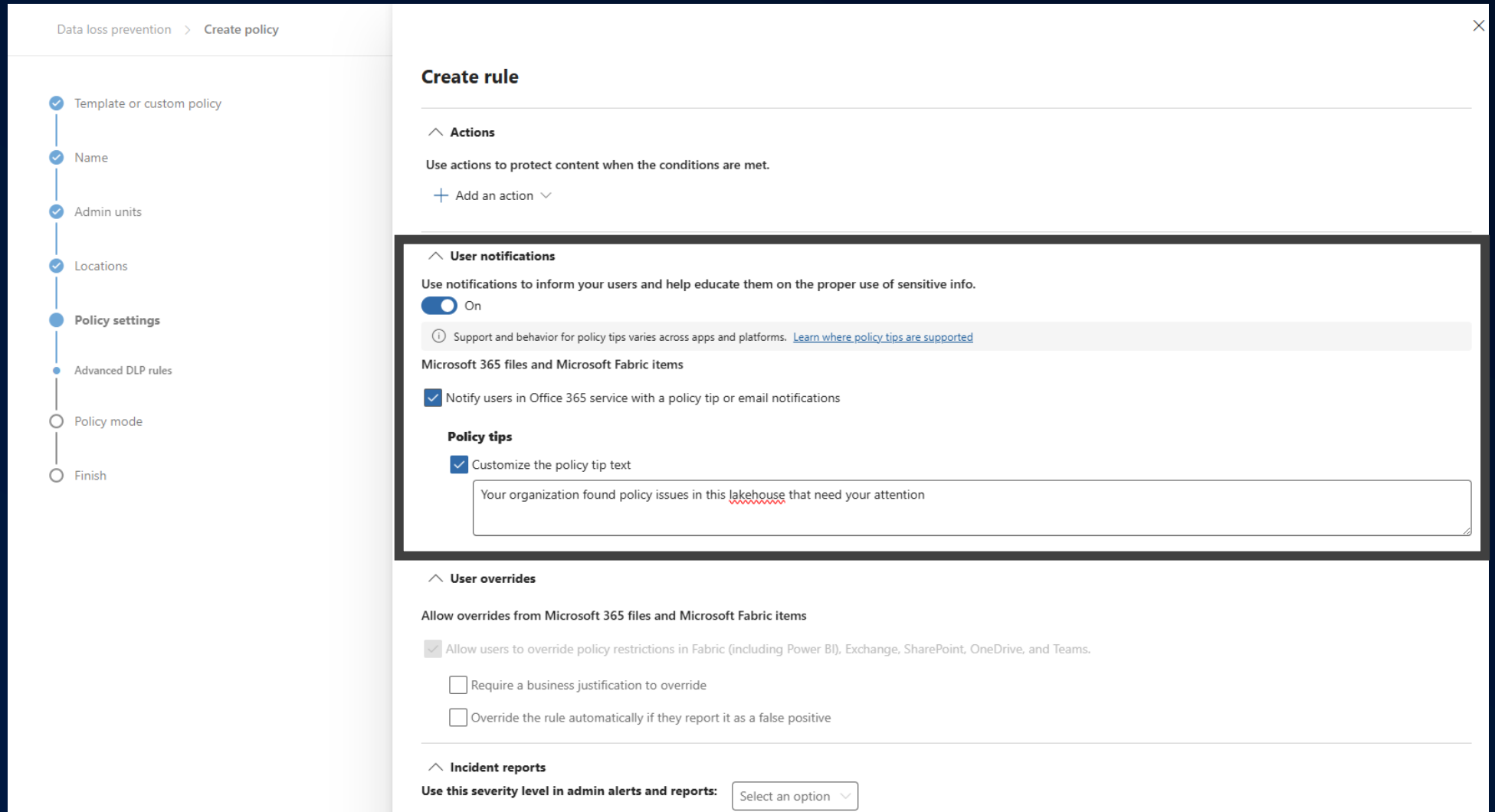
Purview Data Loss Prevention



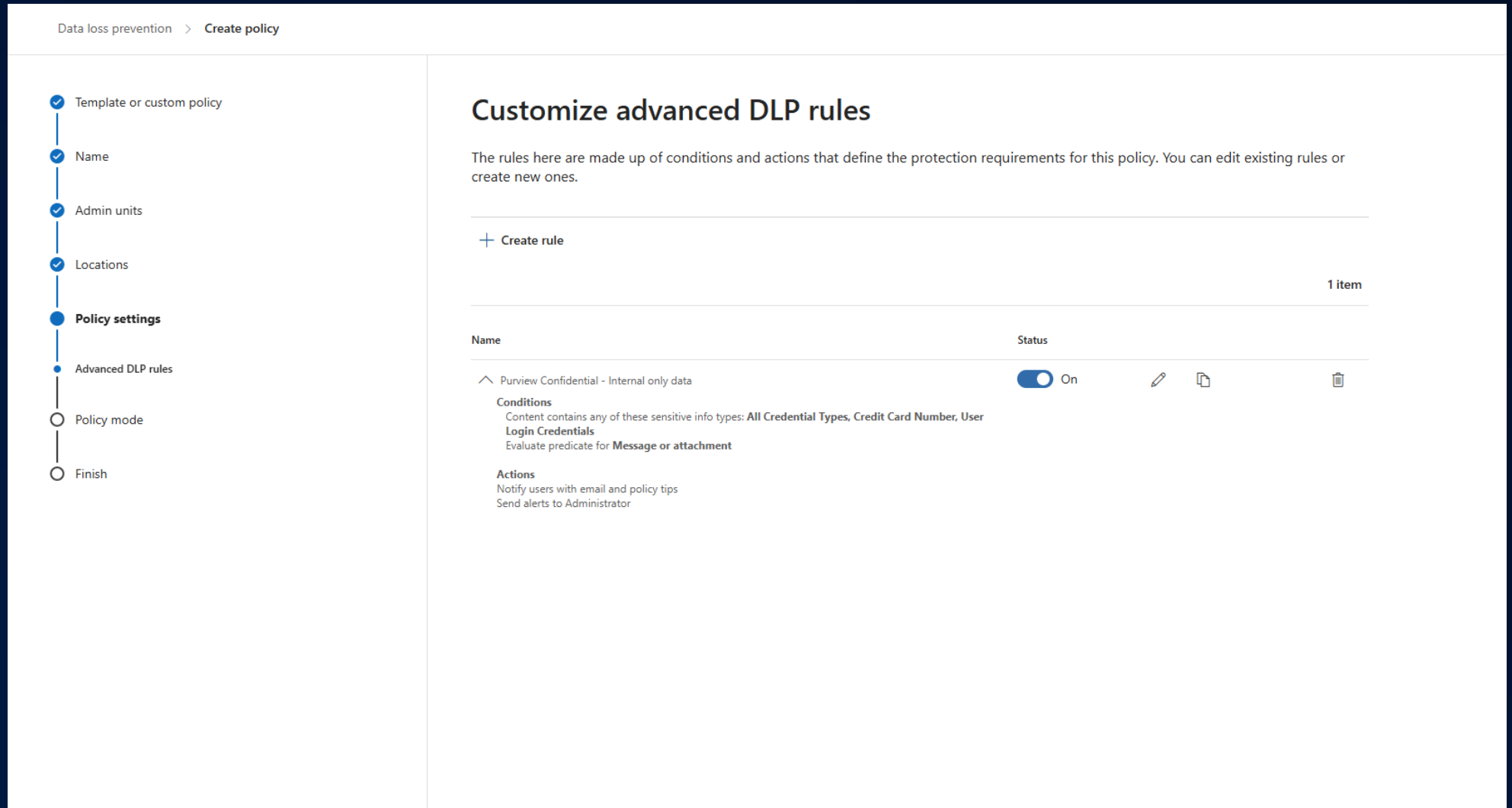
Purview Data Loss Prevention



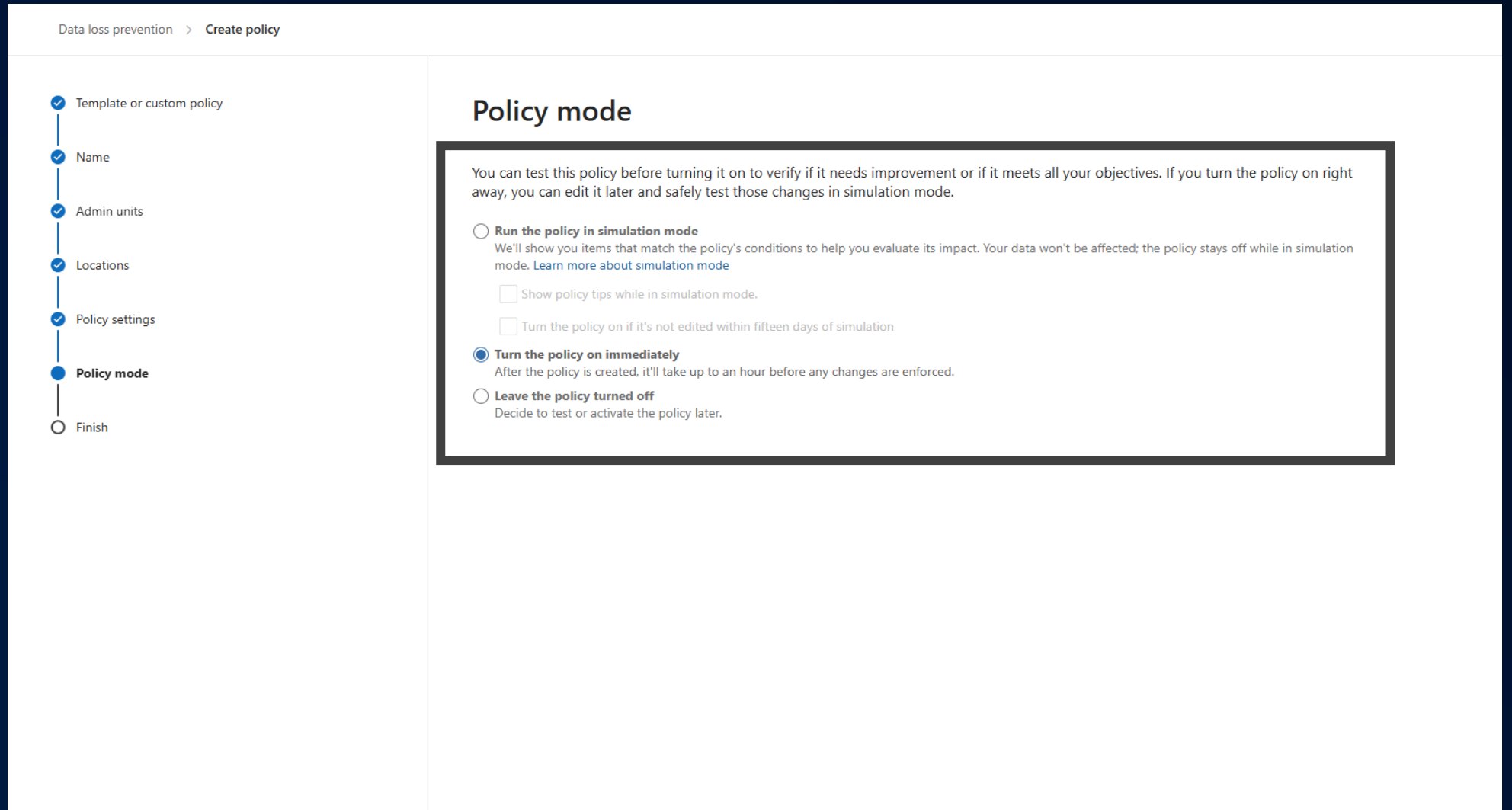
Purview Data Loss Prevention



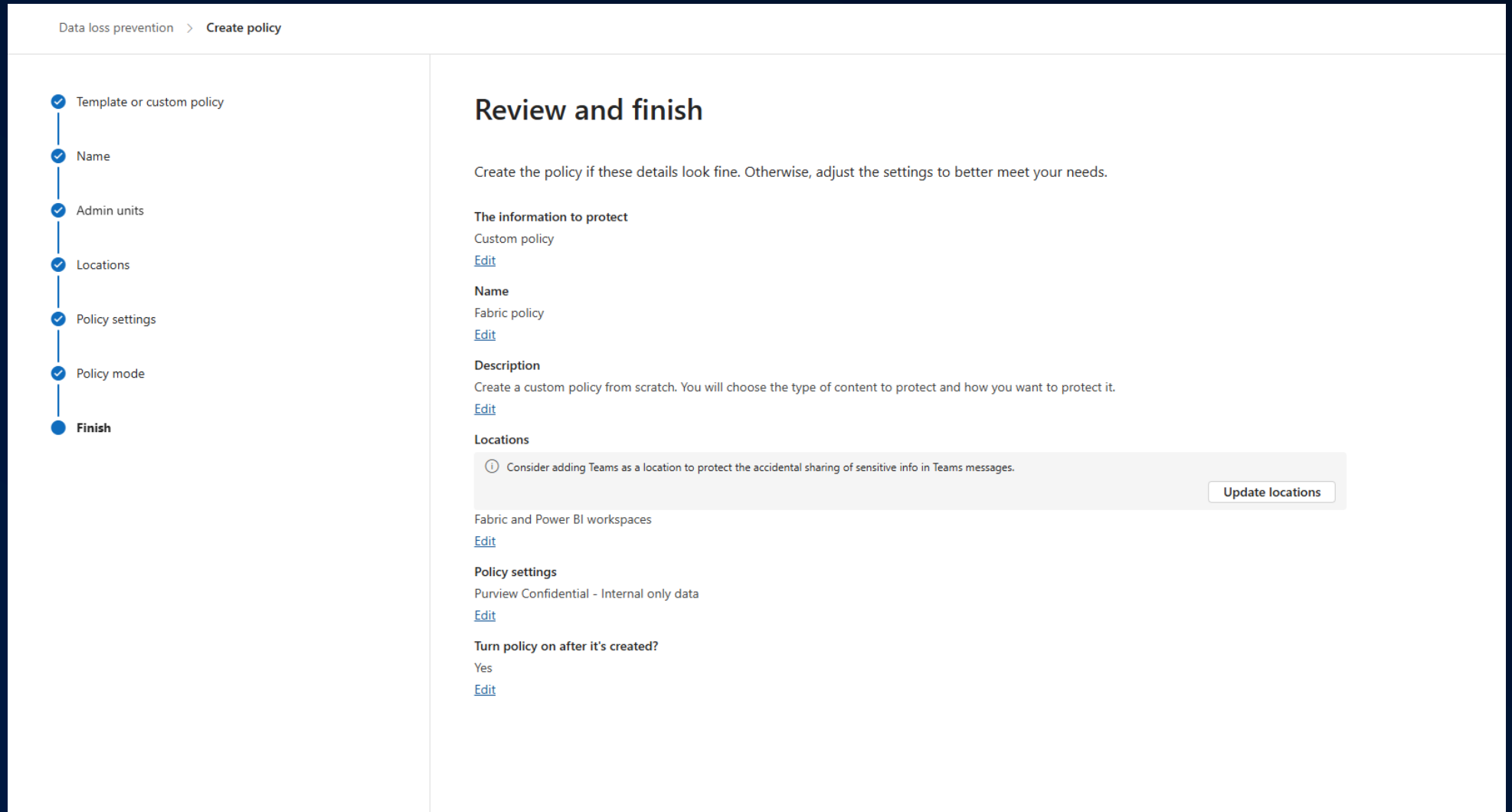
Purview Data Loss Prevention



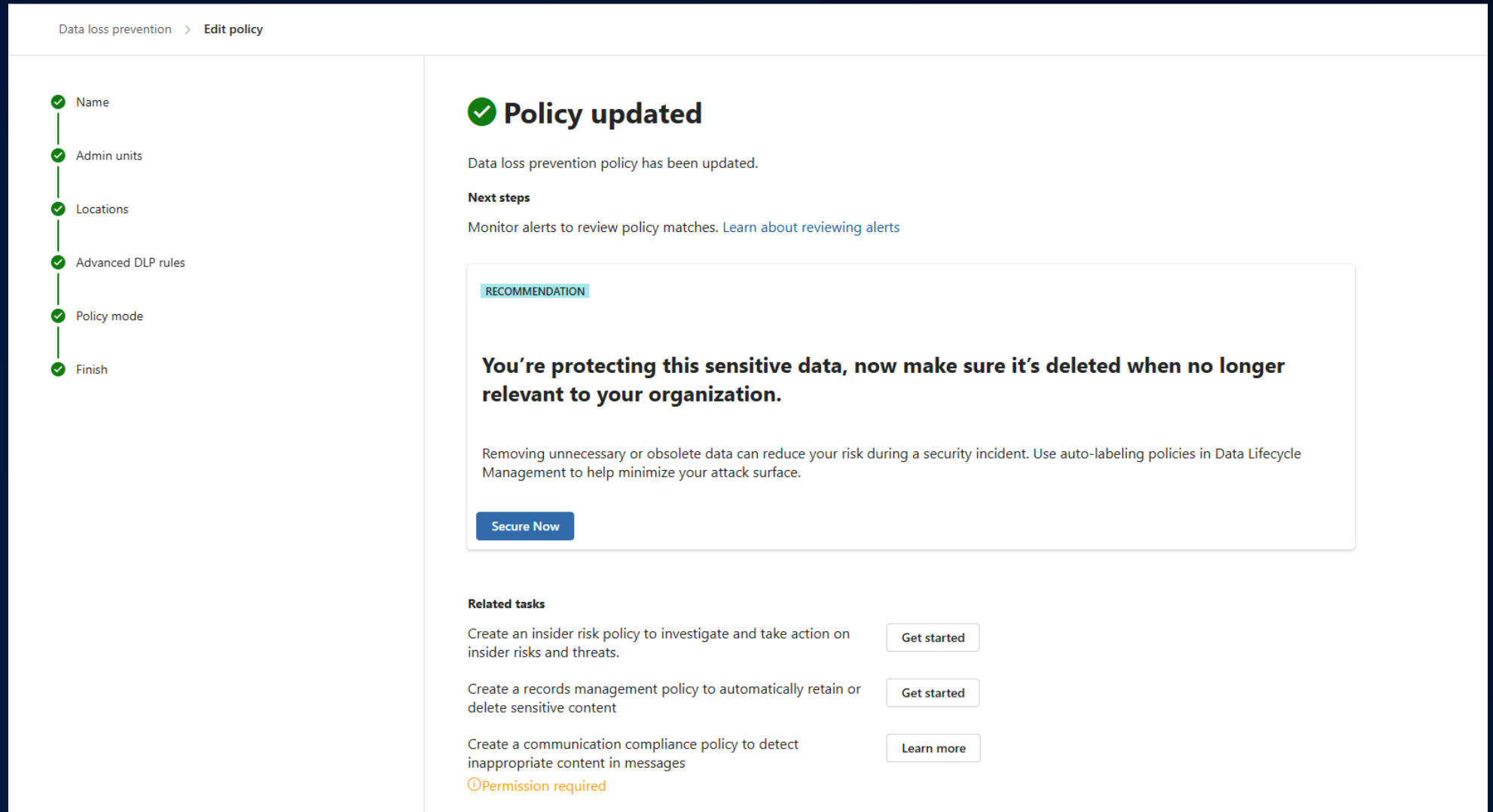
Purview Data Loss Prevention



Purview Data Loss Prevention



Purview Data Loss Prevention



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

FEEDBACK

