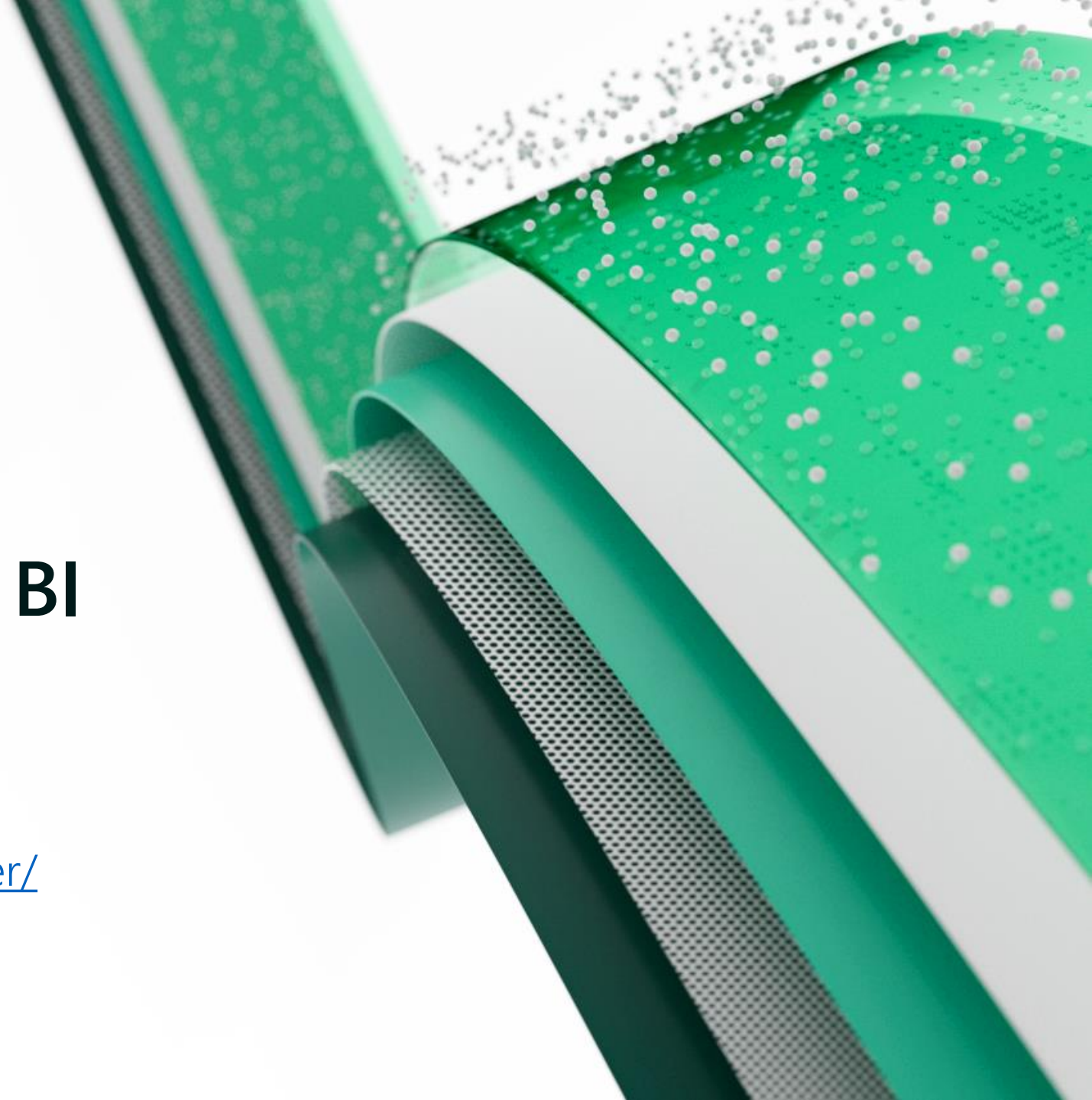
Microsoft | Microsoft Fabric



Governance in Power BI

Blocker or Enabler?

Oliver Engels /in/oengels/

Gabi Münster /in/gabimuenster/

Agenda

- What is Data Governance?
- How is Data Governance percieved in a self-service scenario?
- How can we solve the conflicts?
- How can the existing functionality help with this?

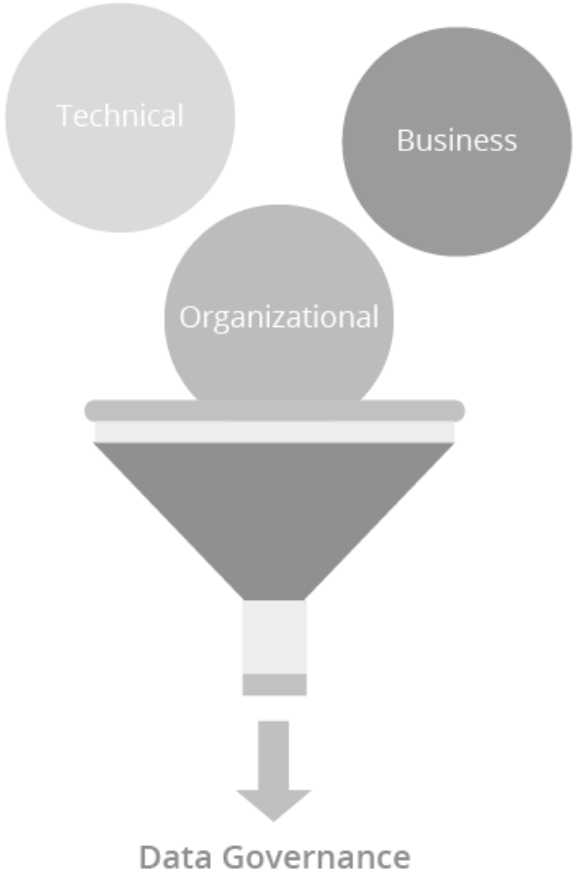
What is the objective of Data Governance?

Formal management of data within an organization



Data Governance Levels

- The organization (the “where” and “who”)
- Business aspects (the “what”)
- Technical aspects (the “how”)



Key sentences of Data Governance

+ Data is acquired from **reliable sources**
+ **Predefined data quality standards** are meet
+ It can be used to be further processed
+ It conforms with **well-defined business rules**
+ It is defined and modified by the **right person**
+ It follows a **well-documented change control process**
+ It is **aligned** to the **organizational strategy**
+ Its **trustworthiness remains intact** while data flows through various transformation cycle

Perception of governance from self-service

+ Repressive, limiting, blocking
+ Main goal is to prevent data access
+ A lot of overhead

Perception of self-service from governance

+ Anarchy

+ No control over usage and sharing of data
  → Risk of over-sharing
  → Risk of violation of regulatory requirements

+ Managing self-service requires immense effort

Consequences of extremes

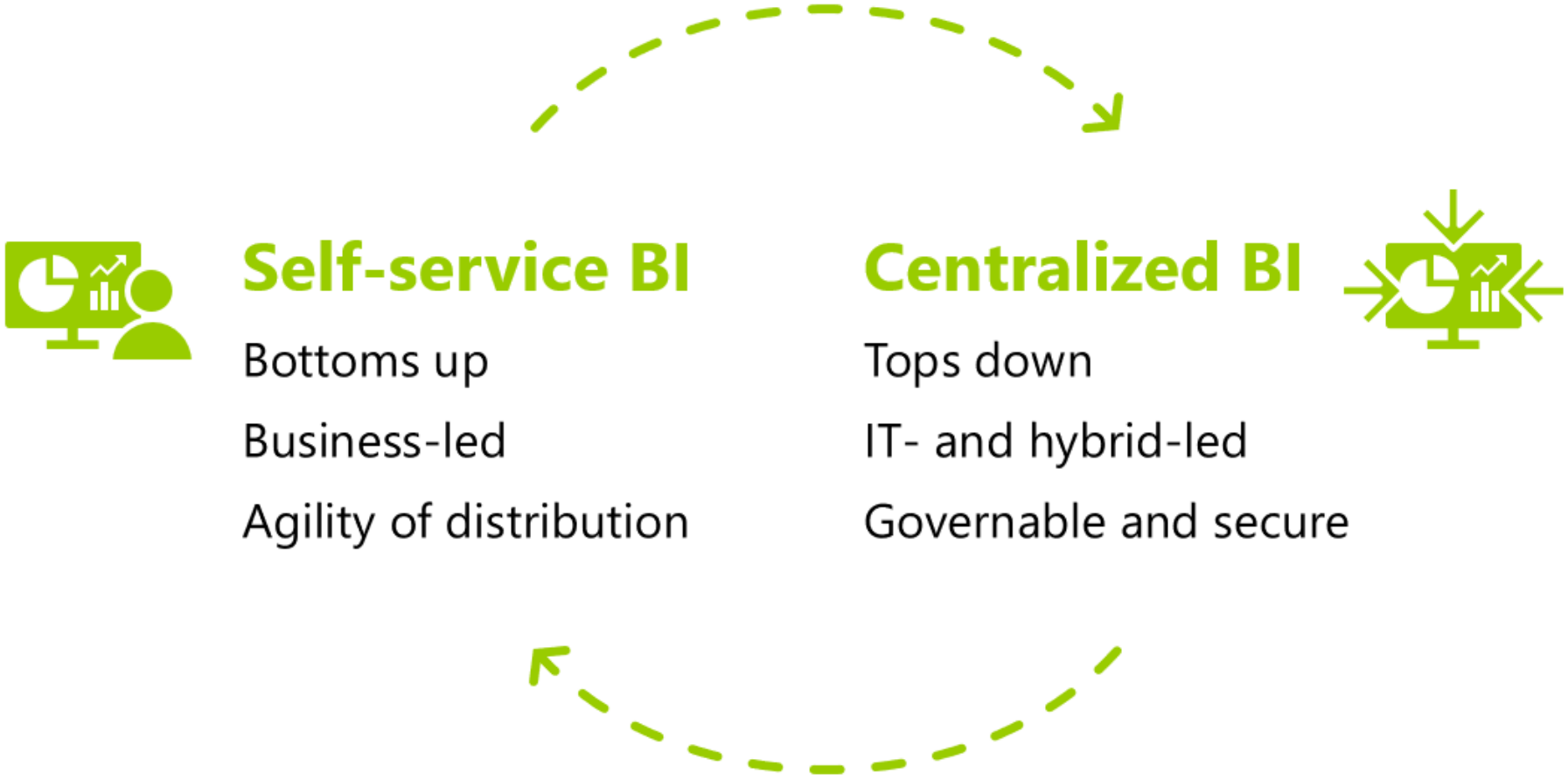
- Self-service w/o Governance
  - High risk for misuse of data and oversharing
    → can lead to insecurity and lack of adoption
  - High level of insecurity about where to find the right data
    → can lead to wrong results or lack of adoption
  - High risk of redundant and conflicting results
    → can lead to increased effort and lack of trust in results
  - Data Silos

- Overpowering Governance
  - High risk for „shadow it“
    → Users will always find a way to get access to data
    → data will be stored in unmanaged / undetected sources and oversharing cannot be prevented
  - Dissatisfaction with information management
    → Users will feel „untrustworthy“ and blocked in their work
    → High potential for conflicts between business departments and central IT

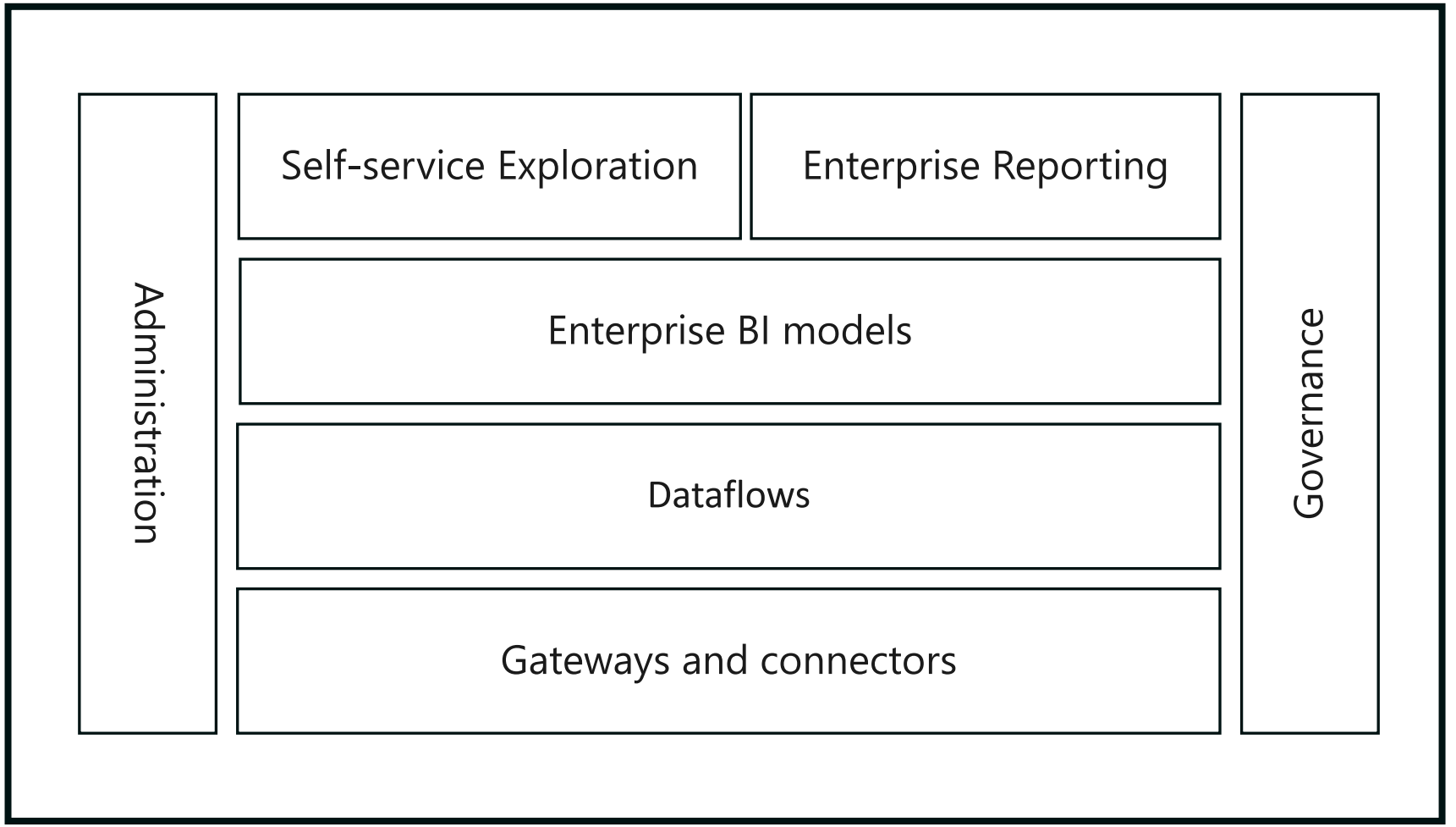
Find the right balance



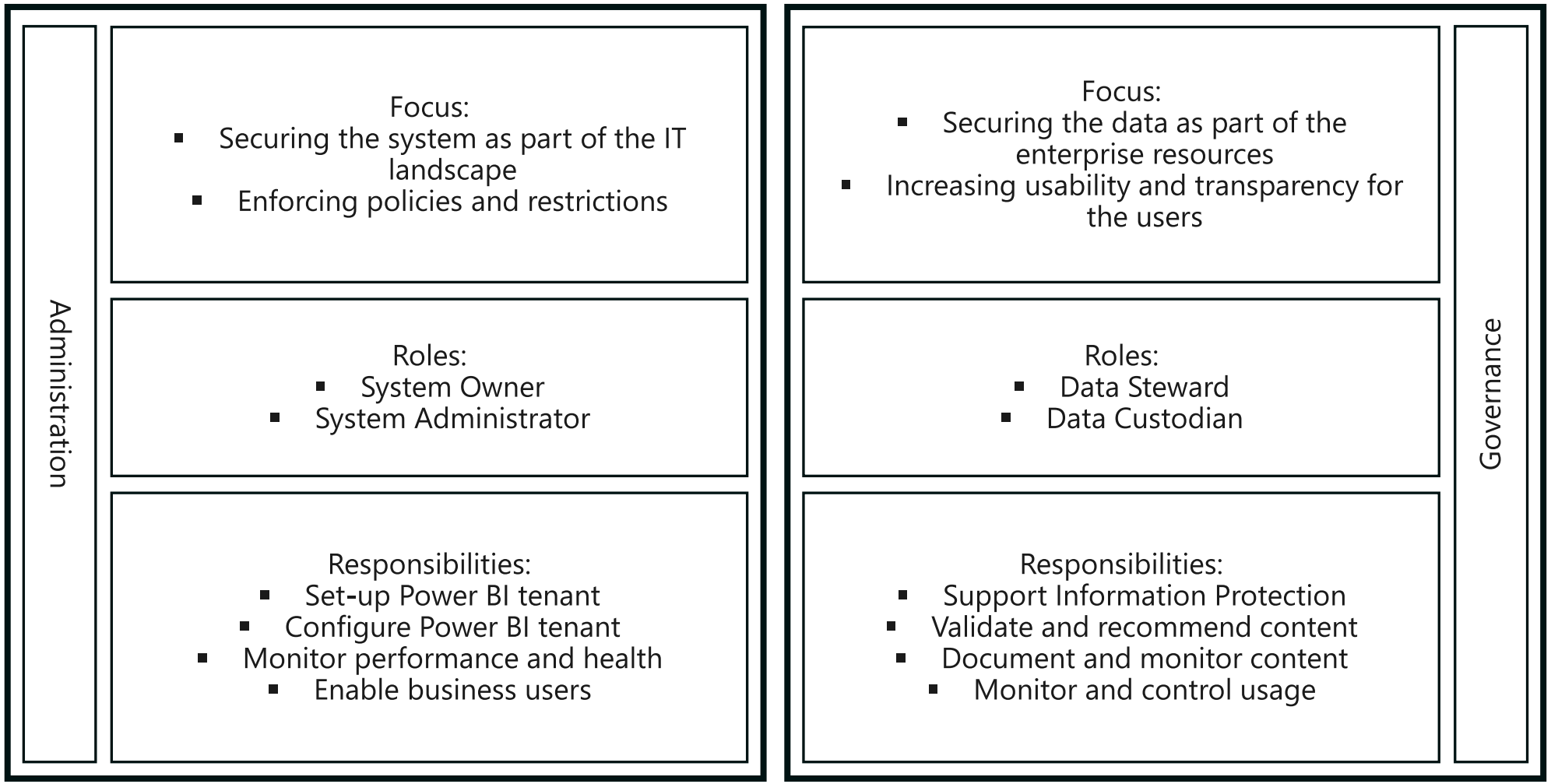
Where to find the balance in Power BI?



Self-service vs. Enterprise reporting: Different, but much in common



Objectives of Administration vs. Governance



Governance Roles – Data Steward



- Identifying and acquiring new data sources
- Creating and maintaining consistent reference data and master data definitions
- Publishing relevant data to appropriate users in an organization, and monitoring the published data sources for usage/relevance/quality feedback
- Creating and managing business metadata for published data sources to ensure that it is easily discoverable, and meaningful to information workers
- Resolving data integrity issues across stakeholders
- Analyzing data for quality and reconciling data issues

http://office.microsoft.com/en-us/office365-sharepoint-online-enterprise-help/understanding-the-role-of-data-stewards-in-data-management-HA104079191.aspx

Governance Roles – Data Custodian



+ Access to the data is authorized and controlled
+ Data stewards are identified for each data set
+ Technical processes sustain data integrity
+ Processes exist for data quality issue resolution in partnership with Data Stewards
+ Technical controls safeguard data
+ Data added to data sets are consistent with the common data model
+ Versions of Master Data are maintained along with the history of changes
+ Change management practices are applied in maintenance of the database
+ Data content and changes can be audited

http://en.wikipedia.org/wiki/Data_custodian

Simplify governance and security with Purview

Create a unified analytics and governance solution



Reshape how you access, manage, and act on data and insights by connecting every data source and analytics service together in Fabric



Manage, govern, and monitor your data estate with a governance solution designed for Microsoft Fabric

Unified governance | Unmatched compliance | Data ownership

Microsoft Purview

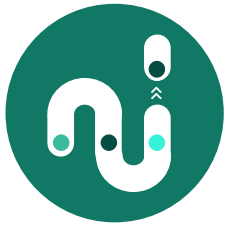
Secure and govern your data



Comprehensive data security

Secure data across its lifecycle, wherever it lives

Data Loss Prevention
Insider Risk Management
Information Protection



Modern data governance

Govern data seamlessly to empower your organization

Data Catalog
Data Estate Insights
Data Sharing (Preview)
Data Policy (Preview)
Business & Data Glossary
Data Quality Management
Master Data Management



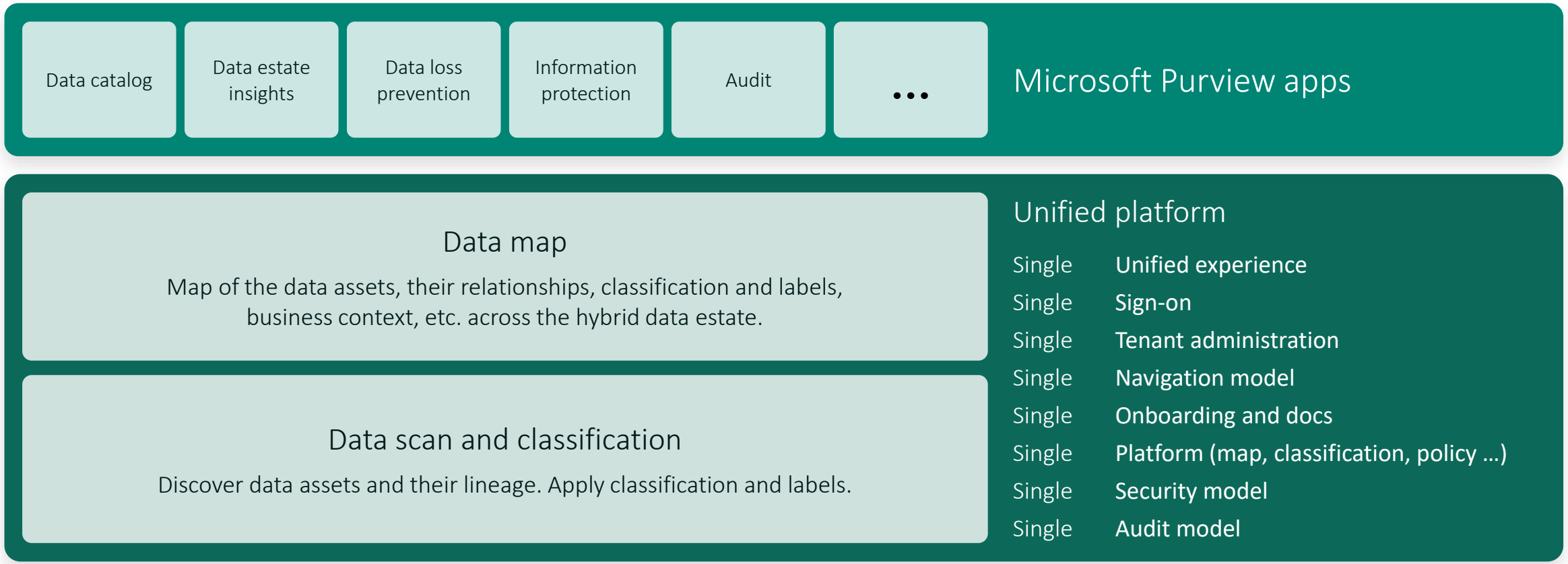
Risk and compliance posture

Manage critical risks and regulatory requirements

Compliance Manager
eDiscovery
Communication Compliance
Data Lifecycle Management Records Management

Unified Platform: Data Map, Data Classification, Data Labels, Audit, & Data Connectors

Govern and security data across your multi-cloud data estate with Microsoft Purview



On-prem and multi-cloud | Unstructured and structured data | Operational, analytical, SaaS

Gain full visibility and control with Fabric and Purview

Purview-powered features included in Fabric

- Admin portal and monitoring
- Capacity metrics
- Domains and workspaces
- One security
- Endorsements
- Data lineage and impact analysis
- Metadata scanning
- Purview Hub in Fabric
- Purview Information Protection policies[1]
- Purview Data Loss Prevention policies[1]
- Purview Audit[1]
- Free Purview Data Map and Catalog

Microsoft Purview services ideal for Fabric

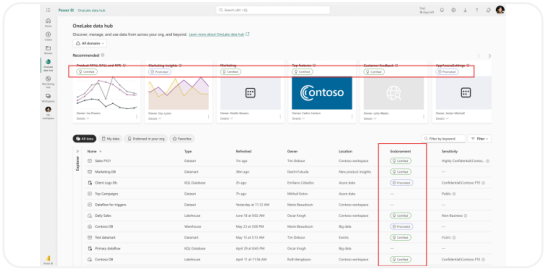
- Purview Data Map[2]
- Purview Data Catalog[2]
- Purview Data Estate Insights[2]
- Purview Data Sharing[2]
- Purview Data Policy[2]

[1]*Microsoft 365 E5 Compliance license required*

[2]*Microsoft Purview data governance capacity required*

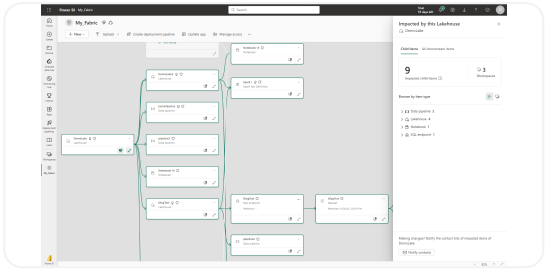
Centrally govern and protect tenant-wide while empowering business groups to manage their own data

Govern data across Fabric



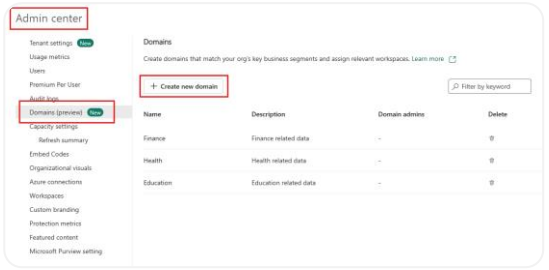
Admin portal + monitoring

Centrally manage, review and apply tenant and capacity settings for the entire Fabric tenant.



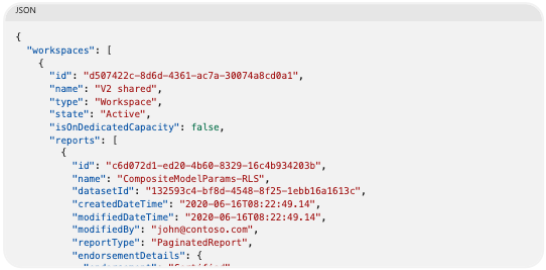
Capacity metrics

Gain visibility into capacity utilization and usage trends with daily aggregation so you can plan and scale your capacity accordingly.



One security

Use the universal security model to define security definitions once and they will live in OneLake with the data and will be enforced uniformly inside and outside of Fabric.



Domains and workspaces

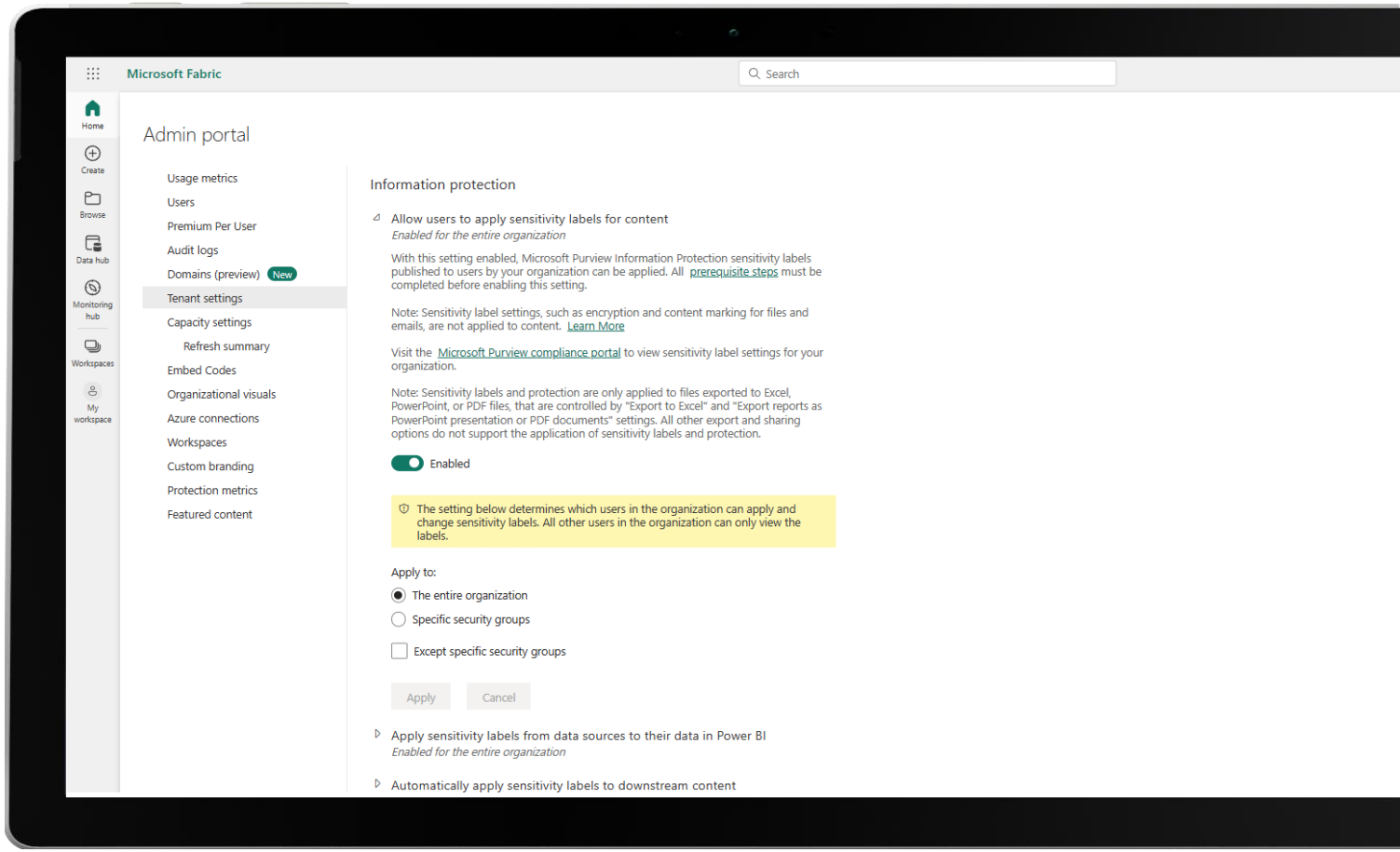
Group items like lakehouses, warehouses, and reports into workspaces. Group data and workspaces together into a domain to create a federated, governed data mesh.

Admin portal and monitoring

View usage metrics, users, audit logs, domains, workspace settings, connections, and much more all from a single, unified admin portal.

Centrally manage, review and apply tenant and capacity settings for the entire Fabric tenant.

Uncover insights for effective governance using the admin monitoring workspace which containing pre-built reports and datasets.

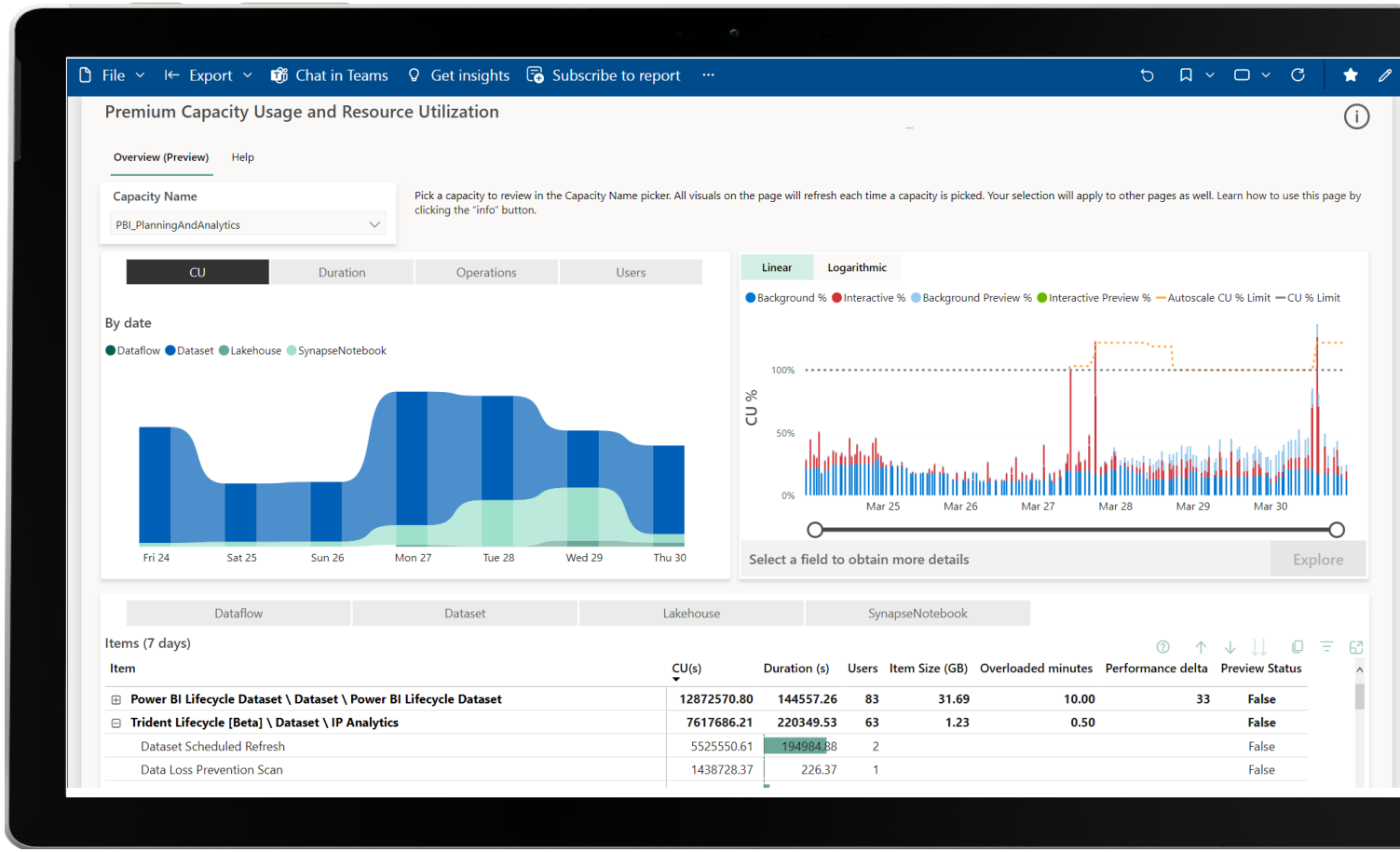


Capacity metrics

Gain visibility into capacity utilization and usage trends with daily aggregation so you can plan and scale your capacity accordingly.

See trends of usage across the different experiences hosted in Fabric and view the duration and type of operations along with user trends to measure adoption.

Zoom deeper into the data with Timepoint Drill which lets you explore usage data with the full fidelity used by the SaaS capacity platform.

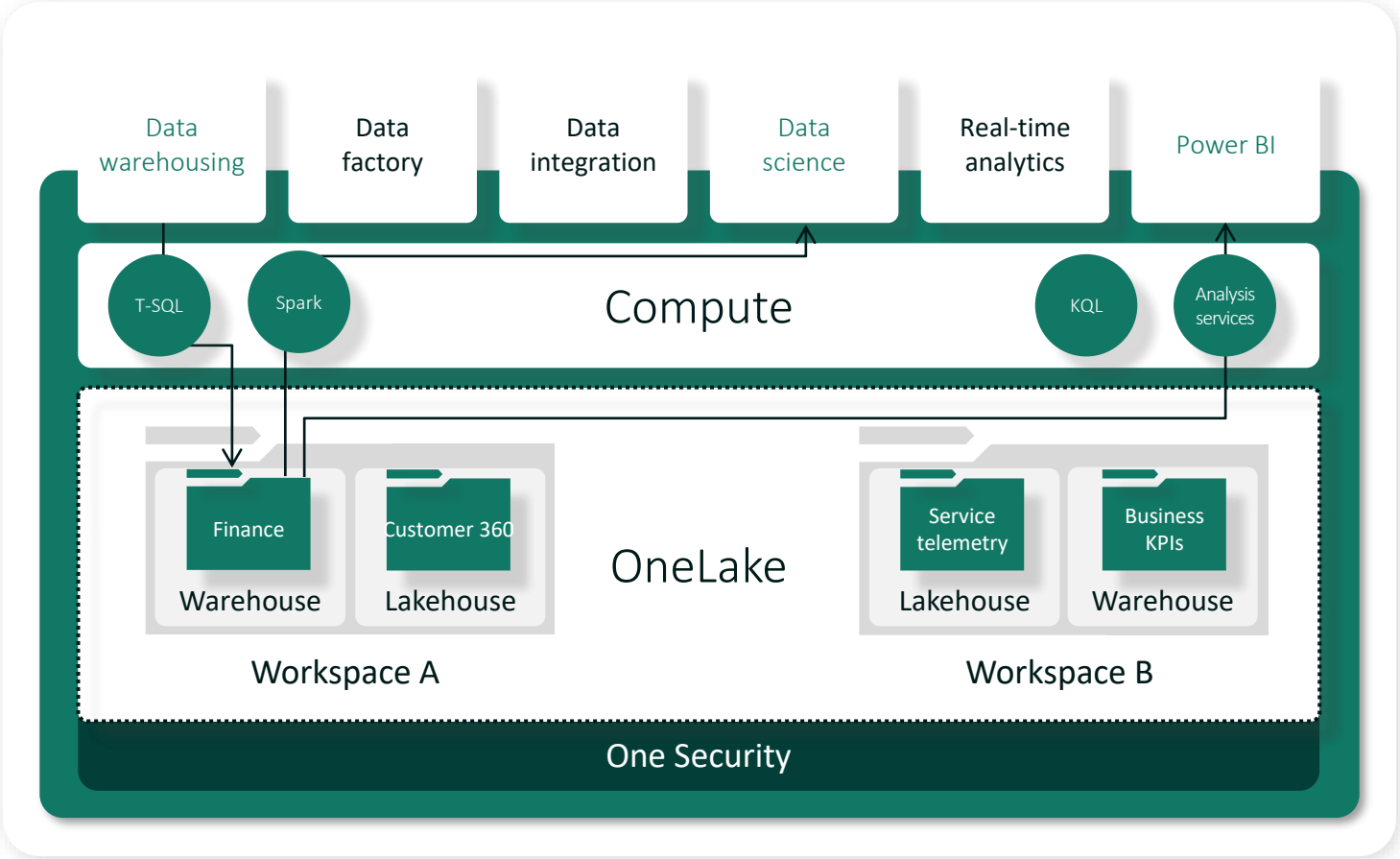


One security (roadmap)

One Security, a shared universal security model defined in OneLake, secures your data without copying it to another location.

More granular security can be defined once in OneLake. This includes column level security, row level security, data masking, etc.

Security definitions will flow across all shortcuts and will be enforced in all engines including non-Fabric engines.

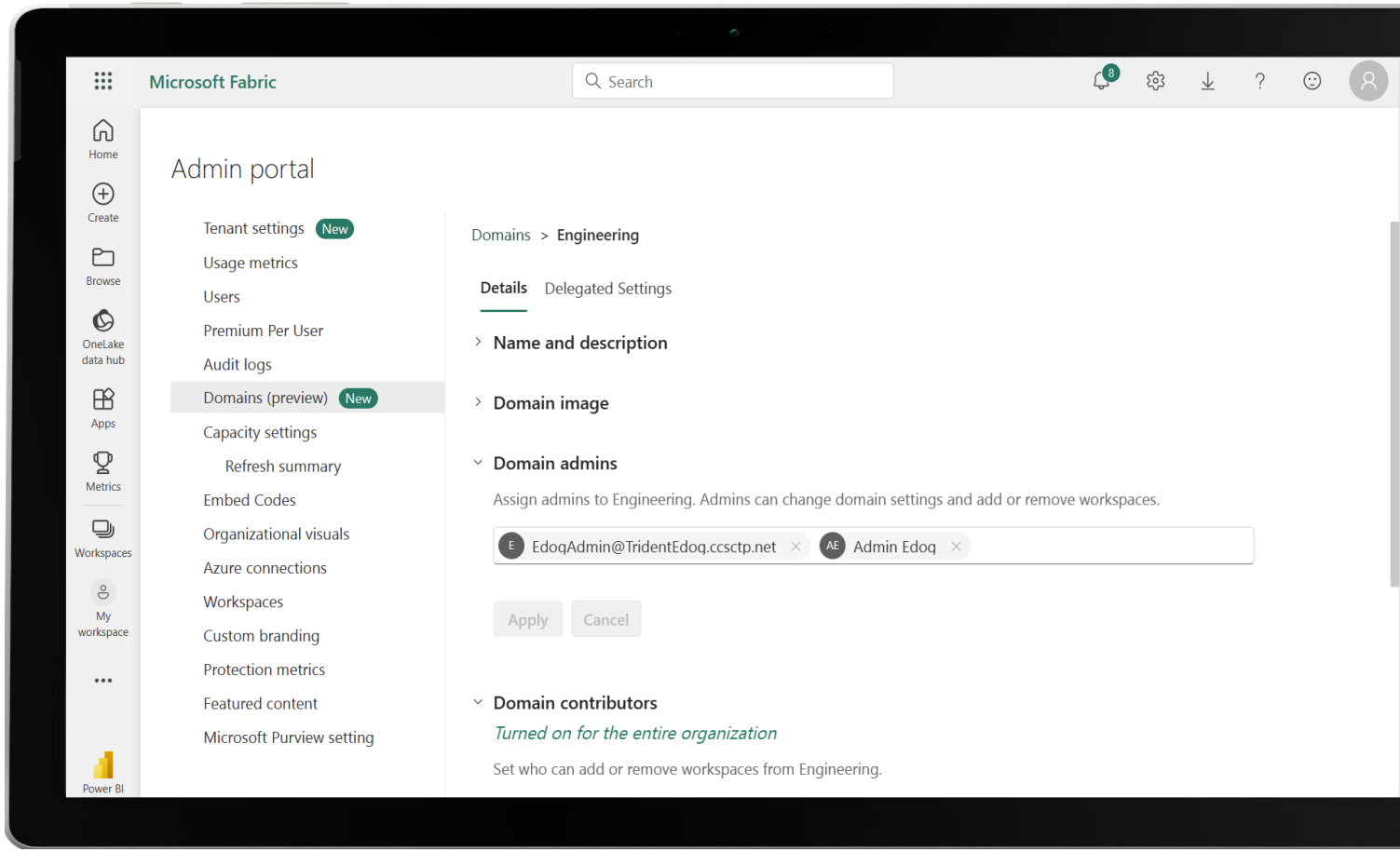


Domains

Create a federated data mesh by grouping together data relevant to a particular area or field (e.g., department) in a domain.

Find relevant data faster by filtering and finding content by domain.

Assign domain roles and admins and delegate some governance control to the domain-level, enabling each business unit to define its own rules and restrictions according to its specific business needs.



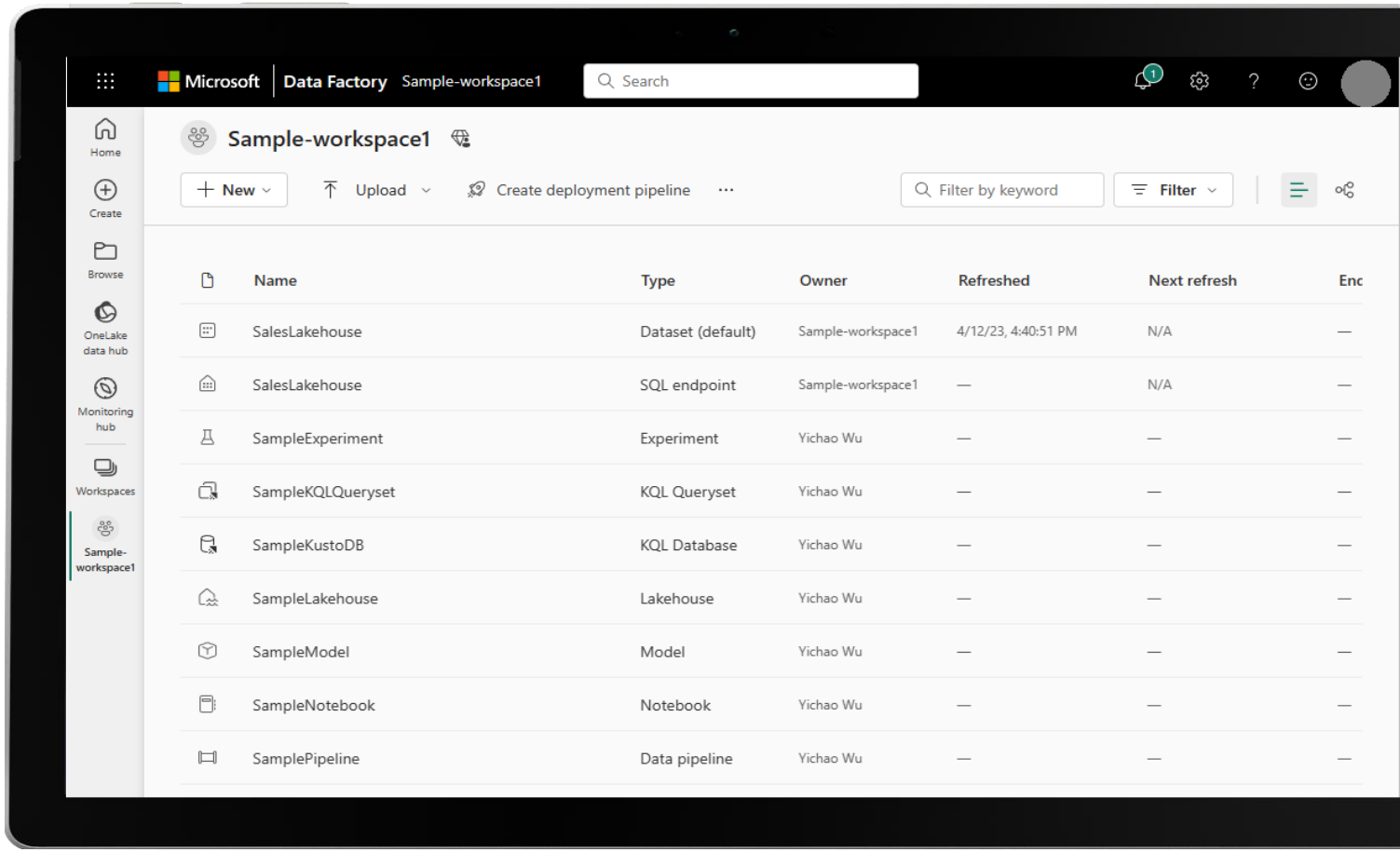
Workspaces

Collaborate with colleagues to create collections of items such as lakehouses, warehouses, and reports in a workspace.

Associate workspaces with a domain in the admin portal and to adopt that domain's governance policies.

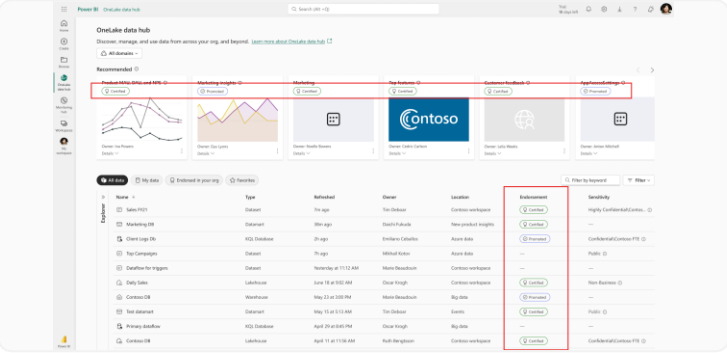
Create a new, custom default Spark pool for the workspace (if granted permissions by the capacity admin).

Workspace admins have the flexibility to set default settings for their users.



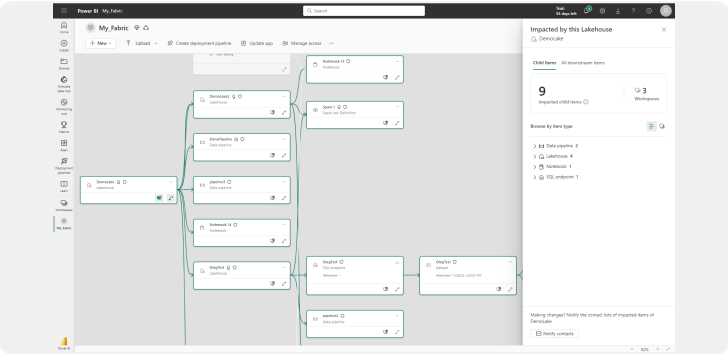
Give your data professionals the tools they need to maintain a single source of truth for your data

Govern data across Fabric



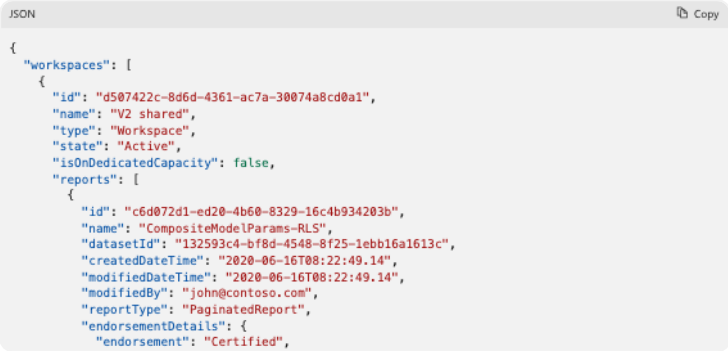
Endorsements

Endorse high-quality content in Fabric to create curated sources of truth and increase discoverability and reuse



Data lineage and impact analysis

See lineage view of analytical projects to see how data flows through items and perform impact analysis to assess impact of changes



Metadata scanning

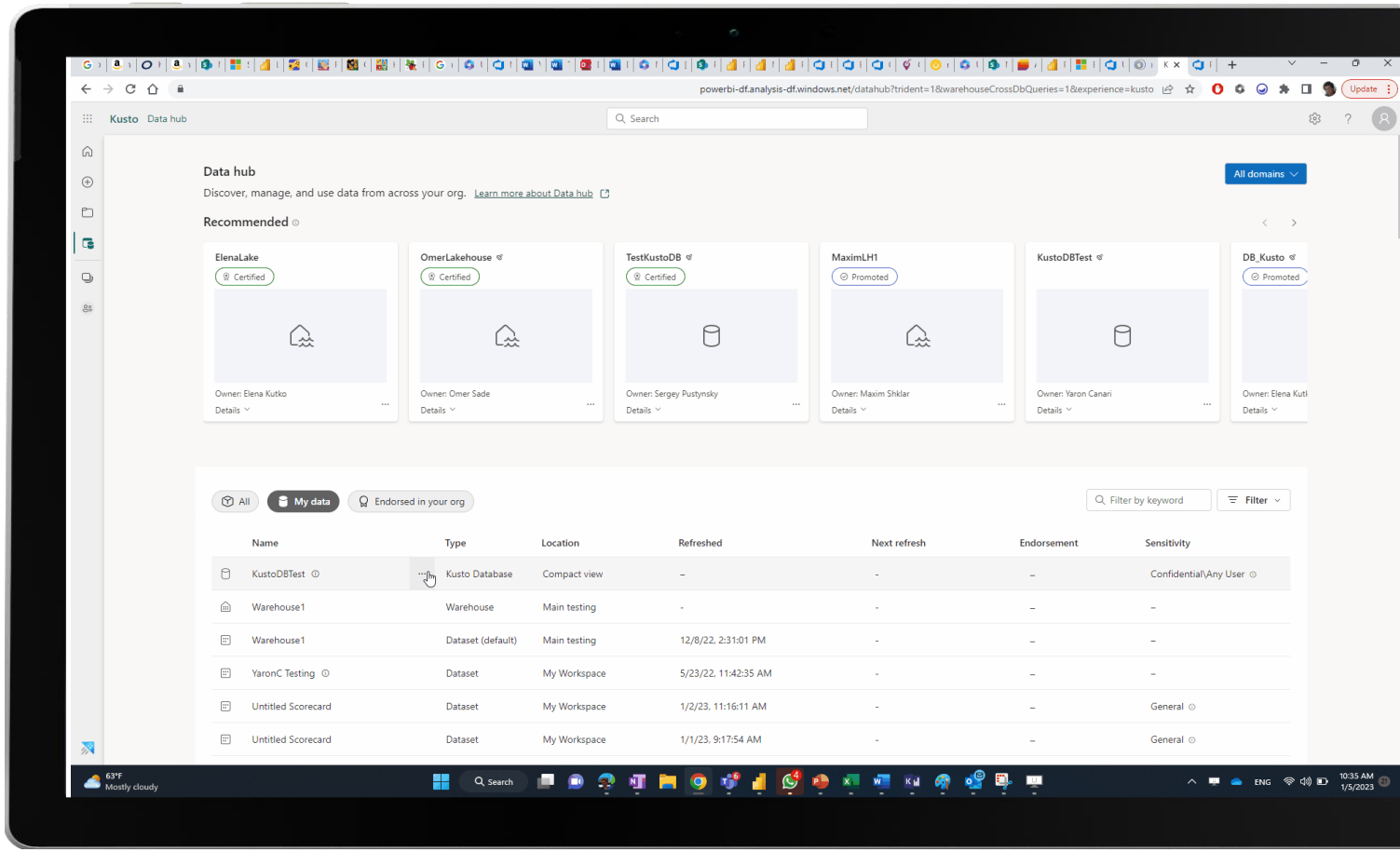
Extract information such as item name, owner, sensitivity label, and endorsement status for all items across Fabric

Endorsements

Data owners can endorse valuable, high-quality content in Fabric to create curated sources of truth, increase their discoverability, and encourage reuse.

Authorized users can certify data that meets the organization's quality standards and anyone can promote data they find valuable and recommend for others to use.

Endorsed items get higher visibility in Fabric data discovery experiences.

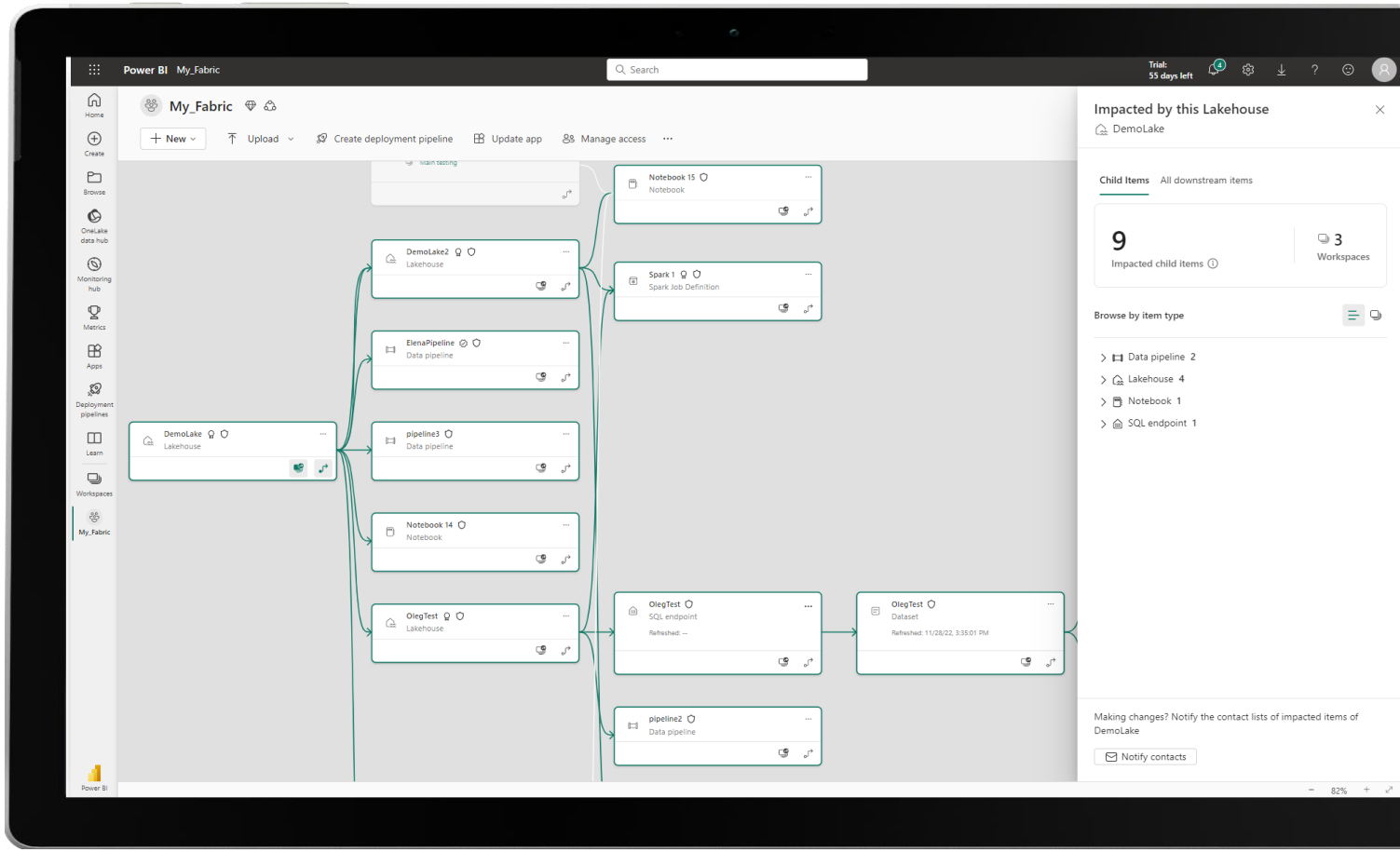


Data Lineage and impact analysis

See lineage view of complex analytical projects to understand how the data flows through all Fabric items, including lakehouses, data warehouses, pipelines, datasets and reports.

Troubleshoot data refresh issues while tracing the data back from the destination to the source and monitor refresh status.

Perform impact analysis to assess impact for upcoming changes.

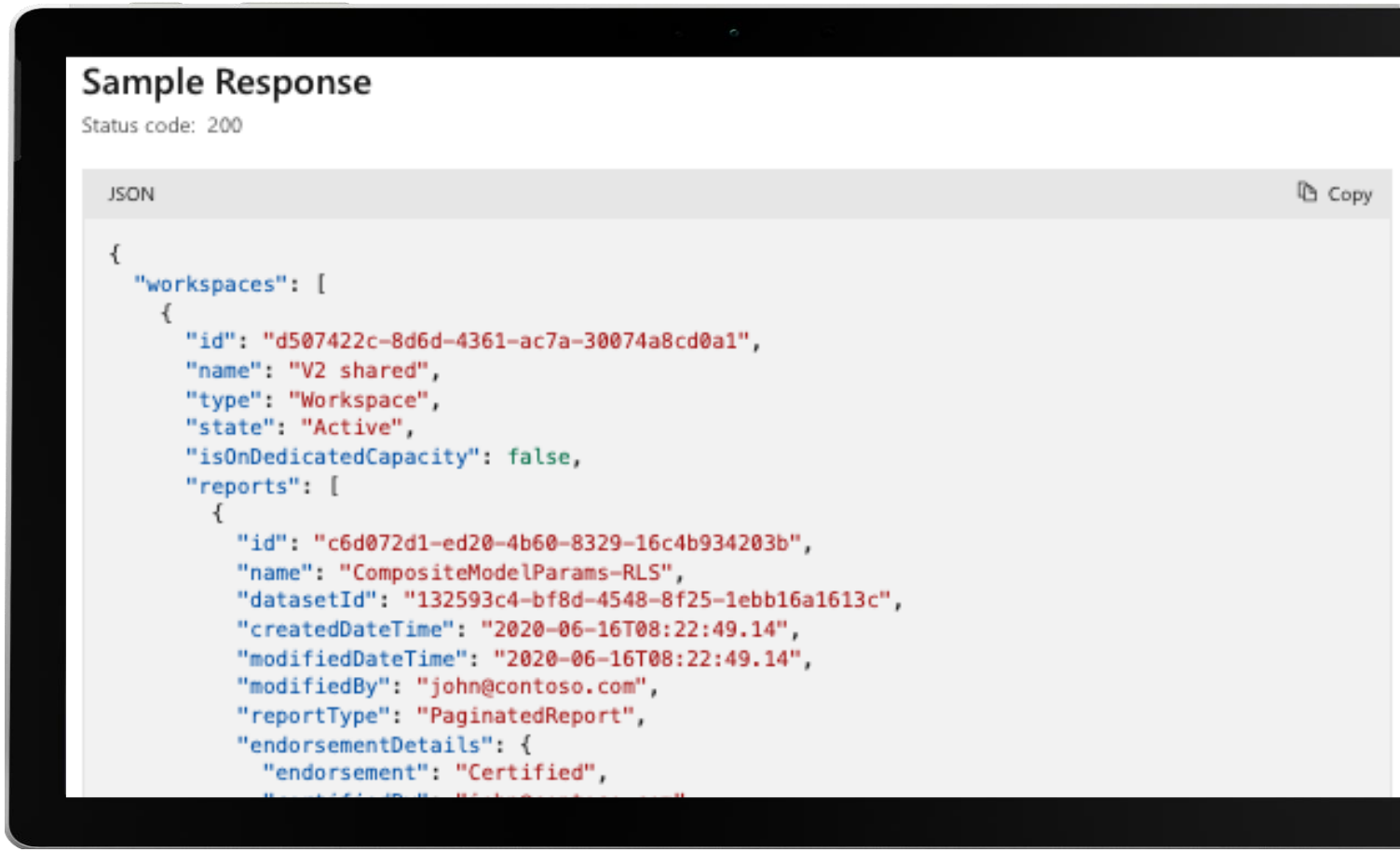


Metadata scanning via API

Fabric's Scanner APIs enables effective scanning of Fabric's tenant metadata and lineage, including item's name, owner, sensitivity label, endorsement, data source, etc.

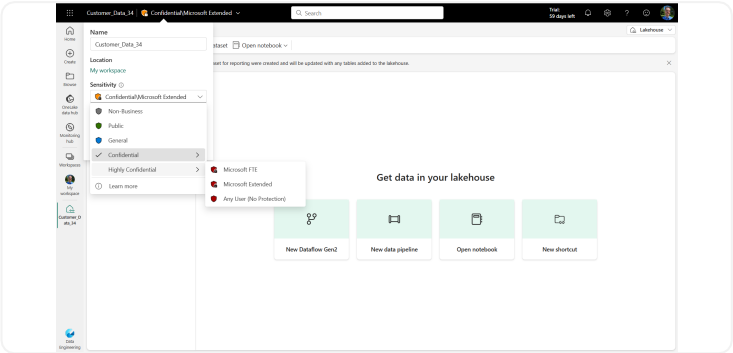
Robust enterprise capabilities like authentication with service principal and incremental scans.

Supports 1st and 3rd party catalog tool integration.



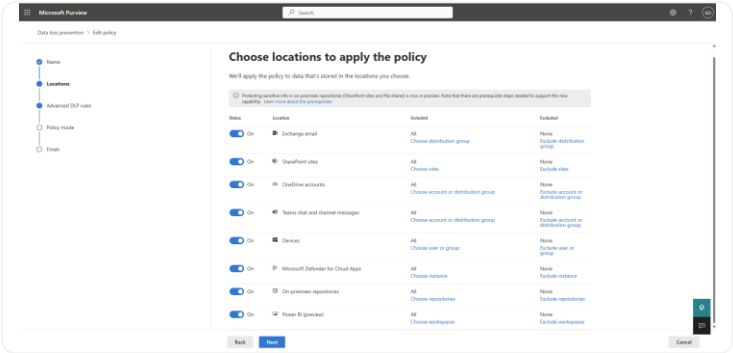
Use Purview-powered security and compliance features to protect your data in OneLake

Secure and protect data across your organization



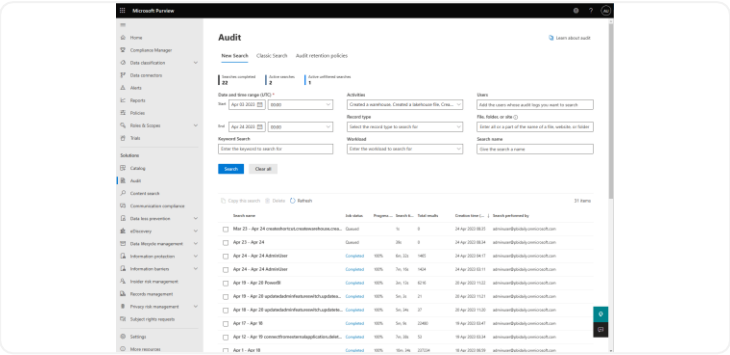
Information Protection*

Label Fabric items with organization's sensitivity labels



Data Loss Prevention*

Automatically detect the upload of sensitive data



Audit*

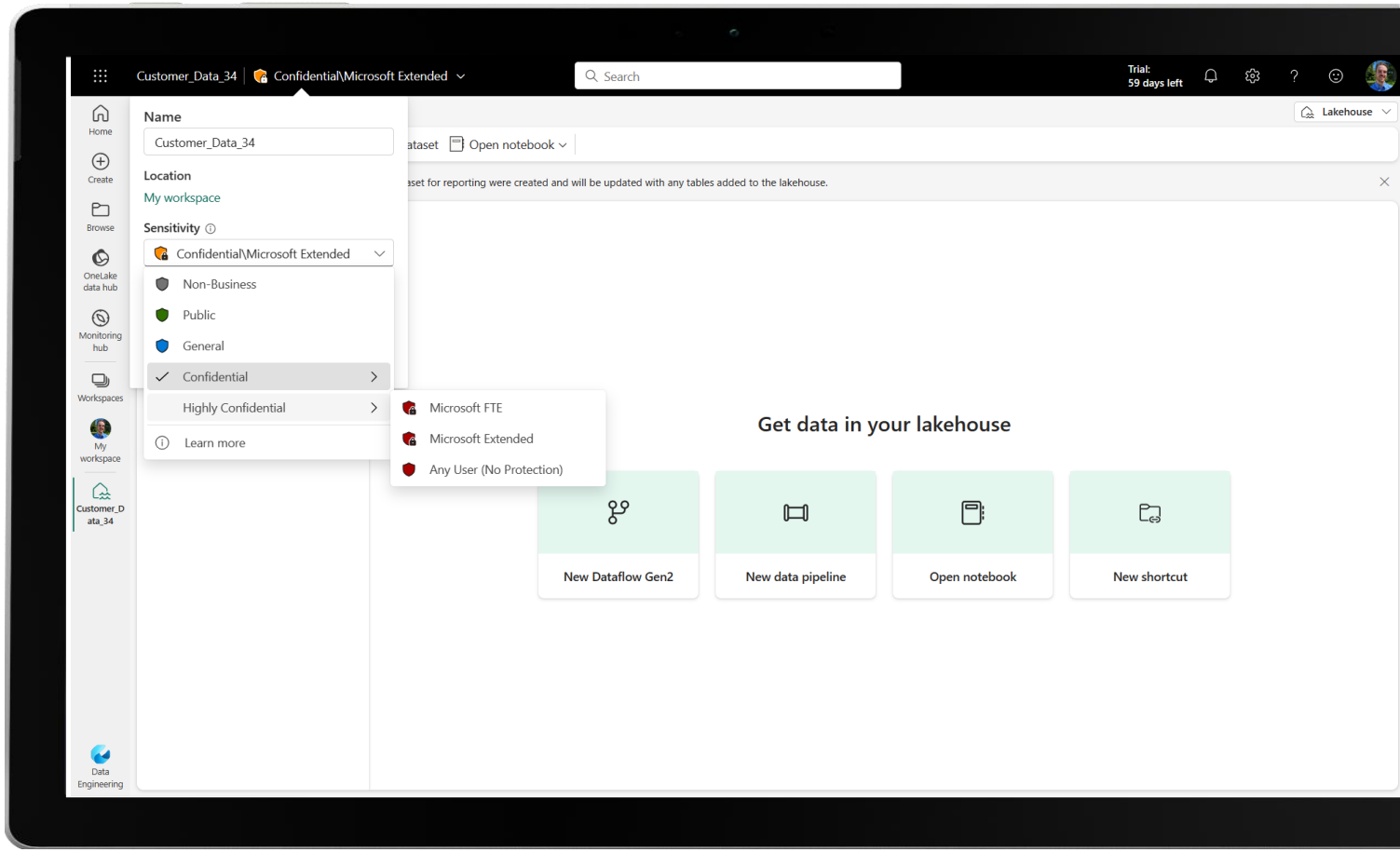
Log user activities from Microsoft Fabric to support forensic investigations

**Microsoft 365 E5 Compliance license required*

Microsoft Purview Information Protection for Fabric

Label Fabric items with organization's sensitivity labels, used in Microsoft 365 apps.

Sensitivity labels follow the data automatically as it flows from data lake to business users within Fabric and to Office.

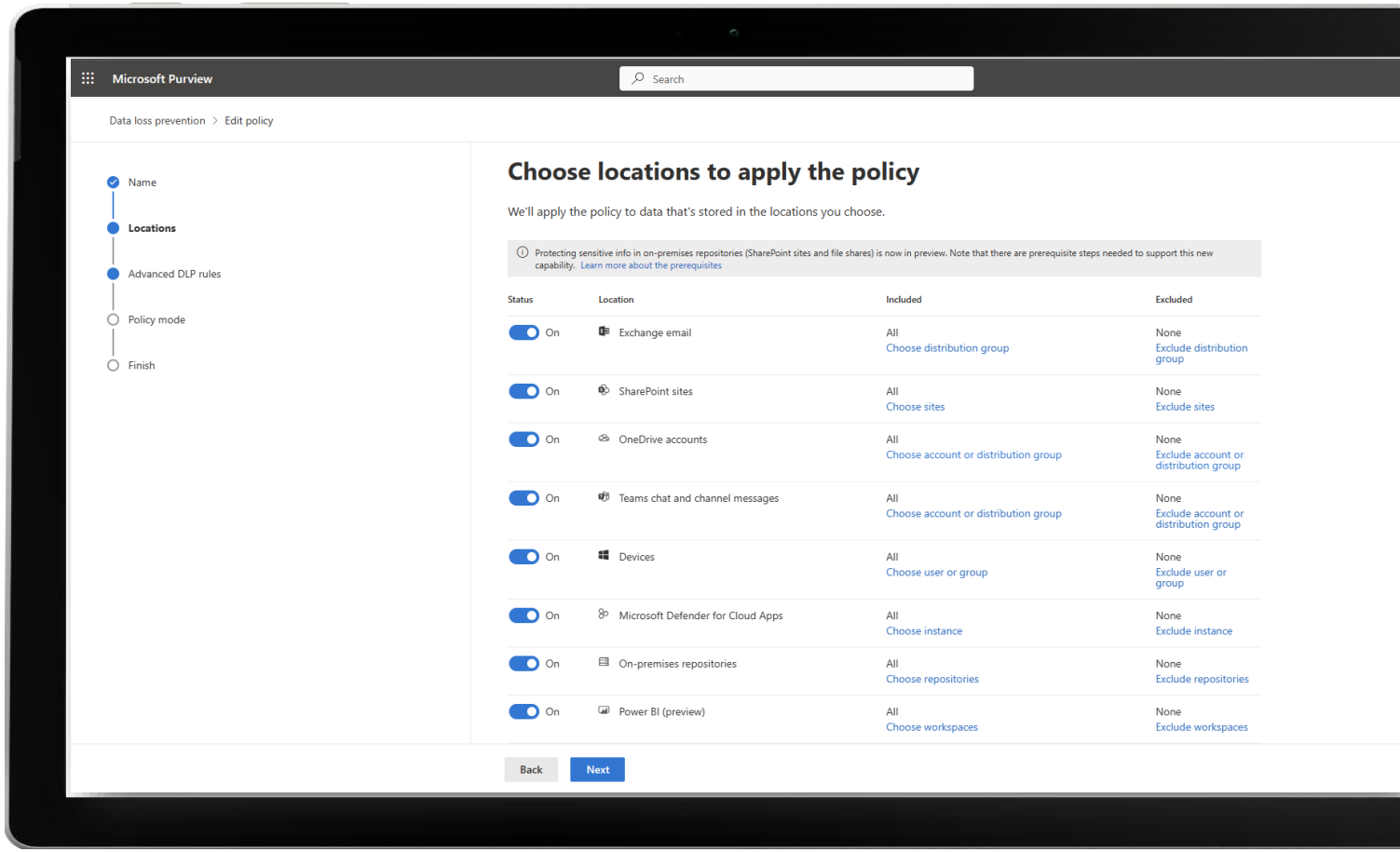


**Microsoft 365 E5 Compliance license or similar required*

Microsoft Purview Data Loss Prevention policies

Automatically detection of upload of sensitive data, supporting trigger alerts for admins and custom policy tip to data owners.

Data owners can provide feedback using report a false positive action.



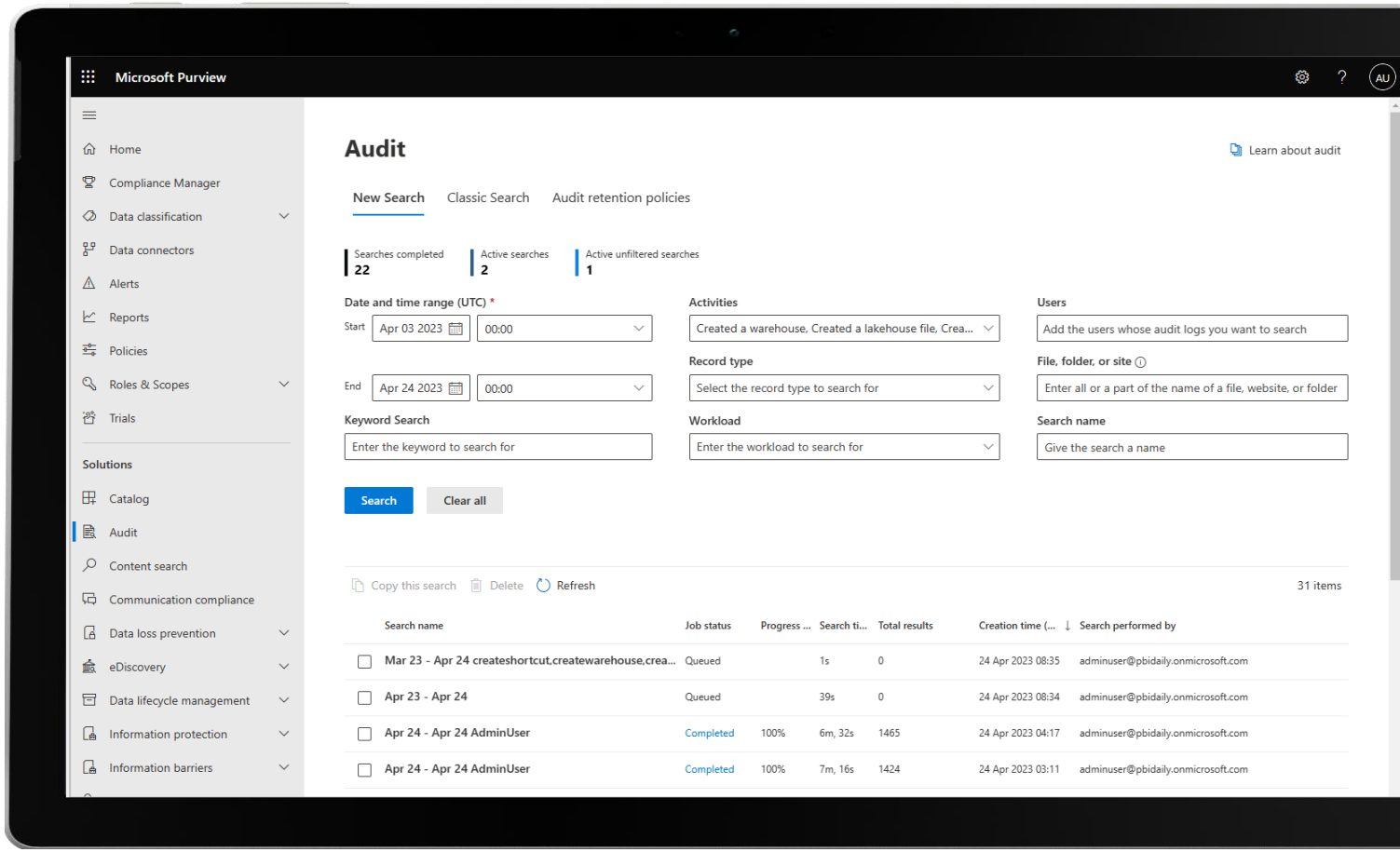
**Microsoft 365 E5 Compliance license or similar required*

Microsoft Purview Audit

Support forensic investigations, preserve audit logs to meet regulatory requirements and gain high-bandwidth access to data.

Microsoft Fabric user activities are logged and available in the Microsoft Purview audit log.

Use the Fabric admin monitoring workspace to explore audit logs in Purview.



**Microsoft 365 E5 Compliance license or similar required*

Microsoft

Thank you

