Understanding Microsoft Information Protection

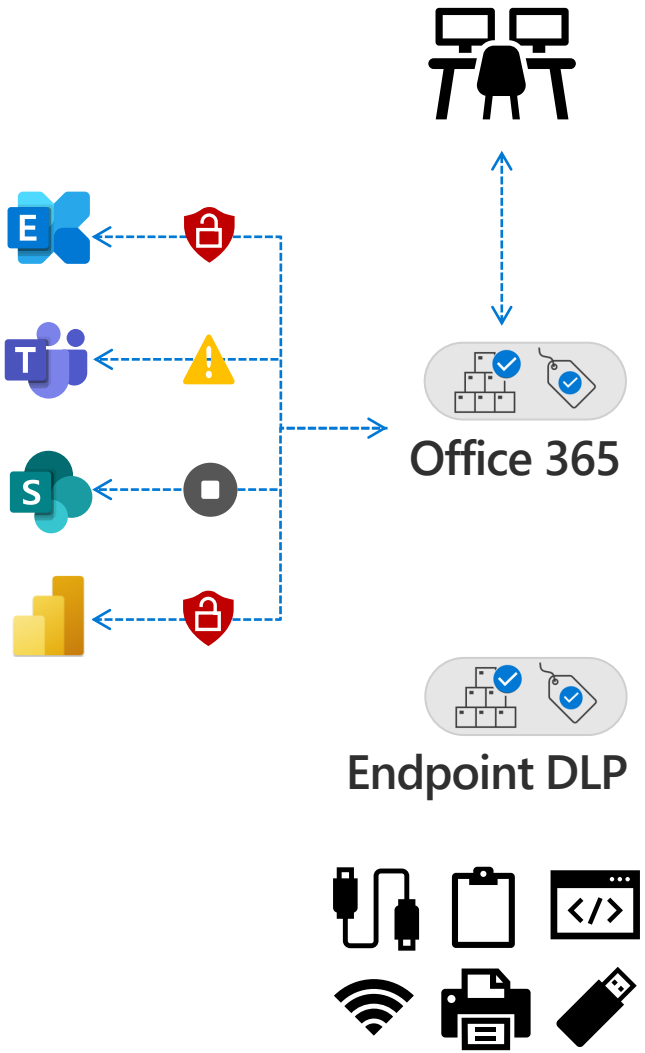
Mark Warnes, Architect (Kocho)

Vrunda Monnappa, Digital Technical Specialist (Microsoft)

Kocho

BECOME GREATER

Microsoft Purview Information Protection



Office 365

Endpoint DLP

Data Classification Service

Sensitive Information Types

Sensitivity Labels

Out of the Box
CCN/SSN/License
Double Key Encryption
Named entity
10 templates (Finance, IP, Legal, Healthcare...)

Custom
RegEx
Dictionary
Fingerprint
Exact Data Match (EDM)

Trainable Classifiers
Sample Content
Test
Validate
Publish

Public
General
Confidential
...

Extendable via SDK to 3rd party tools

Defender for Cloud Apps

On-premises

Microsoft Purview data governance services

Advanced compliance solutions

eDiscovery (Premium)

Insider Risk Management

Communication Compliance

Microsoft Priva

Microsoft Information Protection

Data Classification Analytics

MIP Scanner

Understand your data landscape and identify important data across your hybrid environment

Sensitivity Labels

Apply classifications to mark your data, including file-based protection

Data Loss Prevention

Apply checks and controls around data to prevent inappropriate sharing

Know your data

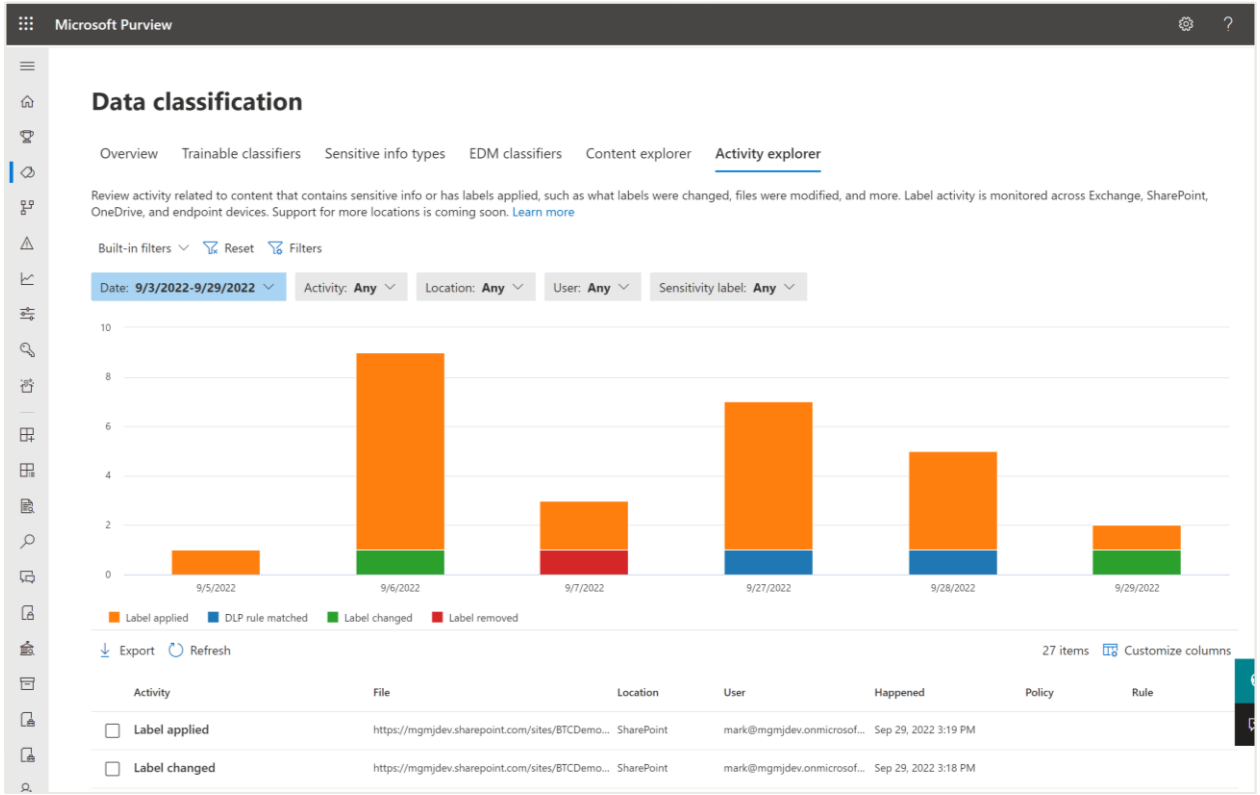
Data Classification

Overview of types of info in your environment

Use out-of-box and define custom classifiers

See where data resides with Content Explorer

See what is happening with your data with Activity Explorer



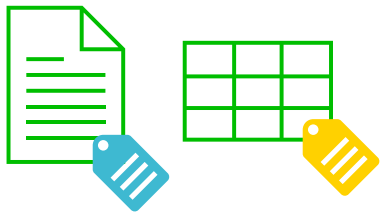
MIP Scanner

Extend data classification to on-premises file repositories

Protect your data

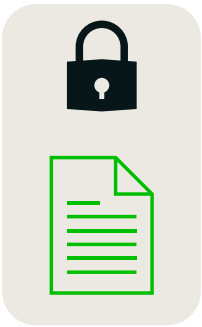
Sensitivity Labels

Central unified labels for classifying & protecting files, emails, sites, groups & assets



Apply to documents within Office apps and SharePoint libraries

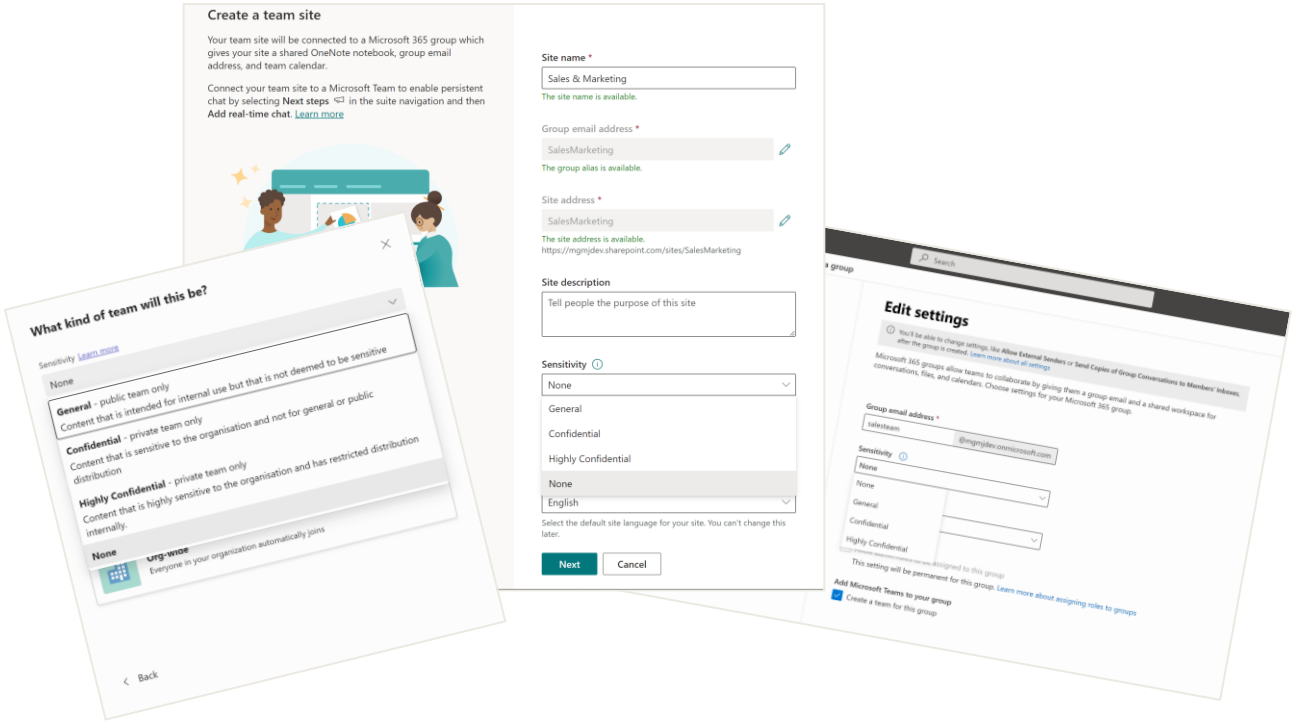
Add visual markings with customised text



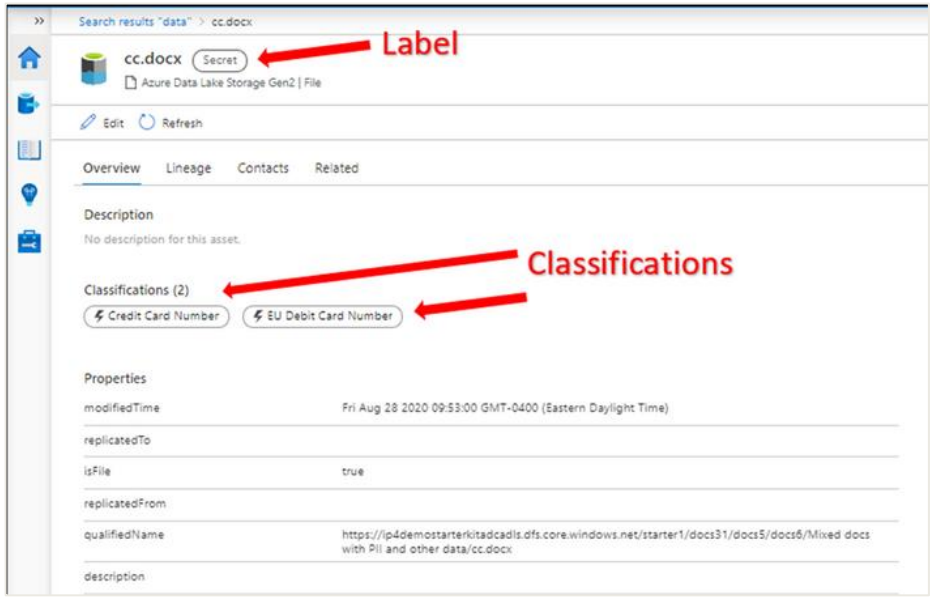
Encrypt contents, control access, and define usage rights

Auto-apply labels by matching document content with M365 classifiers

Protect your data



Apply to SharePoint sites, Teams and Groups to define privacy and access settings



Apply labels to files and schematized data assets in Microsoft Purview Data Map (including SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more)

Prevent data loss

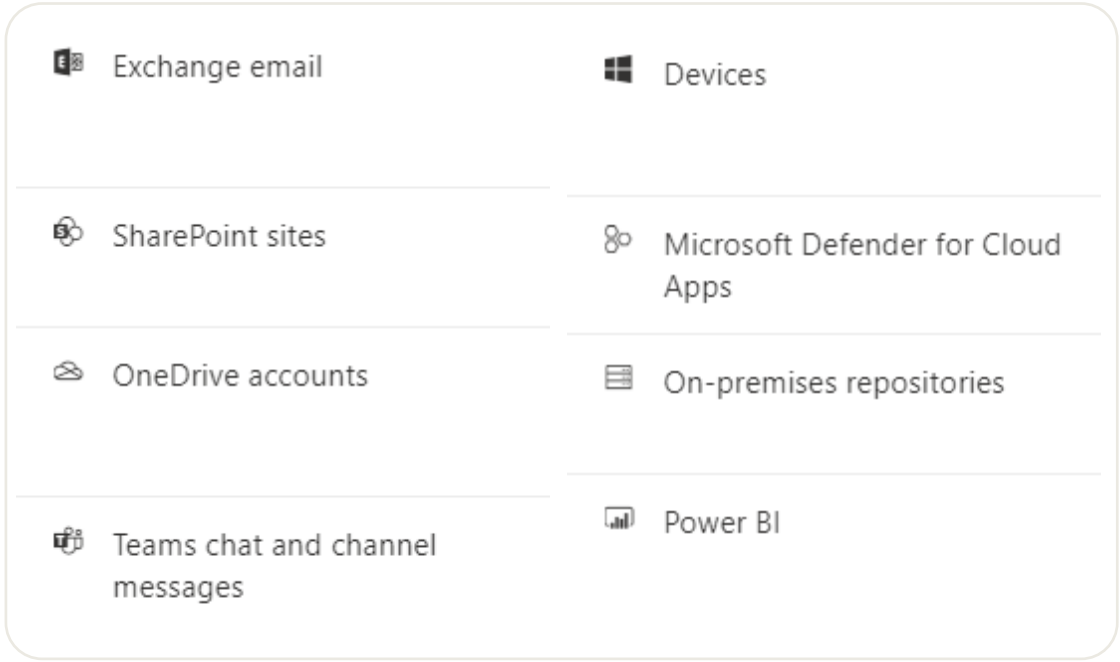
Data Loss Prevention

Make sure sensitive information in email, docs and more isn't shared with the wrong people

Centralised, unified policies for simpler management

Detect sensitive info and/or other attributes

Define actions to restrict access or manipulate the content

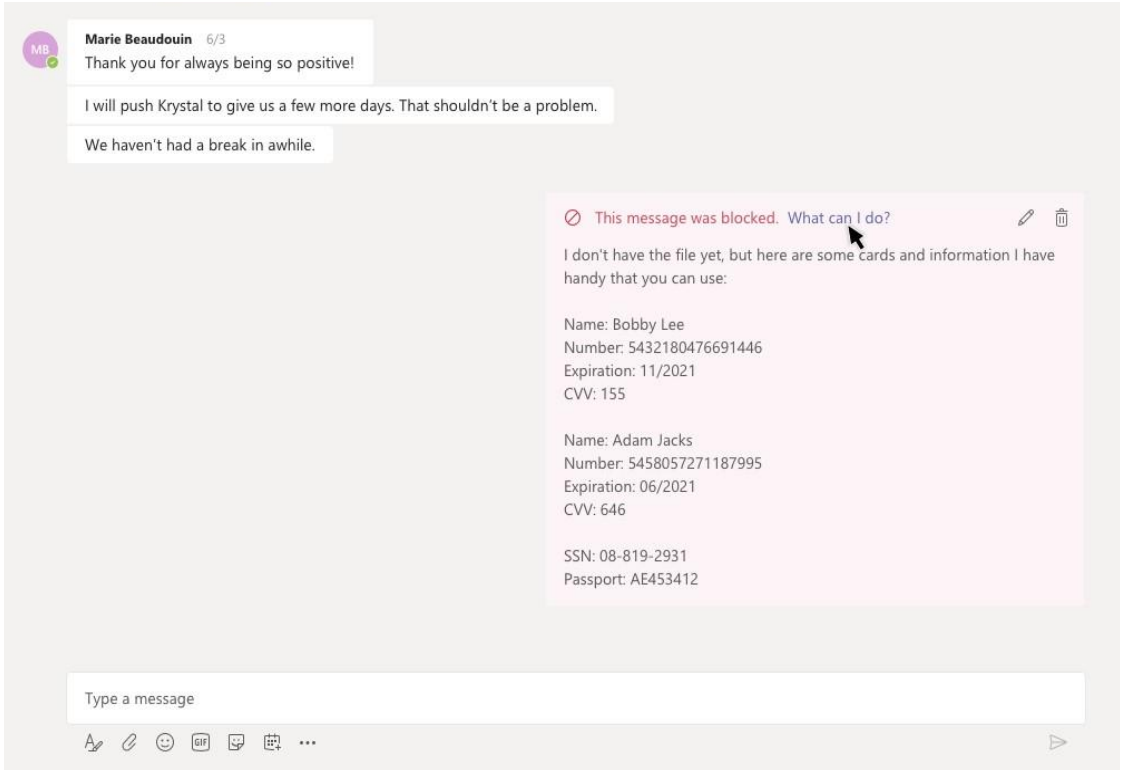


Raise alerts to security team for further analysis or action

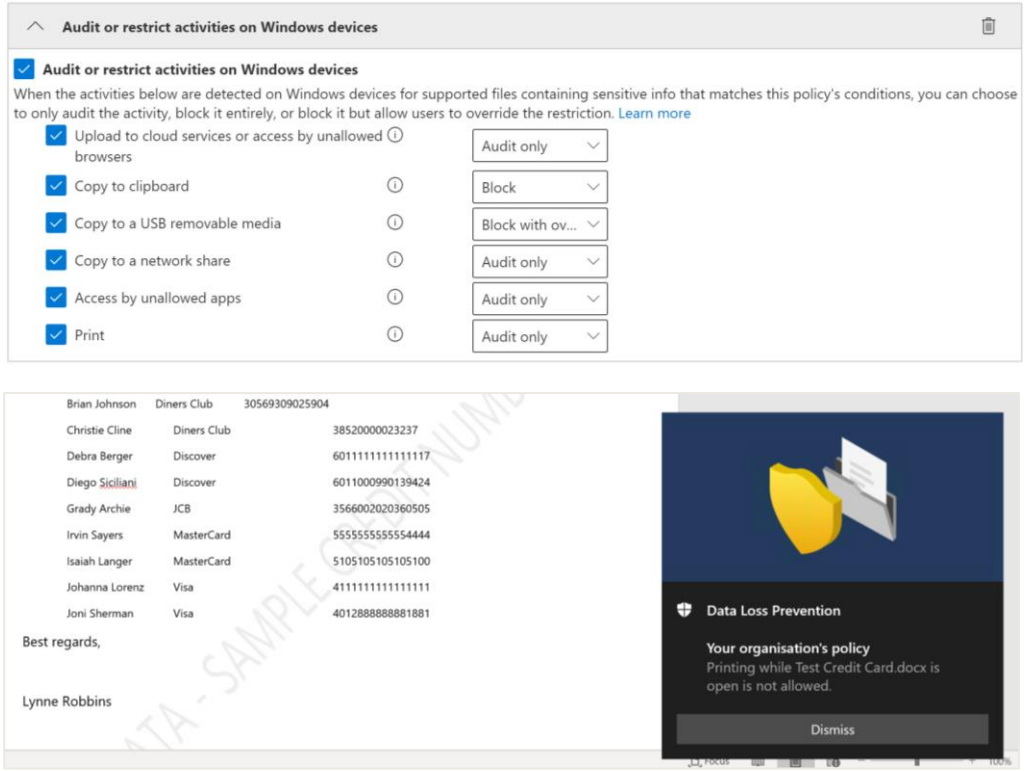
Extend DLP control onto endpoints, third-party cloud apps, and on-prem file shares

Prevent data loss

Automatically block messages which contain sensitive information, and educate and guide end-users with notifications and “policy tips”

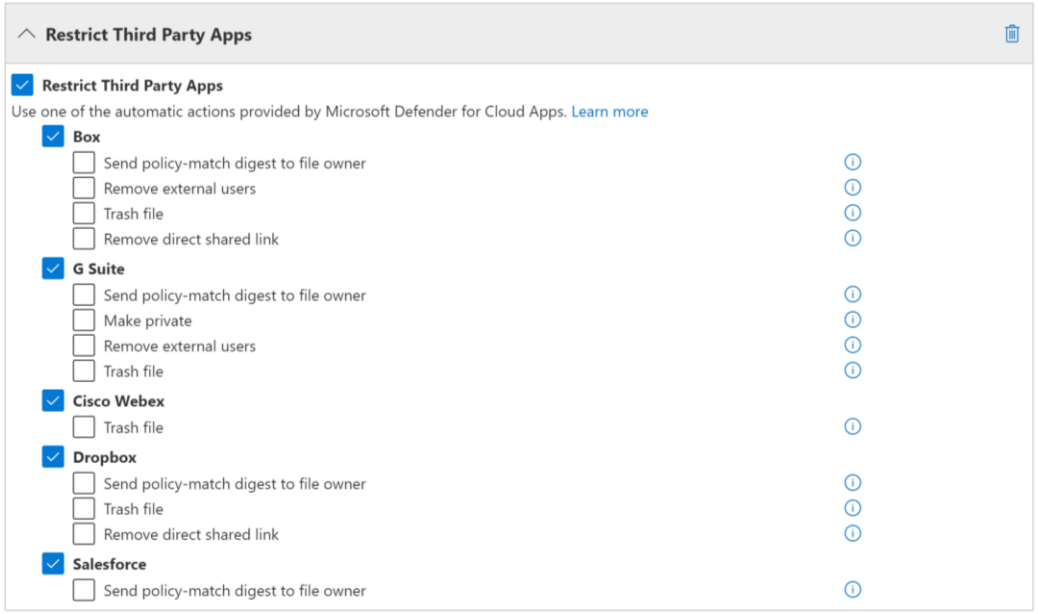


Monitor and protect sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices

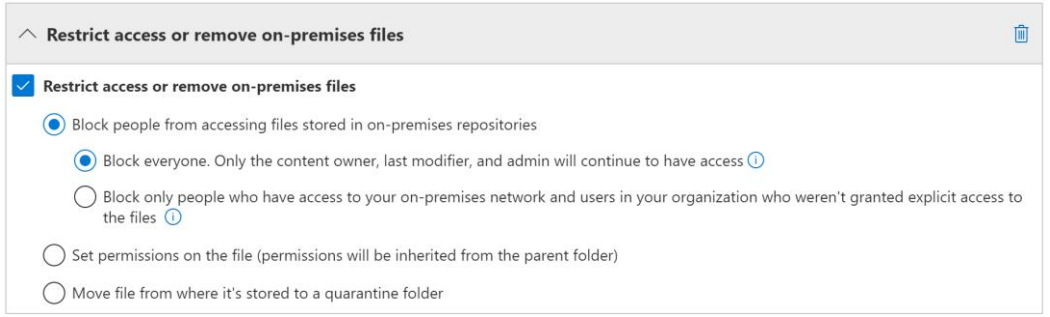


Prevent data loss

Extends into Microsoft Defender for Cloud Apps to detect and control sensitive info in third-party apps



Uses the MIP scanner to apply actions to on-premises file repositories

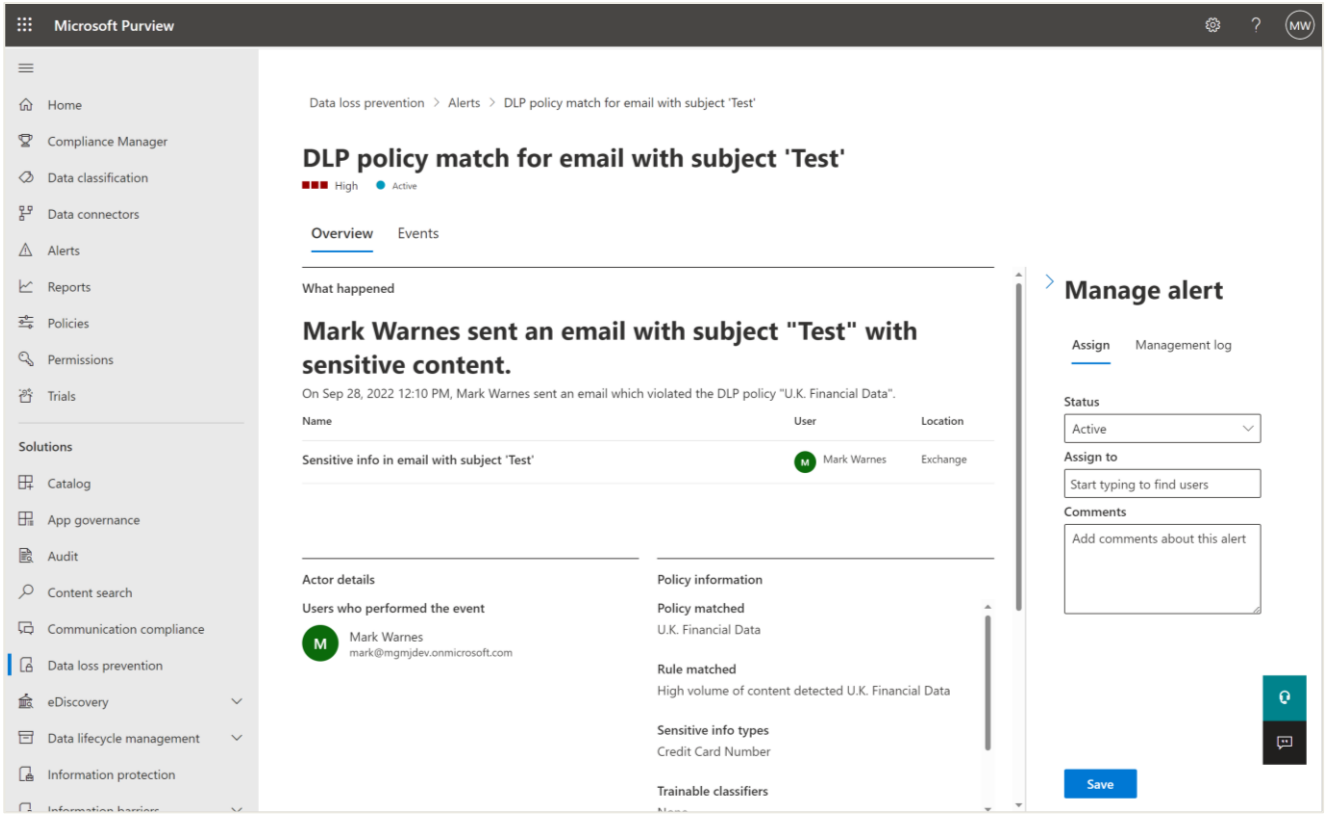


Prevent data loss

Alerts dashboard allows deep investigation of a policy match

Shows details of single and aggregate event alerts

Manage the workflow with assignments, notes and alert status



Microsoft

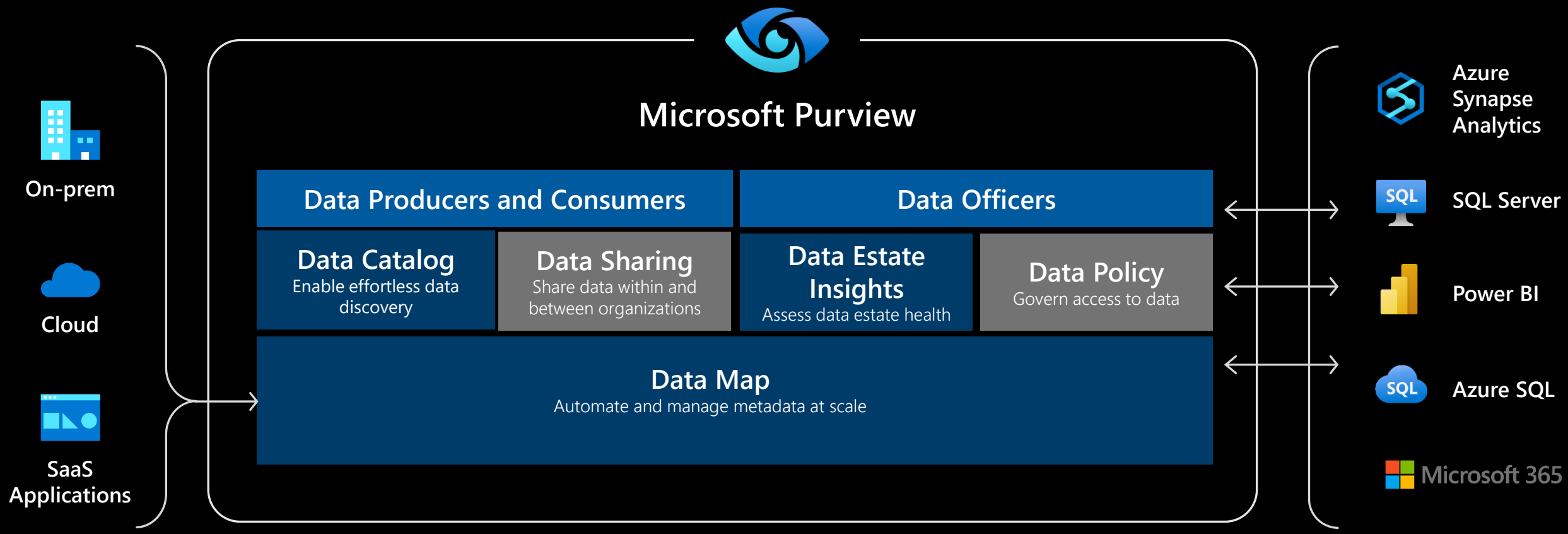
Microsoft Purview

(Unified Experience)

Unified Data Management Microsoft Purview

Generally Available

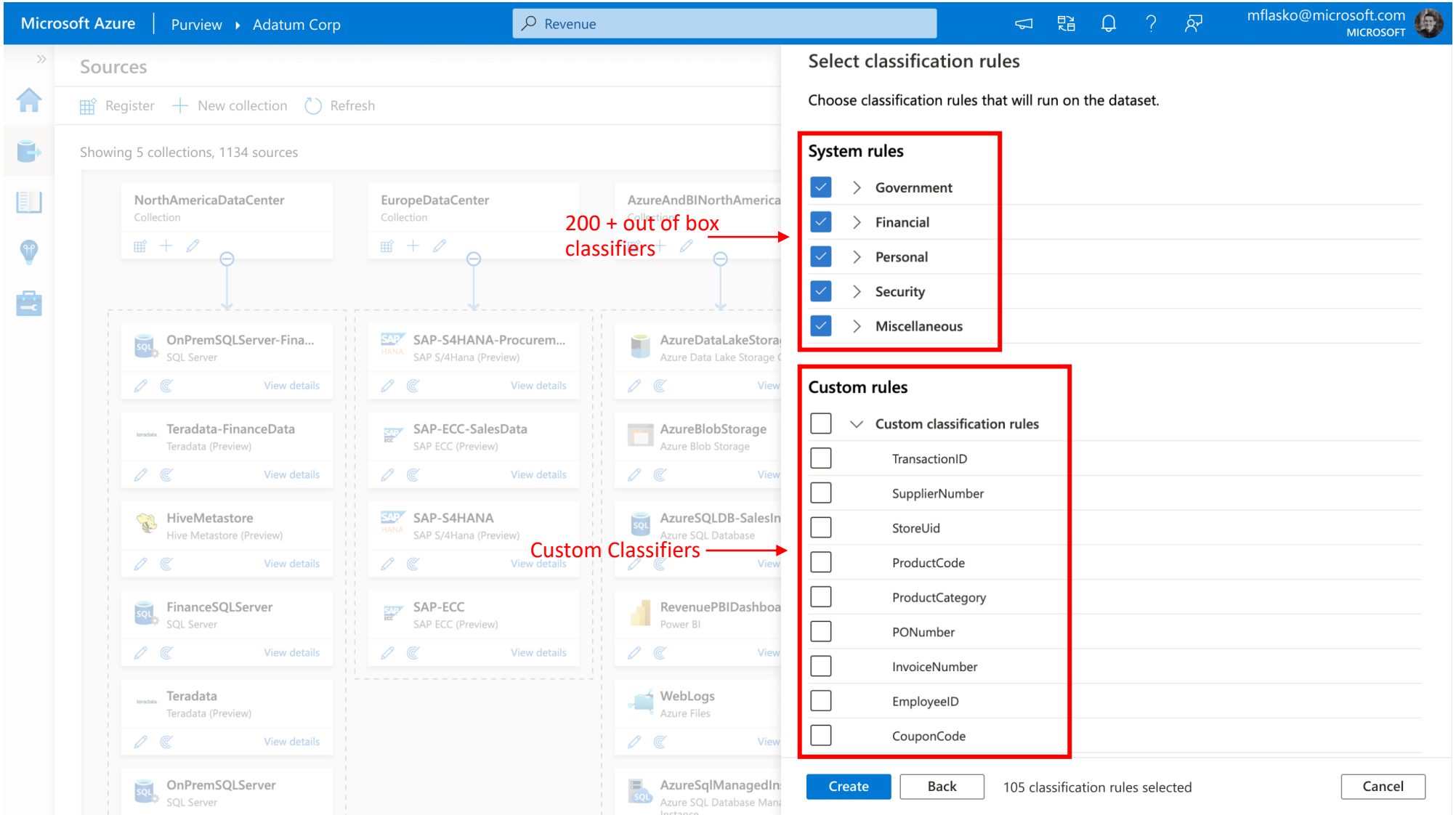
Preview



Microsoft

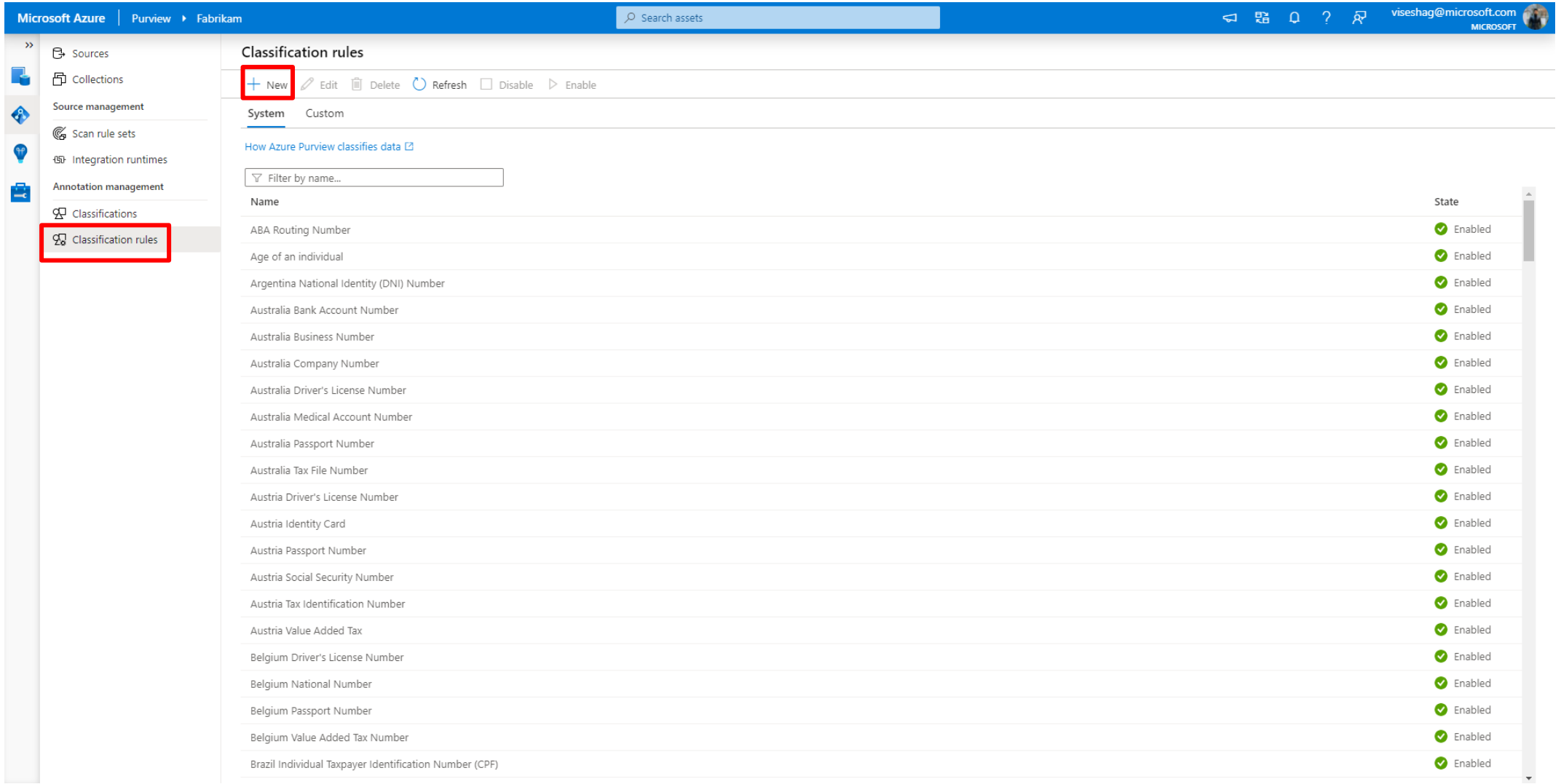
Scan Sources

Discover sensitive data using 200+ built in classifiers, define your own custom classifiers



Data Map – Custom Classification rules

Define your own data pattern along with thresholds to reduce false positives



Microsoft Purview Data Estate Insights

Data Estate Insights

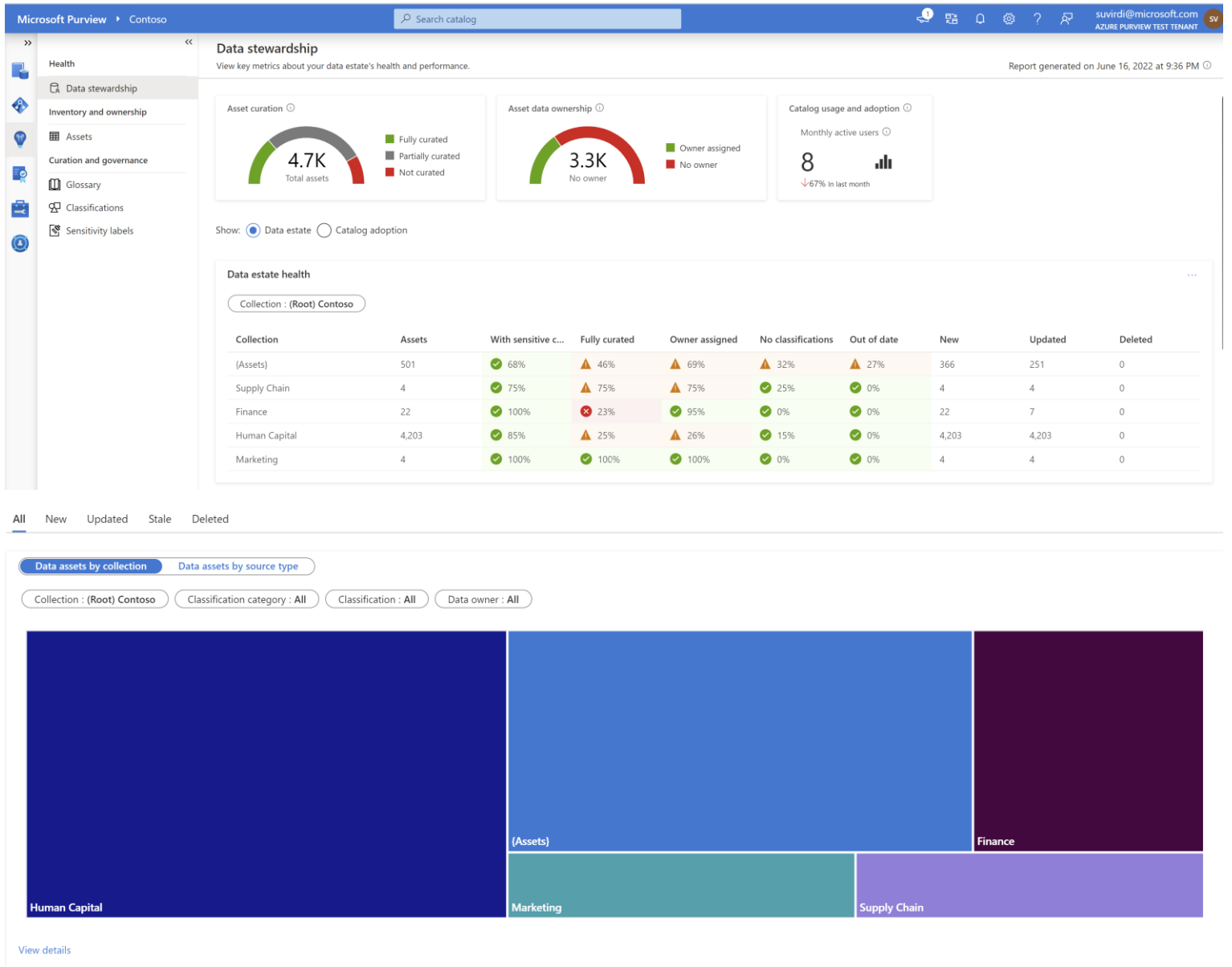
(Bird's eye view of your Data Estate)

Data Estate Insights

Bird's eye view of data landscape

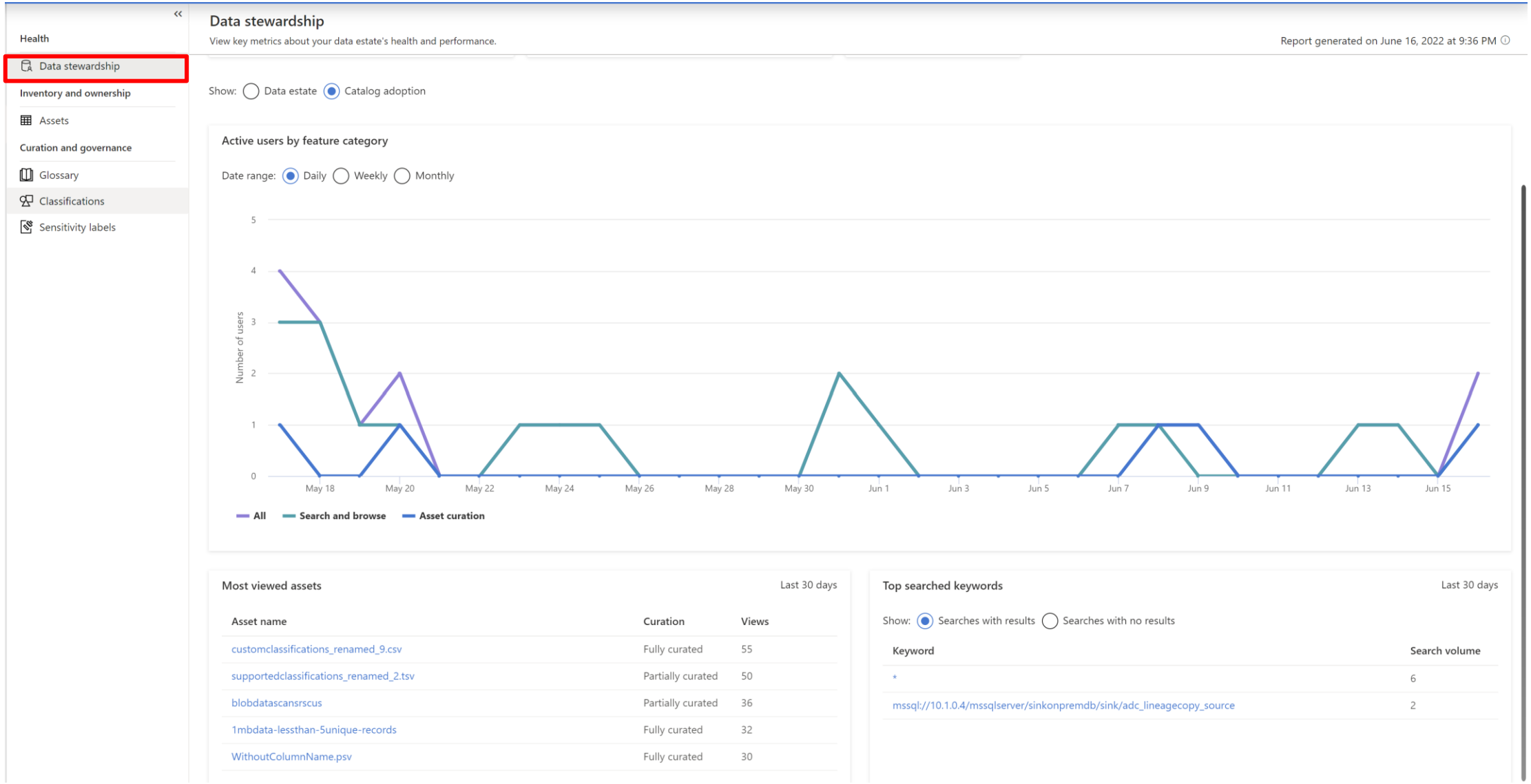
Benefits

- Intended to help users such as Chief Data Officers quickly understand their data estate at large and gain key insights such as where sensitive data resides
- Asset Insights to see where all data resides across Collections and range of source types. Glossary insights to understand changes made to business terms and how much coverage glossary has over your data map
- Sensitive data Insights to simplify compliance risk assessment across operational and transactional data sources. Assess risk and derive audit trails of data qualified by sensitivity and business relevance



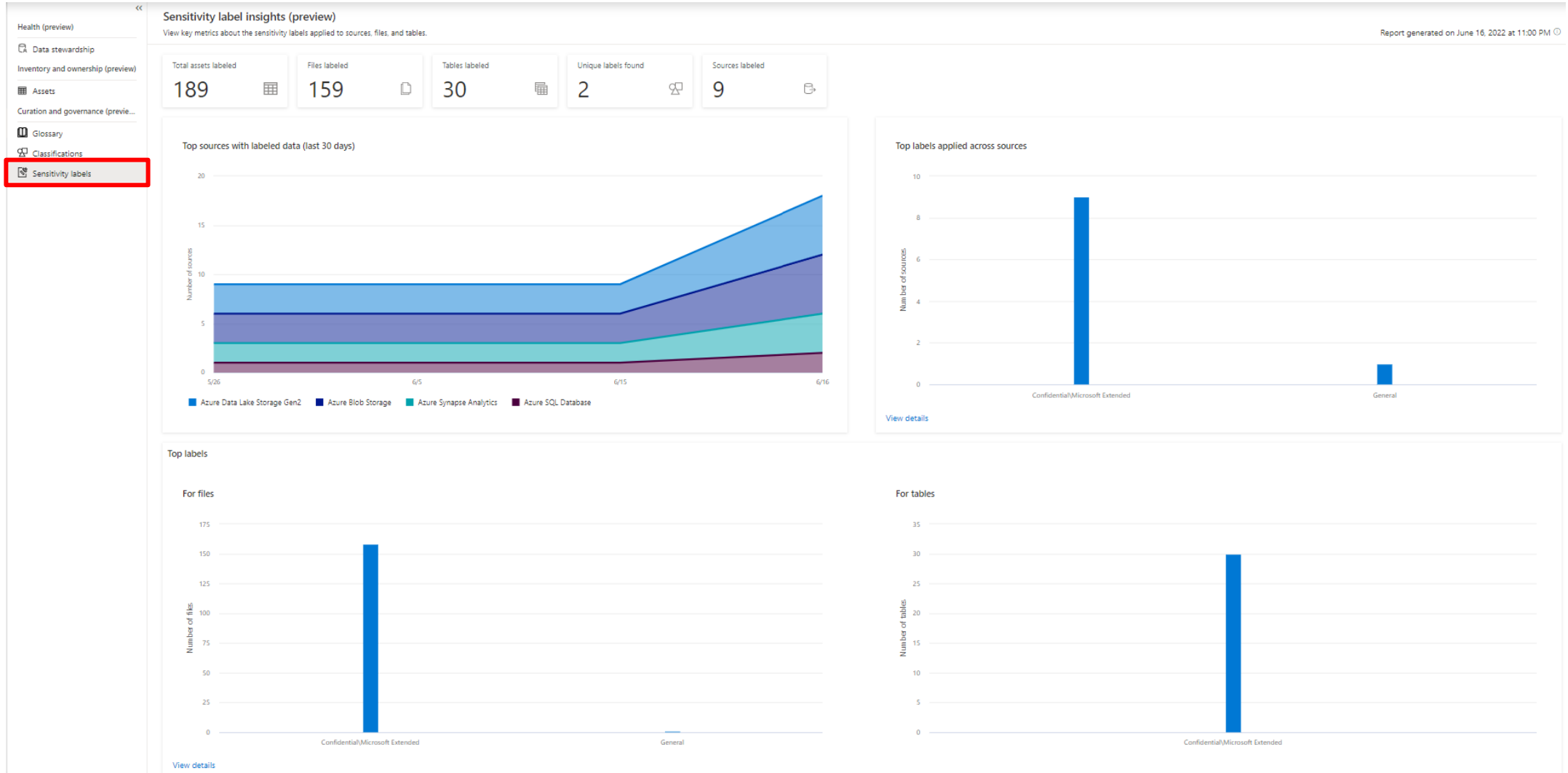
Data stewardship

A view of the data estate health and insights into the catalog's adoption



Sensitivity Labels

Understand what sensitivity labels have been applied across the data estate



Microsoft Purview Integrations: Public Preview

Power BI + Microsoft Purview: Better Together

Discover

Discover Power BI assets (tenant, workspace level) in Purview Catalog

Browse & Search

Find Power BI assets (dashboards, reports, datasets etc.) in Purview catalog

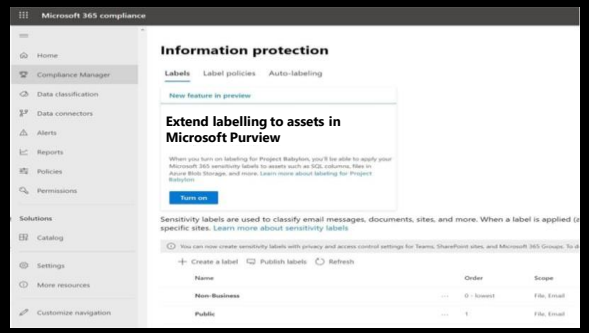
Enhanced metadata, lineage, sensitivity labels & endorsements

View enhanced metadata, lineage, sensitivity labels, endorsement labels in Purview for Power BI assets

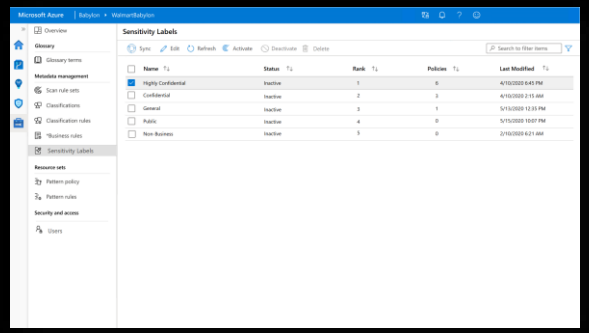
Microsoft 365 + Microsoft Purview: Better Together

Scenario

Consistent classification and Labels across M365, Azure, SQL Svr, Power BI



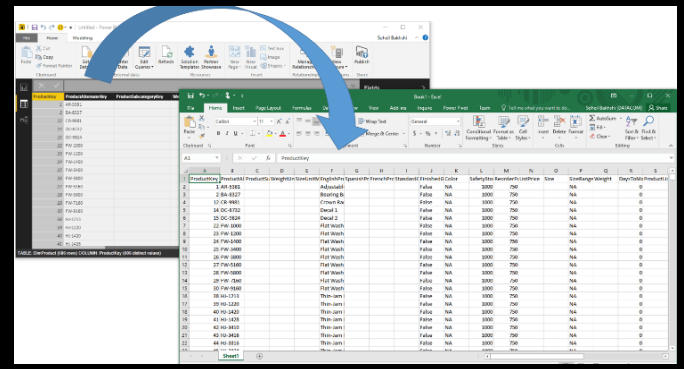
Discover Purview from M365 Compliance Center & get started with classifiers and labels



Classification & Labels applied across breadth of Data Estate by Purview

Auto labelling

Labels automatically cascade via lineage



Information worker exports data from Power BI & saves to Excel with same sensitivity label

M365 -> Azure -> PBI -> M365

Roadmap

- → Label and protection applied to PDFs exported from Office apps
- → Updated user experience for picking and seeing sensitivity labels in Office apps
- → Complex condition support in DLP rule authoring experience (create advanced rules using a combination of AND/OR/NOT operators)
- → Application of a “default label” to an unlabeled file uploaded to a SharePoint Online document library

Kocho

BECOME GREATER

Thank you

→ Any questions?