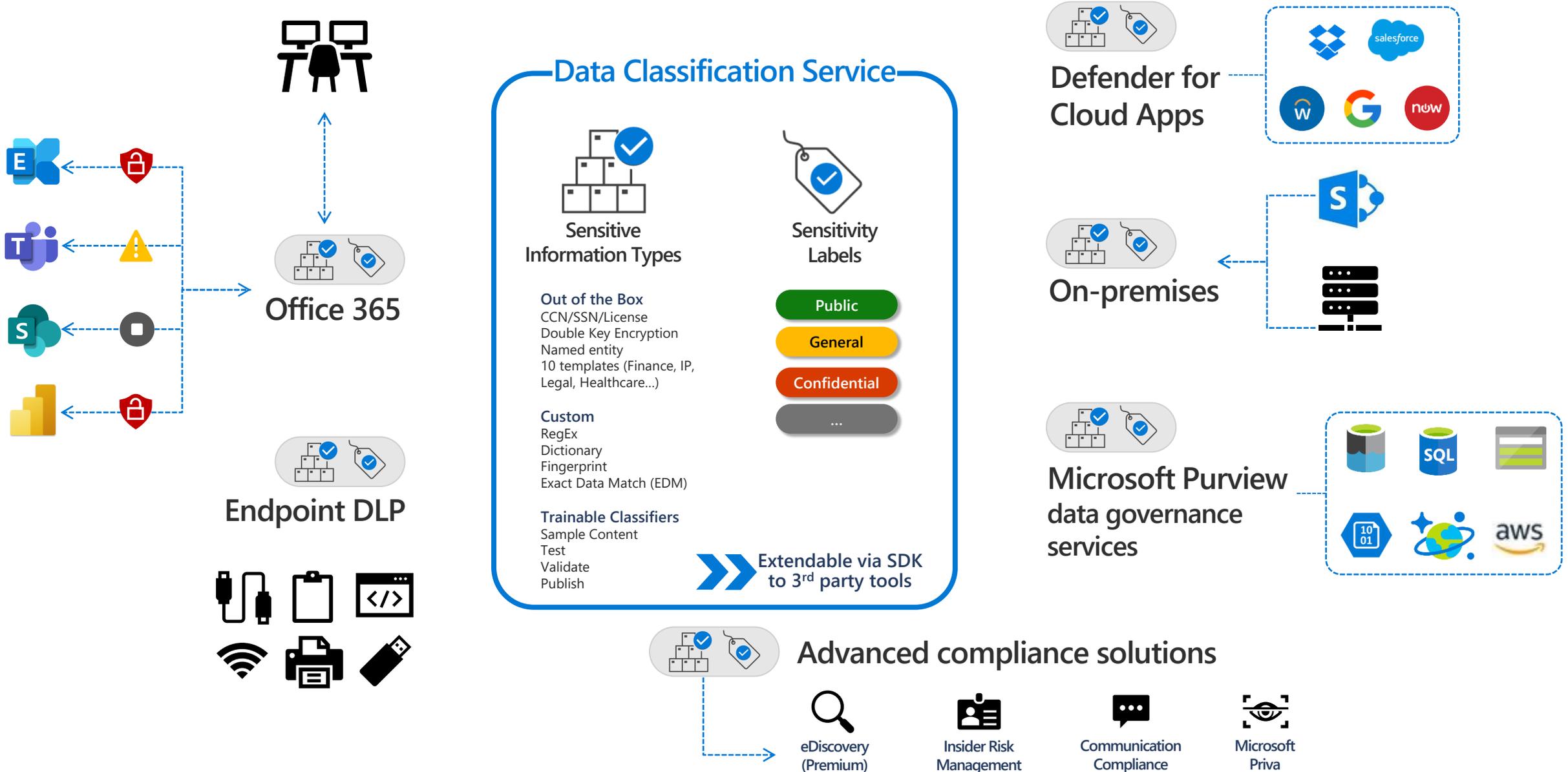


# Understanding Microsoft Information Protection

- Mark Warnes, Architect (Kocho)
- Vrunda Monnappa, Digital Technical Specialist (Microsoft)

# Microsoft Purview Information Protection



# 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

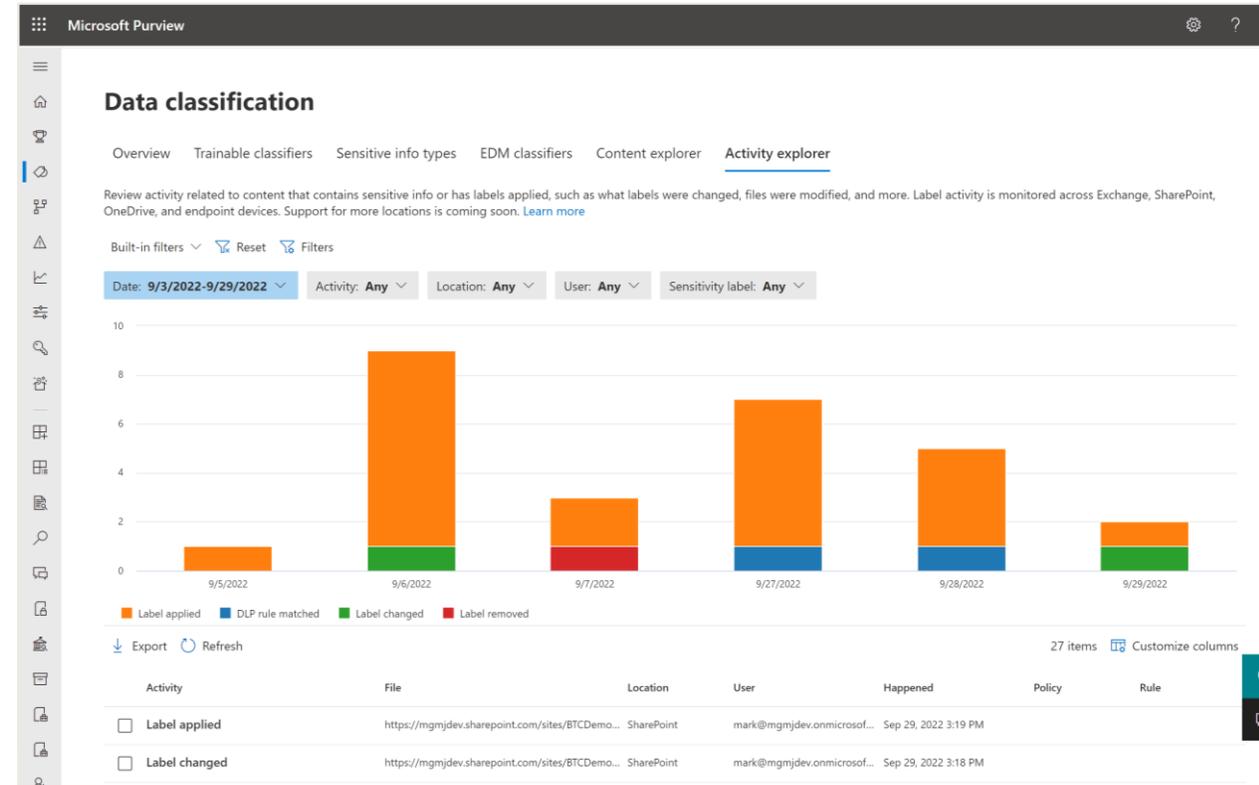
Use out-of-box and define custom classifiers

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

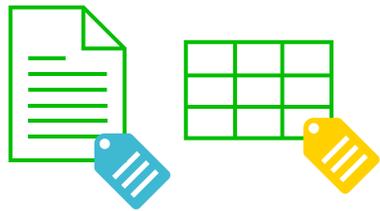


# Protect your data



## Sensitivity Labels

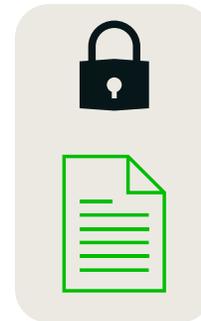
Central unified labels for classifying & protecting files, emails, sites, groups & assets



Apply to documents within Office apps and SharePoint libraries



Add visual markings with customised text

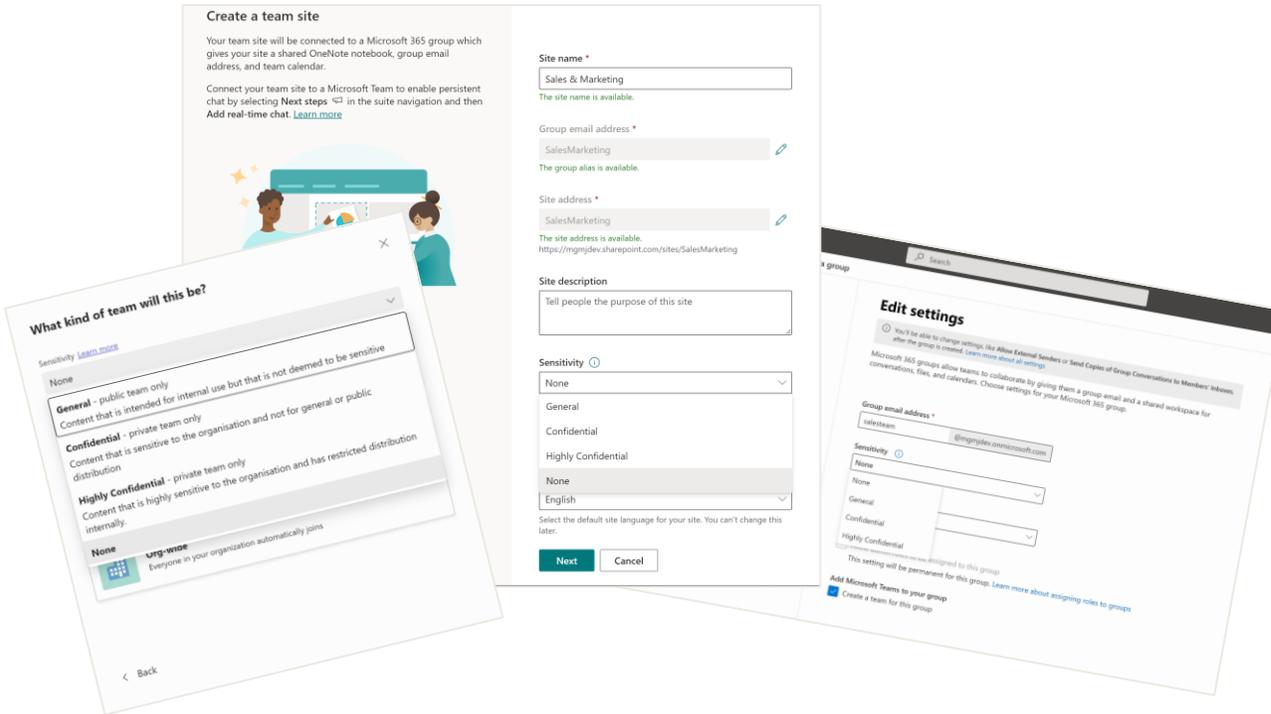


Encrypt contents, control access, and define usage rights

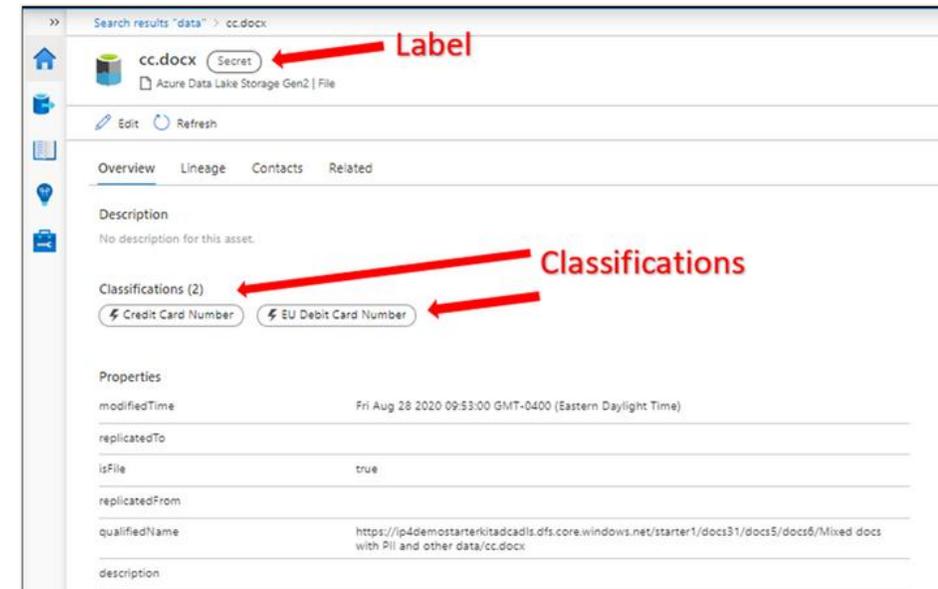


Auto-apply labels by matching document content with M365 classifiers

# 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



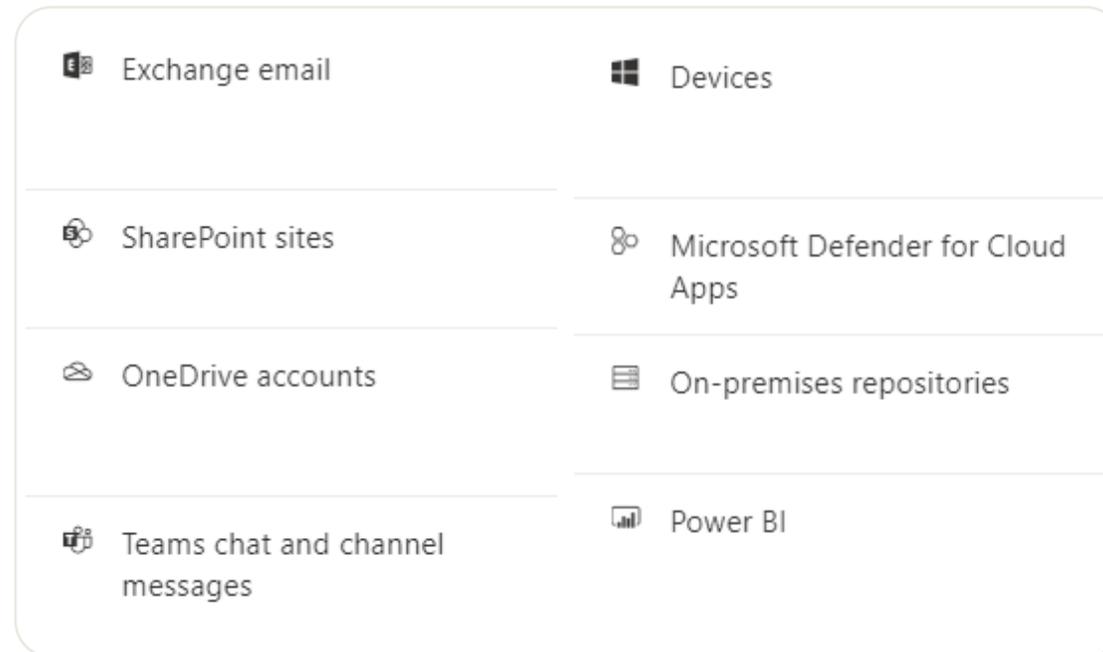
## Data Loss Prevention

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

Marie Beaudouin 6/3  
Thank you for always being so positive!

I will push Krystal to give us a few more days. That shouldn't be a problem.

We haven't had a break in awhile.

**This message was blocked. What can I do?**

I don't have the file yet, but here are some cards and information I have handy that you can use:

Name: Bobby Lee  
Number: 5432180476691446  
Expiration: 11/2021  
CVV: 155

Name: Adam Jacks  
Number: 5458057271187995  
Expiration: 06/2021  
CVV: 646

SSN: 08-819-2931  
Passport: AE453412

Type a message

**Audit or restrict activities on Windows devices**

**Audit or restrict activities on Windows devices**

When the activities below are detected on Windows devices for supported files containing sensitive info that matches this policy's conditions, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction. [Learn more](#)

- Upload to cloud services or access by unallowed browsers Audit only
- Copy to clipboard Block
- Copy to a USB removable media Block with ov...
- Copy to a network share Audit only
- Access by unallowed apps Audit only
- Print Audit only

Brian Johnson	Diners Club	30569309025904
Christie Cline	Diners Club	3852000023237
Debra Berger	Discover	6011111111111117
Diego Sicilian	Discover	6011000990139424
Grady Archie	JCB	3566002020360505
Irvin Sayers	MasterCard	5555555555554444
Isaiah Langer	MasterCard	5105105105105100
Johanna Lorenz	Visa	4111111111111111
Joni Sherman	Visa	4012888888881881

Best regards,

Lynne Robbins

**Data Loss Prevention**

Your organisation's policy  
Printing while Test Credit Card.docx is open is not allowed.

Dismiss

# Prevent data loss



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

^ Restrict Third Party Apps 

**Restrict Third Party Apps**  
Use one of the automatic actions provided by Microsoft Defender for Cloud Apps. [Learn more](#)

**Box**

- Send policy-match digest to file owner 
- Remove external users 
- Trash file 
- Remove direct shared link 

**G Suite**

- Send policy-match digest to file owner 
- Make private 
- Remove external users 
- Trash file 

**Cisco Webex**

- Trash file 

**Dropbox**

- Send policy-match digest to file owner 
- Trash file 
- Remove direct shared link 

**Salesforce**

- Send policy-match digest to file owner 

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

^ Restrict access or remove on-premises files 

**Restrict access or remove on-premises files**

- Block people from accessing files stored in on-premises repositories
  - Block everyone. Only the content owner, last modifier, and admin will continue to have access 
  - Block only people who have access to your on-premises network and users in your organization who weren't granted explicit access to the files 
- Set permissions on the file (permissions will be inherited from the parent folder)
- Move file from where it's stored to a quarantine folder

# 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

The screenshot displays the Microsoft Purview Alerts dashboard. The left sidebar contains navigation options: Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Trials, and Solutions (Catalog, App governance, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery, Data lifecycle management, Information protection, Information barriers). The main content area shows the path: Data loss prevention > Alerts > DLP policy match for email with subject 'Test'. The alert title is "DLP policy match for email with subject 'Test'" with a severity of "High" and status of "Active". The "Overview" tab is selected, showing the event: "Mark Warnes sent an email with subject 'Test' with sensitive content." The event occurred on Sep 28, 2022 at 12:10 PM. A table lists the sensitive information: "Sensitive info in email with subject 'Test'" detected by Mark Warnes (User) at Exchange (Location). The "Actor details" section shows "Users who performed the event" with Mark Warnes (mark@mngmjdev.onmicrosoft.com). The "Policy information" section shows "Policy matched: U.K. Financial Data" and "Rule matched: High volume of content detected U.K. Financial Data". The "Sensitive info types" section lists "Credit Card Number". The "Trainable classifiers" section is partially visible. On the right, the "Manage alert" panel includes "Assign" and "Management log" tabs, a "Status" dropdown set to "Active", an "Assign to" field with a search prompt, a "Comments" text area, and a "Save" button.

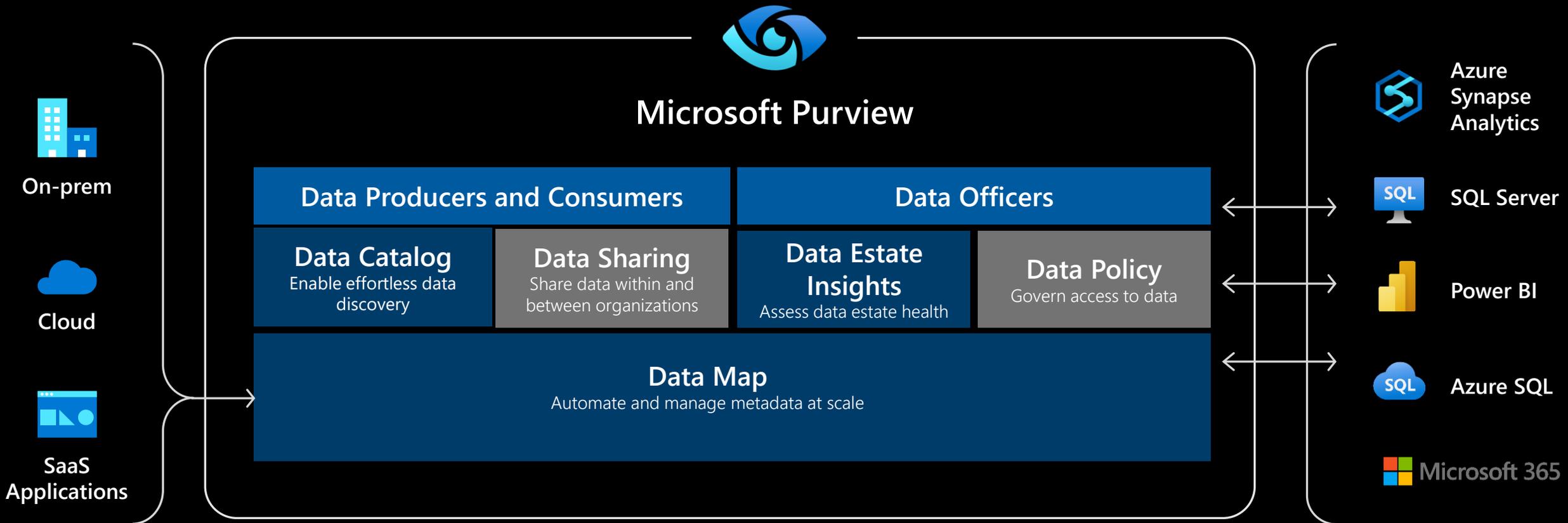


# Microsoft Purview

(Unified Experience)

# Unified Data Management Microsoft Purview

Generally Available  
Preview



# Scan Sources

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

The screenshot displays the Microsoft Purview DataMap interface. The top navigation bar shows 'Microsoft Azure | Purview | Adatum Corp' and a search bar containing 'Revenue'. The main area is titled 'Sources' and shows a grid of data sources. A red dashed box highlights a group of sources, with a red arrow pointing to them from the text '200 + out of box classifiers'. Another red arrow points from the text 'Custom Classifiers' to a specific source card. On the right, a 'Select classification rules' dialog is open, showing a list of rules. A red box highlights the 'System rules' section, which includes 'Government', 'Financial', 'Personal', 'Security', and 'Miscellaneous', all of which are checked. Another red box highlights the 'Custom rules' section, which includes 'Custom classification rules' (unchecked) and several other rules like 'TransactionID', 'SupplierNumber', etc., all of which are unchecked. At the bottom of the dialog, it says '105 classification rules selected' and has 'Create', 'Back', and 'Cancel' buttons.

Microsoft Azure | Purview | Adatum Corp

Revenue

mflasko@microsoft.com

Sources

Register + New collection Refresh

Showing 5 collections, 1134 sources

NorthAmericaDataCenter Collection

EuropeDataCenter Collection

AzureAndBINorthAmerica Collection

200 + out of box classifiers

OnPremSQLServer-Fina... SQL Server

SAP-S4HANA-Procurem... SAP S/4Hana (Preview)

AzureDataLakeStora... Azure Data Lake Storage C

Teradata-FinanceData Teradata (Preview)

SAP-ECC-SalesData SAP ECC (Preview)

AzureBlobStorage Azure Blob Storage

HiveMetastore Hive Metastore (Preview)

SAP-S4HANA SAP S/4Hana (Preview)

AzureSQLDB-SalesIn Azure SQL Database

FinanceSQLServer SQL Server

SAP-ECC SAP ECC (Preview)

RevenuePBIDashboa Power BI

Teradata Teradata (Preview)

WebLogs Azure Files

OnPremSQLServer SQL Server

AzureSqlManagedIn Azure SQL Database Manag Instance

Select classification rules

Choose classification rules that will run on the dataset.

System rules

- > Government
- > Financial
- > Personal
- > Security
- > Miscellaneous

Custom rules

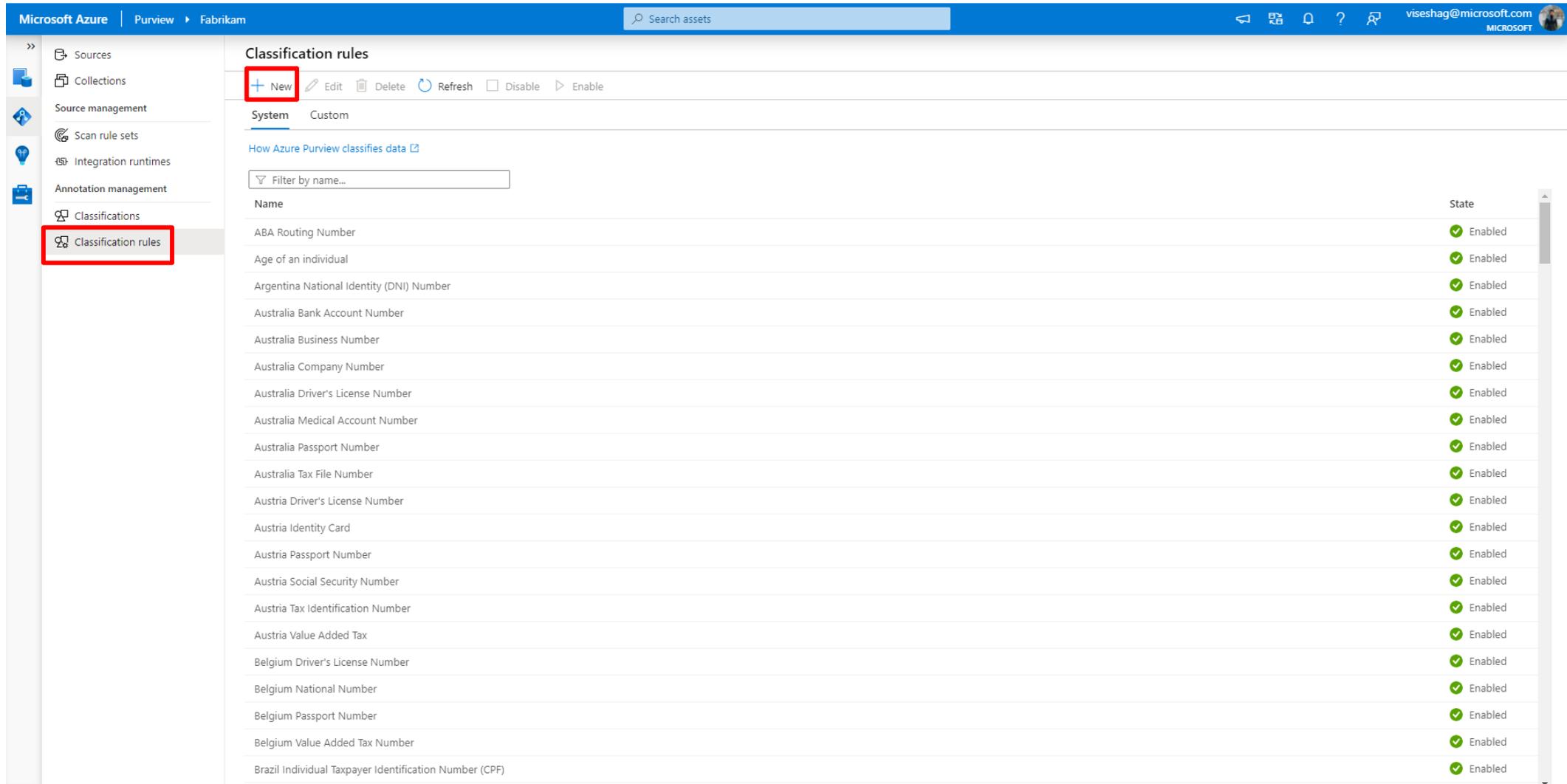
- Custom classification rules
- TransactionID
- SupplierNumber
- StoreUid
- ProductCode
- ProductCategory
- PONumber
- InvoiceNumber
- EmployeeID
- CouponCode

Create Back 105 classification rules selected Cancel

Custom Classifiers

# Data Map – Custom Classification rules

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



The screenshot displays the Microsoft Purview interface for managing classification rules. The left sidebar shows the navigation menu with 'Classification rules' selected. The main content area shows the 'Classification rules' page with a '+ New' button highlighted in red. Below the button, there are tabs for 'System' and 'Custom', and a search filter 'Filter by name...'. A table lists various system rules, all of which are currently 'Enabled'.

Name	State
ABA Routing Number	Enabled
Age of an individual	Enabled
Argentina National Identity (DNI) Number	Enabled
Australia Bank Account Number	Enabled
Australia Business Number	Enabled
Australia Company Number	Enabled
Australia Driver's License Number	Enabled
Australia Medical Account Number	Enabled
Australia Passport Number	Enabled
Australia Tax File Number	Enabled
Austria Driver's License Number	Enabled
Austria Identity Card	Enabled
Austria Passport Number	Enabled
Austria Social Security Number	Enabled
Austria Tax Identification Number	Enabled
Austria Value Added Tax	Enabled
Belgium Driver's License Number	Enabled
Belgium National Number	Enabled
Belgium Passport Number	Enabled
Belgium Value Added Tax Number	Enabled
Brazil Individual Taxpayer Identification Number (CPF)	Enabled



# Microsoft Purview Data Estate Insights

## Data Estate Insights

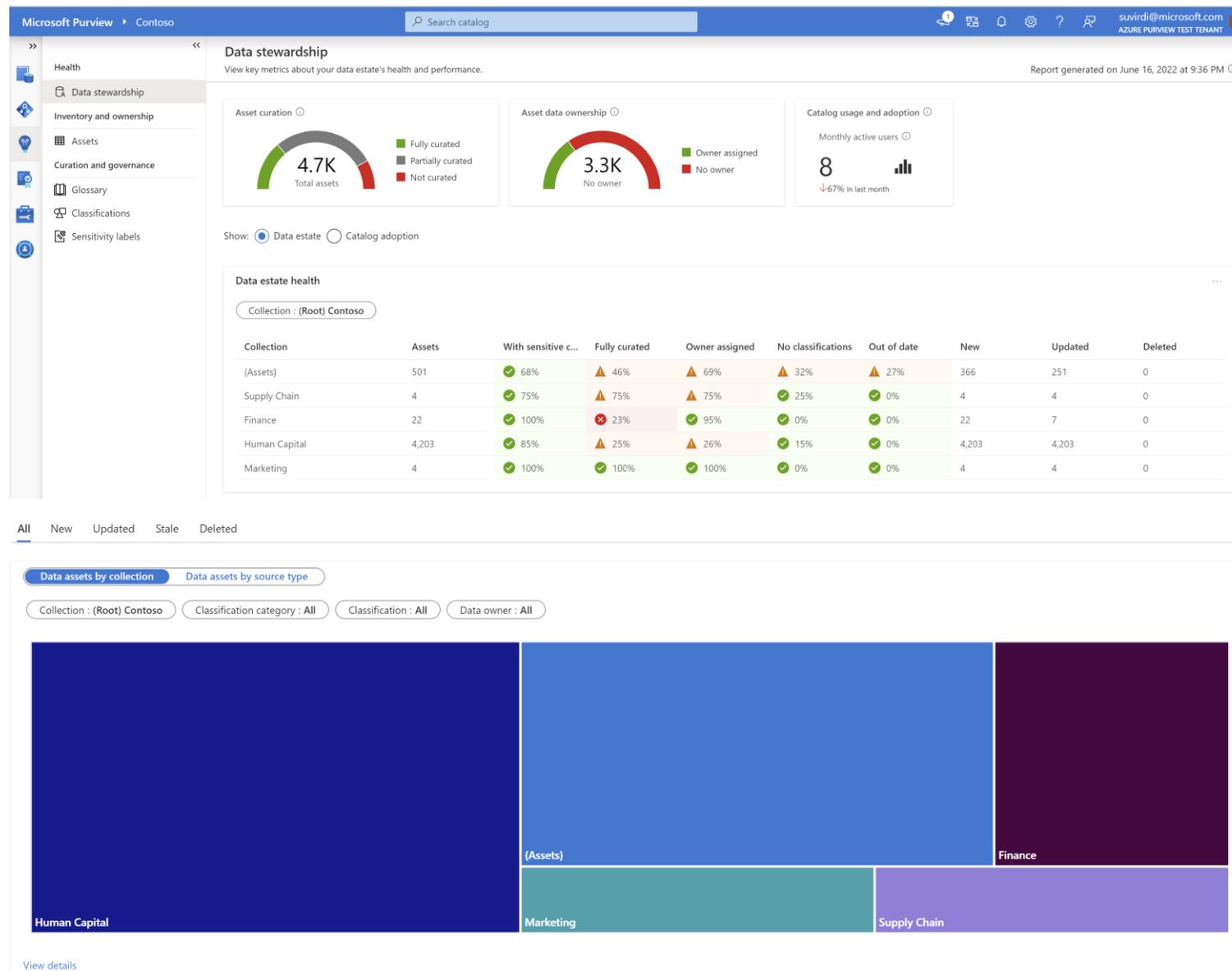
(Bird's eye view of your Data Estate)

# 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

Health

**Data stewardship**

Inventory and ownership

Assets

Curation and governance

Glossary

Classifications

Sensitivity labels

## Data stewardship

View key metrics about your data estate's health and performance.

Report generated on June 16, 2022 at 9:36 PM ⓘ

Show:  Data estate  Catalog adoption

**Active users by feature category**

Date range:  Daily  Weekly  Monthly

Date	All	Search and browse	Asset curation
May 18	4	3	1
May 19	3	3	0
May 20	2	1	1
May 21	0	1	0
May 22	0	0	0
May 23	0	1	0
May 24	0	1	0
May 25	0	1	0
May 26	0	0	0
May 27	0	0	0
May 28	0	0	0
May 29	0	0	0
May 30	0	0	0
May 31	0	2	0
Jun 1	0	1	0
Jun 2	0	0	0
Jun 3	0	0	0
Jun 4	0	0	0
Jun 5	0	0	0
Jun 6	0	0	0
Jun 7	0	1	0
Jun 8	0	1	1
Jun 9	0	0	1
Jun 10	0	0	0
Jun 11	0	0	0
Jun 12	0	0	0
Jun 13	0	1	0
Jun 14	0	1	0
Jun 15	2	0	1

**Most viewed assets** Last 30 days

Asset name	Curation	Views
<a href="#">customclassifications_renamed_9.csv</a>	Fully curated	55
<a href="#">supportedclassifications_renamed_2.tsv</a>	Partially curated	50
<a href="#">blobdatascansrcsus</a>	Partially curated	36
<a href="#">1mbdata-less-than-5-unique-records</a>	Fully curated	32
<a href="#">WithoutColumnName.psv</a>	Fully curated	30

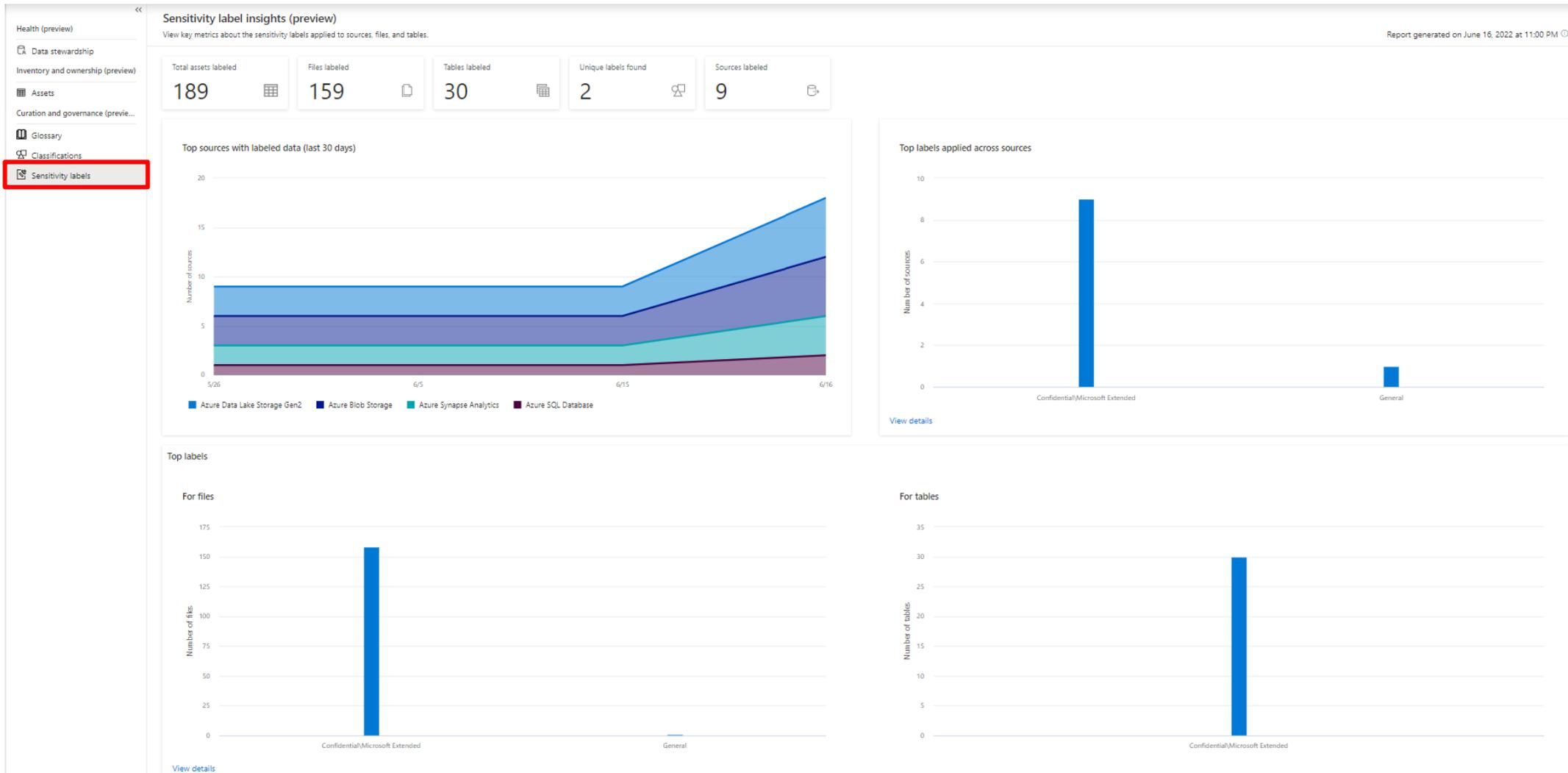
**Top searched keywords** Last 30 days

Show:  Searches with results  Searches with no results

Keyword	Search volume
*	6
<a href="#">mssql://10.1.0.4/mssqlserver/sinkonpremdb/sink/adc_lineagecopy_source</a>	2

# 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



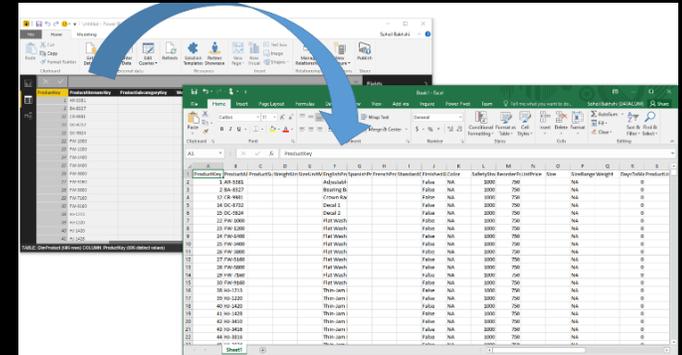
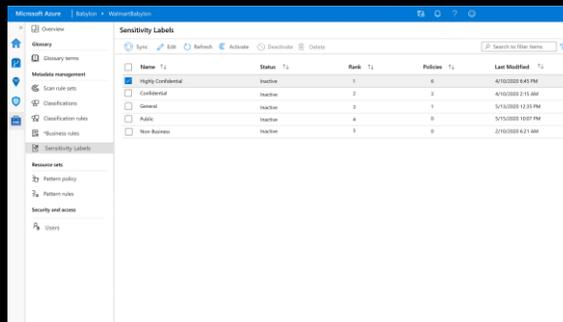
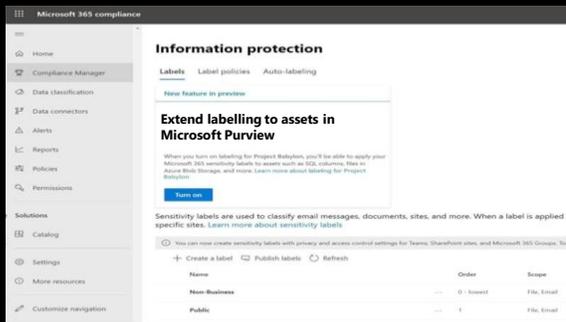
## Enhanced metadata, lineage, sensitivity labels & endorsements

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



# Thank you

—————> Any questions?