VISUALIZE YOUR DATA WITH MICROSOFT PURVIEW

Speaker: Jeremy Nathan

Jeremy’s LinkedIn:

- Microsoft Certified Trainer (MCT)
- Microsoft PL-300 Power BI Data Analyst
- Instructor at JN Training
- Hobbies: Hiking, running, lifting weights, skiing
- Email: jnathan@jncomputertraining.com
- LinkedIn: https://www.linkedin.com/in/jeremy-nathan-mct/

JEREMY NATHAN

Chattanooga, TN

SLIDES HERE

https://github.com/jeremynathan/purview

SUBMIT A SESSION

Chattanooga Microsoft Azure Fabric User Group

https://sessionize.com/chattanooga-microsoft-azure-fabric-data

DATA DRIVEN COMMUNITY

Join:

https://www.meetup.com/cloud-data-driven/events/305569239/

Speak:

https://sessionize.com/cloud-data-driven-user-group-2025

AGENDA

- Purview Pricing
- Setting Up Microsoft Purview
- Set Up Permissions
- Types of Data You Can Scan
- Create Scans of Azure SQL Server Database
- Create a custom classification and rule

WHAT IS MICROSOFT PURVIEW?

- Data Security
- Data Governance
- Compliance
- Data Loss Prevention (DLP)
- Insider Risk Management
- Adaptive Protection

SUPPORTED DATA SOURCES

- Databases
  - Supports SQL-based systems like Azure SQL Database, SQL Server on-premises, Oracle, Teradata
  - Includes NoSQL databases such as Azure Cosmos DB
- Data Lakes
  - Scans Azure Data Lake Storage (ADLS) Gen1 and Gen2
- File Systems
  - Includes on-premises file shares and cloud-based storage like Azure Blob Storage

DATA SECURITY AND QUALITY

- Enhanced Data Security
  - Robust access control system with roles and permissions
  - Prevents unauthorized data access
  - Cloud-based service adds protection against physical access
- Improved Data Quality
  - Reliable and accurate data management
  - Effective data cleaning
  - Offers various data-enhancing features

LICENSING REQUIREMENTS

- Microsoft 365 Licensing
  - Requires Microsoft 365 E3 or E5 license

- To use Copilot you need to purchase Copilot Security Compute Units (SCUs) at $4 per SCU

PAY-AS-YOU-GO PRICING MODEL

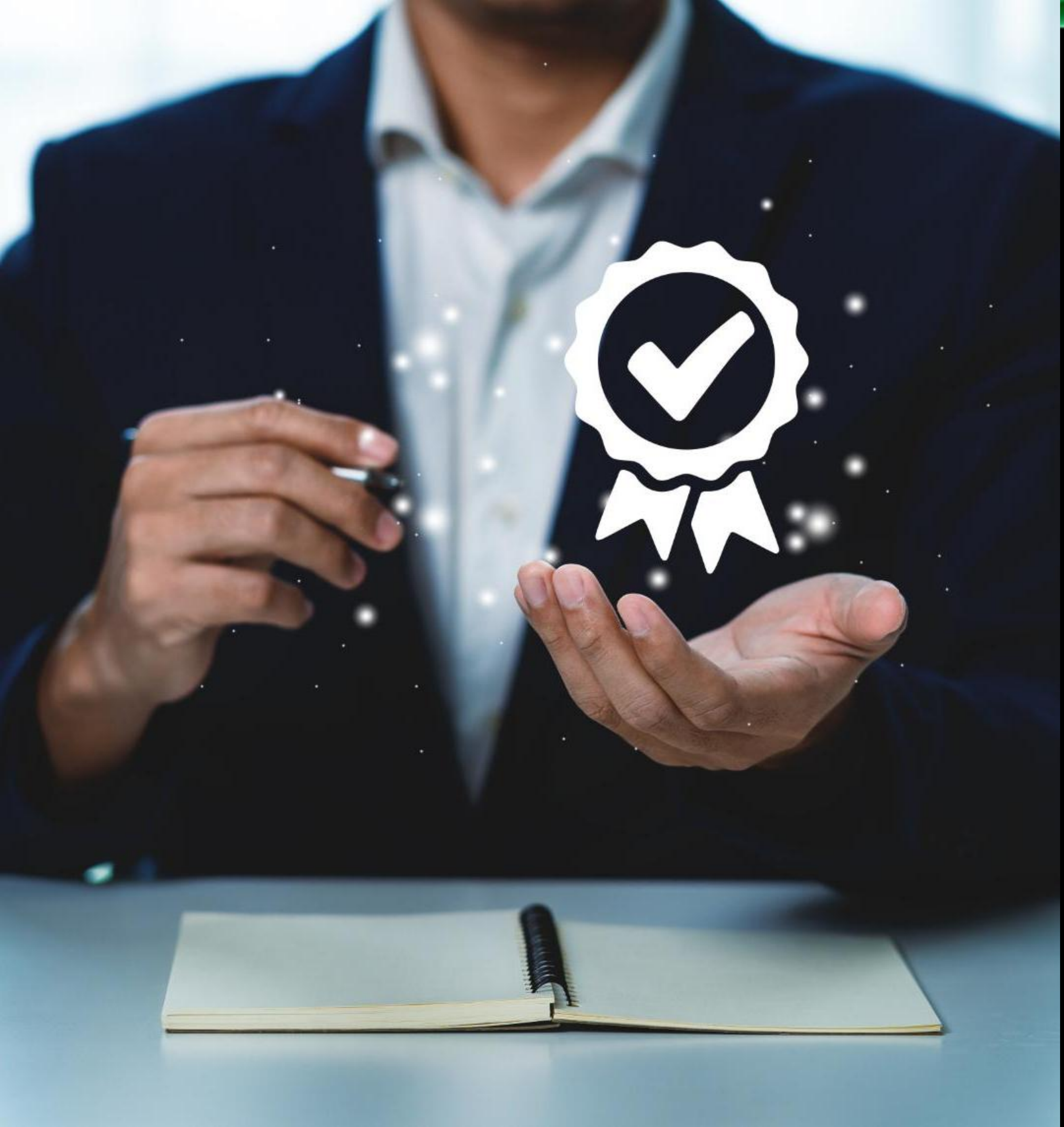
- Approximately $0.0165 per asset per day
- Around $0.50 per asset per month
- For example, each report in Power BI is one asset https://azure.microsoft.com/en-us/pricing/details/purview/

COST CALCULATIONS FOR OTHER DATA SOURCES

- Cost for Other Data Sources
  - Based on scan duration and computational resources
  - Example: 32 vCores for one minute at $0.011 per vCore-minute costs $0.34
- Data Map Enrichment - Advanced Resource Set
  - Rate: $0.21 per vCore-hour
  - Total cost: $153.30
- Report Generation
  - Rate: $0.82 per vCore-hour
  - Total expense: $598.60

CREATING A PURVIEW ACCOUNT

- Navigate to Azure Portal
  - Go to portal.azure.com
  - Access Home > Purview > Create
- Select Subscription
  - Ensure correct subscription is chosen
- Choose Resource Group
  - Create a new resource group or select an existing one
  - New resource group should meet Azure naming requirements
- Resource Group Naming Requirements
  - Length: 1 to 90 characters
  - Characters: Only alphanumeric, underscores, parentheses, hyphens, and periods
- Type Microsoft Purview Account Name

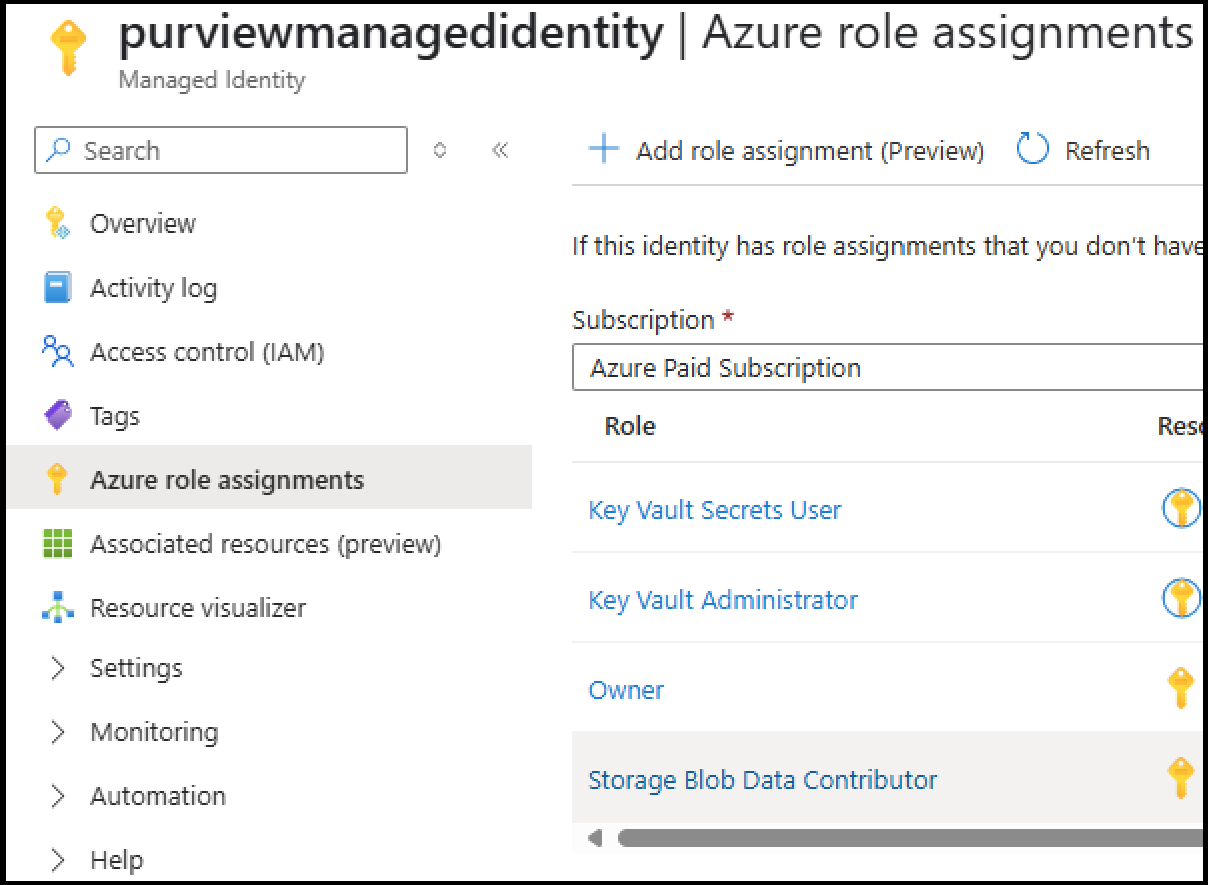


AUTHENTICATION OPTIONS

- Managed Identity
  - Most straightforward option
  - Uses Purview’s built-in identity
- Delegated Authentication
  - More complex setup
  - Purview acts on behalf of another authenticated user

MANAGED IDENTITY SETUP

1. Navigate to portal.azure.com
2. Search for managed identities
3. Create a managed identity
4. Azure role assignments, Add role assignment of Storage Blob Data Contributor



purviewmanagedidentity | Azure role assignments

Managed Identity

If this identity has role assignments that you don't have

Subscription *

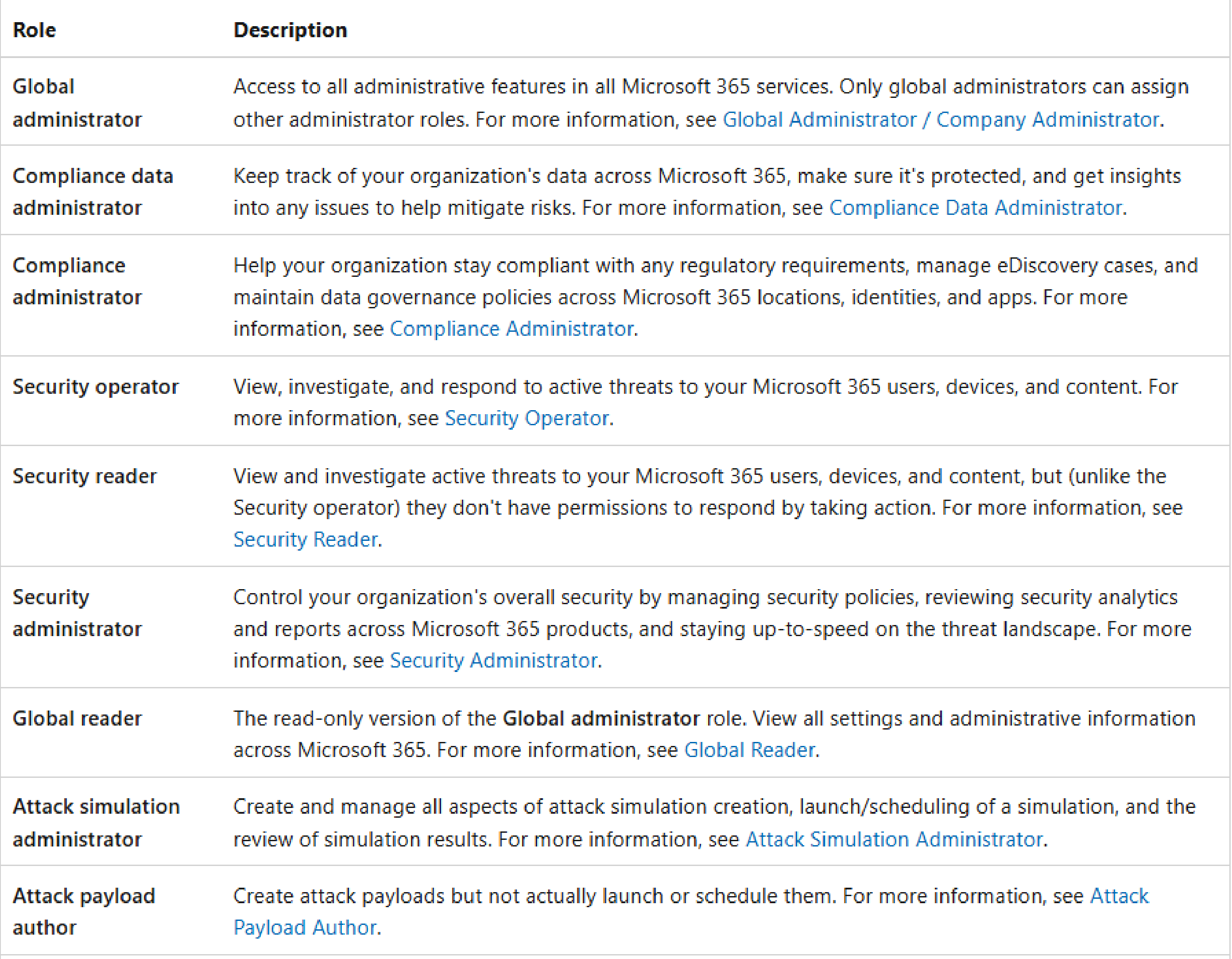
Azure Paid Subscription

Role	Res
Key Vault Secrets User	
Key Vault Administrator	
Owner	
Storage Blob Data Contributor	

ACCESS CONTROL STRATEGIES

- Minimize Global Administrator Role Usage
  - Improves security for the organization
  - Reduces the number of users with extensive permissions
- Implement Least Privilege Access Control
  - Grant administrators only the permissions they need
  - Enhances overall security
- Follow Microsoft's Recommended Practices
  - Use roles with the fewest permissions
  - Plan access control strategy effectively

AZURE ROLES IN PURVIEW



Role	Description
Global administrator	Access to all administrative features in all Microsoft 365 services. Only global administrators can assign other administrator roles. For more information, see Global Administrator / Company Administrator.
Compliance data administrator	Keep track of your organization's data across Microsoft 365, make sure it's protected, and get insights into any issues to help mitigate risks. For more information, see Compliance Data Administrator.
Compliance administrator	Help your organization stay compliant with any regulatory requirements, manage eDiscovery cases, and maintain data governance policies across Microsoft 365 locations, identities, and apps. For more information, see Compliance Administrator.
Security operator	View, investigate, and respond to active threats to your Microsoft 365 users, devices, and content. For more information, see Security Operator.
Security reader	View and investigate active threats to your Microsoft 365 users, devices, and content, but (unlike the Security operator) they don't have permissions to respond by taking action. For more information, see Security Reader.
Security administrator	Control your organization's overall security by managing security policies, reviewing security analytics and reports across Microsoft 365 products, and staying up-to-speed on the threat landscape. For more information, see Security Administrator.
Global reader	The read-only version of the **Global administrator** role. View all settings and administrative information across Microsoft 365. For more information, see Global Reader.
Attack simulation administrator	Create and manage all aspects of attack simulation creation, launch/scheduling of a simulation, and the review of simulation results. For more information, see Attack Simulation Administrator.
Attack payload author	Create attack payloads but not actually launch or schedule them. For more information, see Attack Payload Author.

https://learn.microsoft.com/en-us/purview/purview-permissions

UPDATING USER PERMISSIONS

1. Sign In to the Azure Portal
   1. Open a browser and navigate to the Azure portal
   2. Sign in with an administrator account
2. Navigate to Azure Active Directory
   1. Select 'Azure Active Directory' from the menu or search bar
3. Go to Users
   1. Select 'Users' under the 'Manage' section
4. Select the User to Update
   1. Search for the user and open their profile
5. Update User Role or Permissions
6. Review and Save Changes
7. Notify the User

ADD MANAGED IDENTITY TO AZURE SQL

In your SQL query editor type

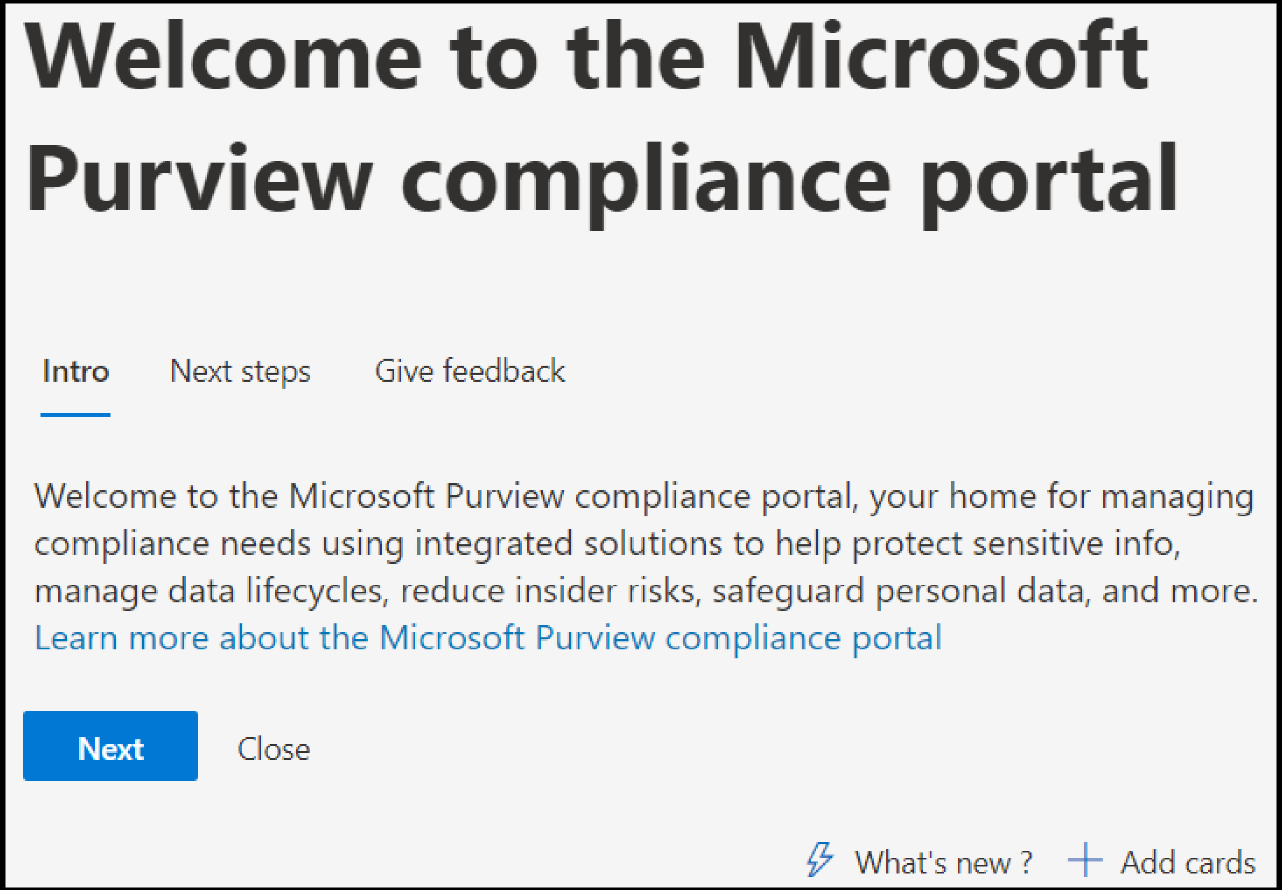
```
-- 1. Create external user for the Purview Managed Identity
CREATE USER [Purview-Managed-Identity-Name-Here] FROM EXTERNAL PROVIDER;
```

1. -- 2. Grant read access by adding the user to db_datareader role

```
ALTER ROLE db_datareader ADD MEMBER [Purview-Managed-Identity-Name-Here];
```

PURVIEW LOCATION

https://purview.microsoft.com/



Welcome to the Microsoft Purview compliance portal

Welcome to the Microsoft Purview compliance portal, your home for managing compliance needs using integrated solutions to help protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more. Learn more about the Microsoft Purview compliance portal

- Purview for Compliance
  - Located in the same site as Purview Governance
  - Free version is limited
- Purview in Compliance Home Page
  - Opens in Defender's Compliance home page
- Purview Governance
  - Scans and views data
  - Requires a Purview account
  - This produces costs

CREATING A DOMAIN

- Domains in Microsoft Purview
  - Foundational elements of the Data Map
  - Represent a top-level hierarchy
  - Provide structure in the data map
  - Enable domain administrators to maintain isolation
  - Control access through collections, data sources, scans, and roles

- Steps to Create a Domain
  1. Navigate to Domains from the Data Map tab
  2. Click the “+ New Domain (Preview)” button
  3. Enter the domain details
  4. Provide an identifying name

CREATING A COLLECTION

- Purpose of Collections in Purview
  - Support organizational or suborganizational mapping of metadata
  - Manage and maintain data sources, scans, and assets within a business unit
- Characteristics of Collections
  - Belong to a domain
- Steps to Create a Collection
  1. Click Data Map
  2. Click Domains
  3. Expand the drop-down menu of the desired domain

CREATING A DATA SOURCE

- Registering Data Source
  - Click “Register”
- Accessing Data Map
  - Click on the Data Map tab
- Selecting Domain
  - Click “Domains”
  - Choose the desired domain

SCAN A DATA SOURCE

- Click the bullseye icon to scan
- Setting the Scan
    - Set the scan to Auto-detect
    - Auto-detect covers all three levels
- Running the Scan
    - Continue, save, and run the scan
    - Scan rule sets and scan triggers are features

HOW TO REDUCE COSTS

- Delete Domains, Collections and Data Sources

CHALLENGES AND LEARNING CURVE

- Common Challenges
  - Initial setup complexity
  - Integration of various components
  - Steep learning curve
- Benefits
  - Effective data management
  - Secure data storage
  - Enhanced data protection

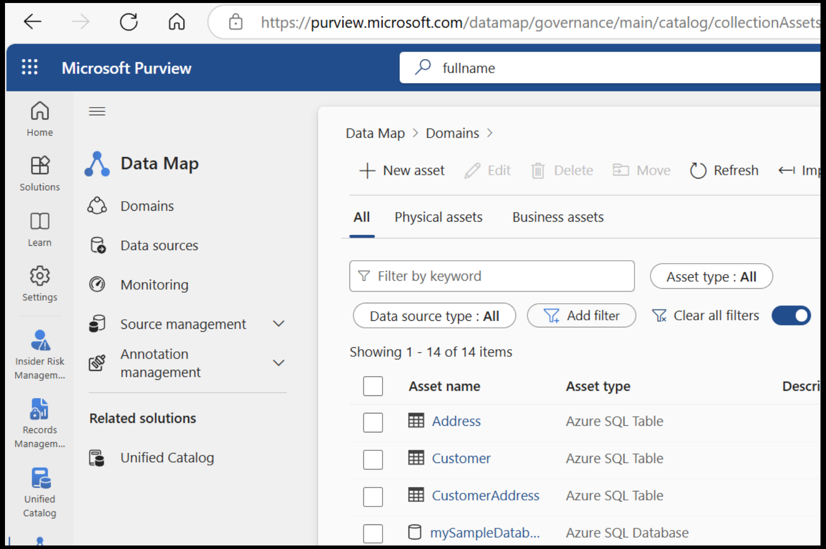
DATA COMPLIANCE

- Information Protection
  - Sensitivity Labels
- Communication Compliance
  - From Outlook, Teams, etc.
- Data Lifecycle Management
  - Retention labels
  - Data Classifiers

SYSTEM CLASSIFIERS VS CUSTOM CLASSIFIERS

- System classifiers are made automatically by Purview

- Custom classifiers are ones you can make yourself



Showing 1 - 14 of 14 items

Asset name	Asset type	Descri
Address	Azure SQL Table	
Customer	Azure SQL Table	
CustomerAddress	Azure SQL Table	
mySampleDatab...	Azure SQL Database	

CREATE A CUSTOM CLASSIFICATION

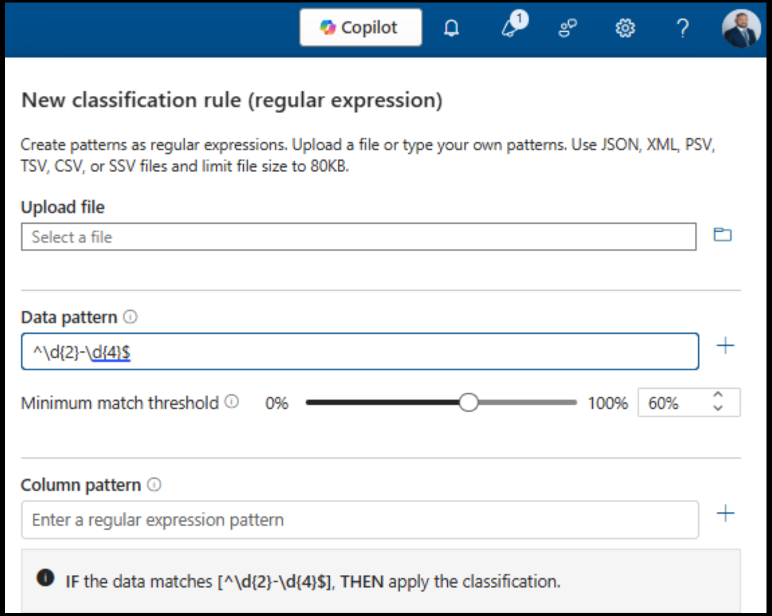
- Click on Solutions in Purview, Data Map, expand Annotation management, click on Classifications, Custom tab, +New, type in a name such as API key, token, medicine, chemical formula, designs…spaces are not allowed…but underscores will work

CREATE A CLASSIFICATION RULE

- Click Classification rules on the left-side of the screen, click + New, make a rule name, search for Classification name you made, click regular expression, click continue

- Upload a CSV file with 3 or more columns to test classification rule, click Create

- Here we use ^\d{2}-\d{4}$ for 2 digits followed by a – with 4 more digits



New classification rule (regular expression)

Create patterns as regular expressions. Upload a file or type your own patterns. Use JSON, XML, PSV, TSV, CSV, or SSV files and limit file size to 80KB.

Upload file

Select a file

Data pattern ⓘ

^\d{2}-\d{4}$

Minimum match threshold ⓘ 0% 100% 60%

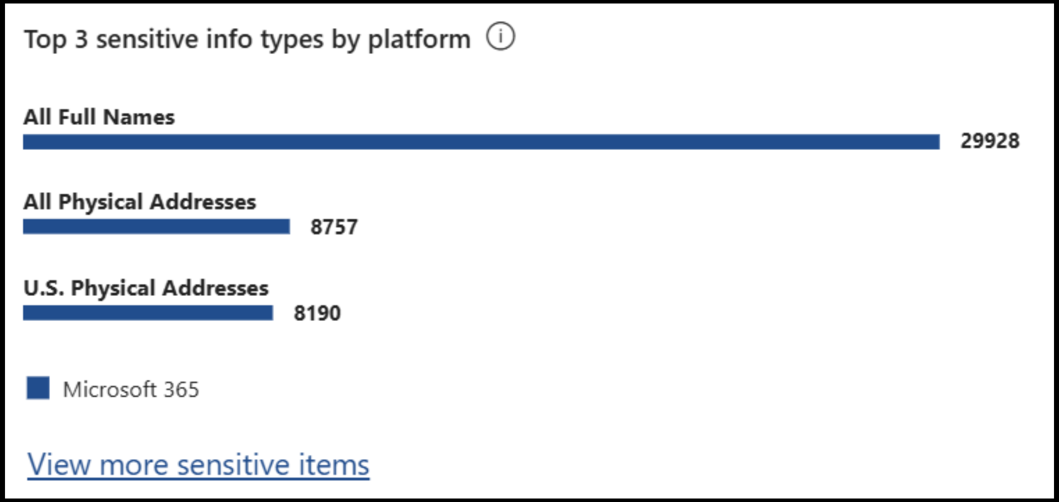
Column pattern ⓘ

Enter a regular expression pattern

IF the data matches [^\d{2}-\d{4}$], THEN apply the classification.

VIEW DATA SENSITIVITY LABELS

1. Scroll down on https://purview.microsoft.com/
2. Click View more sensitive items
3. This takes you to Information Protection https://purview.microsoft.com/informationprotection
4. Expand explorers and click data explorer
5. Select the location



THE END

FEEDBACK

You are welcome to provide any feedback about the session.

Thank you for participating!

JEREMY NATHAN

Email: jnathan@jncomputertraining.com

GitHub:
https://github.com/jeremynathan/purview

LinkedIn:
https://www.linkedin.com/in/jeremy-nathan-mct/