Microsoft Purview
&
Zero Trust principles approach

Bartlomiej Graczyk

Lead Cloud Solution Architect, Data & Analytics

bagra@microsoft.com

https://www.linkedin.com/in/bartlomiejgraczyk/

https://twitter.com/GraczykBartek

https://github.com/DataInsiders

Microsoft Purview enables unified data governance

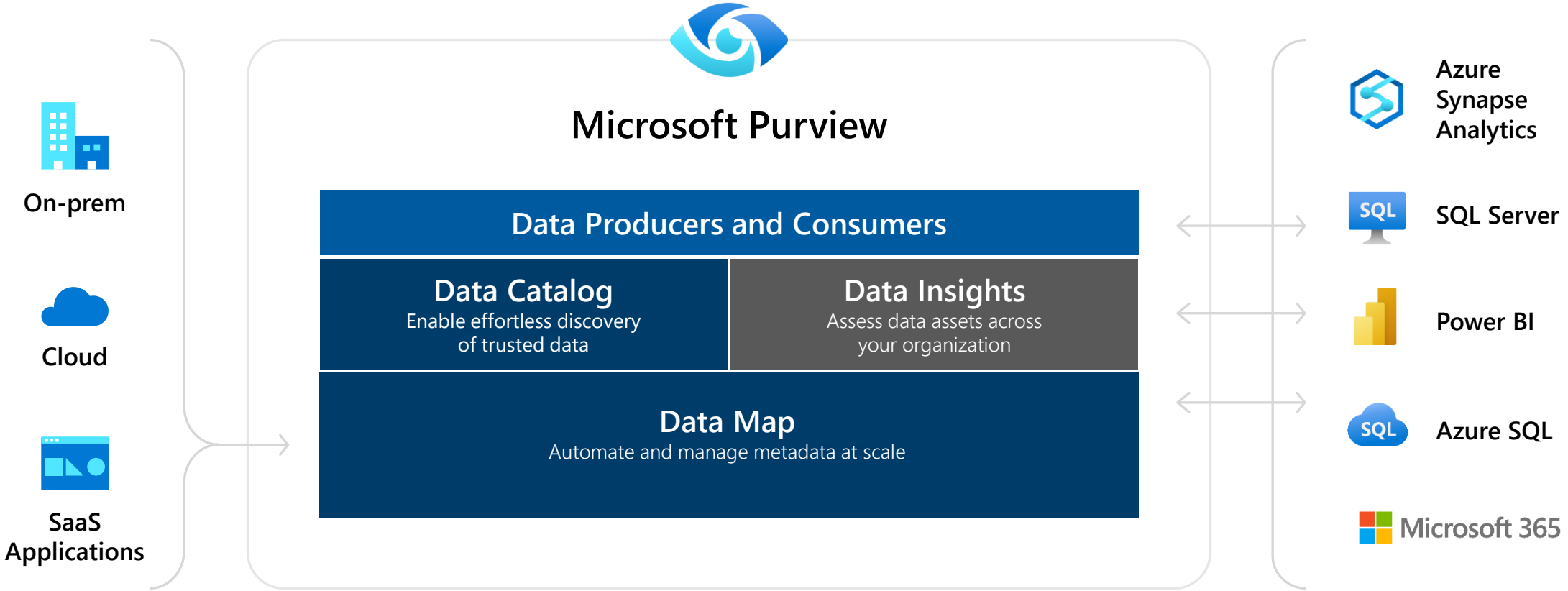
Reimagine data governance in the cloud

Set the foundation for effective data governance

Maximize business value of data for data consumers

Gain strategic insight into data use across the estate

Unified Data Governance with Microsoft Purview



Zero Trust principles

Verify explicitly

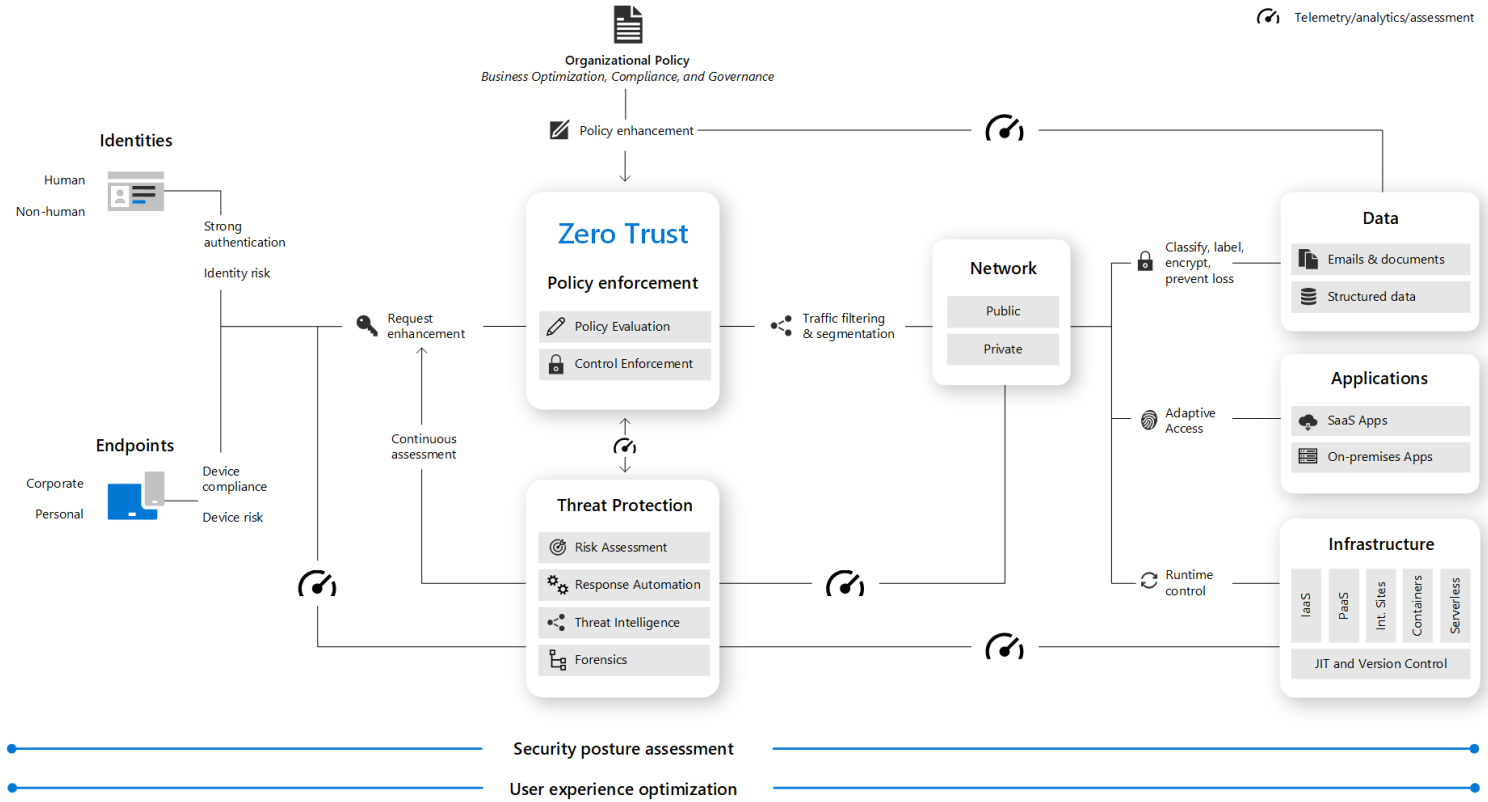
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

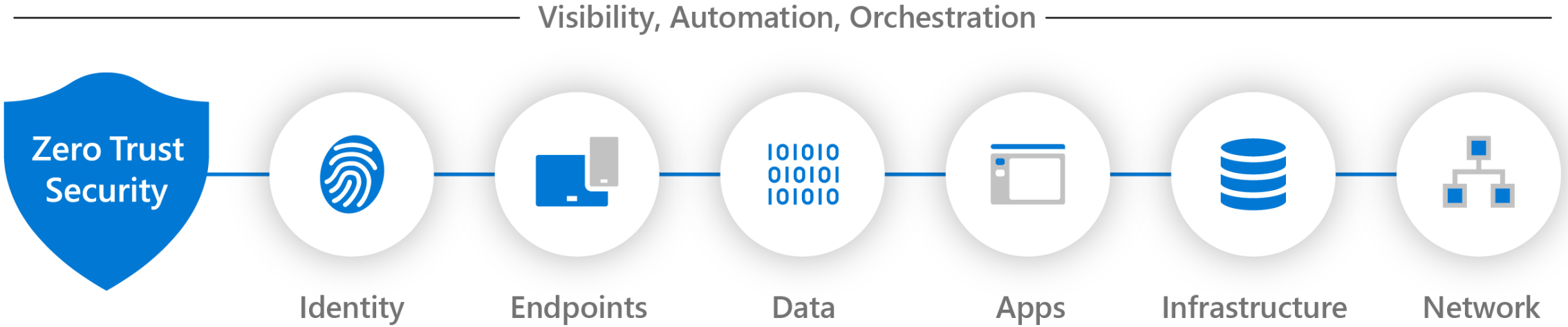
Use least privileged access

Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.




Visibility, Automation, Orchestration
Zero Trust Security
Identity
Endpoints
Data
Apps
Infrastructure
Network

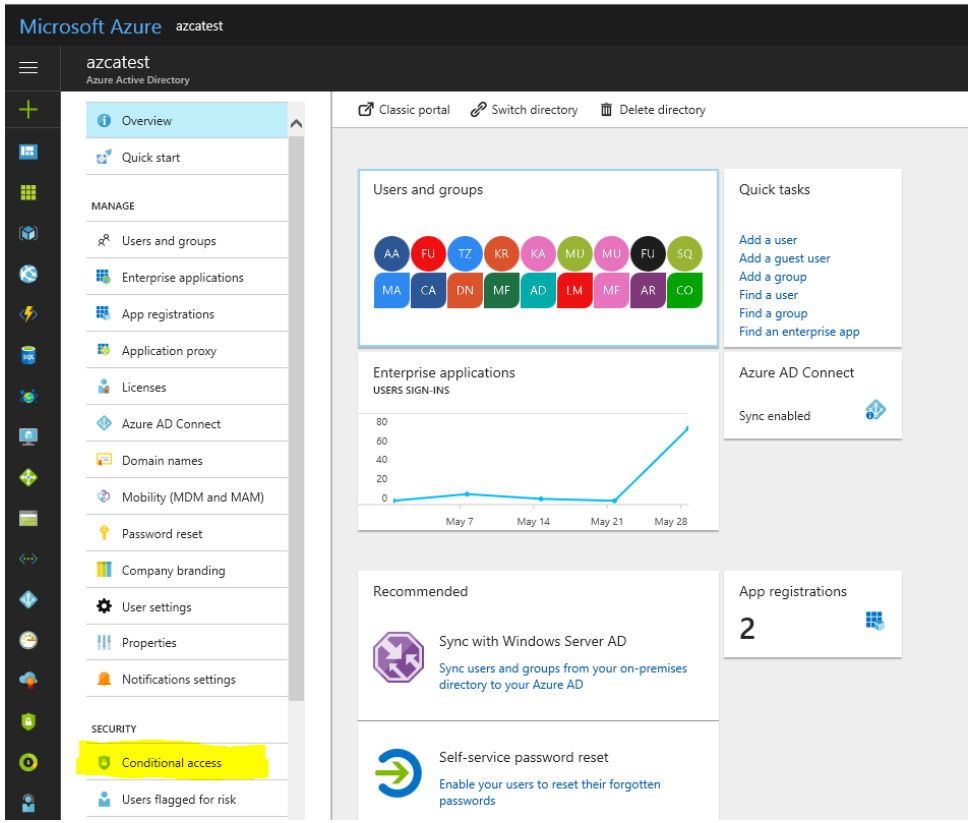
Top recommendations for Zero Trust

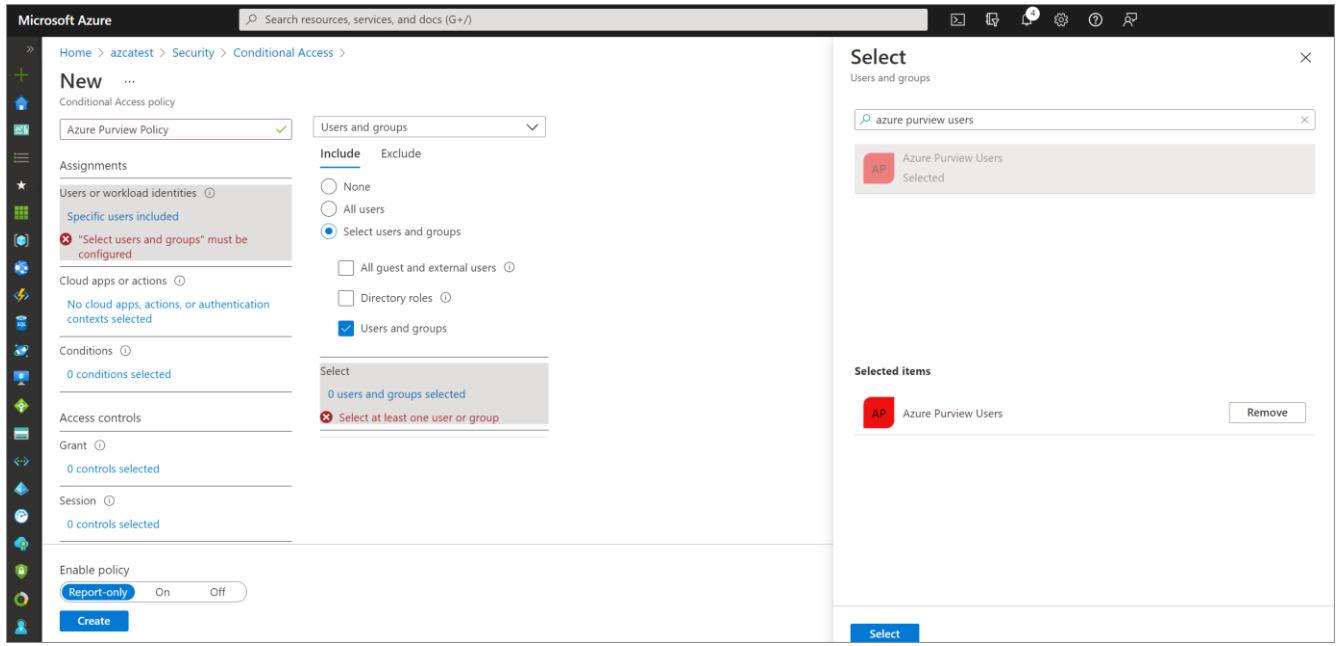
Use a trusted, standards-based authentication library. Using a library will save you the time of developing a solution on your own. Microsoft provides several authentication libraries, including the Microsoft Authentication Library (MSAL), Microsoft Identity Web authentication library, and the Azure SDKs for managed identities. These give you access to features such as conditional access, device registration and management, and the latest innovations such as passwordless and FIDO2 authentication without needing to write any extra code.

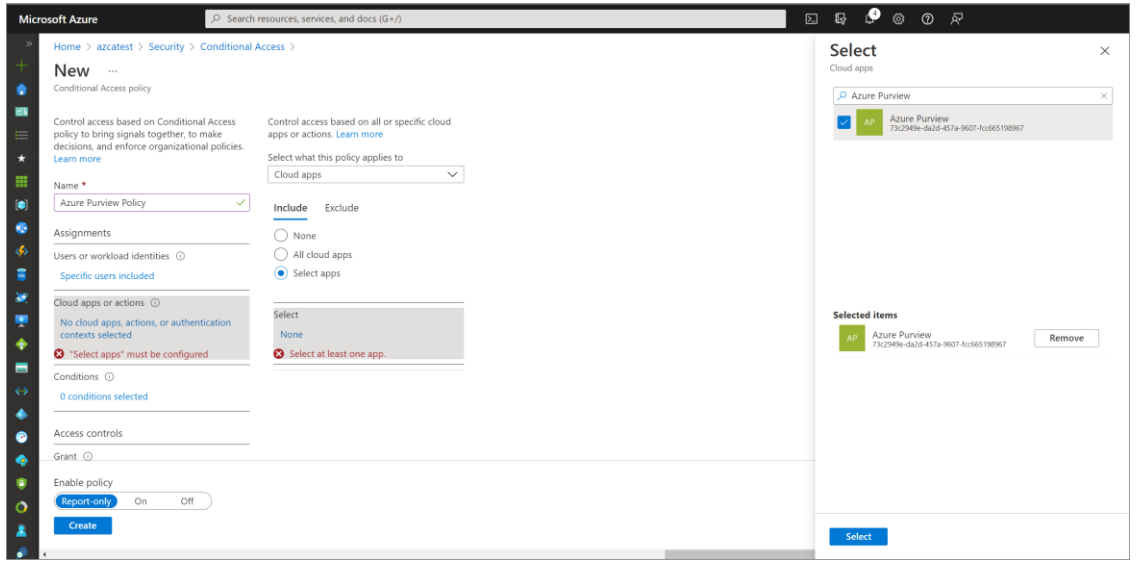
Follow the Azure AD application registration security best practices. An Azure AD application registration is a critical part of your business application. Any misconfiguration or lapse in hygiene of your application can result in downtime or compromise.

Keep credentials out of your code. This enables credential rotation by IT administrators without bringing down or redeploying an app. You can use a service such as Azure Key Vault or Azure Managed Identities.

Design for least privileged access. This is a key tenet of Zero Trust. You should always provide the least privilege required for the user to do their job


Microsoft Azure
azcatest
azcatest
Azure Active Directory
Overview
Quick start
MANAGE
Users and groups
Enterprise applications
App registrations
Application proxy
Licenses
Azure AD Connect
Domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings
SECURITY
Conditional access
Users flagged for risk
Classic portal
Switch directory
Delete directory
Users and groups
Quick tasks
Add a user
Add a guest user
Add a group
Find a user
Find a group
Find an enterprise app
Enterprise applications
USERS SIGN-INS
Azure AD Connect
Sync enabled
Recommended
Sync with Windows Server AD
Sync users and groups from your on-premises directory to your Azure AD
Self-service password reset
Enable your users to reset their forgotten passwords
App registrations
2


Microsoft Azure
Search resources, services, and docs (G+/)
Home > azcatest > Security > Conditional Access >
New
Conditional Access policy
Azure Purview Policy
Assignments
Users or workload identities
Specific users included
"Select users and groups" must be configured
Cloud apps or actions
No cloud apps, actions, or authentication contexts selected
Conditions
0 conditions selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Enable policy
Report-only
On
Off
Create
Users and groups
Include
Exclude
None
All users
Select users and groups
All guest and external users
Directory roles
Users and groups
Select
0 users and groups selected
Select at least one user or group
Select
Users and groups
azure purview users
Azure Purview Users
Selected
Selected items
Azure Purview Users
Remove
Select


Microsoft Azure
Search resources, services, and docs (G+/)
Home > azcatest > Security > Conditional Access >
New
Conditional Access policy
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
Azure Purview Policy
Assignments
Users or workload identities
Specific users included
Cloud apps or actions
No cloud apps, actions, or authentication contexts selected
"Select apps" must be configured
Conditions
0 conditions selected
Access controls
Grant
Enable policy
Report-only
On
Off
Create
Control access based on all or specific cloud apps or actions. Learn more
Select what this policy applies to
Cloud apps
Include
Exclude
None
All cloud apps
Select apps
Select
None
Select at least one app.
Select
Cloud apps
Azure Purview
Azure Purview
Selected items
Azure Purview
Remove
Select

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Azure Purview Policy

Assignments

Users or workload identities

Specific users included

Cloud apps or actions

1 app included

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Enable policy

Report-only | On | Off

Create

Grant

Control access enforcement to block or grant access. Learn more

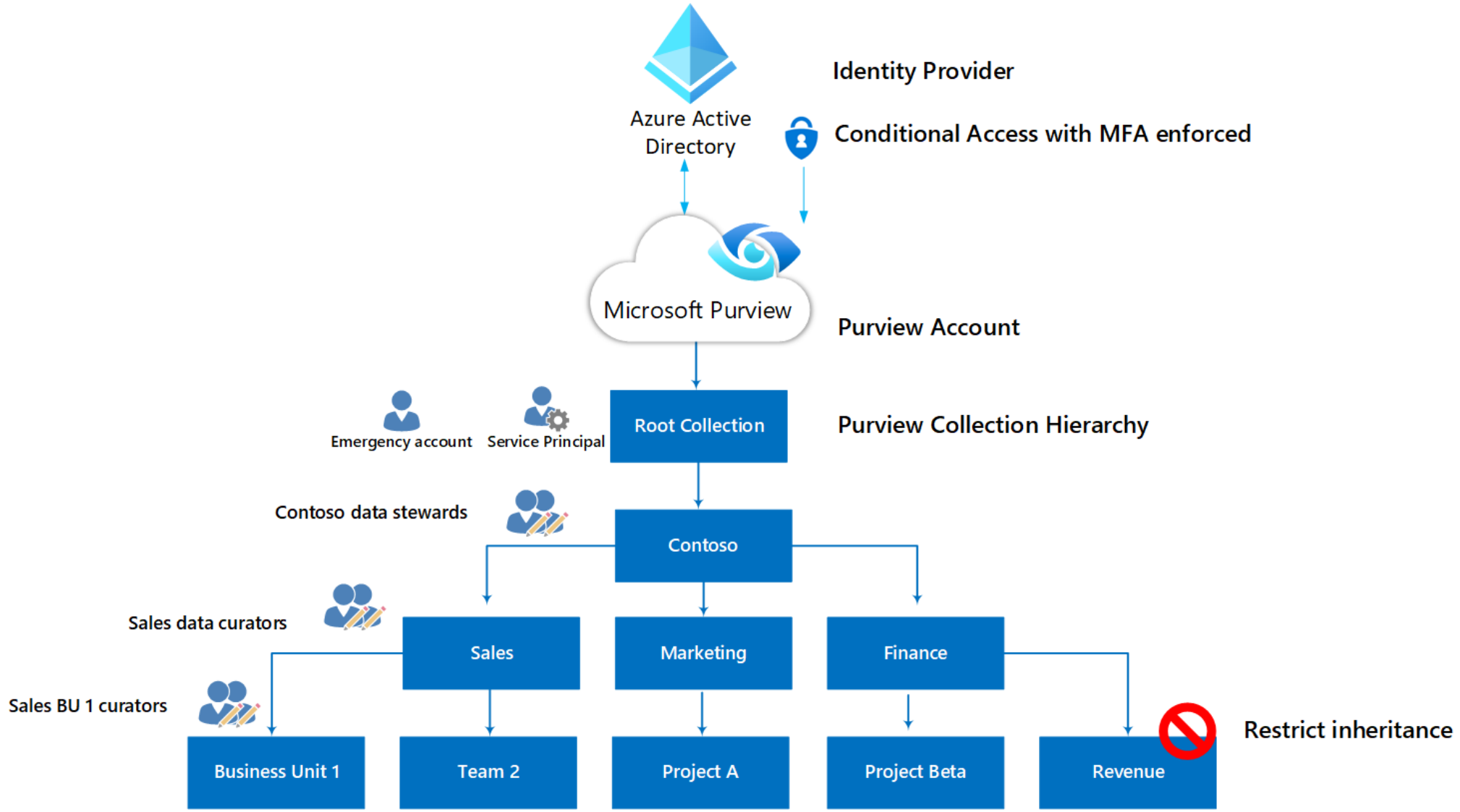
- ( ) Block access
- (•) Grant access

- [x] Require multi-factor authentication
- [ ] Require device to be marked as compliant
- [ ] Require Hybrid Azure AD joined device
- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy
  See list of policy protected client apps
- [ ] Require password change

For multiple controls

- (•) Require all the selected controls
- ( ) Require one of the selected controls

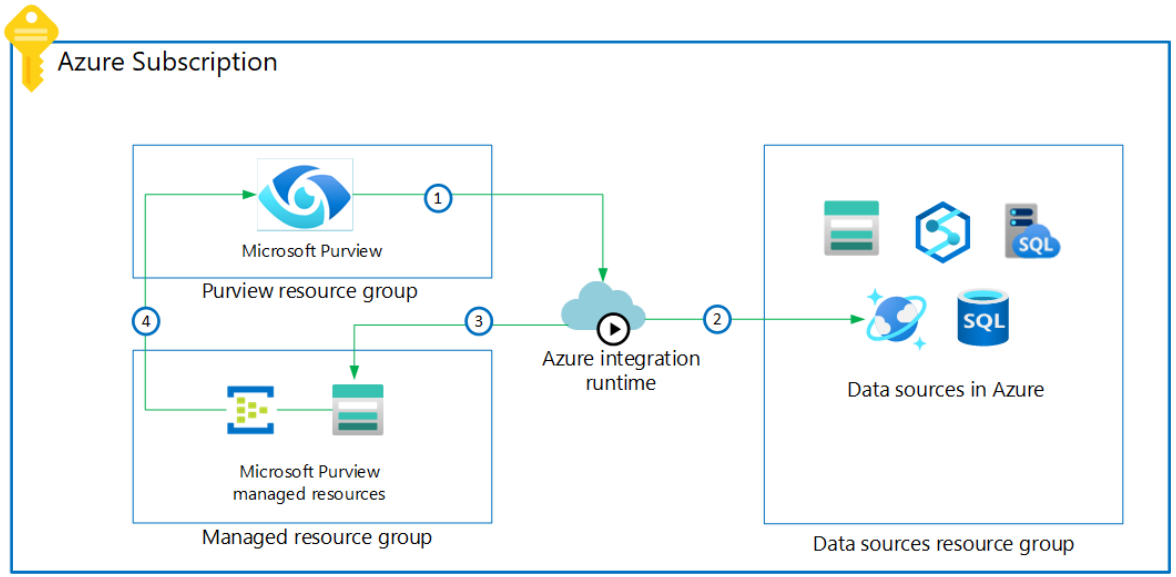
Select


Azure Active Directory
Identity Provider
Conditional Access with MFA enforced
Microsoft Purview
Purview Account
Emergency account
Service Principal
Root Collection
Purview Collection Hierarchy
Contoso data stewards
Contoso
Sales data curators
Sales
Marketing
Finance
Sales BU 1 curators
Business Unit 1
Team 2
Project A
Project Beta
Revenue
Restrict inheritance

To connect to a data source Microsoft Purview requires a credential with read-only access to the data source system.

It is recommended prioritizing the use of the following credential options for scanning, when possible:

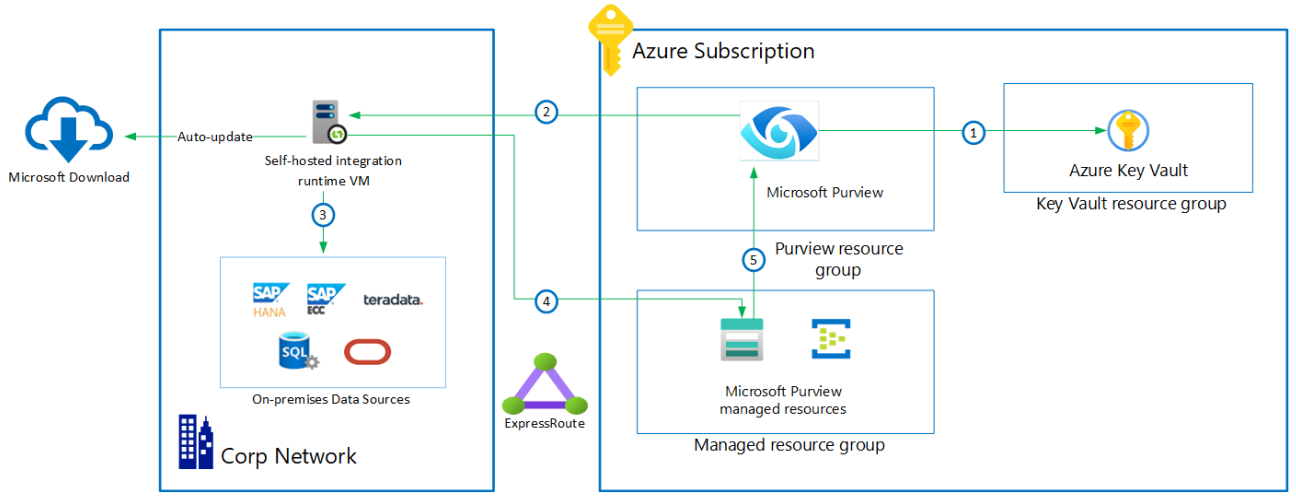
1. Microsoft Purview Managed Identity
2. User Assigned Managed Identity
3. Service Principals
4. Other options such as Account key, SQL Authentication, etc.

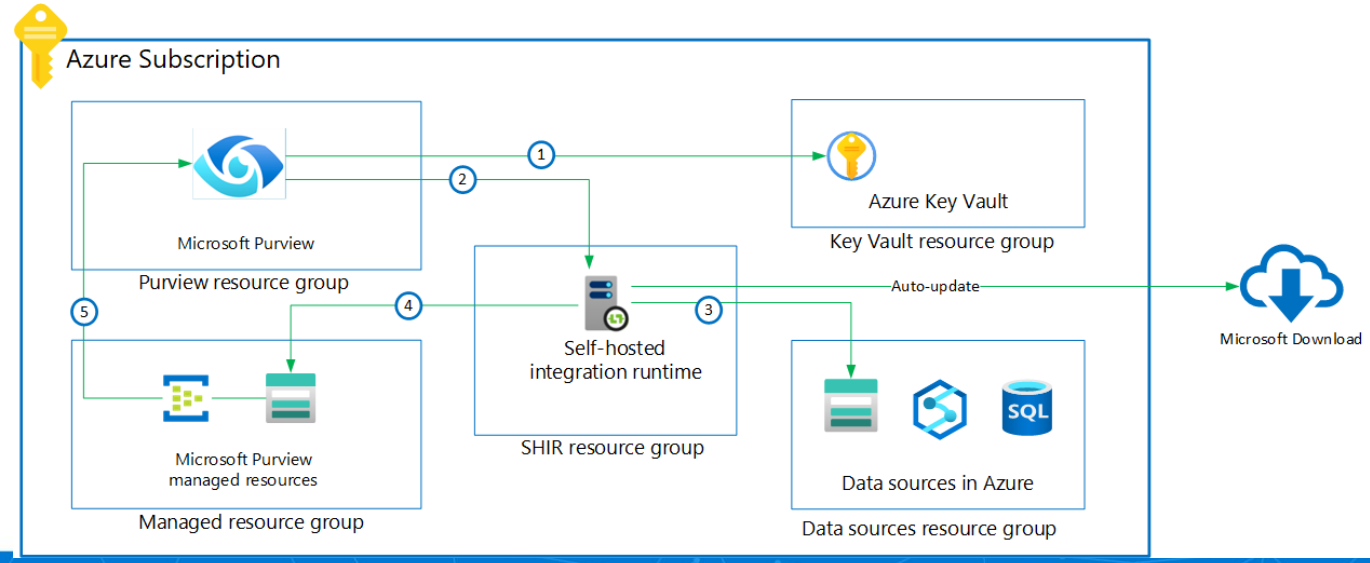


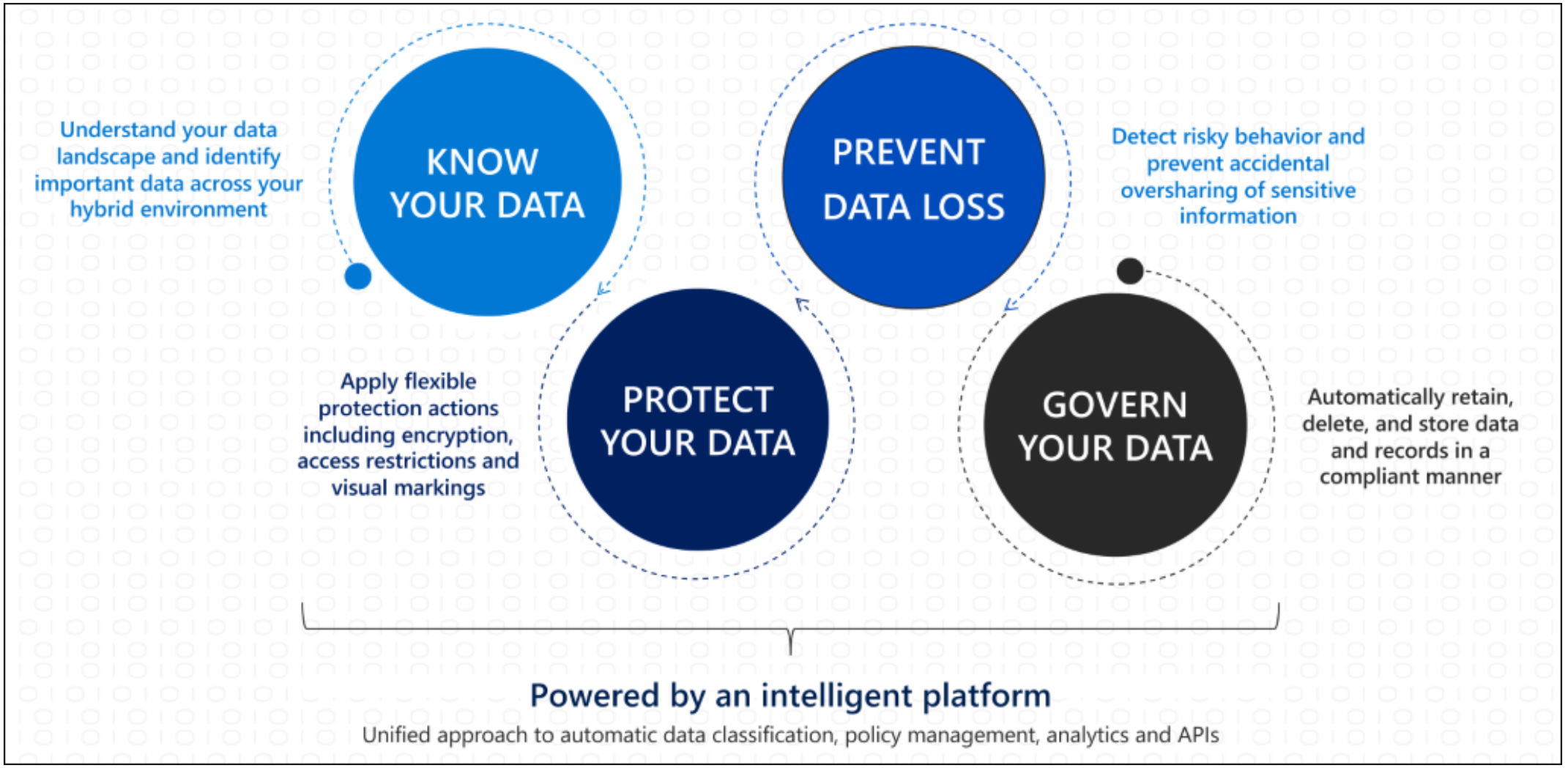
To connect to a data source Microsoft Purview requires a credential with read-only access to the data source system.

It is recommended prioritizing the use of the following credential options for scanning, when possible:

1. Microsoft Purview Managed Identity
2. User Assigned Managed Identity
3. Service Principals
4. Other options such as Account key, SQL Authentication, etc.






Understand your data landscape and identify important data across your hybrid environment
KNOW YOUR DATA
PREVENT DATA LOSS
Detect risky behavior and prevent accidental oversharing of sensitive information
Apply flexible protection actions including encryption, access restrictions and visual markings
PROTECT YOUR DATA
GOVERN YOUR DATA
Automatically retain, delete, and store data and records in a compliant manner
Powered by an intelligent platform
Unified approach to automatic data classification, policy management, analytics and APIs

Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

- **Files & emails**

  Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

- **Groups & sites**

  Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

- **Schematized data assets**

  Apply labels to files and schematized data assets in Azure Purview. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Information protection

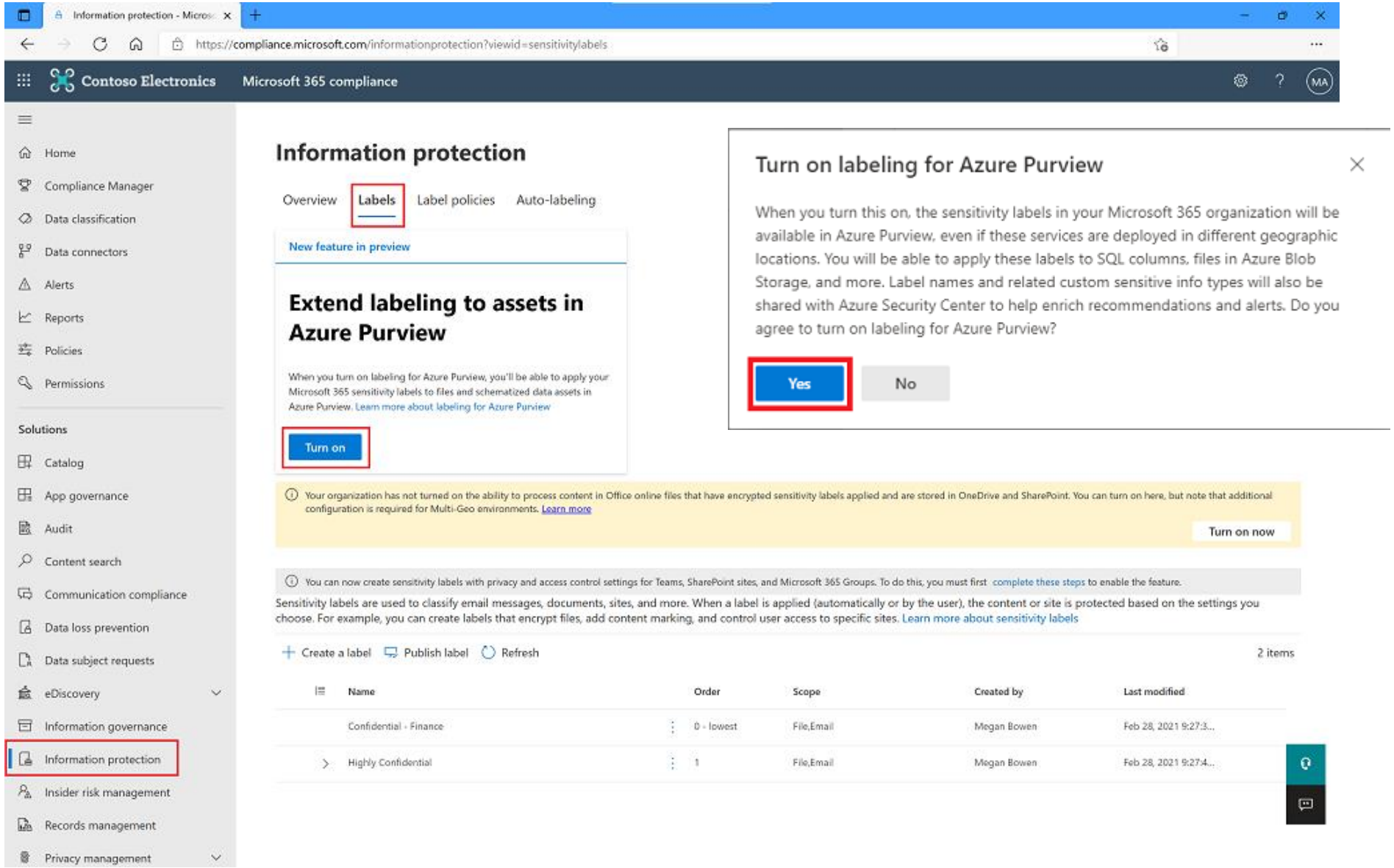
Labels | Label policies | Auto-labeling

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is a
the content or site is protected based on the settings you choose. For example, you can create labe
marking, and control user access to specific sites. Learn more about sensitivity labels

+ Create a label | Publish labels | Refresh

Name	Order	Created by	Last modified
Personal	0 - lowest	Robin Kline	1/4/2020
Public	1	Robin Kline	1/4/2020
General	2	Robin Kline	1/4/2020
Confidential		bin Kline	1/4/2020
Highly Confidential		bin Kline	6/13/2020

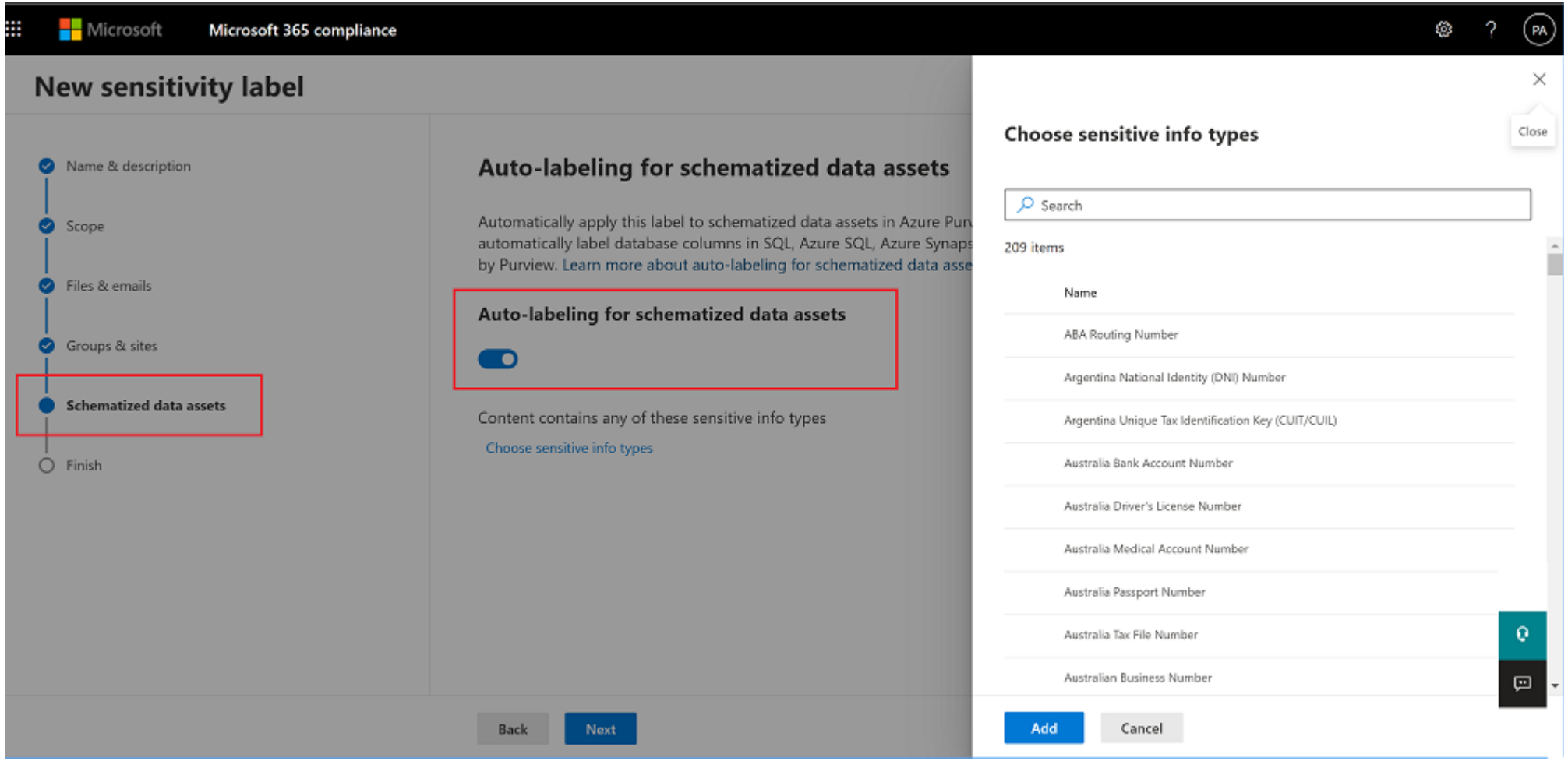
+ Add sub label
↑ Move up
↓ Move down



Microsoft

[How to automatically apply sensitivity labels to your data in Microsoft Purview Data Map - Microsoft Purview | Microsoft Docs]

Azure Club


Microsoft
Microsoft 365 compliance
PA
New sensitivity label
Name & description
Scope
Files & emails
Groups & sites
Schematized data assets
Finish
Auto-labeling for schematized data assets
Automatically apply this label to schematized data assets in Azure Pur
automatically label database columns in SQL, Azure SQL, Azure Synaps
by Purview. Learn more about auto-labeling for schematized data asse
Auto-labeling for schematized data assets
Content contains any of these sensitive info types
Choose sensitive info types
Back
Next
Choose sensitive info types
Close
Search
209 items
Name
ABA Routing Number
Argentina National Identity (DNI) Number
Argentina Unique Tax Identification Key (CUIT/CUIL)
Australia Bank Account Number
Australia Driver's License Number
Australia Medical Account Number
Australia Passport Number
Australia Tax File Number
Australian Business Number
Add
Cancel

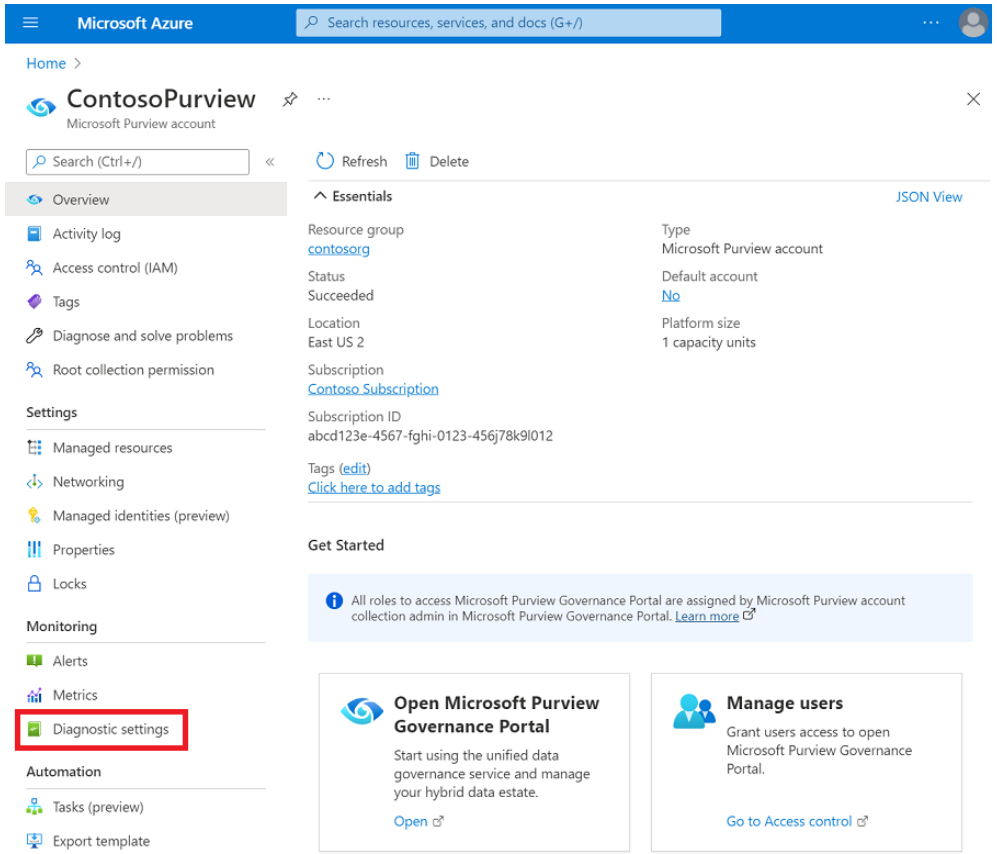
- Microsoft Purview extracts only the metadata from different data source systems into Microsoft Purview Data Map during the scanning process.

- You can deploy a Microsoft Purview account inside your Azure subscription in any supported Azure regions.

- All metadata is stored inside Data Map inside your Microsoft Purview instance. This means the metadata is stored in the same region as your Microsoft Purview instance.

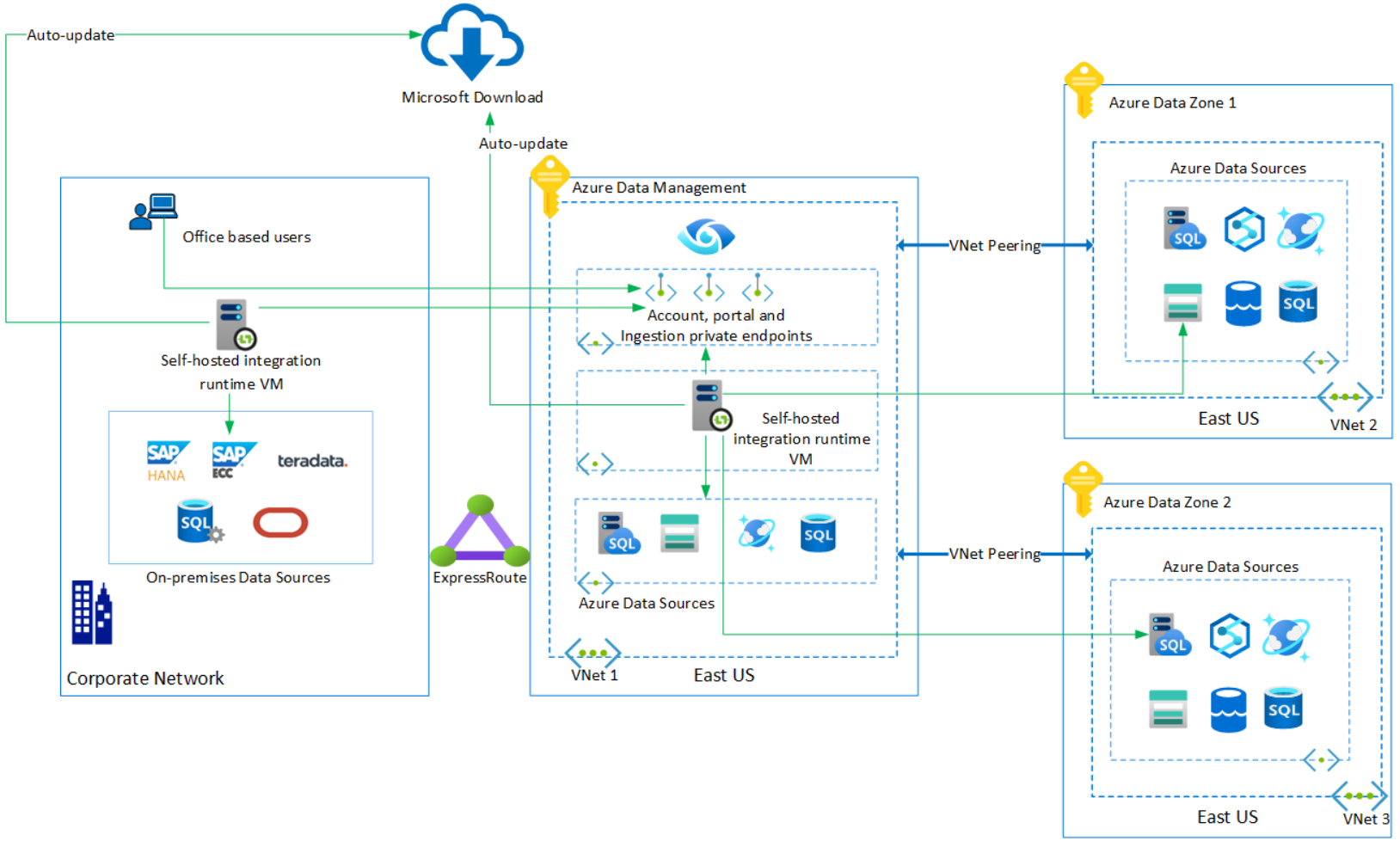
- For Microsoft Purview, data is encrypted at rest using Microsoft-managed keys and when data is in transit, using Transport Layer Security (TLS) v1.2 or greater.

Audit logs, diagnostics, and activity history

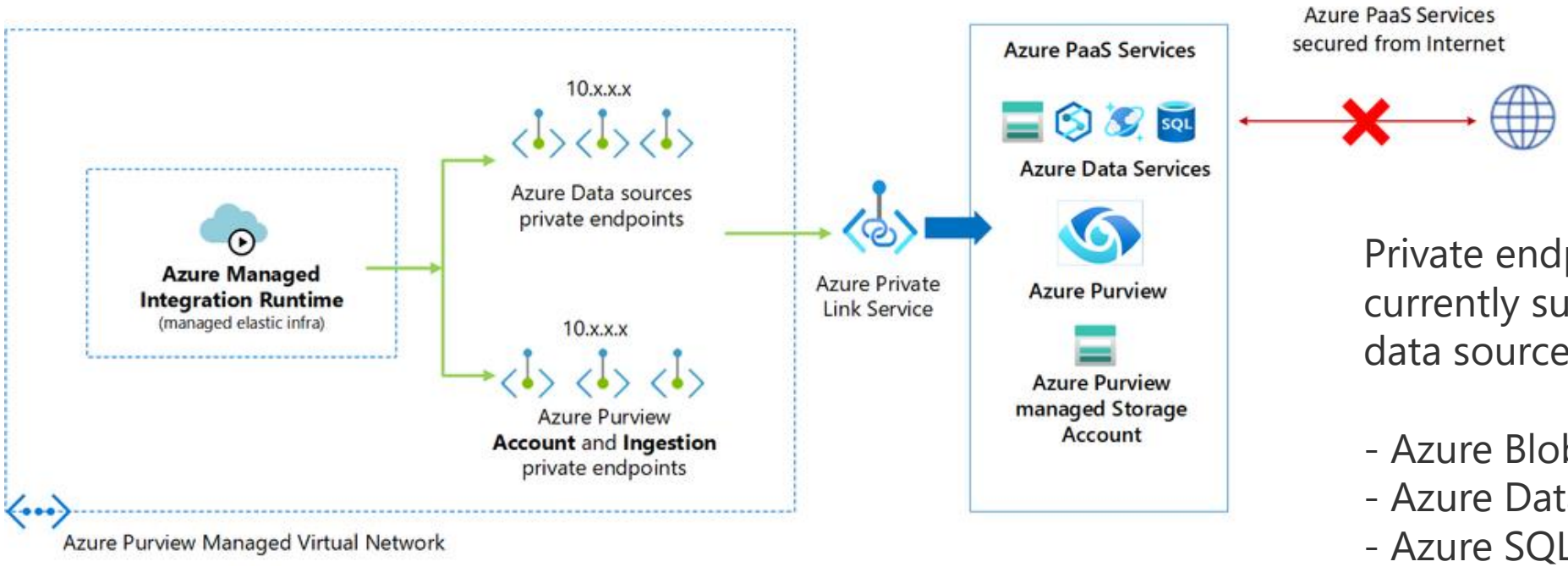


Category	Activity	Operation
Management	Scan rule set	Create
Management	Scan rule set	Update
Management	Scan rule set	Delete
Management	Classification rule	Create
Management	Classification rule	Update
Management	Classification rule	Delete
Management	Scan	Create
Management	Scan	Update
Management	Scan	Delete
Management	Scan	Run
Management	Scan	Cancel
Management	Scan	Create
Management	Scan	Schedule
Management	Data source	Register
Management	Data source	Update
Management	Data source	Delete

Single region, multiple virtual networks



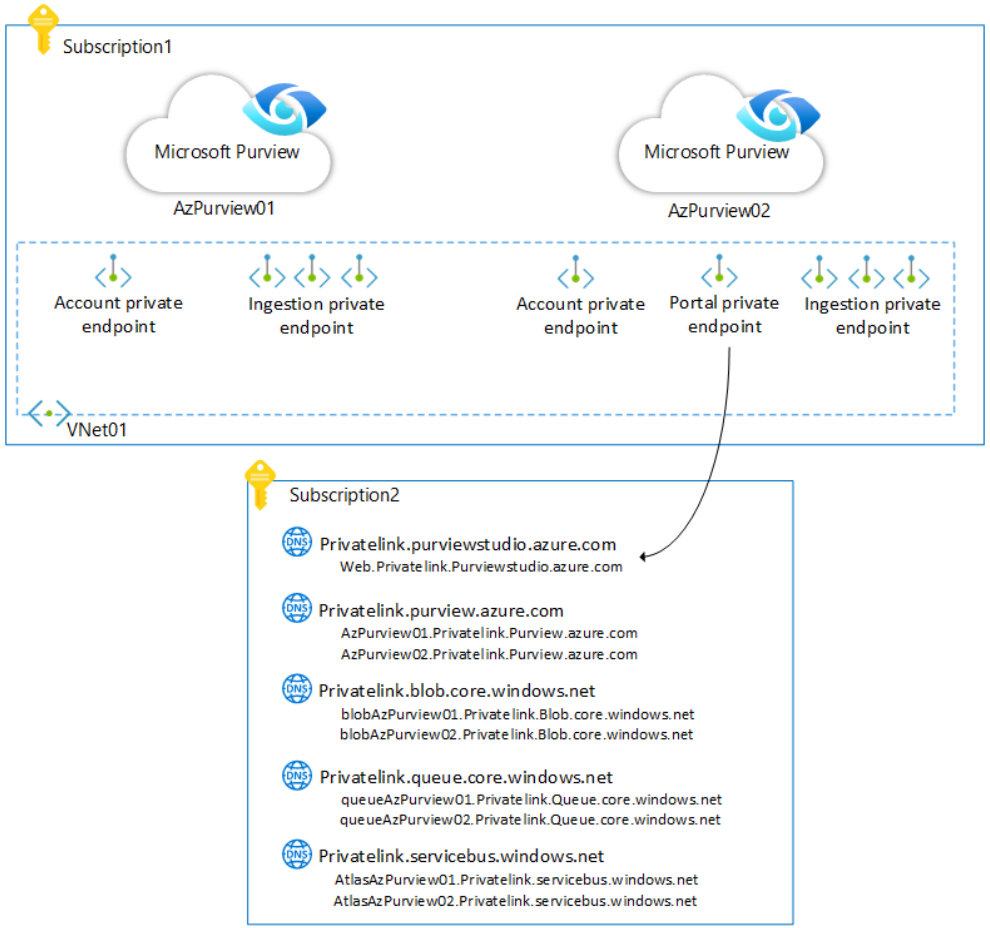
Managed Virtual Network

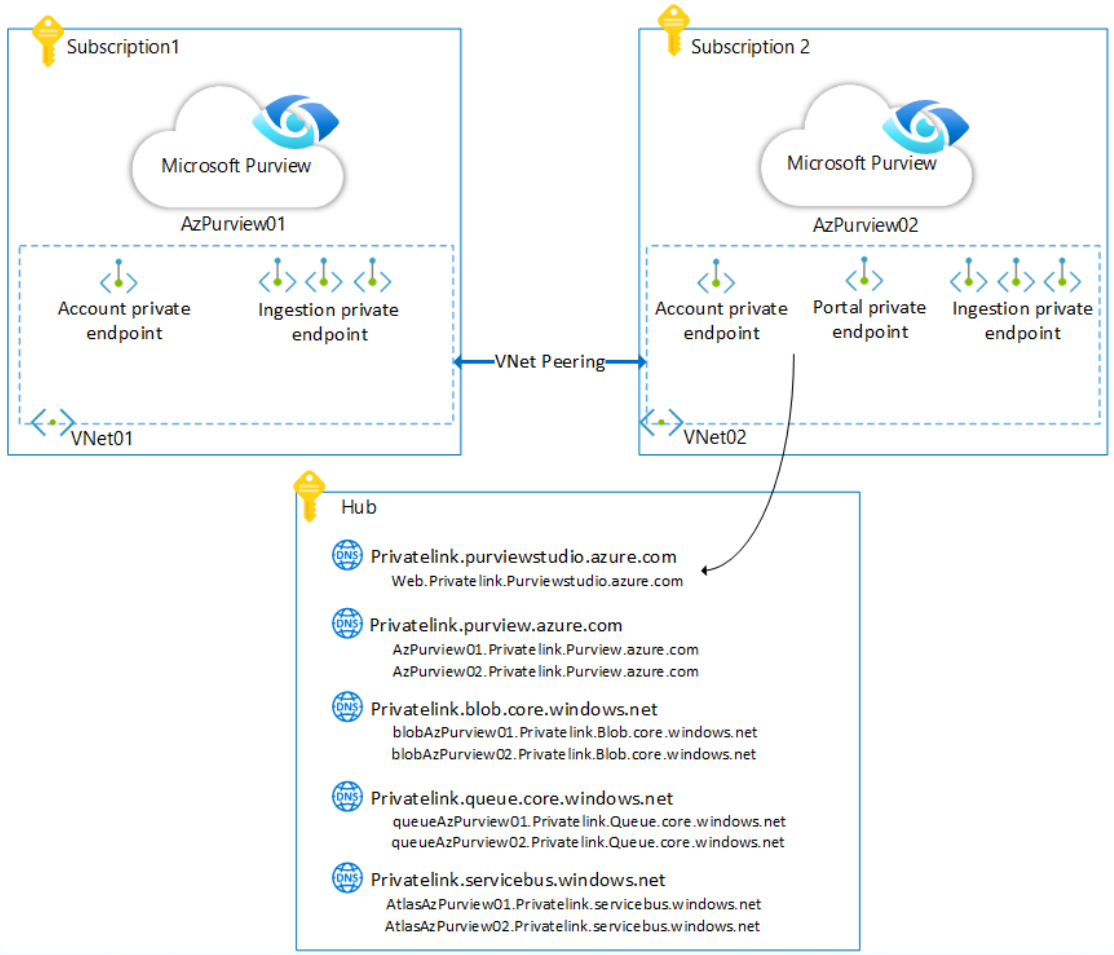


Private endpoint connections are currently support for the following data source types:

- Azure Blob Storage
- Azure Data Lake Storage Gen 2
- Azure SQL Database
- Azure Cosmos DB
- Azure Synapse Analytics
- Azure Files
- Azure Database for MySQL
- Azure Database for PostgreSQL

DNS configuration with private endpoints





Microsoft Purview
&
Zero Trust principles approach

Bartlomiej Graczyk

Lead Cloud Solution Architect, Data & Analytics

bagra@microsoft.com

https://www.linkedin.com/in/bartlomiejgraczyk/

https://twitter.com/GraczykBartek

https://github.com/DataInsiders