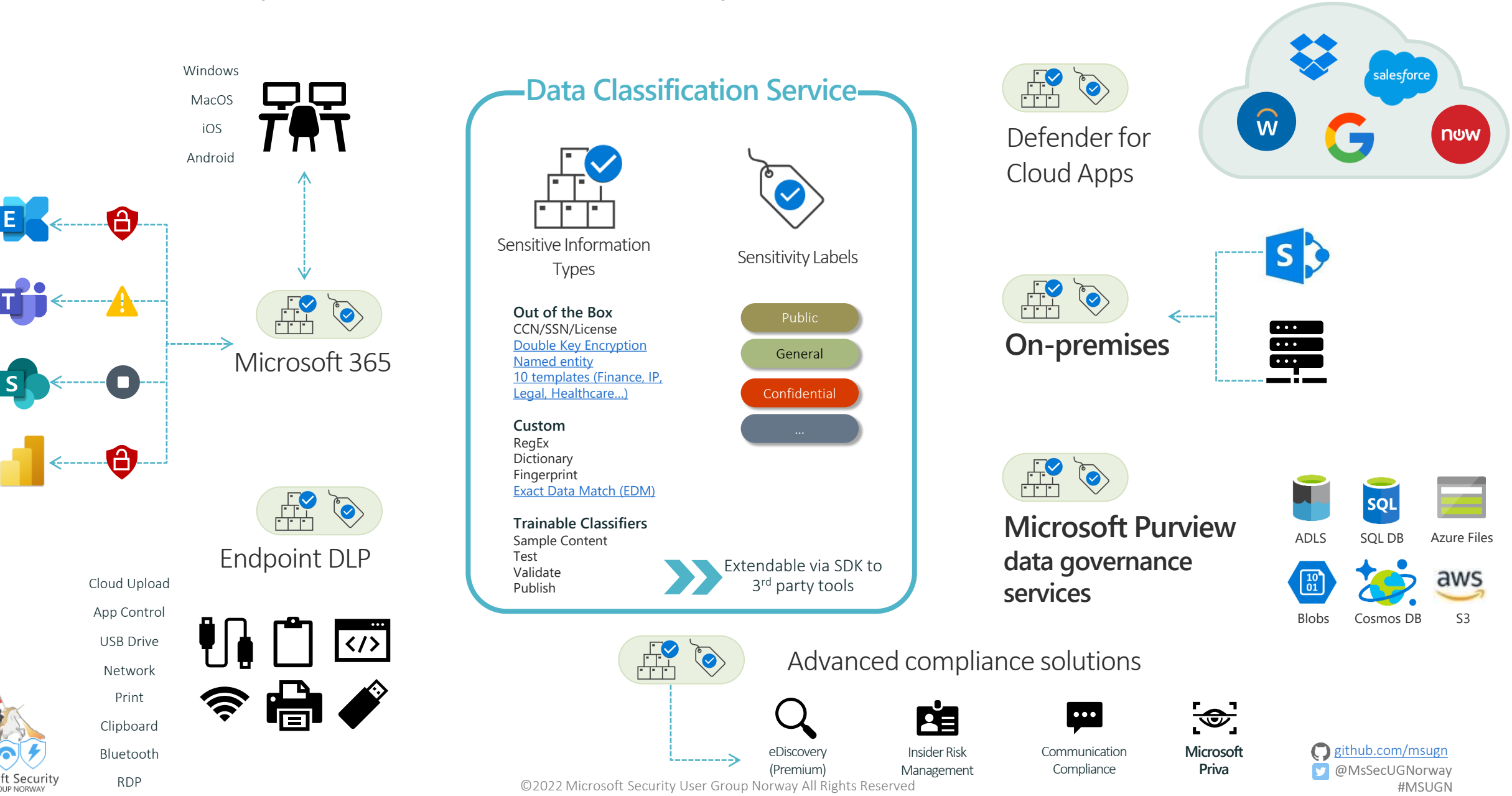


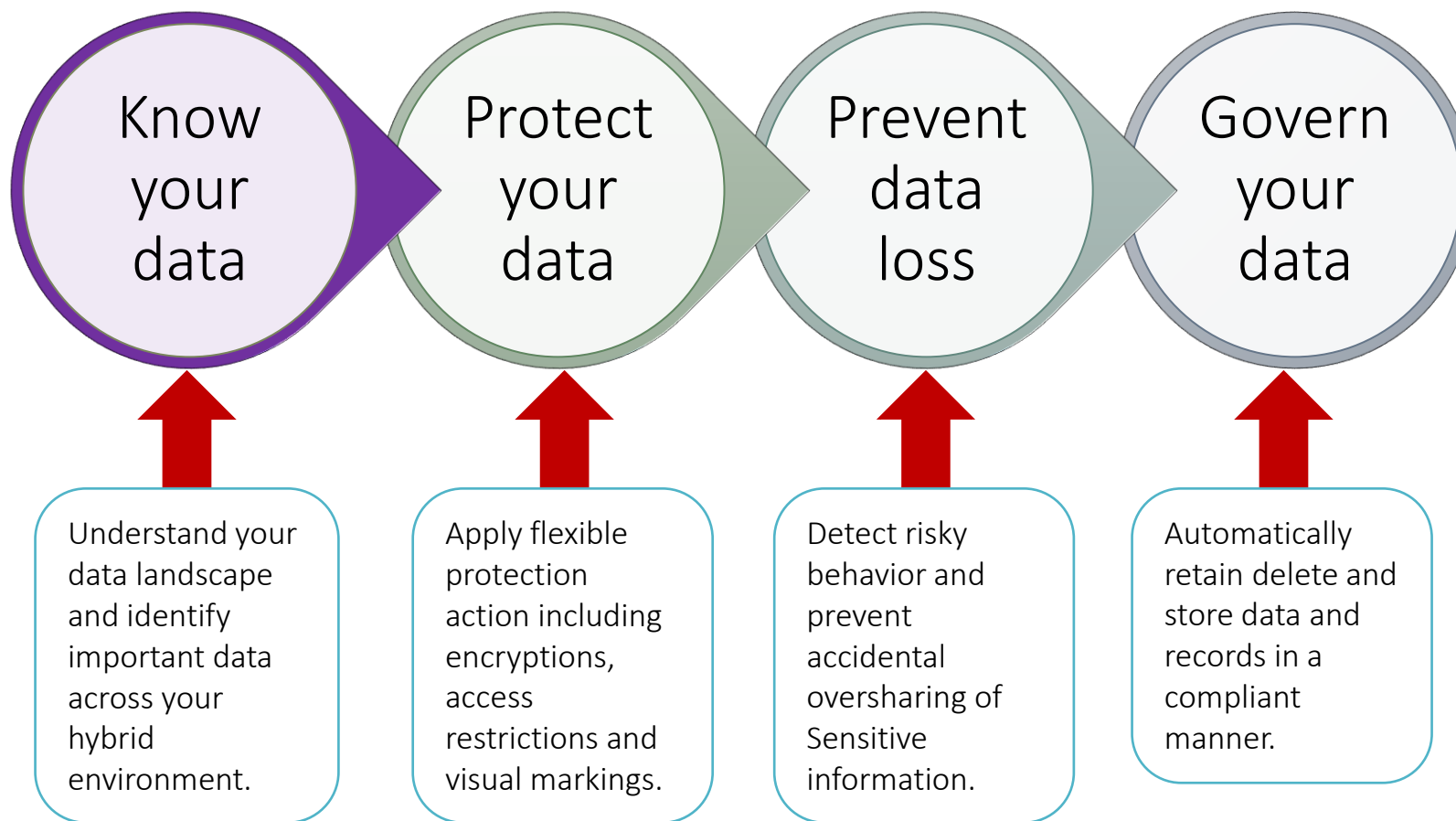


Data Harmony with Purview

Microsoft Purview unified solution



Information protection and data lifecycle management



Know your Data,

- Discovery & Mapping phase

- What kind of information do you have?
- Where in the infrastructure that the information is stored.
- How or if it is secured/governed

- Regulations your organization are expected to follow?

- Do you have a governance plan for Microsoft 365?
- Get a mandate to implement classification and governance

Where's my data?

Content explorer

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)

Filter on labels, info types, or categories

All locations > SharePoint

Sensitive info types

DataRiskCheck-Purview

2

All Full Names

2

DataRiskCheck-EmployeeID

2

All Medical Terms And Conditions

1

Diseases

1


Surgical Procedures


1


Sensitivity labels

Personal

4

 The number of site/folder items listed below and on the left is a calculation and may not match the total number of actual items you'll see when you open a specific site/folder.

 Export

 Search



Name

Files



https://labglenad.sharepoint.com/sites/demo

2



Data classification

Classifiers:

- Trainable classifiers
- Sensitive information types (SIT)
- EDM classifiers

Labels:

- Information Protection labels
- Retention labels

Classifiers Demo

Prevent data loss demo

Activity Explorer

Filter

Date range: 10/01/2019 – 10/19/2019



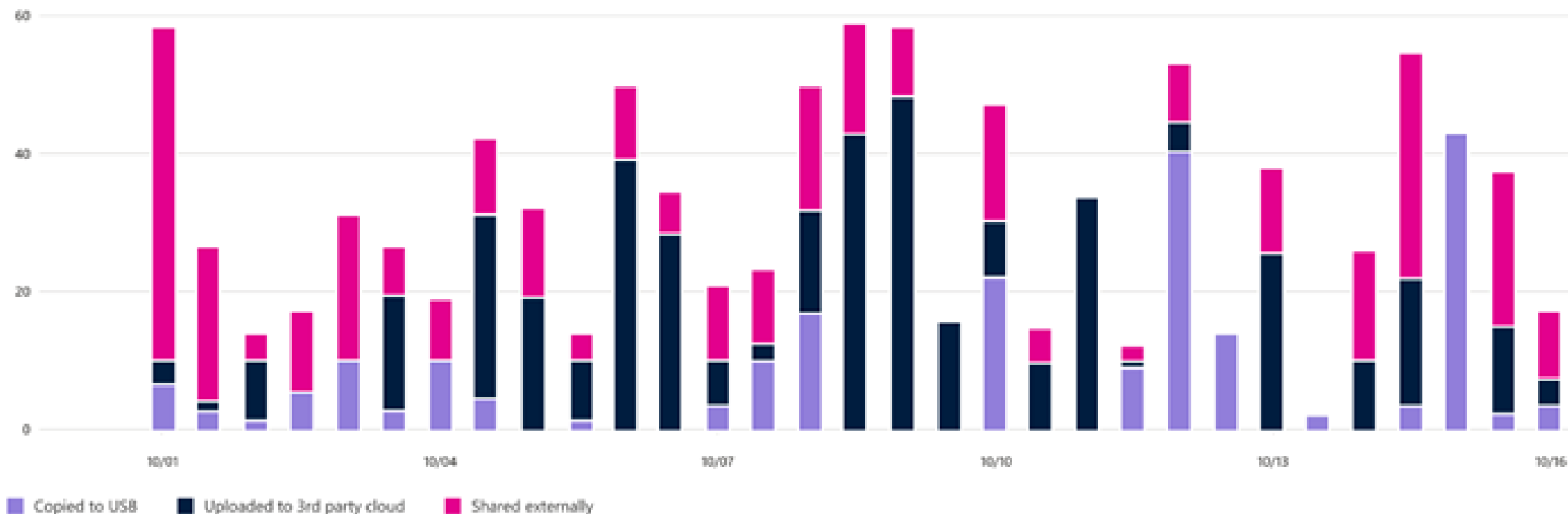
Activities: Copied to USB, Uploaded to 3rd party cloud, +1



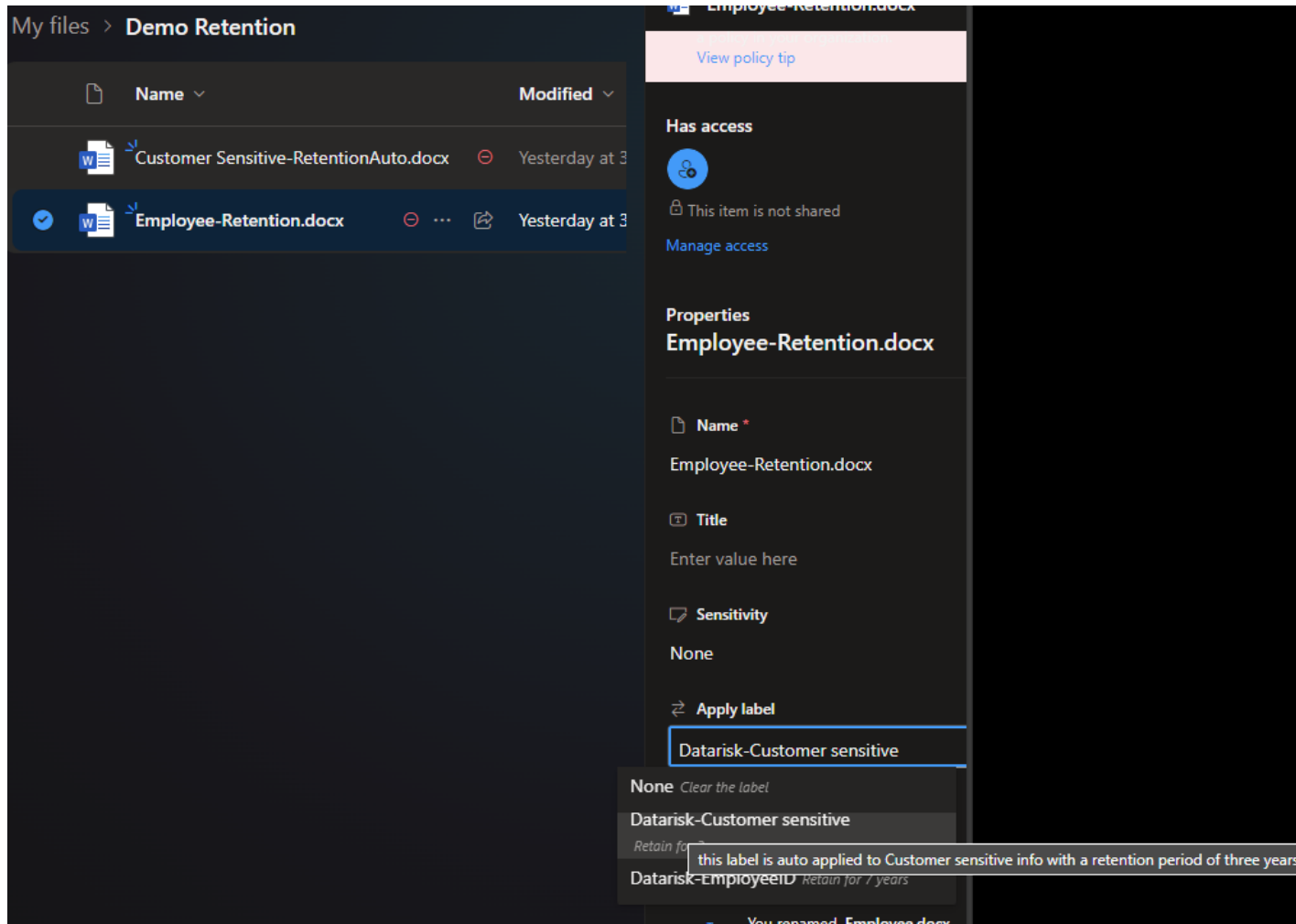
Locations: Any



File types: JPG, PNG



Govern Your Data, Data Lifecycle Management



Retention 365 Copilot interactions

Data lifecycle management > Edit retention policy



- ✓ Name
- ✓ Administrative Units
- **Type**
- **Locations**
- Retention settings
- Finish

Choose where to apply this policy

The policy will apply to content that's stored in the locations you choose.

ⓘ You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

ⓘ Policies that apply to Teams chats or Teams channel messages can't include other locations.

Status	Location	Applicable Content	Included	Excluded
<input checked="" type="checkbox"/> On	 Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. More details	1 team Edit	None Edit
<input checked="" type="checkbox"/> On	 Teams chats and Copilot interactions	Messages from individual chats, group chats, meeting chats, bot chats, and interactions with Microsoft Copilot for Microsoft 365. More details	2 users Edit	None Edit

Compliance Manager & Assessment Templates

Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Trials

Solutions

Catalog

App governance

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Information protection

Information barriers

Insider risk management

Records management

Privacy risk management

Subject rights requests

Settings

More resources

Customize navigation

Compliance Manager

OverviewImprovement actionsSolutionsAssessmentsAssessment templatesAlertsAlert policies

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

Kickstart your compliance with free premium assessment templates


Start a 90-day free trial to create assessments that meet your organization's unique needs. Choose up to 25 templates from our library of 300+ assessments covering industry, regional, and national regulations and certifications. [Learn about this trial](#)

By proceeding, you agree to the [Microsoft Purview trial terms & conditions](#).

Start trial

Overall compliance score

Your compliance score: 56%



13492/23830 points achieved

Your points achieved ⓘ

1607/ 11522

Microsoft managed points achieved ⓘ

11885/ 12308

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

Key improvement actions

Not completed768

Completed60

Out of scope0

Improvement action	Impact	Test status	Group	Action type
Enable self-service password reset	+27 points	Partially tested	Default Group	Technical
Conceal information with lock screen	+27 points	None	Default Group	Technical
Use boundary protection devices for uncl...	+27 points	None	Default Group	Technical
Provide just-in-time notification or syste...	+27 points	None	Default Group	Technical
Block outdated ActiveX controls	+27 points	Failed high risk	Default Group	Technical
Enable 'Consistent MIME Handling'	+27 points	None	Default Group	Technical
Enable 'MIME Sniffing Safety Feature'	+27 points	None	Default Group	Technical
Protect against potentially unwanted ap...	+27 points	Failed high risk	Default Group	Technical
Restrict ActiveX Install	+27 points	None	Default Group	Technical


[View all improvement actions](#)

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.


Solution	Score contribution	Remaining actions
Audit	0/61 points	7
Azure	0/121 points	7
Azure Active Dir...	218/1079 points	48
Communication...	0/10 points	4
Compliance Ma...	27/3550 points	423
Data classificati...	0/57 points	3
Data lifecycle m...	0/28 points	2
Data loss preve...	0/189 points	7
Defender for Cl...	0/137 points	13

[View all solutions](#)



Microsoft Security
USER GROUP NORWAY

©2022 Microsoft Security User Group Norway All Rights Reserved



github.com/msugn
[@MsSecUGNorway](https://twitter.com/MsSecUGNorway)
#MSUGN

Summary of recommendations before M365 Copilot

Action	Location / Licence
Check Public / Private SharePoint sites	SPO Admin center, PowerShell scripts (E3)
Check Public / Private Teams	Teams Admin center, PowerShell scripts (E3)
Update privacy on Sites and Teams	SPO & Teams Admin center, PowerShell scripts (E3)
Review Audit logs for sharing activities	Audit (E3) / Audit Premium (E5 (*))
Review Content Explorer for sensitive data location	Content Explorer (E5)
Update Privacy on Shared data	SPO & Teams Admin center, PowerShell scripts (E3)
Use Sensitivity labels to restrict access	Manual labels (E3), Automated labels (E5)
Use DLP to warn/block sharing activities	SPO/ExO DLP (E3) – Teams/Endpoint DLP (E5)
Use Retention labels to manage data lifecycle	Manual labels (E3), Automated labels (E5)
Involve site owners to review site accesses	Site owners
Implement Syntex SAM to fine tune SPO	Syntex SAM
Label Site Sensitivity (to change and exclude them from the tenant-level index)	Sensitivity labels (E5)
Exclude specific SPO Sites from Search + Semantic Index	SPO Admin center (E3)
Identify inactive sites and archive them	SPO Admin center (E3) + preview feature
Manage risk and adaptative protection	IRM (E5)





Why is a data governance solution needed?



Hybrid Workplace



No traditional perimeter security



Dark Data



Distributed data estate



Unified view for Risk and Compliance



Data sharing

The rabbit hole goes deep...



Azure Synapse Analytics



What data is this?



Is this data sensitive?



Whose data or share is this?



Amazon RDS



Is this the current data?



Google BigQuery



©2022 Microsoft Security User Group Norway All Rights Reserved

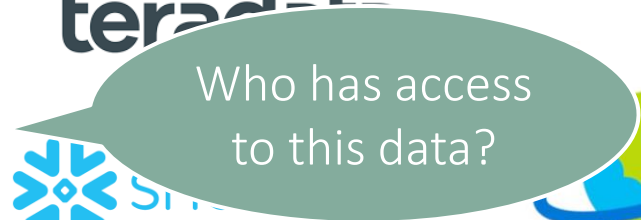


Does this data have personal identification information?

File Sharing



cassandra

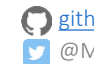


Who has access to this data?



Power BI

Microsoft Security User Group Norway



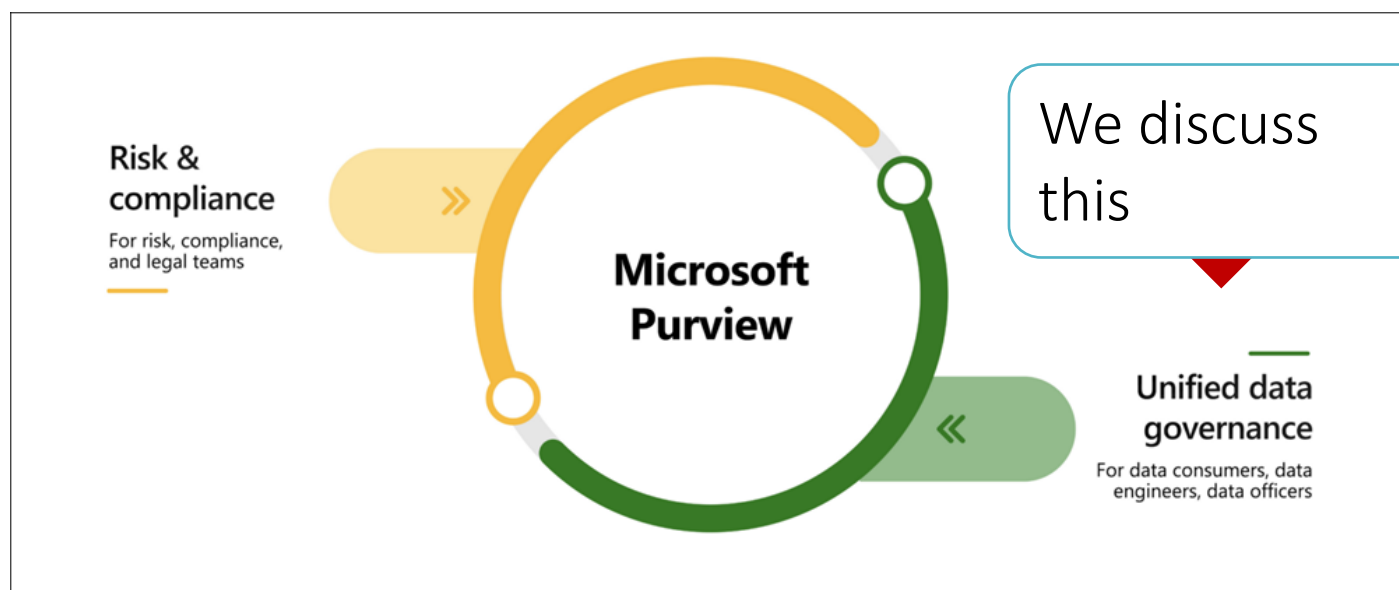
github @N



Azure Cosmos DB

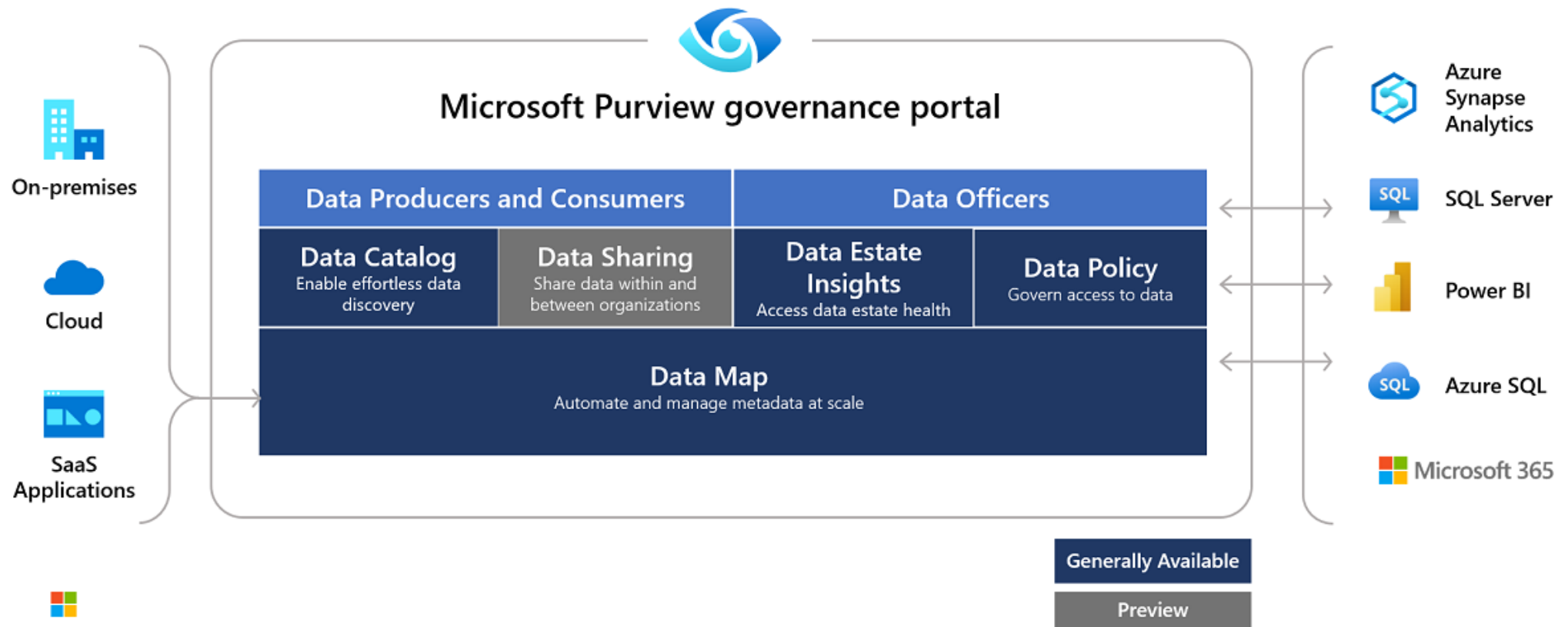
What is Microsoft Purview?

“Microsoft Purview is a family of data governance, risk, and compliance solutions that can help your organization govern, protect, and manage your entire data estate.” - Microsoft Docs



Apache **Atlas**

Data governance with Microsoft Purview



Migrate to the new portal

Microsoft Purview tenant account

Your Microsoft Purview account will be chosen as a tenant level account. To continue upgrading this account, select Confirm and launch the new portal. [Learn more](#)

1

New

Welcome to Microsoft Purview

The first step in our evolution

Microsoft Purview has a new look and capabilities that make it easier than ever to govern and protect your data. Start your journey with these capabilities:


- ✓ Automatically inventory data in Microsoft Azure, and Microsoft Fabric
- ✓ Explore your data in a searchable Data Catalog
- ✓ Identify and protect your sensitive and business-critical data

Try Microsoft Purview out and let us know what you think.

☐ Don't show this again

Microsoft Purview & Fabric

Classic



Access your classic portal

To access your classic Microsoft Purview portal (formerly Azure Purview), select Open.

→

2

Data enrichment



Business Glossary Terms

- Define the business vocabulary for an organization
- bridge the gap between technical data and its everyday context
- Example: Financial report for Company X



Classification

- Assigned descriptors to an assets to tell what kind of data it is
- Example: Passport number, Credit card number



Sensitivity labels

- used to identify the categories of classification types
- group security policies that you want to apply to each category
- Example: Sensitive, Confidential



Managed attributes

- a set of user-defined attributes that provide more description or context for assets
- Usually has a name and a value
- Example: Department- Finance

Permissions

Collection Admin

Define, configure collection

Assign roles to collection

Data source admin

Identify and prepare data source

Register sources

Ingest sources via scan or api

Data curator (Data owner)

Review collection assets

Assign assets managers

Define classification rules

Move assets

Review request for asset deletion

Data curator (Data Steward)

Review or update meta data

Review or update glossary terms

Request asset movement to new collection

Review asset access

Request asset metadata deletion

Data reader

Search data/glossary and classification

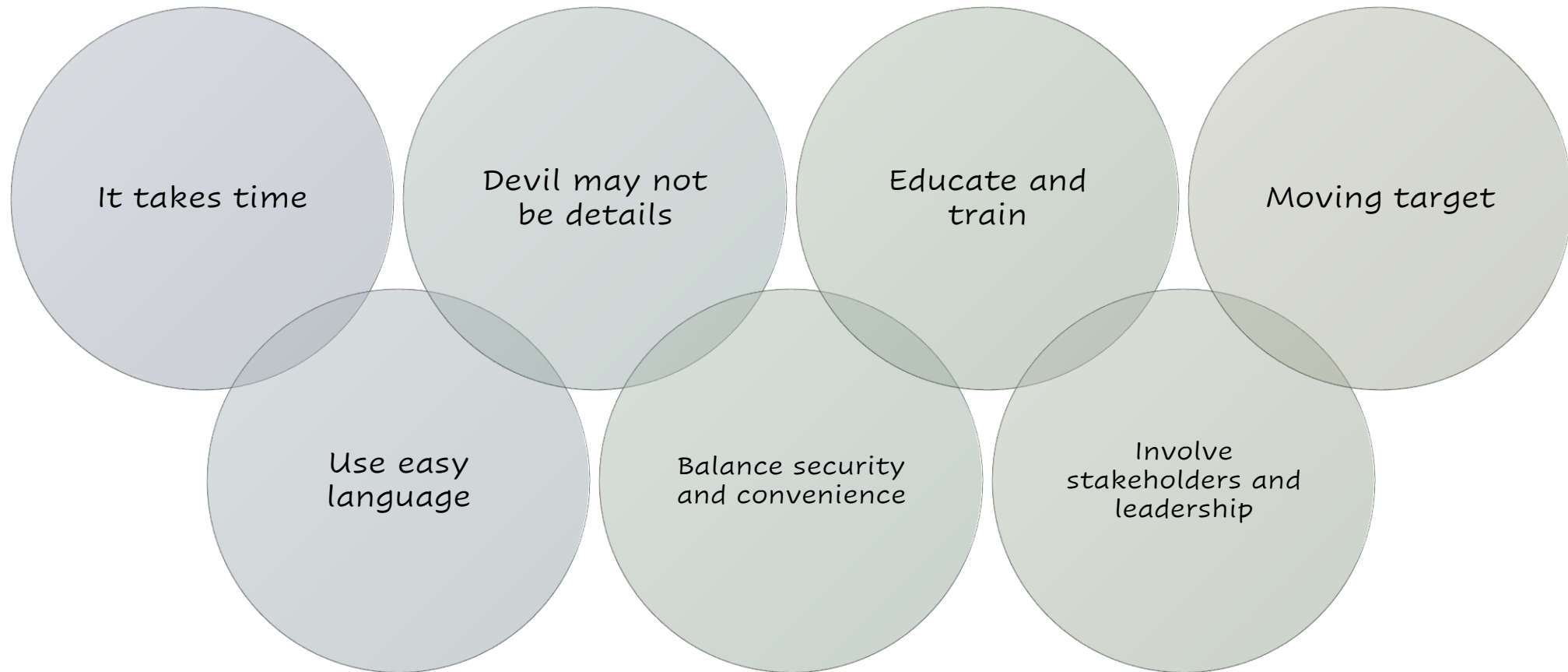
Access sensitivity, classification, ownership information

Review asset access

Request asset metadata deletion



Wrap up





Glen Nygaard

Lead Architect, Atea

<https://www.linkedin.com/in/glenmnygaard/>



Mohit Sharma

Chief Consultant, Atea

<https://www.linkedin.com/in/mohitsharma13/>

