

# Securing and Protecting Content in Power BI

---

Melissa Coates

Data Architect | Consultant | Trainer

CoatesDataStrategies.com



Slides & recordings: [CoatesDS.com/Presentations](https://CoatesDS.com/Presentations)

Content last updated: February 22, 2023

# Melissa Coates



Owner of [Coates Data Strategies](#)

Data architect specializing in Power BI governance & administration

Author of [Power BI Adoption Roadmap](#)

Author of [Power BI Implementation Planning](#)

Creator of [Power BI Deployment & Governance](#) online course

## Power BI Deployment & Governance

Comprehensive online course



Governance  
Adoption & data culture  
Center of Excellence  
Data architecture  
Content management  
Data trustworthiness  
Security & protection  
System oversight



Comprehensive set of video recordings  
Live group Q&A sessions  
Live hands-on workshops  
Customizable templates  
Recommended actions  
Access for 6 months



# Agenda

## Securing and Protecting Content in Power BI

Time	Topic	Demos
Part 1: 1:00 – 2:00	Building blocks: security & info protection	Sensitivity labels & DLP scan
	Users, groups & service principals	Group owner
	Workspace roles	Workspace roles
	App permissions	App audiences
<b>2:00 – 2:15</b>	<b>Open Q&amp;A #1</b>	
<b>2:15 – 2:30</b>	<b>Break time</b>	
Part 2: 2:30 – 3:30	Per-item permissions	Sharing links & direct access
	Request access workflow	Access requests
	Dataset permissions	Dataset perm & inheritance
	Data discovery	Data hub & discovery
	Different data based on user identity	
	Security strategies & suggestions	
<b>3:30-4:00</b>	<b>Open Q&amp;A #2</b>	

Eastern time zone

Melissa Coates





# Links to Materials

## Securing and Protecting Content in Power BI

### Agenda

Time	Topic	Speaker
<b>Agenda</b> <b>Securing and Protecting Content in Power BI</b>		
<b>Part 1</b>		
1:00 - 2:00	Building blocks, security & info protection	Christopher Daniels & EdF Moran
	Users, groups & service principals	Chris Moran
	Workspaces roles	Michelle O'Neil
	App permissions	App & Admin
2:00 - 2:15	Open Q&A #1	
<b>Break Time</b>		
2:15 - 2:30	Per-item permissions	Showing data & ID based access
	Request access workflow	Access requests
<b>Part 2</b>		
3:00 - 3:30	Dataset permissions	Dataset permissions
	Data discovery	Discover your BI intelligence
	Showing data based on user identity	Data role & discovery
3:30 - 4:00	Open Q&A #2	
	Security strategies & suggestions	Security strategies & suggestions
	Michelle O'Neil	Michelle O'Neil

### Part 1

Building Blocks:  
Security &  
Information Protection

Users,  
Groups &  
Service Principals

Power BI  
Workspace Roles

Power BI  
Organizational App  
Permissions

Open Q&A #1

Break Time  
We restart in...

### Part 2

Per-Item Permissions

Request Access  
Workflow

Dataset Permissions

Data Discovery

Showing Different  
Data Based on  
User Identity

Security Strategies  
& Suggestions

### Final Q&A

Open Q&A



# Questions We Want To Answer

## Securing and Protecting Content in Power BI

Awareness of the most important concepts:

- ✓ How security needs affect the workspace design approach
- ✓ When to use app permissions vs. workspace roles vs. per-item sharing
- ✓ How security settings are inherited
- ✓ How sharing links work
- ✓ How direct access sharing works
- ✓ Ways to use app audiences
- ✓ When to use the 'build' or 'write' permission for a dataset
- ✓ How the 'discoverable' setting for a dataset is helpful
- ✓ How the 'request access' workflow works
- ✓ When row-level security is necessary
- ✓ How information protection correlates with security



# Things We Don't Have Time to Cover

## Securing and Protecting Content in Power BI

Important topics...but out of scope due to time:

- Dataflow & datamart permissions
- Cross-tenant dataset sharing
- Scorecard & metric permissions
- Strategies for external users
- E-mail subscriptions
- Gateway & data source security
- Azure Active Directory: identity management & authentication
- Networking: secure virtual networks & private links
- Power BI Report Server security options
- Content embedded in other applications
- Information protection & DLP (in detail)
- Microsoft Purview integration & permissions



For more info, see:

[Power BI security whitepaper](#)



# Target Audience

## Securing and Protecting Content in Power BI



### **Content Creators**

Self-service users who publish & manage content



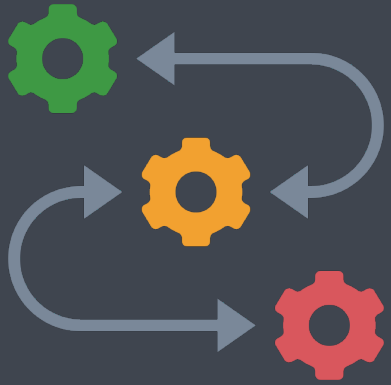
### **BI Team, Center of Excellence, IT, Admins**

People who oversee, manage & set guidelines for users for how Power BI should be used



### **Admins, Auditors**

People who need to understand settings & usage of Power BI so they can audit them



# Building Blocks: Security & Information Protection





# How Do We Protect Data?

**-1-**  
Responsible  
actions taken  
by users

Users have guidance and training, and understand what's expected of them

**-2-**  
Right-sized  
security and  
user  
permissions

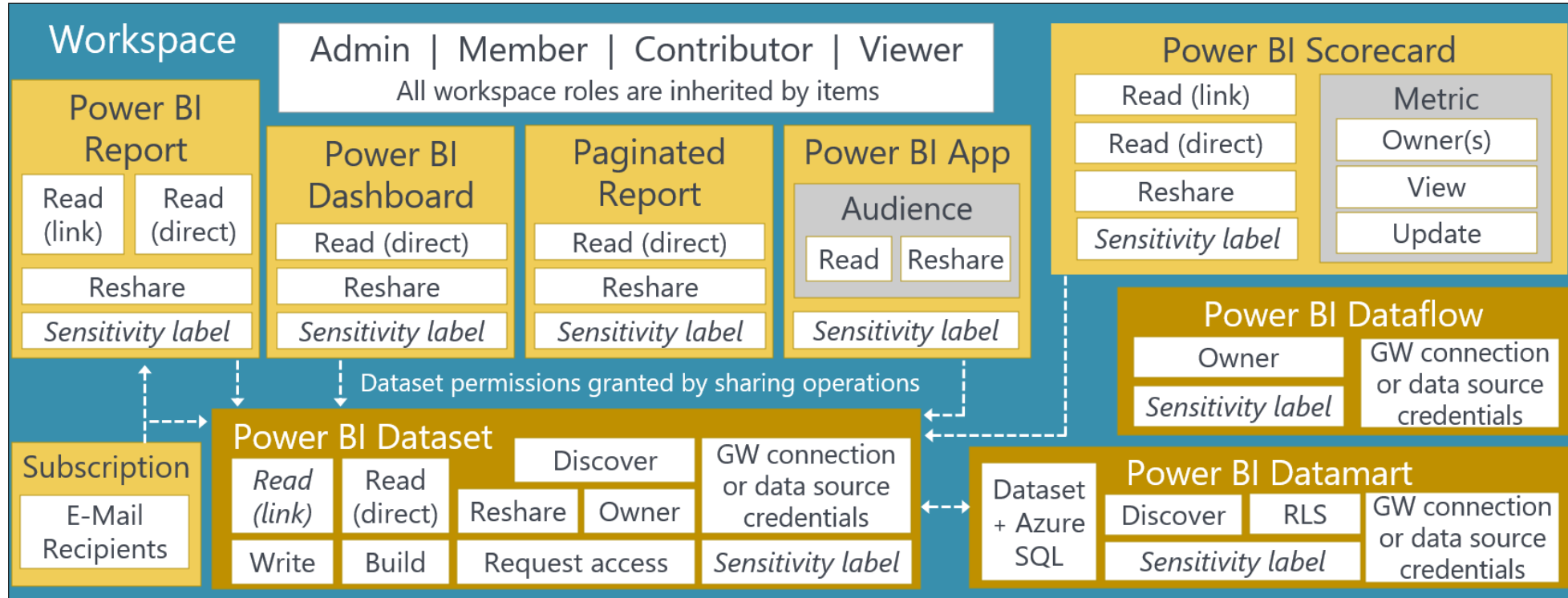
Techniques such as:

- Workspace roles
- App permissions
- Per-item permissions
- Row-level security etc...

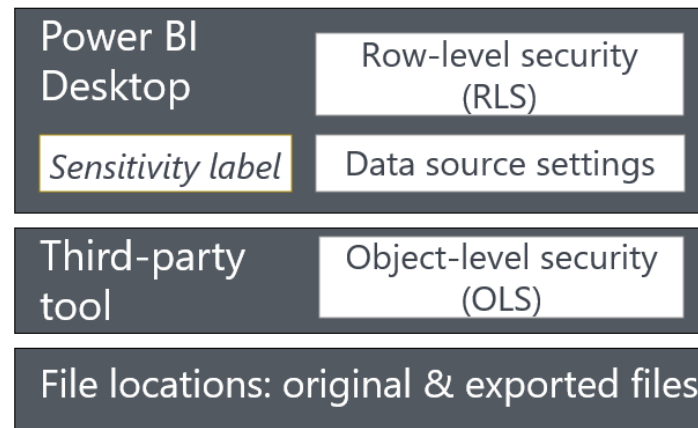
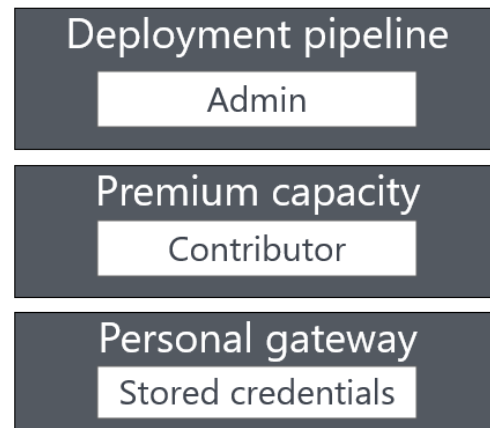
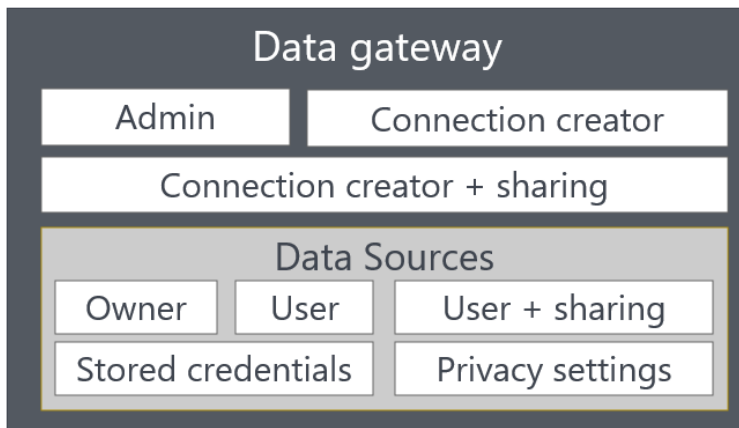
**-3-**  
Information  
protection  
and data loss  
prevention

Capabilities to discover, classify, and protect data

# Permissions Managed by Content Creators/Owners

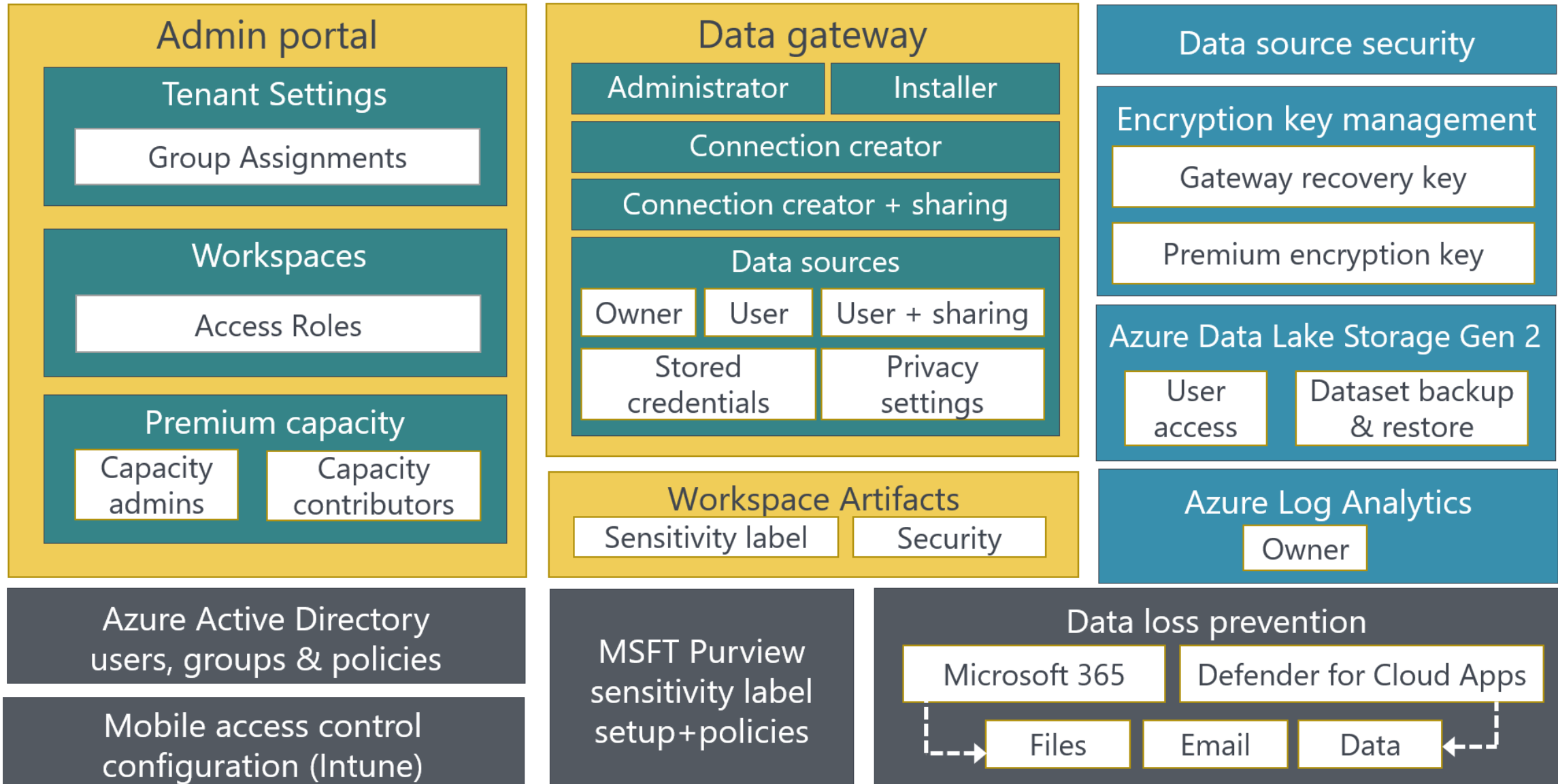


Download original diagram at:  
[CoatesDS.com /Diagrams](https://CoatesDS.com/Diagrams)





# Permissions Managed by Administrators





# Terminology

## Sharing

A **specific feature** in which permissions are set for one individual item. Watch out if the term “sharing” is used **literally or generally**.

## Distribution

A general term for the **delivery of content** for others to consume.

## Collaboration

A general term for **people working together**.  
Ex: data modeler, report designer, and quality assurance.



# Layers of Security in Power BI

Permissions for a Collection of Items

Permissions for Individual Items

Other



# Layers of Security in Power BI

## Collection of Items



Workspace Roles



App Permissions

## Individual Items: Visuals



Reports  
└ Charts



Dashboards



Scorecards  
└ Metrics



Workbooks

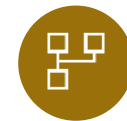
## Individual Items: Data



Datasets



Datamarts



Dataflows

Other

Row-Level Security

Object-Level Security

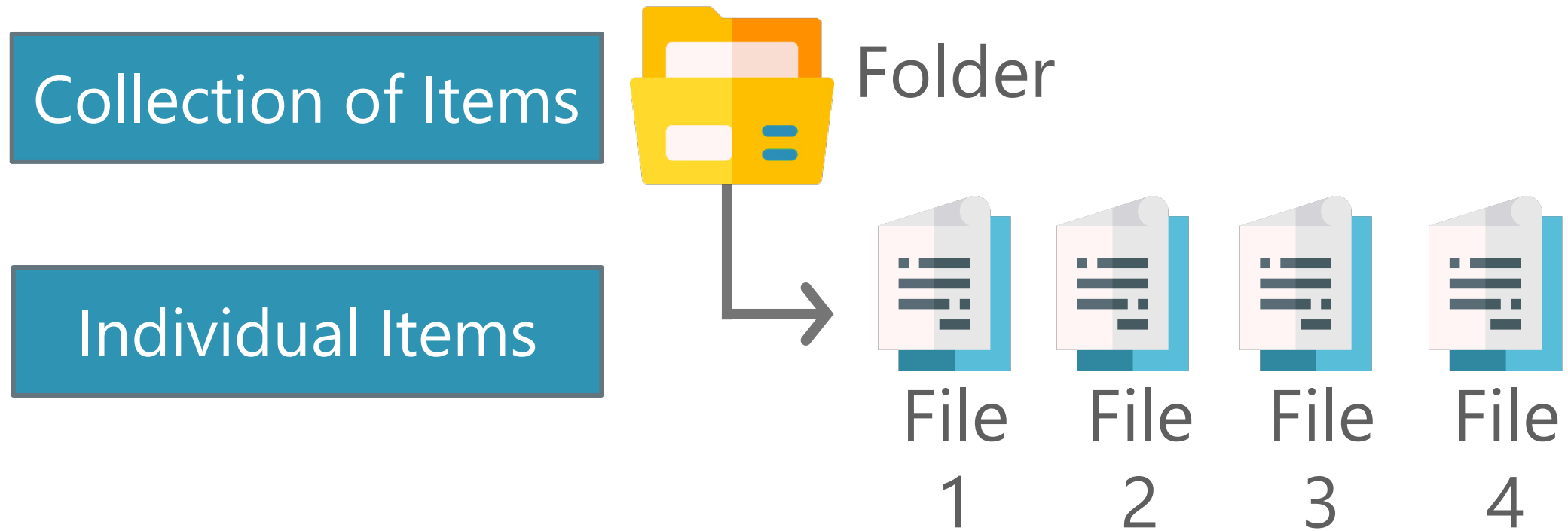
Data Sources & Gateways

Cross-Tenant Sharing

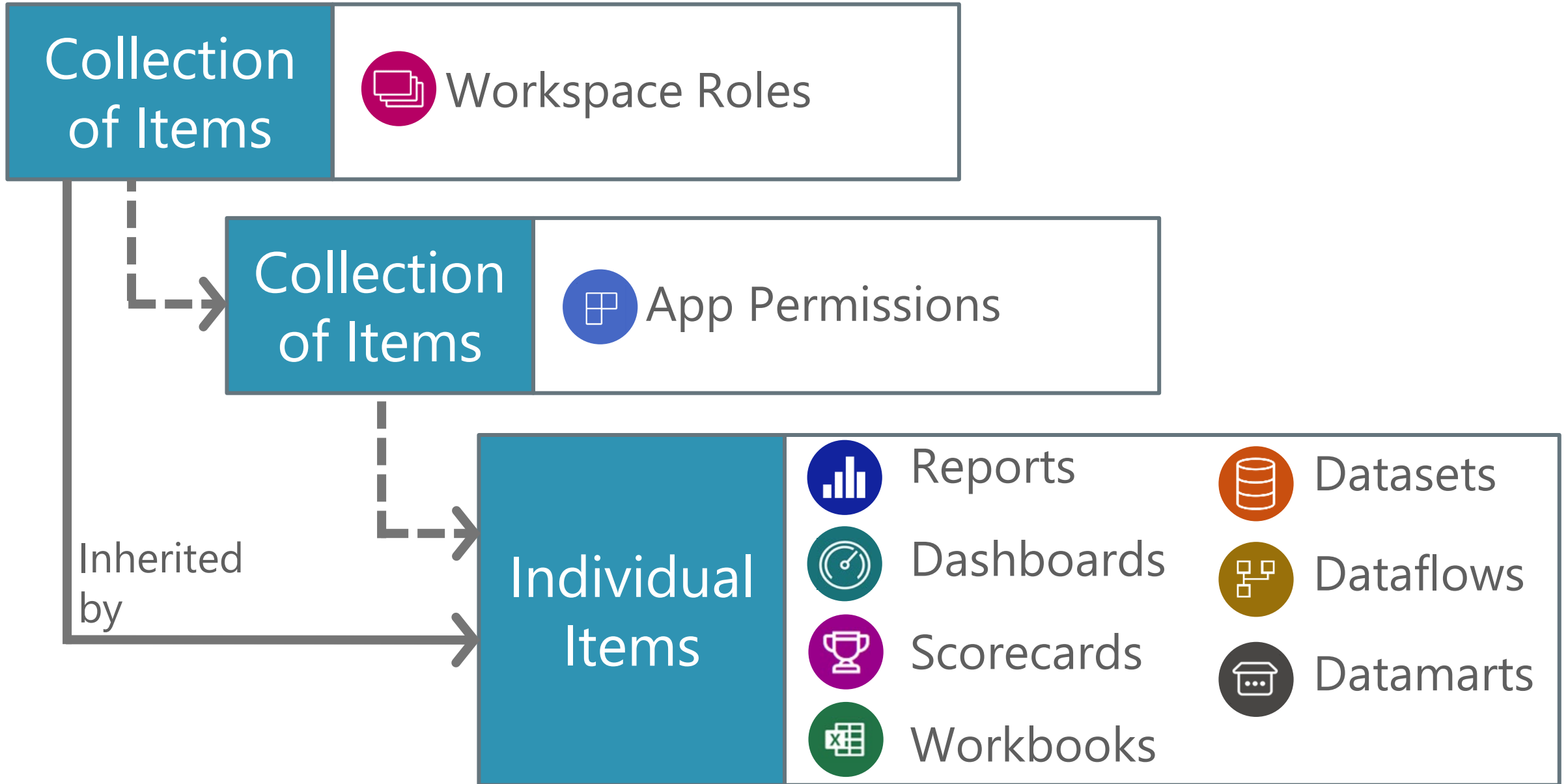


# Security Inheritance

Conceptually -- the same idea as folders and file security:



# Security Inheritance in the Power BI Service







# What's NOT Security?



## Show/hide report pages

- Not “real” security
- It does improve the user experience while navigating reports in the Power BI service
- Still shown if a user gets the URL, or opens in Desktop

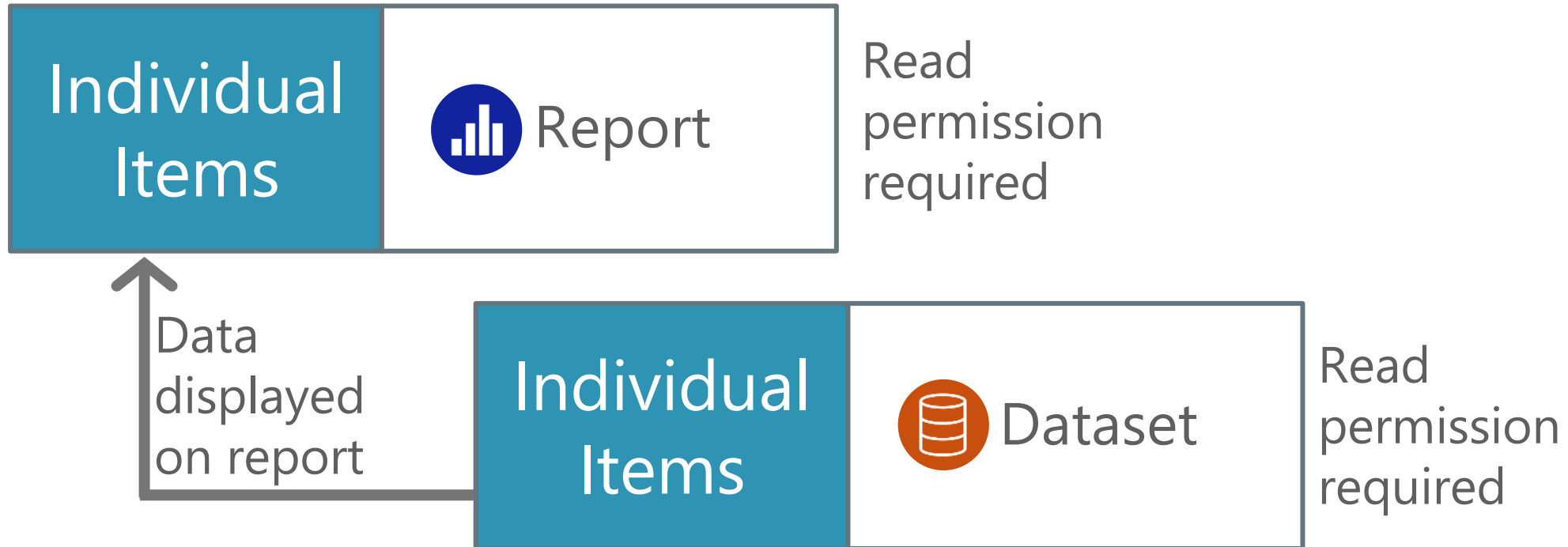


## Perspectives in a dataset

- Not “real” security
- A nice user convenience when navigating the model



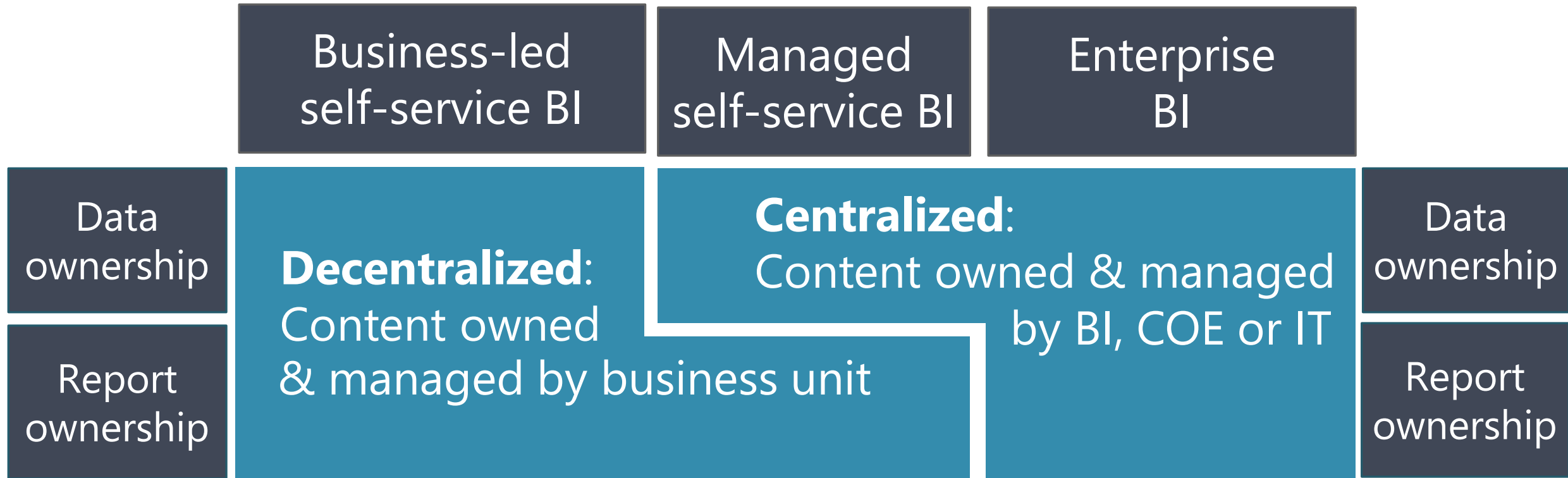
# Viewing Reports & Datasets



- ! Some inherited permissions stay tightly coupled. Others are initially a convenience – they're decoupled & need to be managed separately.



# Who Creates and Manages the Content?



For more info, see Power BI Adoption Roadmap:  
[Content ownership & management](#)

# Who is Consuming the Content?



## Personal

Intended for use by the creator; sharing isn't an objective



## Team

Collaboration & sharing of content with a small # of colleagues who work closely together



## Departmental

Content delivery to a larger # of consumers within a department or business unit



## Enterprise

Content delivery across organizational boundaries to the largest # of target consumers

 For more info, see Power BI Adoption Roadmap: [Content delivery scope](#)



# Security for Self-Service BI: It's a Balance

**User Flexibility**

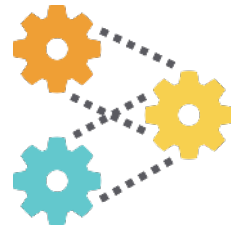


**Risk Reduction**



**Optimal Security**

**Efficiency**





# Access Control



What level of access is necessary?

View only? Update? Delete?

Who determines the correct level of access control?



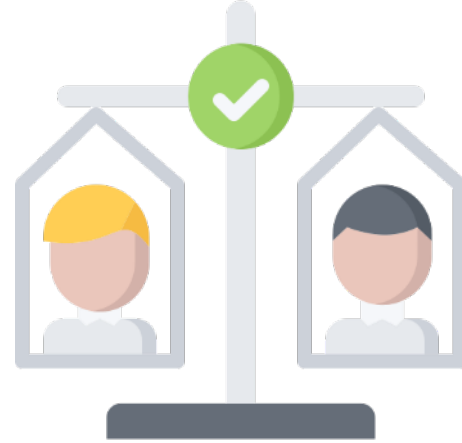
# Principle of Least Privilege



What's the minimum access necessary for someone to do their job, or complete a task?



# Data Democratization



Do we make *using* the data as much of a priority as *protecting* the data?

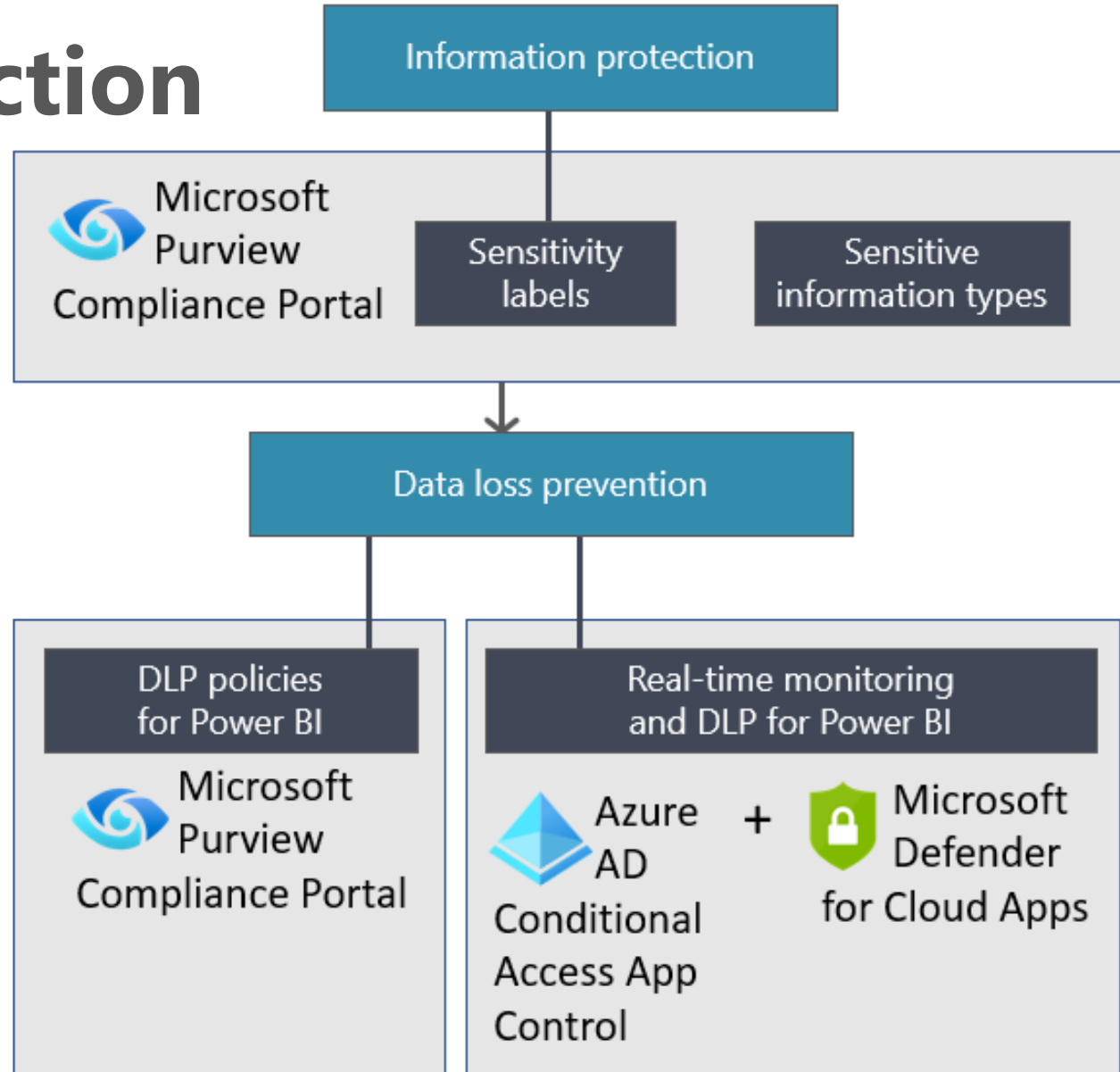


**Credit for this idea:**

Laura Madsen, author of [Disrupting Data Governance](#)



# Where Does Information Protection and Data Loss Prevention Fit In?



For more info see Power BI Implementation Planning: [Info Protection & DLP](#)

# Terminology



## Sensitivity Labels

A set of labels that classifies content. Like a tag that indicates the value of the data and its corresponding policies: what can you do –or not do– with this data?

Ex: Highly confidential  
General internal use



## Sensitive Information Types

Identifying data that's more sensitive (not all data is the same...some is inherently more sensitive).

Ex: Bank account #  
Customer license #  
Credit card #





# Demo

---

**Sensitivity labels  
DLP scan results**



# How Info Protection Correlates to Security



## Power BI Service:

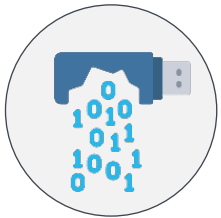
Sensitivity labels do NOT affect access to content.

See [release plan for Purview DLP](#)



## Power BI Desktop, XLSX, PPTX, and PDF exports:

***If encrypted:*** sensitivity labels **\*\*DO\*\*** affect access to content.  
Only authorized users can open protected files.



## Defender for Cloud Apps:

Can prevent some actions in real-time (like downloading a file)



# Users, Groups & Service Principals

# Different Users Have Different Security Needs



**Collection of Items**

(apps & workspaces)

**One Item**

(ex: one report)

**Data Access**

(ex: row-level security)

**Content Creators**



**Data Authors**



**Report Authors**

**Content Consumers**



**Viewers**



# Who We Can Grant Permissions To



User

One person



Group

Security group  
Mail-enabled security group  
Microsoft 365 group  
Distribution list



Service Principal

One automation account  
(Azure AD app)

**Content  
Creators &  
Consumers**

**Scheduled  
Operations**



# Types of Groups We Might Need for Power BI



## Security

What segments of users will you need to apply specific **security** settings?  
*Ex: Workspace roles, app & per-item permissions*



## Communication

What segments of users do you need to **communicate** with?  
*Ex: Announcements of upcoming changes,  
New training or announcing useful new features*



## Features

What segments of users are allowed / disallowed to use certain **features**?  
*Ex: Tenant settings & rolling out changes gradually*





# Why Use Groups Instead of Individuals?

- ✔ Maintain members in one place
- ✔ Improved accuracy (or more easily fixable)
- ✔ Delegate managing members to a group owner



For more info see Power BI  
Implementation Planning:  
[Security: Strategy for using groups](#)



# Why Use Groups Instead of Individuals?

- ✓ Lots of ways to use groups efficiently or in an automated way. Examples:
  - ✓ Dynamic group membership
  - ✓ Group-based licensing assignment
  - ✓ Nested groups
  - ✓ Azure AD roles assigned to a group
  - ✓ Privileged identity management (PIM)



# Demo

---

**Group owner in Azure AD**



# Managing Security with Groups

## Primary Purpose:

Microsoft 365  
Group

Collaboration (ex: SharePoint & Teams)

Security Group

Granting access to resources

Mail-Enabled  
Security Group

Granting access to resources  
+ sending email notifications

Distribution  
Group

Sending broadcast email  
notifications to a list of people

Managed in  
Exchange



# Managing Security with Groups

	<b>Includes Email</b>	<b>Allows Dynamic Members</b>	<b>Power BI Tenant Settings</b>	<b>Power BI Permissions</b>
Microsoft 365 Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Very limited
Security Group		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	A lot of settings
Mail-Enabled Security Group	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Most settings
Distribution Group	<input checked="" type="checkbox"/>			Some settings



# Groups: Watch Out For



Not every type of group works with every type of permission in Power BI.

*Common issues:*

- Some settings require an email address
- M365 groups are NOT supported for:
  - Per-item sharing
  - RLS or OLS
  - Subscriptions
  - Tenant settings



# Groups: Watch Out For



Existing groups that align with the org chart structure don't always work for BI. Be prepared to create new groups.



If managing group members *MUST* go through IT, and there's a big delay, users will do something else to keep moving.

*Tip:* Allow decentralized group owners.

*Tip:* Create a process to respond fast to requests.



# Groups: Watch Out For



You may end up with a large number of groups.

5 groups each



Workspace



App

X3 if you  
introduce  
dev/test/prod



Viewers

Contributors

Members

Admins



Viewers





---

# Power BI Workspace Roles



# Types of Workspaces in the Power BI Service



Personal workspace  
"My workspace"



One owner



Workspace



Four workspace roles



A Power BI administrator  
can get access to a personal  
workspace for 24 hours

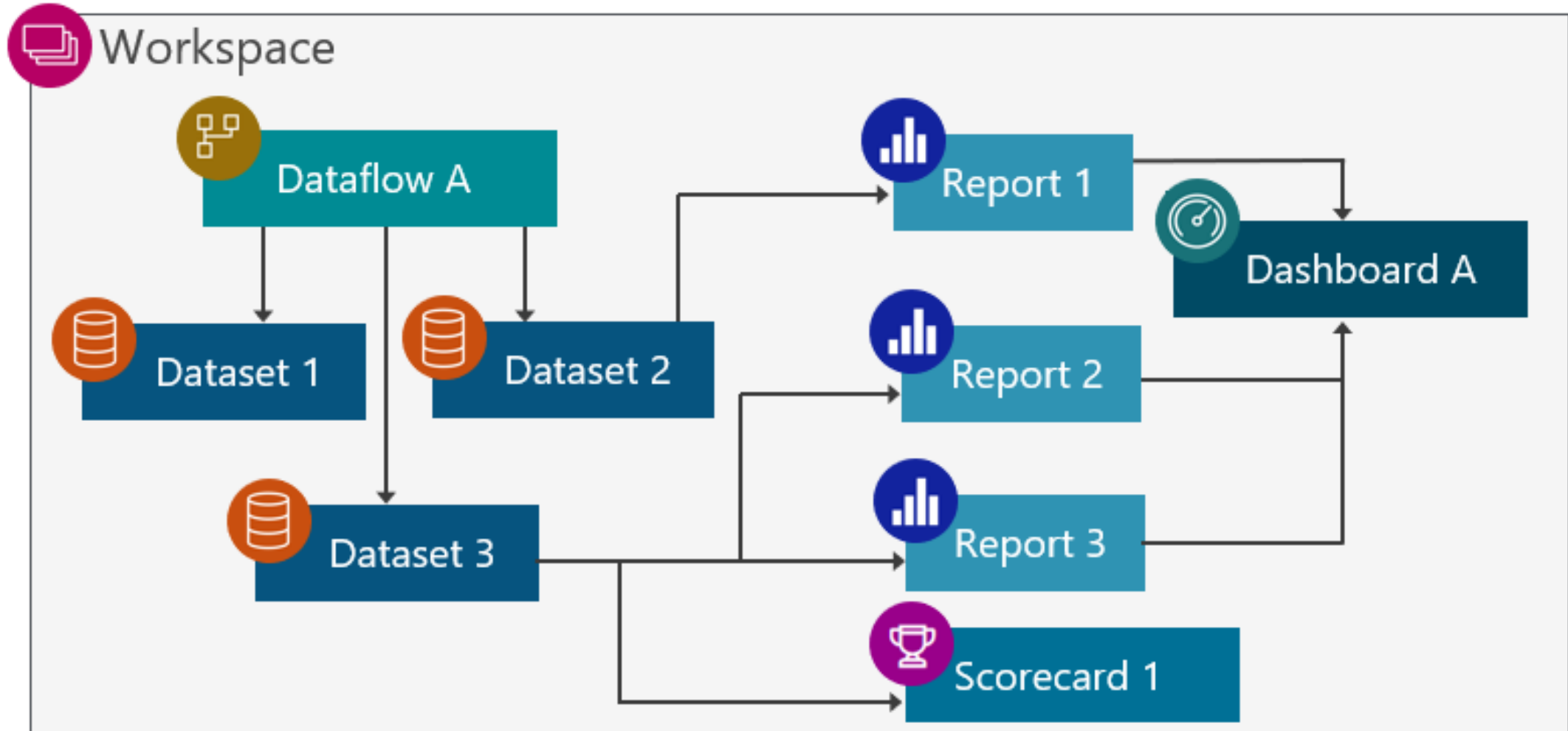


For more info about workspaces, see Power BI Implementation Planning: [Workspaces](#)



# Purpose for Workspaces

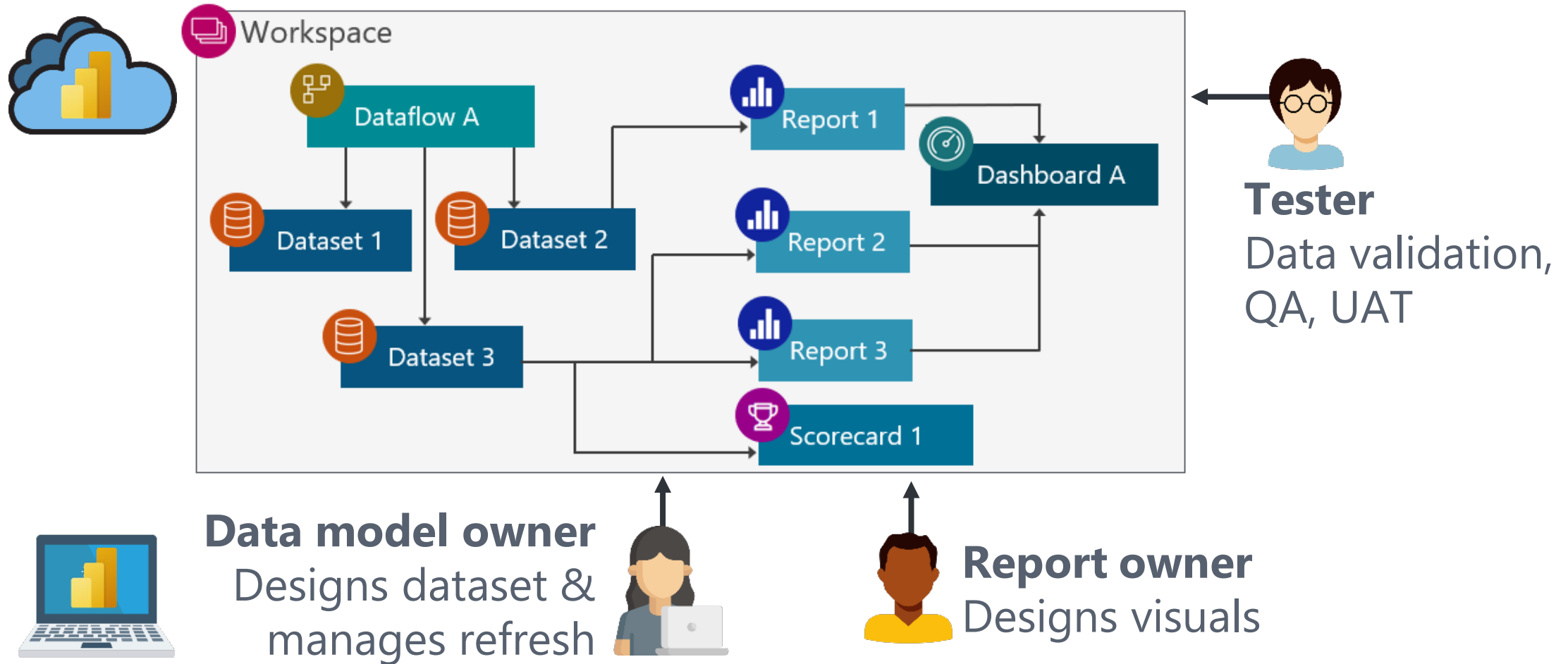
## Purpose #1: Store & organize content





# Purpose for Workspaces

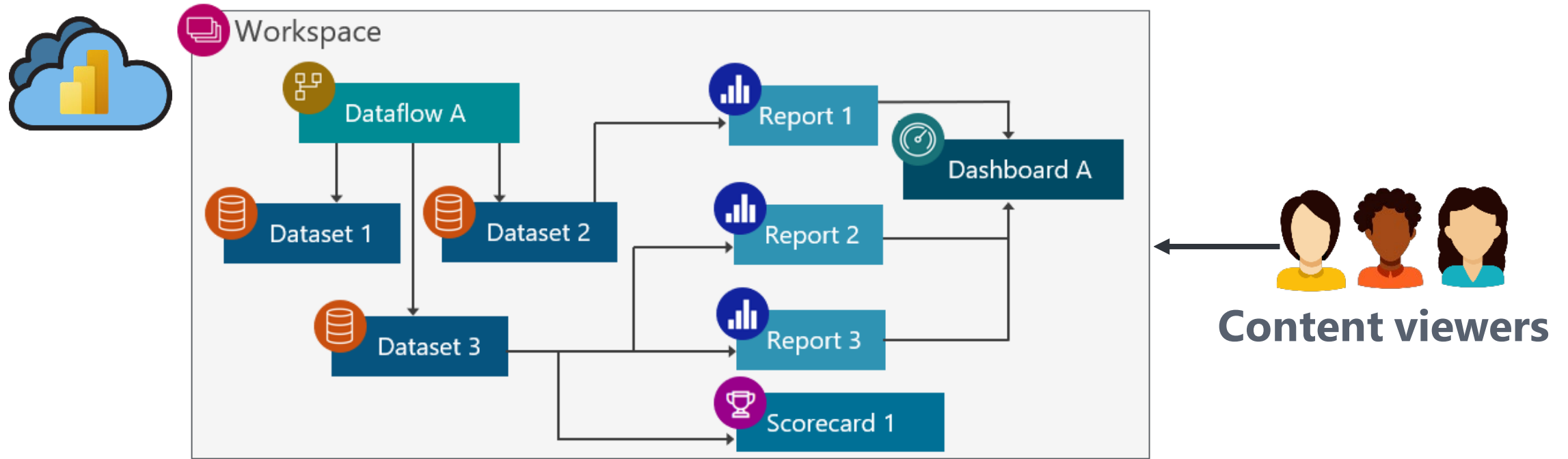
## Purpose #2: Collaboration on content





# Purpose for Workspaces

## Purpose #3: Content distribution for small / informal teams





# Demo

---

**Workspace roles**



# Purpose for Each Workspace Role

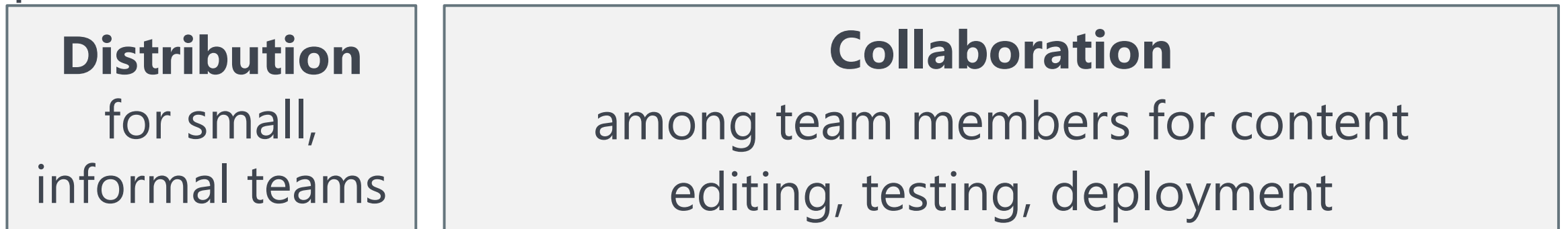
Permission:



Targeted to:



Purpose:





# Supporting Different Groups of Users

## Content Creators



Data  
Authors



Report Authors

## Content Consumers



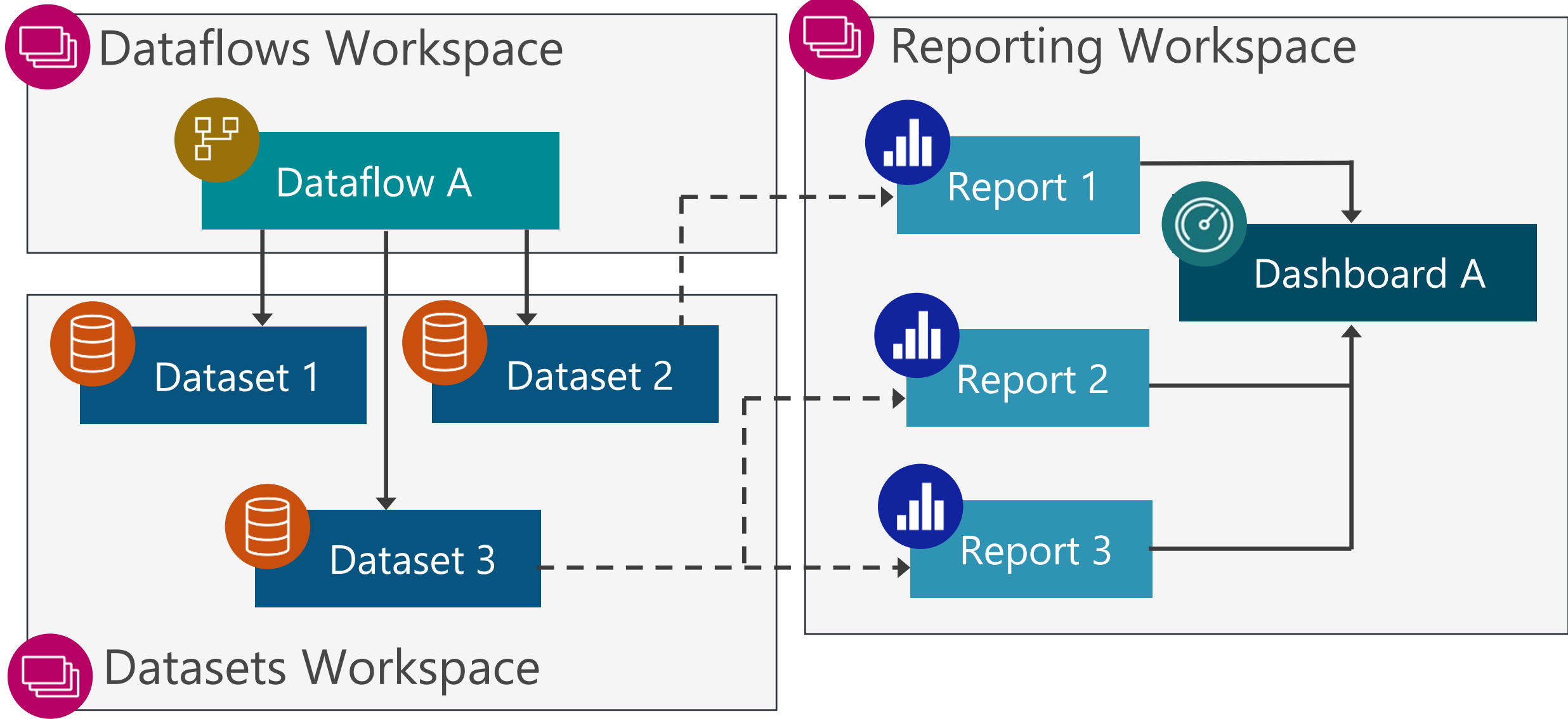
Viewers



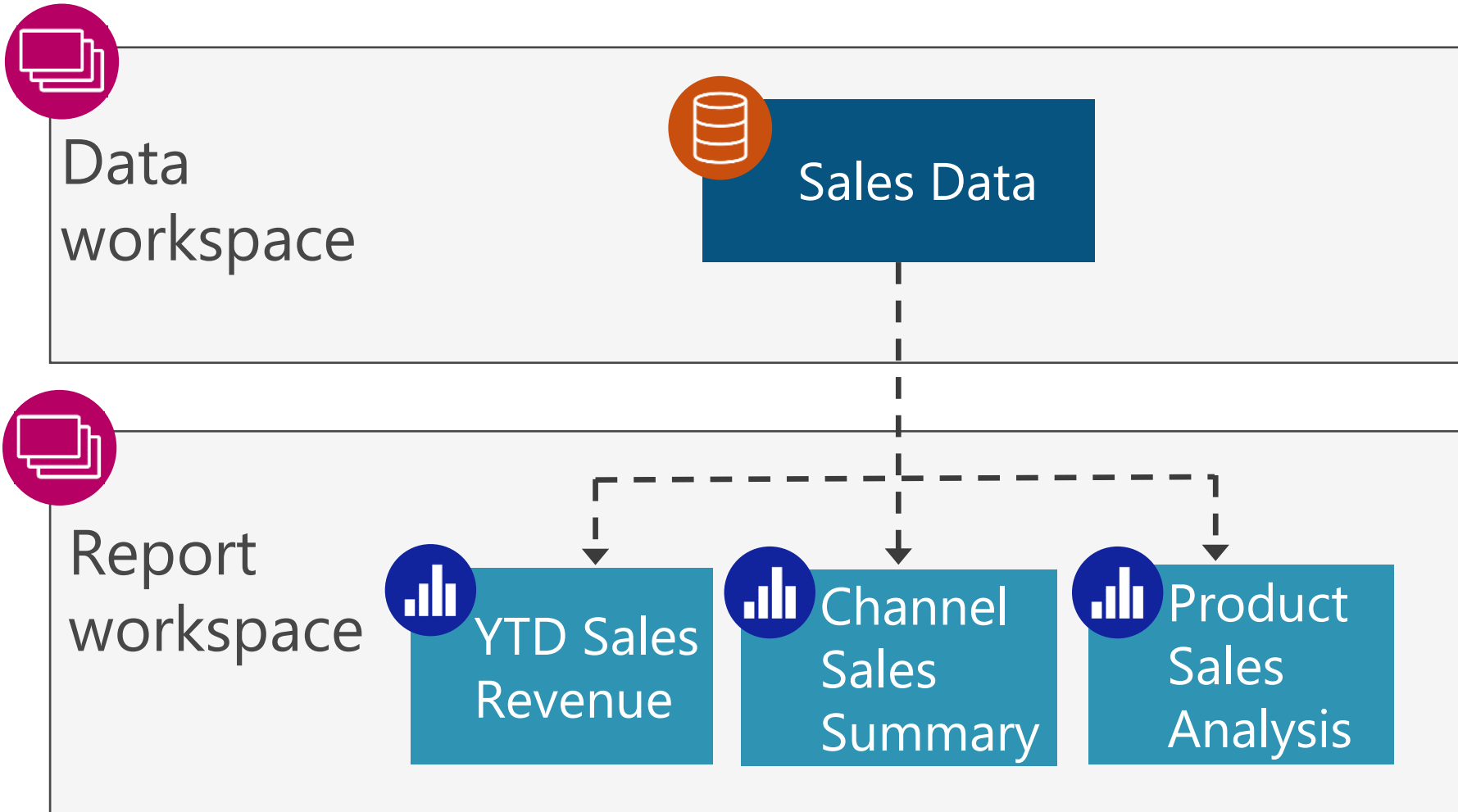
The ability to support different groups of users ***starts*** with how you design & organize workspaces.




# Workspace Organization Will Effect Security

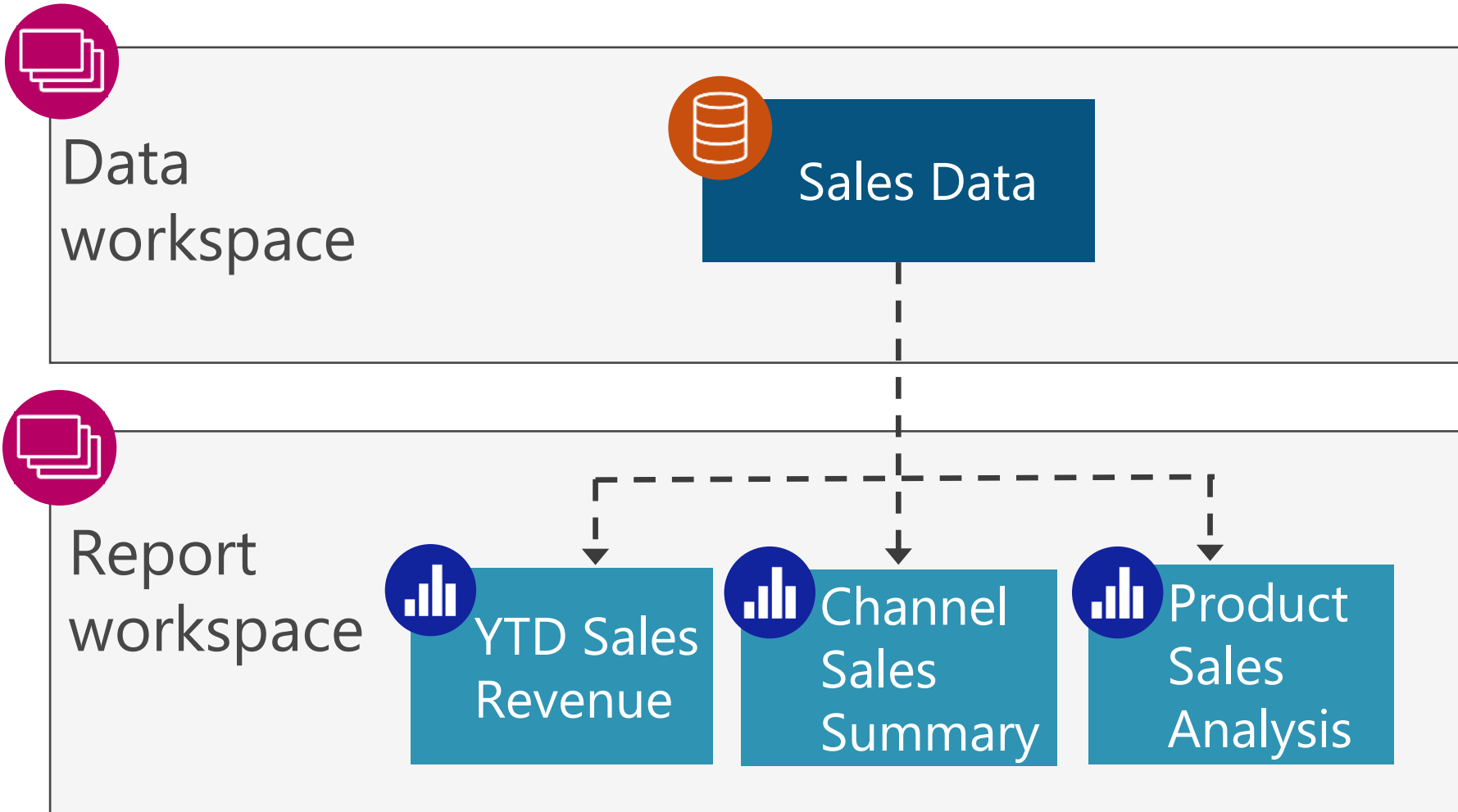


# Data Author Permissions



 **Data authors:**  
Workspace role:  
admin, member  
or contributor  
OR  
The 'write'  
permission on  
the individual  
dataset

# Report Author Permissions

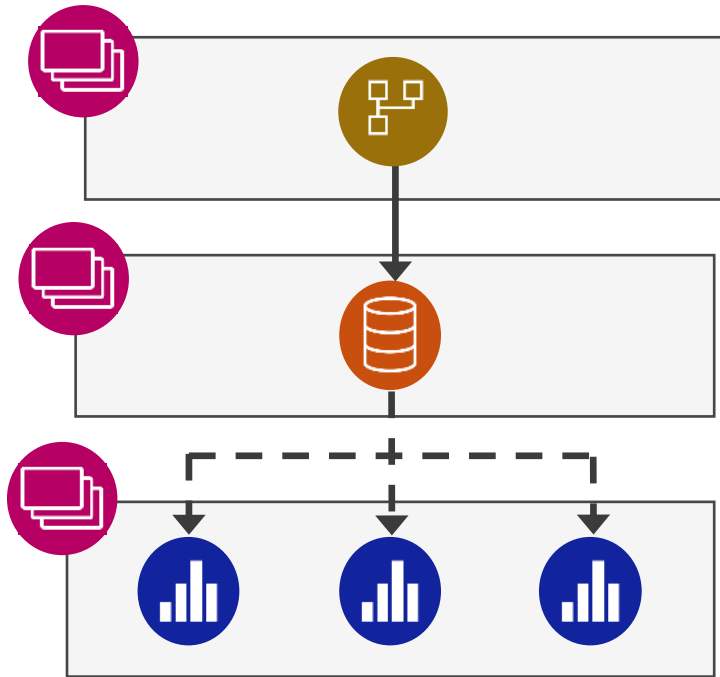


**Report authors:**  
Build on the individual dataset



+  
Workspace role:  
admin, member  
or contributor

# Security Advantages of Separate Workspaces



- Clarity on who may edit vs. view: helpful when separate people are responsible for data vs. reports
- No over-provisioning of permissions; no reliance on the “honor system” for who may edit content

- Row-level and object-level security works for report authors who only have view permissions on the dataset

 More info: [CoatesDS.com/blog/5-tips-for-separating-power-bi-datasets-and-reports](https://CoatesDS.com/blog/5-tips-for-separating-power-bi-datasets-and-reports)



# Workspace Planning Criteria

## 1 What is the content?

- Subject area / topic / purpose
- Level of **sensitivity**

## 2 Who is the content delivered to?

- Content delivery scope / **security boundary**
- License mode (Pro / PPU / Premium) & features
- Licensing needs & integration w/ other services
- Intentions for **app distribution**

## 3 How will the content be managed & by whom?

- Content ownership & management**
- Separation of data vs. reports & visuals

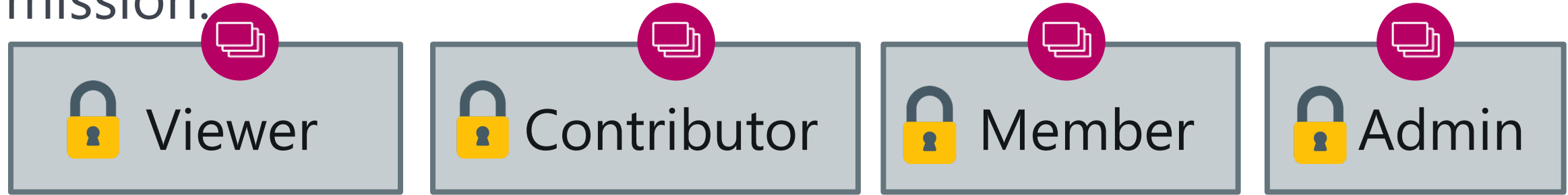
## 4 How will the content be deployed?

- Separation of dev / test / prod
- Application lifecycle management (ALM)
- Data sovereignty & storage needs
- Other technical limitations

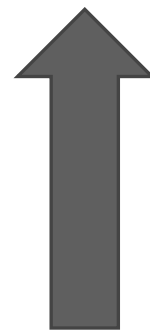
# Workspace Roles: Exceptions to How They Work



Permission:



Targeted to:



A couple of exceptions to what your content creators can expect



# Workspace Roles: Exceptions to How They Work

## Workspace setting:

Contributors to update app

Settings

Sales Analytics

About Premium Azure connections

Advanced ^

Workspace OneDrive

(Optional)

Develop a template app

Template apps are developed for sharing outside your organization. A template app workspace will be created for developing and releasing the app. [Learn more](#)

**Security settings**

Allow contributors to update the app for this workspace

## Tenant setting:

Dataset publishing

Dataset Security

Block republish and disable package refresh  
*Disabled for the entire organization*

Disable package refresh, and only allow the dataset owner to publish updates.

Disabled

**Only the dataset owner will be allowed to publish updates, this includes deployment pipeline dataset updates.**

Apply Cancel

**This setting applies to the entire organization**



# Personal Workspace: Watch Out For



Do not store mission-critical content in a personal workspace.



Only one owner can manage content in a personal workspace. This represents risk (even though an administrator can access for 24 hours).

*Tip:* Use personal workspaces for learning, work in progress, temporary analysis, etc.





# Workspace Roles: Watch Out For



Too many people who can edit content in a workspace = risk of unapproved changes or modifications outside of your normal process.



Workspaces which are broadly defined with a lot of unrelated content. It means you'll have to rely more heavily on per-item sharing.



# Workspace Roles: Watch Out For



The dataset 'build' permission is automatically granted to all workspace contributors, members, and admins.



Row-level security is *ignored* for anyone who has edit permission for the dataset:

- Workspace contributors, members, and admins
- Dataset write permission



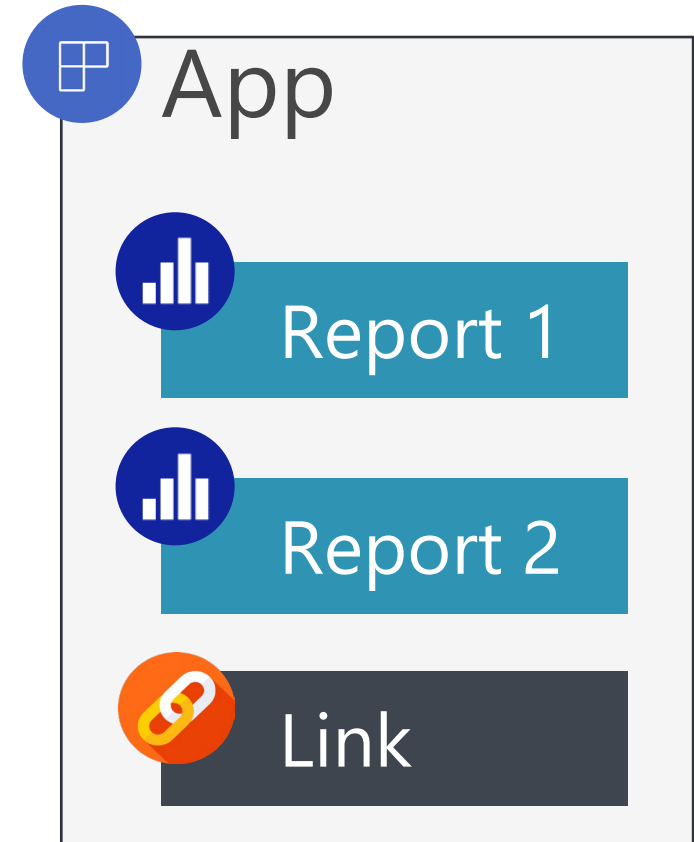
# Power BI Organizational App Permissions



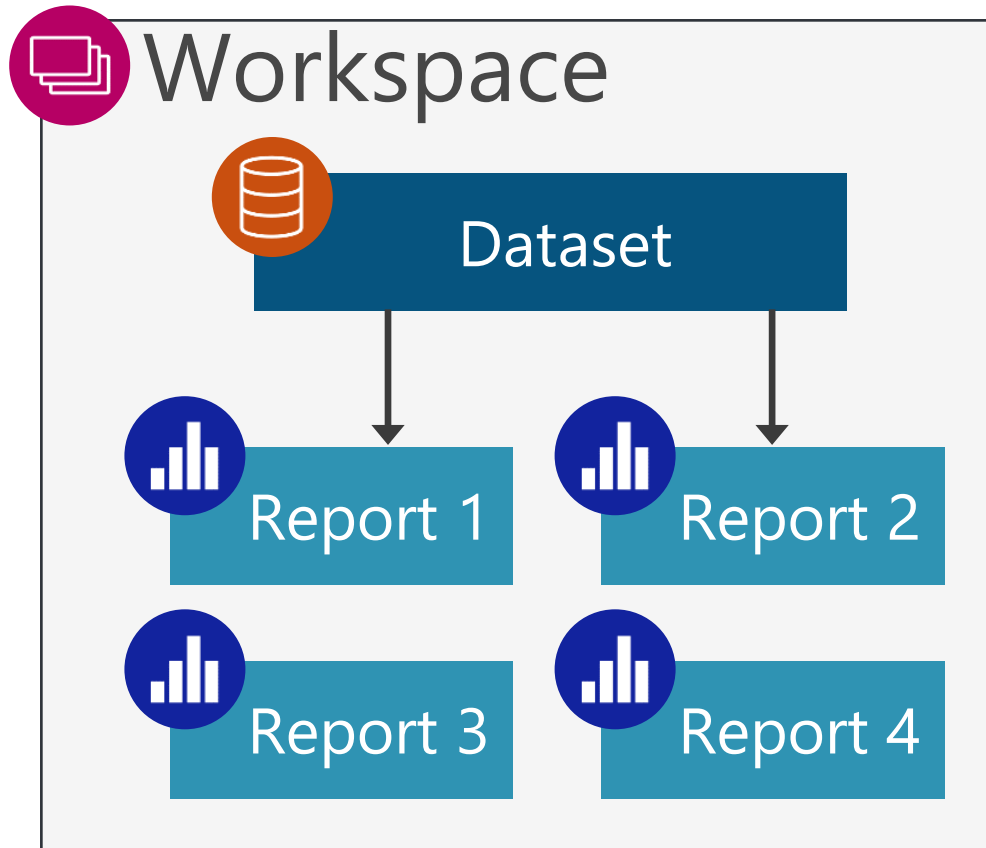
# Purpose for Power BI Organizational App

Broad content distribution scenarios to a large # of people

More formal content distribution scenarios

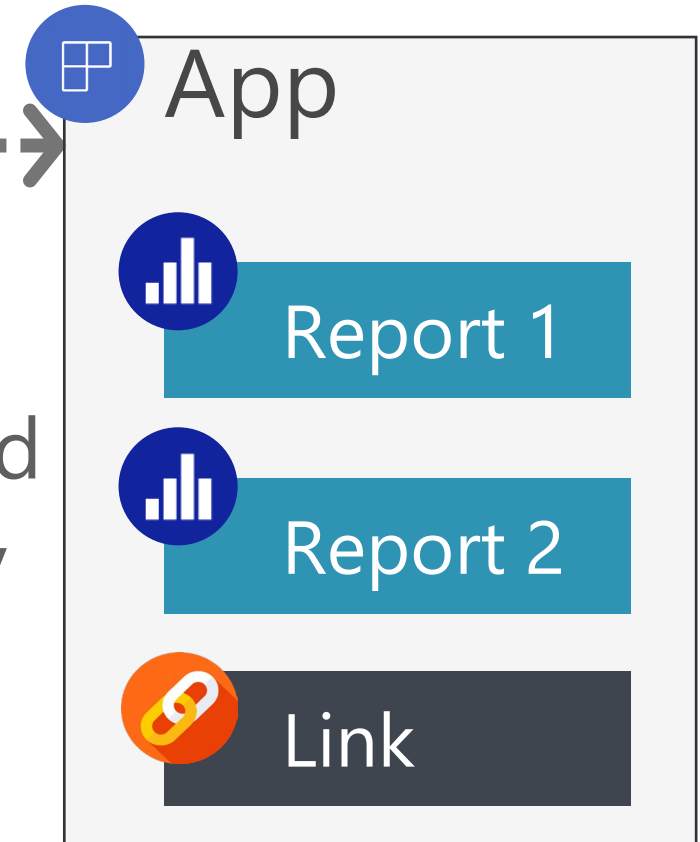


# One App Exists Per Workspace



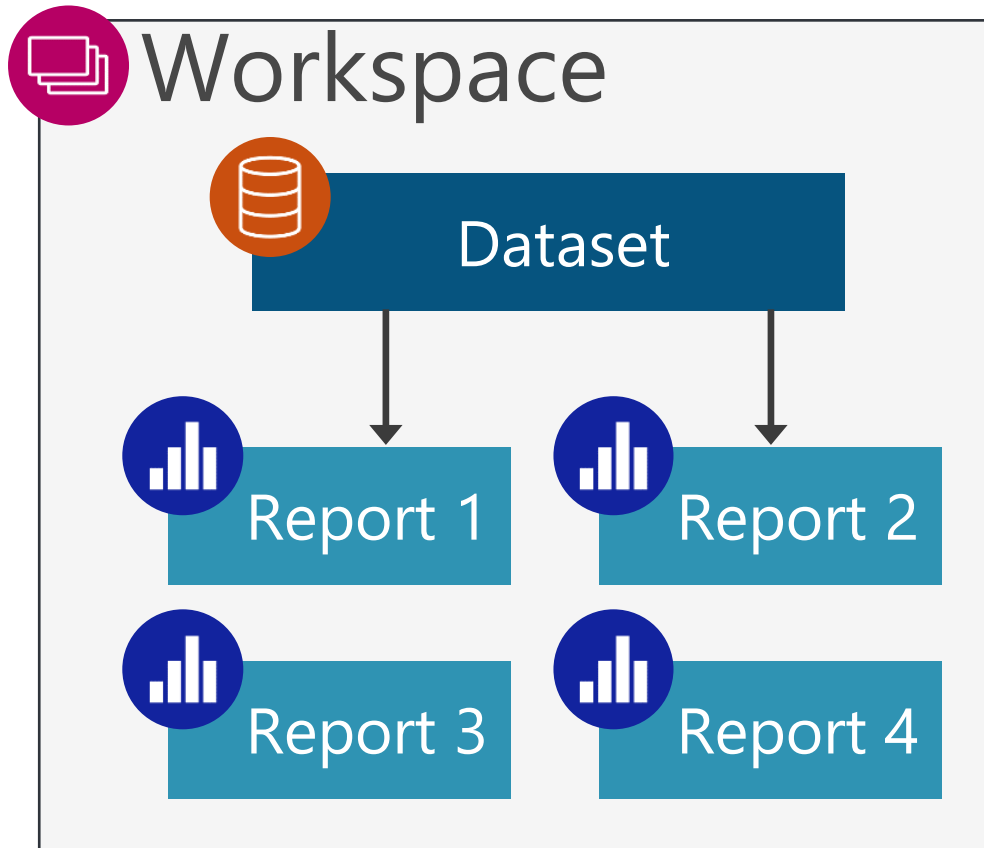
**Workspace roles:  
For content authors**

----->  
A "packaged up" set of items intended for view-only consumers



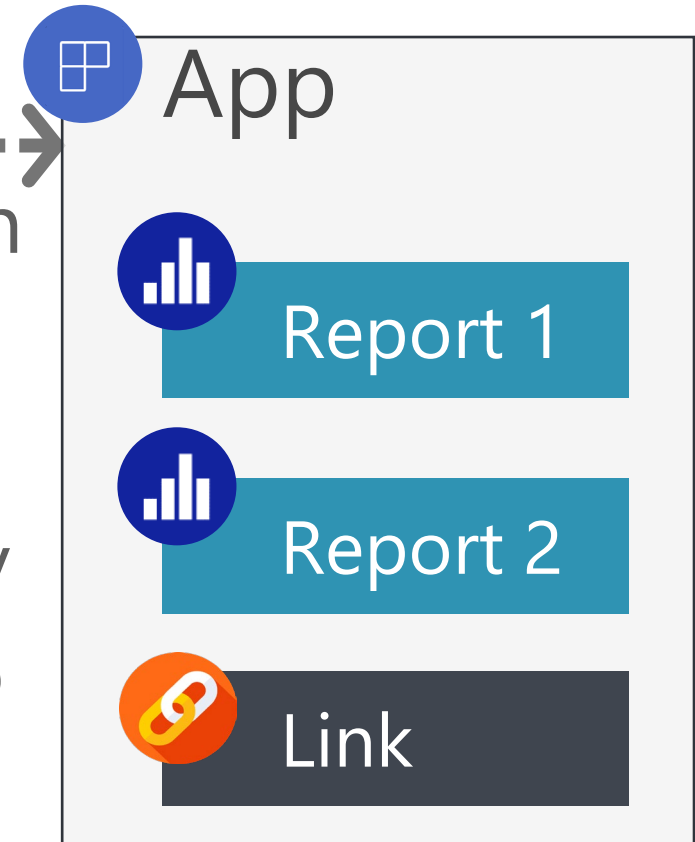
**App permissions:  
For content consumers**

# Workspace Roles are 'Sort Of' Inherited



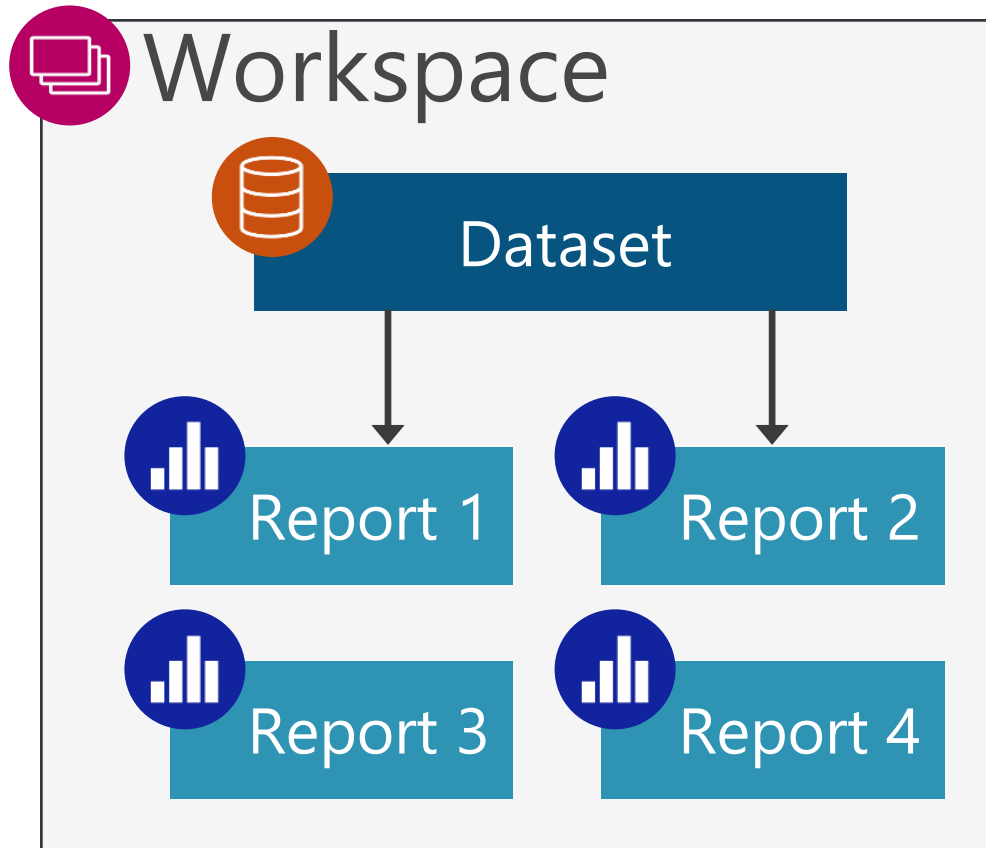
**Workspace roles:  
For content authors**

----->  
Everyone with  
workspace  
access  
automatically  
has access to  
the app

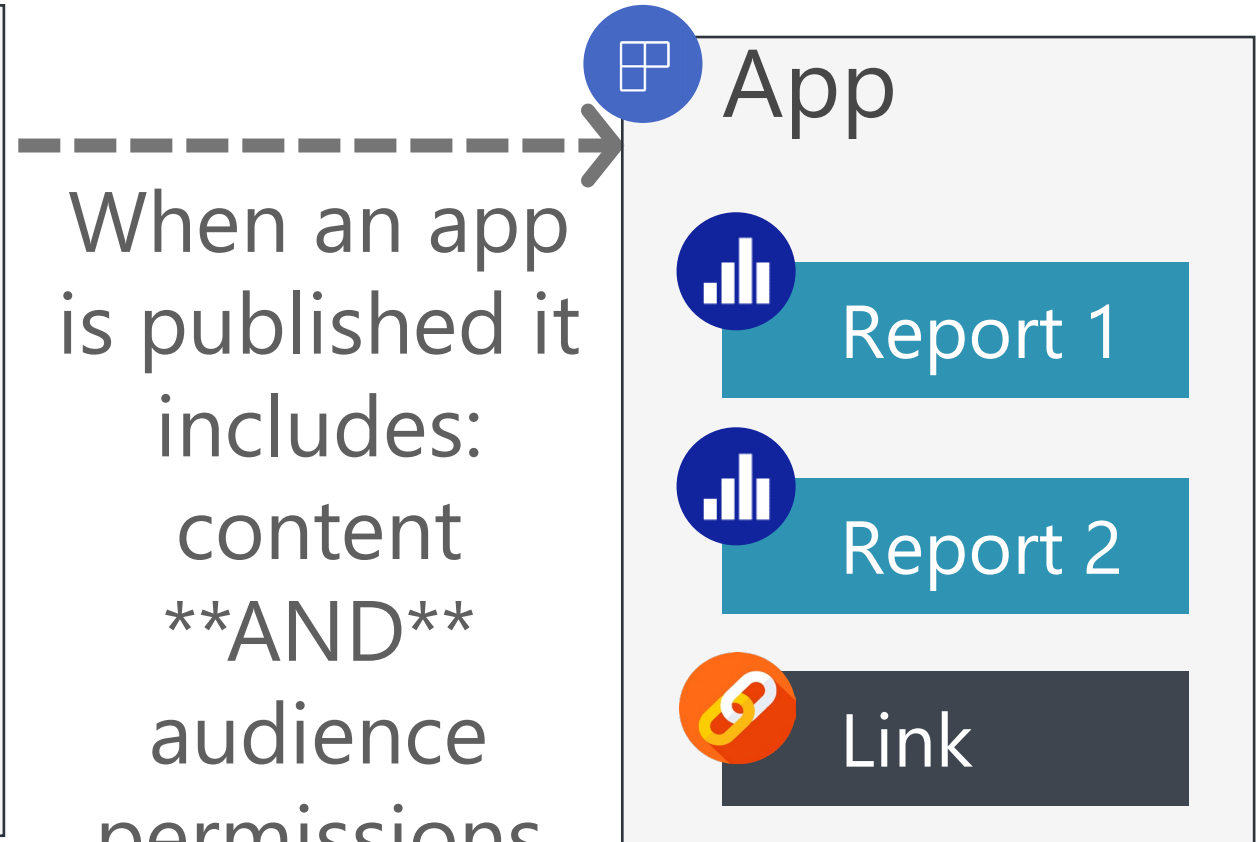


**App permissions:  
For content consumers**

# Permissions & Content are Deployed Together



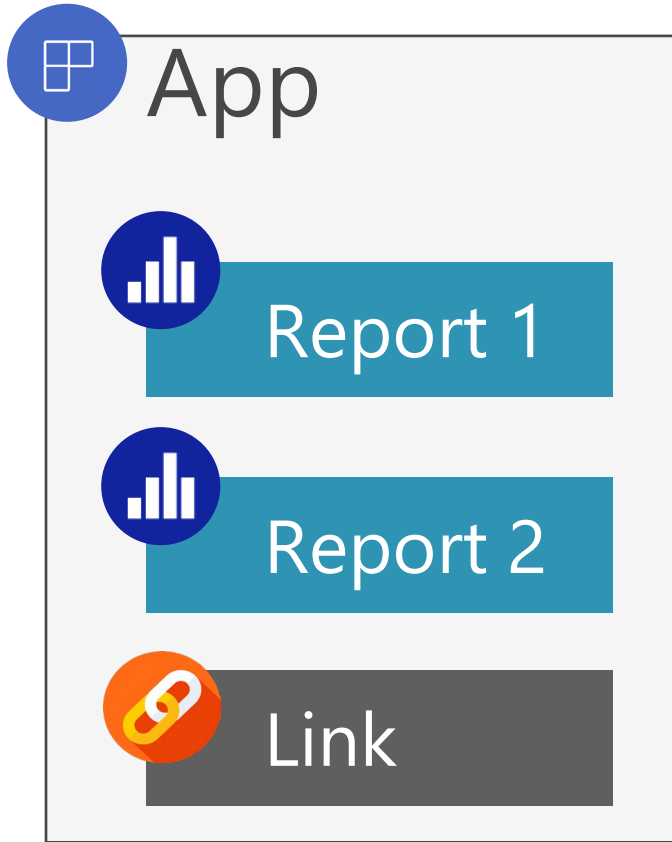
**Workspace roles:  
For content authors**



When an app is published it includes:  
content  
**\*\*AND\*\***  
audience permissions

**App permissions:  
For content consumers**

# Audiences: Mix & Match Consumer & Content



**Allowed to view:**

All 3 items



2 of the 3 items

**App permissions:  
For content consumers**





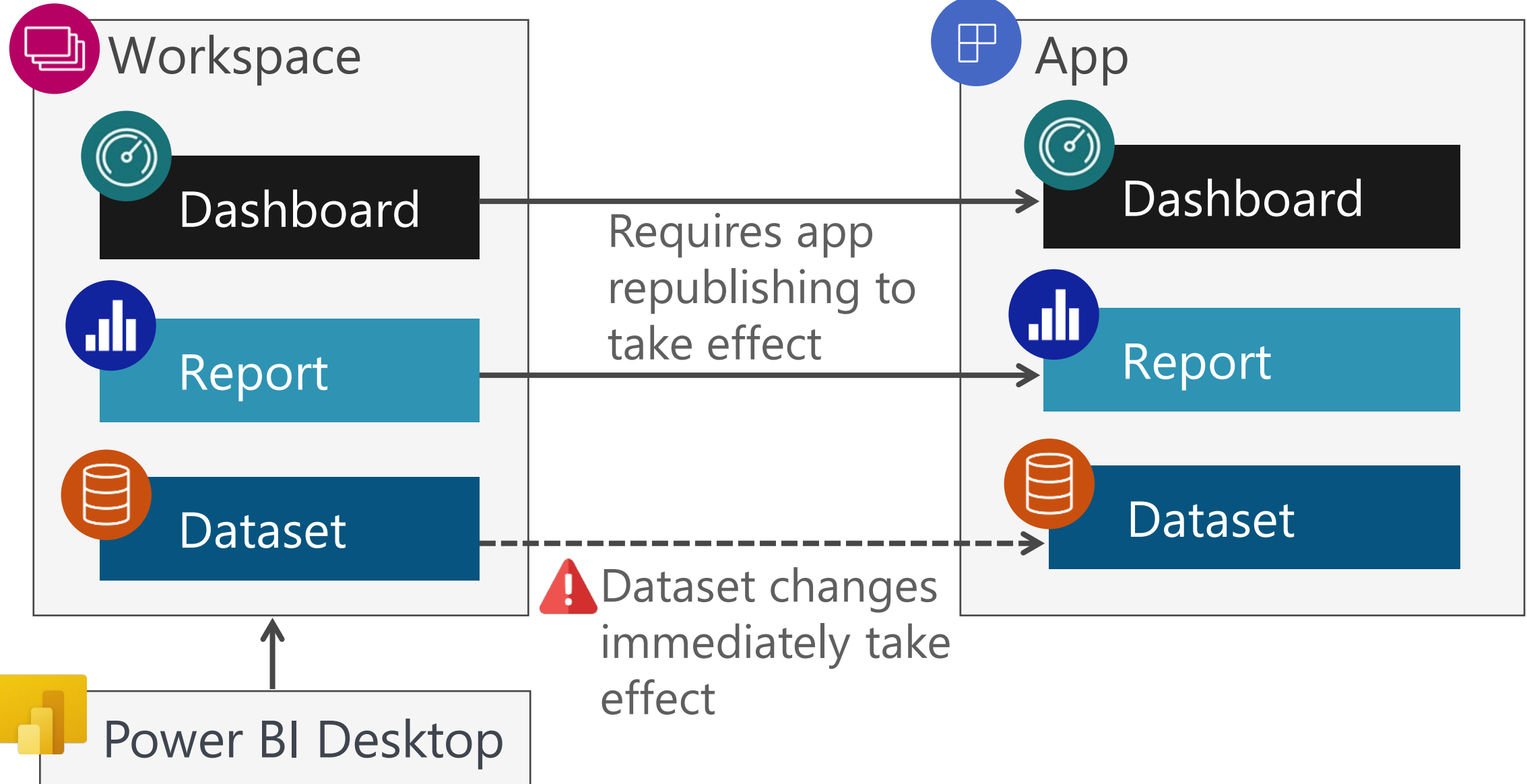
# Demo

---

**App audience permissions**



# Apps: Watch Out For





# Apps: Watch Out For



App permissions AND content are published at the same time.

*Tip:* Mitigate this issue by using security groups instead of individual users for app permissions.

*The one exception:* If you approve app access from a pending request, that's the only way to deploy app permissions without changing content.



## Apps: Watch Out For



New content isn't automatically added to an audience. Each new item needs to be explicitly unhidden for an audience.

This is good because new content can't accidentally "sneak into" the app.



# Open Q&A #1

Time	Topic	Demos
Part 1: 1:00 – 2:00	Building blocks: security & info protection	Sensitivity labels & DLP scan
	Users, groups & service principals	Group owner
	Workspace roles	Workspace roles
	App permissions	App audiences
<b>2:00 – 2:15</b>	<b>Open Q&amp;A #1</b>	
<b>2:15 – 2:30</b>	<b>Break time</b>	
Part 2: 2:30 – 3:30	Per-item permissions	Sharing links & direct access
	Request access workflow	Access requests
	Dataset permissions	Dataset perm & inheritance
	Data discovery	Data hub & discovery
	Different data based on user identity	
	Security strategies & suggestions	
<b>3:30-4:00</b>	<b>Open Q&amp;A #2</b>	

Eastern time zone



# Break Time

We restart in...

# Agenda

## Securing and Protecting Content in Power BI



Time	Topic	Demos
Part 1: 1:00 – 2:00	Building blocks: security & info protection	Sensitivity labels & DLP scan
	Users, groups & service principals	Group owner
	Workspace roles	Workspace roles
	App permissions	App audiences
<b>2:00 – 2:15</b>	<b>Open Q&amp;A #1</b>	
<b>2:15 – 2:30</b>	<b>Break time</b>	
Part 2: 2:30 – 3:30	Per-item permissions	Sharing links & direct access
	Request access workflow	Access requests
	Dataset permissions	Dataset perm & inheritance
	Data discovery	Data hub & discovery
	Different data based on user identity	
	Security strategies & suggestions	
<b>3:30-4:00</b>	<b>Open Q&amp;A #2</b>	

Eastern time zone



# Per-Item Permissions





# Purpose for Per-Item Permissions

Assign permissions directly to an individual item.

They're also inherited from:

- Workspace roles
- App permissions



Reports



Dashboards



Scorecards



Workbooks



Datasets

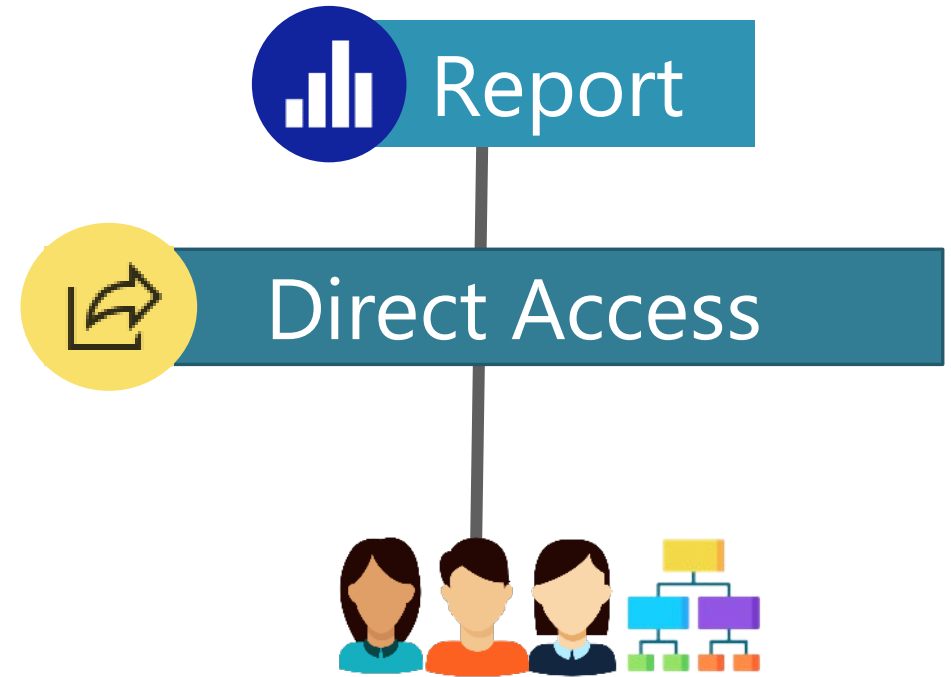
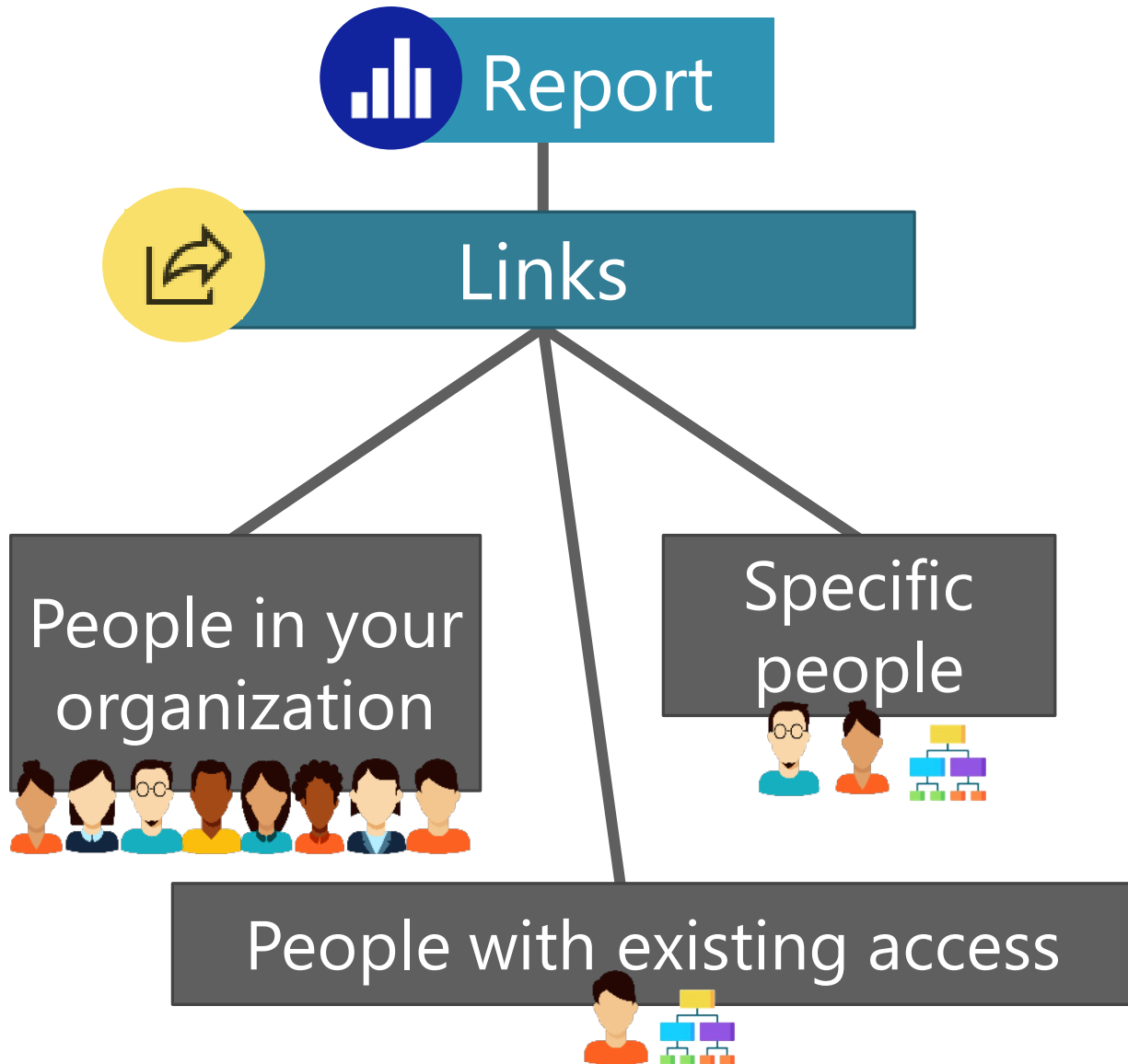


Dataflows



Datamarts

# Two Types of Sharing



# Chart Sharing



 Report

 Chart Sharing: Link to Selection

 Shared View

People with existing access





# Demo

---

**Sharing experience**

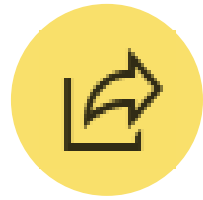
**Report links**

**Report direct access**

**Chart sharing**



# When to Use Per-Item Sharing



**Per-item sharing is most suitable when:**

You want to provide read-only access to only 1 item

BECAUSE

You do *not* want the recipient to view everything in workspace

OR

You do *not* want the recipient to view everything in an app



Think of sharing as an 'exception' to workspace roles



# When to Use Sharing from 'My Workspace'

 **Sharing from a personal workspace is suitable when:**

You want to provide read-only access to 1 item

BECAUSE

You have non-critical, informal, or temporary content that's appropriate for storing in My Workspace



Use sharing from My Workspace sparingly



# Per-Item Report Permissions

Permission:



Read



Reshare

Targeted to:



Report  
consumers



Report  
consumers  
allowed to  
freely reshare

To support  
report authors:  
use workspace  
roles instead!



# Per-Item Sharing: Watch Out For



Overuse of per-item permissions because the 'share' buttons are very prominent in the Power BI service. Less experienced content creators might not know when to use workspace roles or app permissions instead.





# Per-Item Sharing: Watch Out For



Tedious and error-prone if changes are needed for many items (especially if individual users are used instead of security groups).



Users who get in the habit of assigning most permissions to individuals (vs. use of groups).



# Per-Item Sharing: Watch Out For



Default “people in your organization” sharing link.

*Tip:* There’s a tenant setting to disable this option.

*Tip:* Mitigate this issue by using the API to find widely shared artifacts.



# Per-Item Sharing: Watch Out For



Allowing 'reshare' to too many people.



Allowing 'build' on the underlying dataset (when sharing a report) if it isn't necessary for report consumers.



Extensive sharing from personal workspaces.



# Request Access Workflow

# What's the Most Common Way Users Share Content?



User 1

Views a report



Sends a URL  
copied from  
their browser



User 2

Clicks the URL

If User 2 doesn't have permission:  
starts the access request workflow  
**\*\*in some situations\*\***

# Request Access Workflow



User



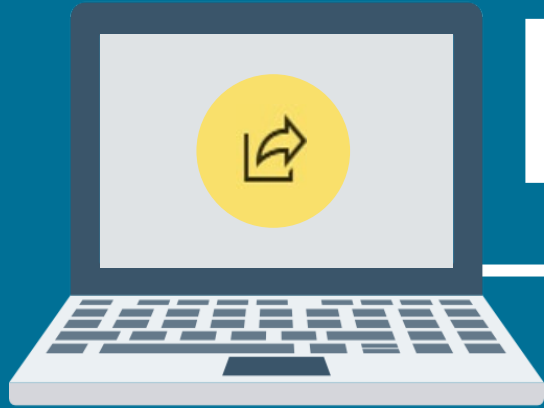
Submits a form to  
request access



Owner

Approves or  
declines the  
pending request

Clicks a URL  
Discovers they  
don't have  
permission



# Demo

---

**Request access workflow**  
**Pending requests**



# Custom Instructions for Requesting Access to a Dataset or Datamart

Helpful when:

- Approval is done by someone other than a dataset owner
- Tracking of access requests (who/when/why is required for compliance / auditing purposes
- An existing form / process / workflow already exists

**Request access**

Select how users will request permissions to access content from this dataset. [Learn more](#)

A request for build permissions is sent in an email to the dataset owner

User requesting access will get the following instructions

*i* Your email address will be visible to users requesting access.

Instructions \*

For standard sales reporting of MTD/QTD/YTD, we'd like for you to use this dataset which is certified. Please request access to the dataset by completing the form located at <https://SalesDataRequestForm.com>. You will be asked for a brief business justification, and the manager of the Center of Excellence will be required to approve the request as well. Access will be audited every 6 months.





# Request Access Workflow: Watch Out For



Users can request access to:

- Most individual items
- Apps

The built-in workflow encourages overuse of per-item permissions.



# Request Access Workflow: Watch Out For



There's no request access workflow for a workspace. The user receives a "sorry you don't have access" message.



# Request Access Workflow: Watch Out For



If you have an internal process (ex: to use groups instead of individuals), the person receiving the access request will need to know to:

1. Decline the request.
2. Instead add the person to a group.



# Request Access Workflow: Watch Out For



Currently, only datasets and dataflows have a custom message to request access.

Ex: to direct users to a form instead.



# Dataset Permissions

# Shared Datasets

Intended for reuse by reports & models



Shared dataset:



Live Connection

Analyze In Excel

DirectQuery



Reports & composite models:



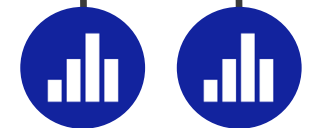
Power BI report



Paginated report



Excel report



# Multiple 'Layers' of Permissions Needed



Visuals

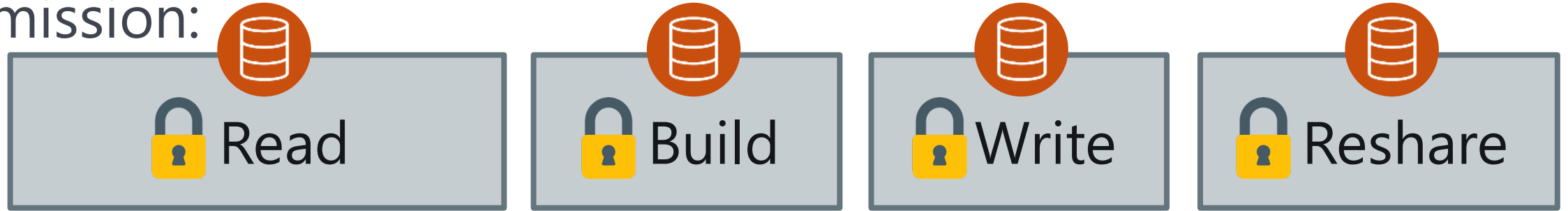


Dataset



# Per-Item Dataset Permissions

Permission:



Targeted to:

 Report consumers

 Report creators

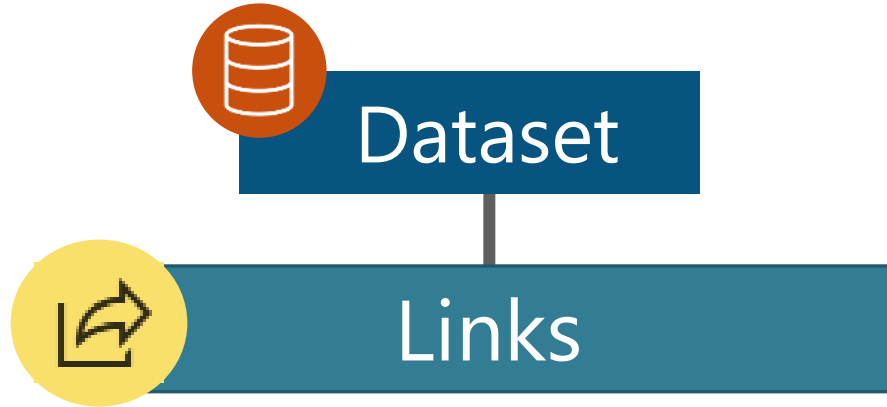
 Dataset creators

 Consumers & creators allowed to freely reshare



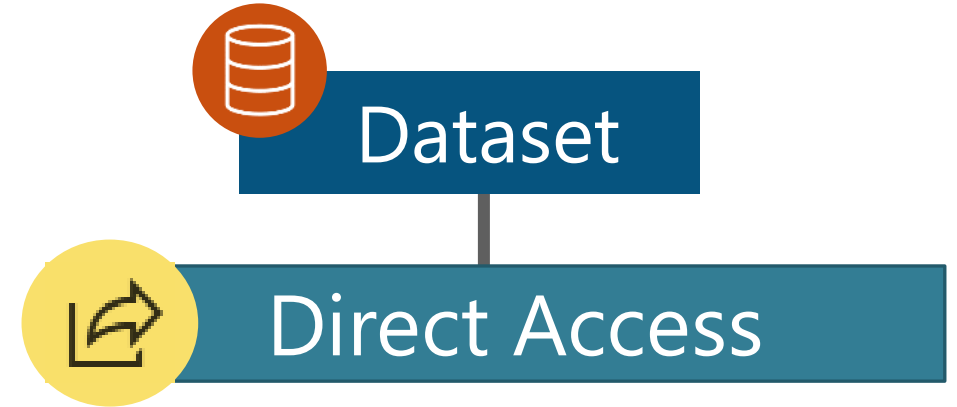


# Dataset-Level Permissions: Two Types



Inherited only: links CANNOT be configured directly for a dataset

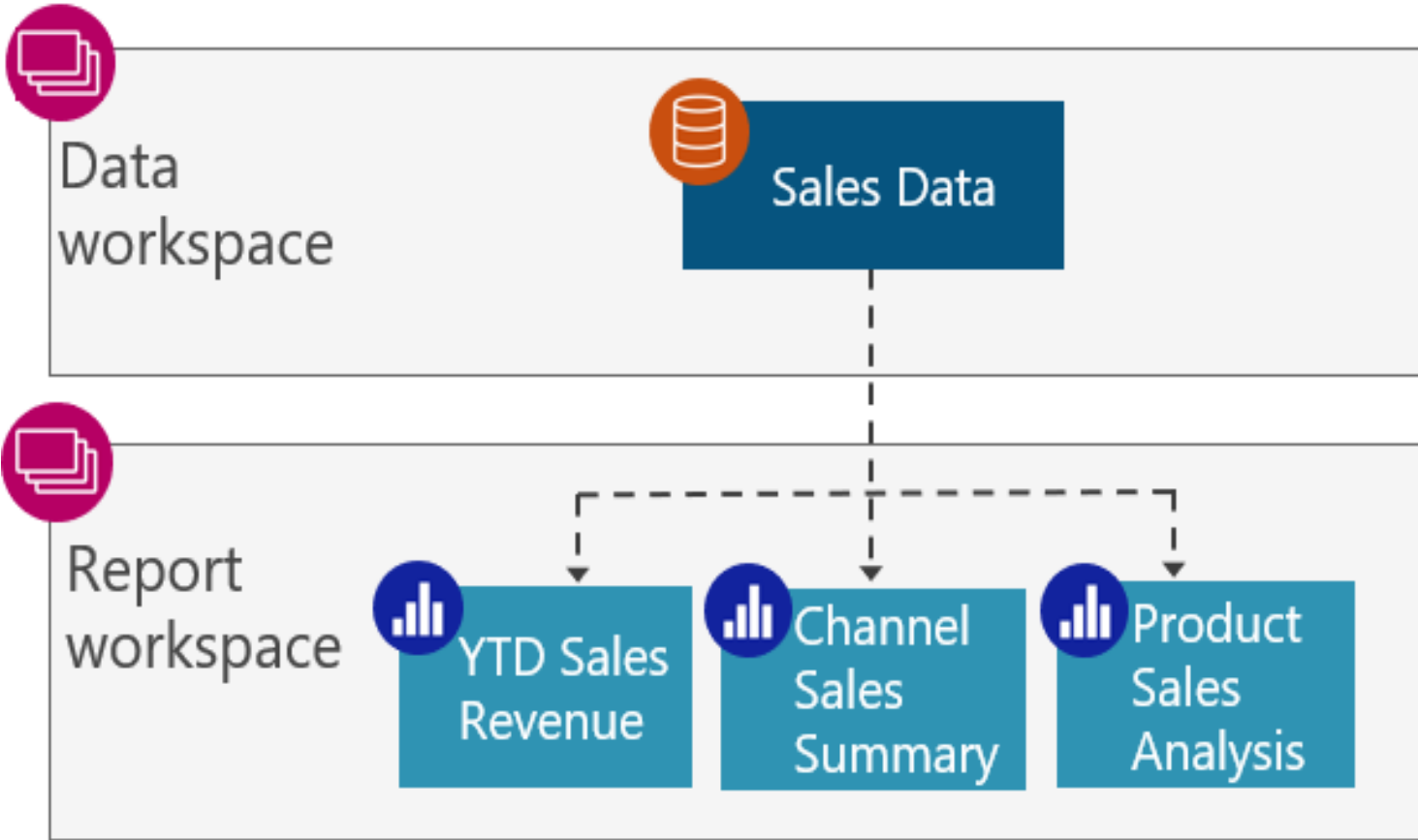
*Stays 'tightly coupled'*



Can be configured directly for a dataset

*NOT 'tightly coupled'*

# Managing Permissions for Content Creators



## Data authors:



Workspace role (admin, member, contributor)  
--or-- dataset write

## Report authors:



Build on the dataset  
+

Workspace role (admin, member, contributor)

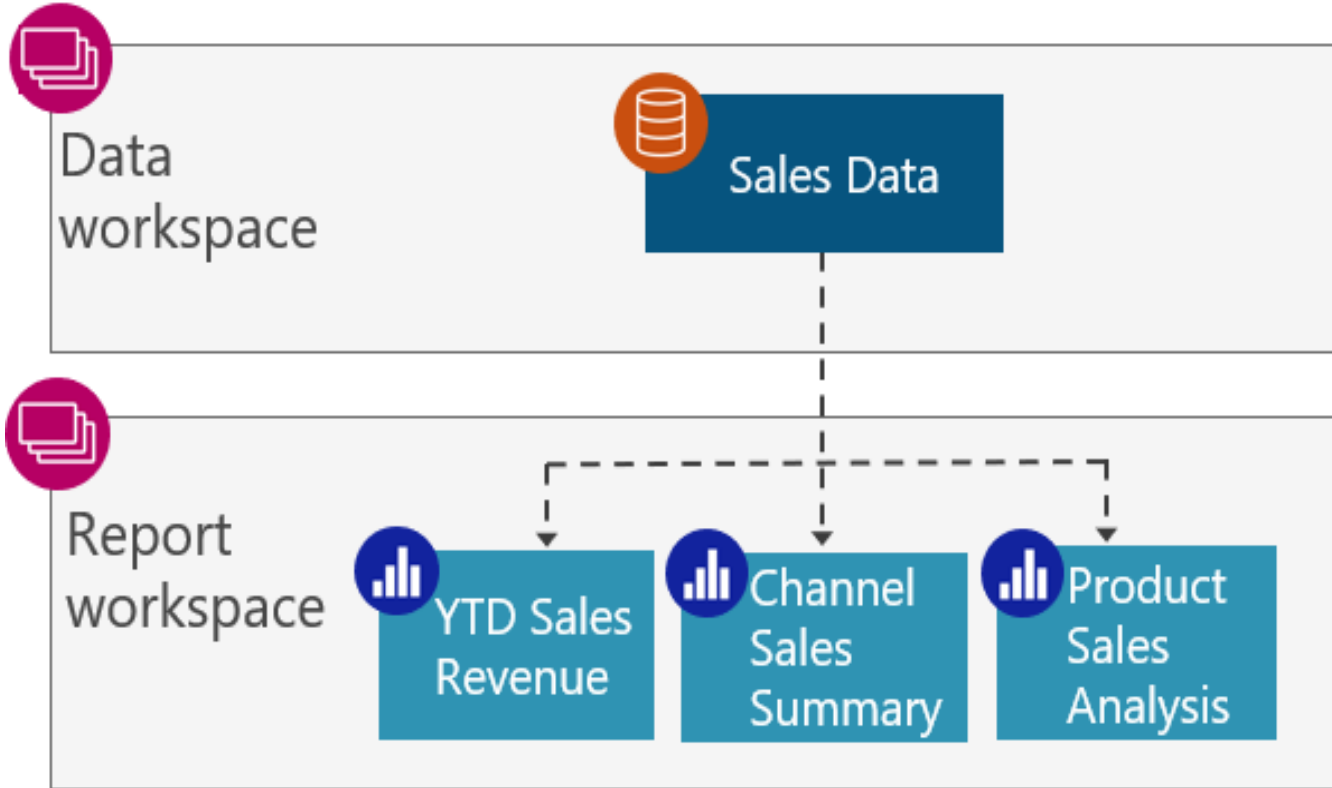


# Demo

---

**Dataset Permissions  
Inheritance**

# Managing Permissions for Content Creators



◀ **Dataset 'build' allows:**  
Create a new report  
Create a composite model  
Use Analyze in Excel  
Query with XMLA endpoint



# External Sharing of Datasets

Sharing data with external partners, customers, vendors, consultants, etc.



**Content creator manages:**

(1) Dataset 'build' permission for external users

(2) The 'external sharing' dataset setting enabled

**Power BI admin manages:**

(1) Tenant settings to enable

Plus other data sources



# Dataset Permissions: Watch Out For




The 'build' and 'write' permissions are enabled by default when granting dataset permissions.

*Tip:* Every content creator should be taught how to know what's really necessary to provide (i.e., why the principle of least privilege is important). Use governance guidelines and policies as necessary.



# Dataset Permissions: Watch Out For

 Granting the 'build' permission for the underlying dataset can be done while sharing a report or publishing an app. However, it's not that common that the consumers and creators are the exact same group of people.

*Tip:* Get in the habit of managing/reviewing/auditing:

- Dataset permissions (separately from)
- Report permissions



# Dataset Permissions: Watch Out For



If the dataset is in a different workspace than the app, the 'build' permission can't be automatically granted when you're publishing an app.

*Tip:* Get in the habit of managing/reviewing/auditing:

- Dataset permissions (separately from)
- Report permissions





# Datamart Permissions: Watch Out For

**Datamart = Azure SQL DB + Dataset**




When sharing a datamart, sharing represents a little something different:

- The ability to build content with the auto-generated dataset, AND
- The ability to connect to the SQL endpoint



# Datamart Permissions: Watch Out For

**Datamart = Azure SQL DB + Dataset**

-  Workspace roles get mapped to database-level roles in the Azure SQL DB. The database roles can't be managed from the database side though.



# Data Discovery

# How Do Content Creators Know a Dataset Exists?



Shared dataset:



Live Connection

Analyze In Excel

DirectQuery



Reports &  
composite  
models:



Power BI report



Paginated report



Excel report



# How Do Content Creators Know a Dataset Exists?



Level 4

**Search a data catalog**

*Metadata of existence is shown*

Level 3

**Discovery in Power BI**

*Metadata of existence is shown*

Level 2

**Search & browse in Power BI**

*Requires existing permissions*

Level 1

**Ask a colleague**



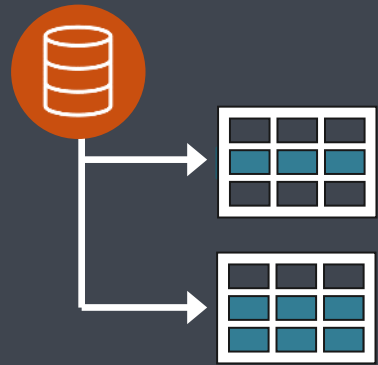
# Demo

---

**Data Hub**

**Discoverable Property**

**Custom Request Access**

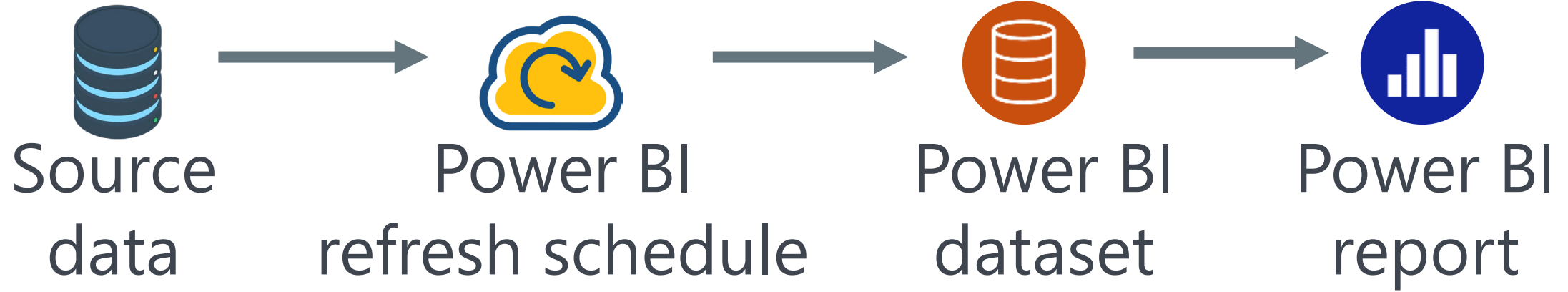


# Showing Different Data Based on User Identity



# What Data Are Users Allowed To See?

## Imported data:



## DirectQuery:

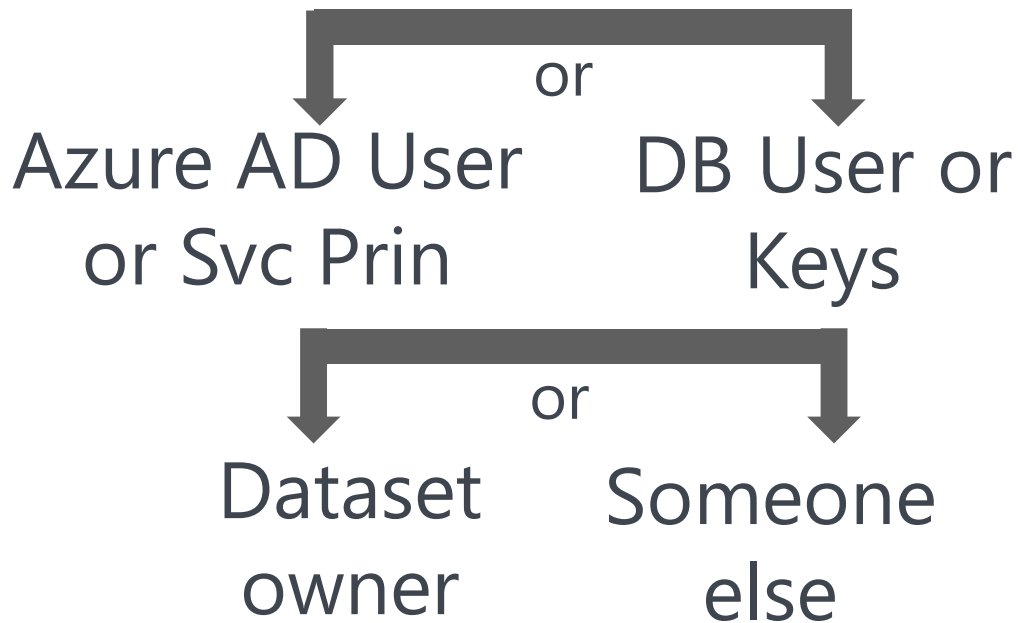




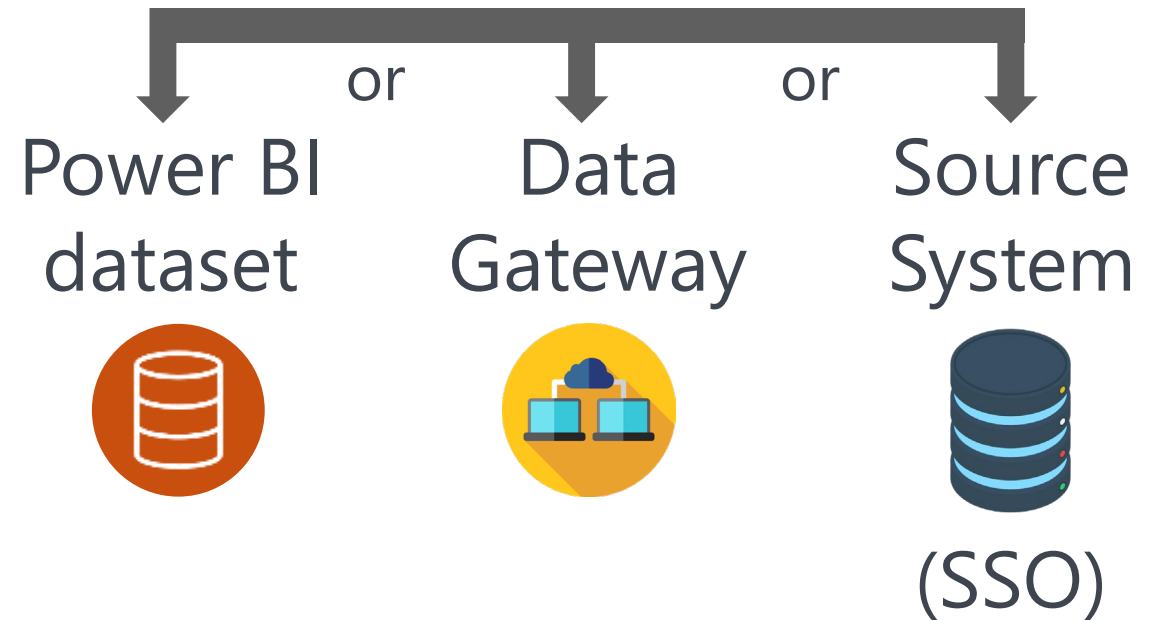


# What Credentials are Used to Retrieve Data & Populate a Dataset?

## Whose credentials are being used to access source data?



## Where are the credentials stored?

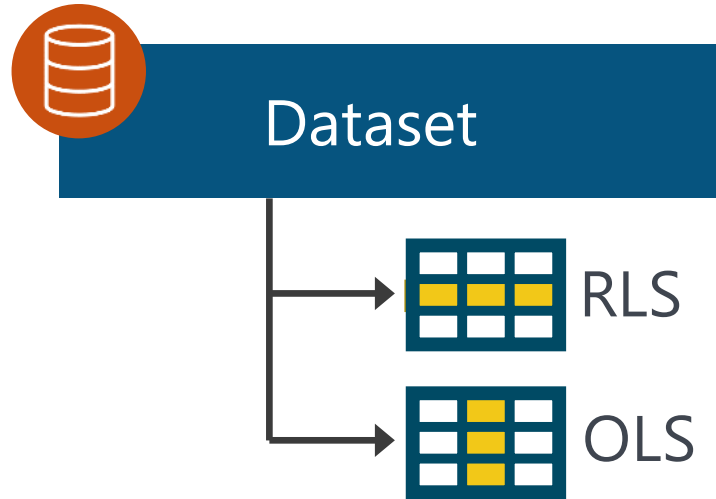


# Different Data Results Based on User Identity



**Row-level security:** Which *rows* a user sees

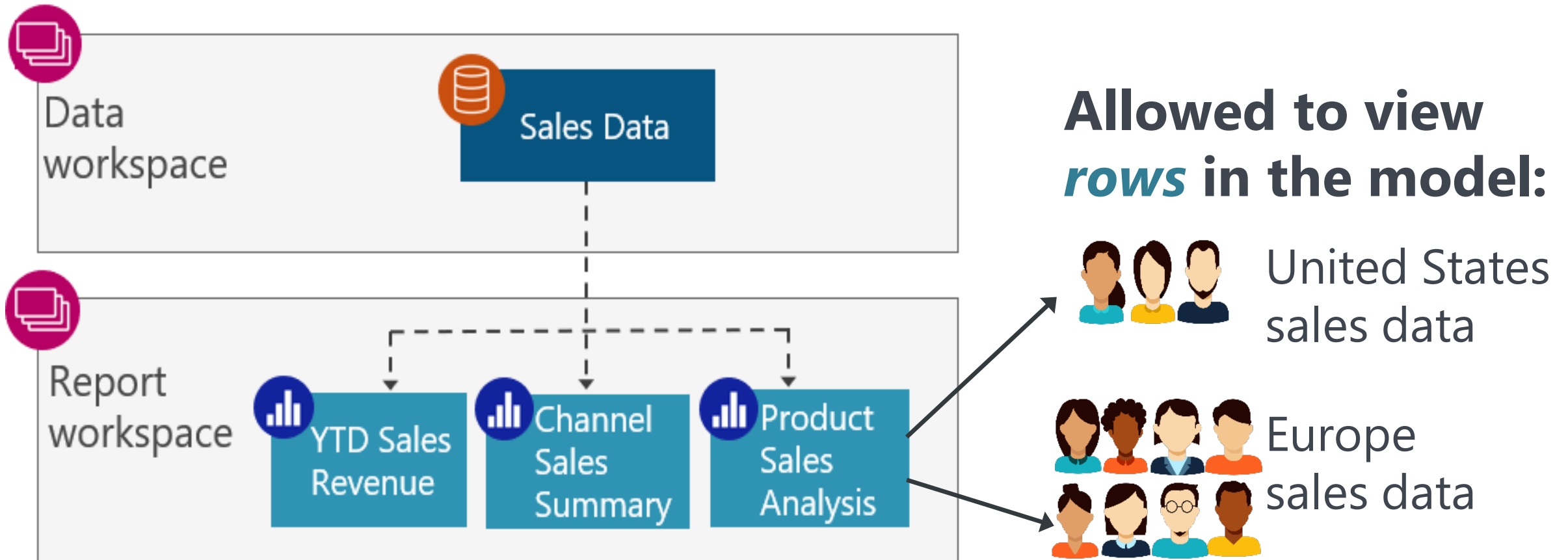
**Object-level security:** Which *columns* a user sees





# Row-Level Security

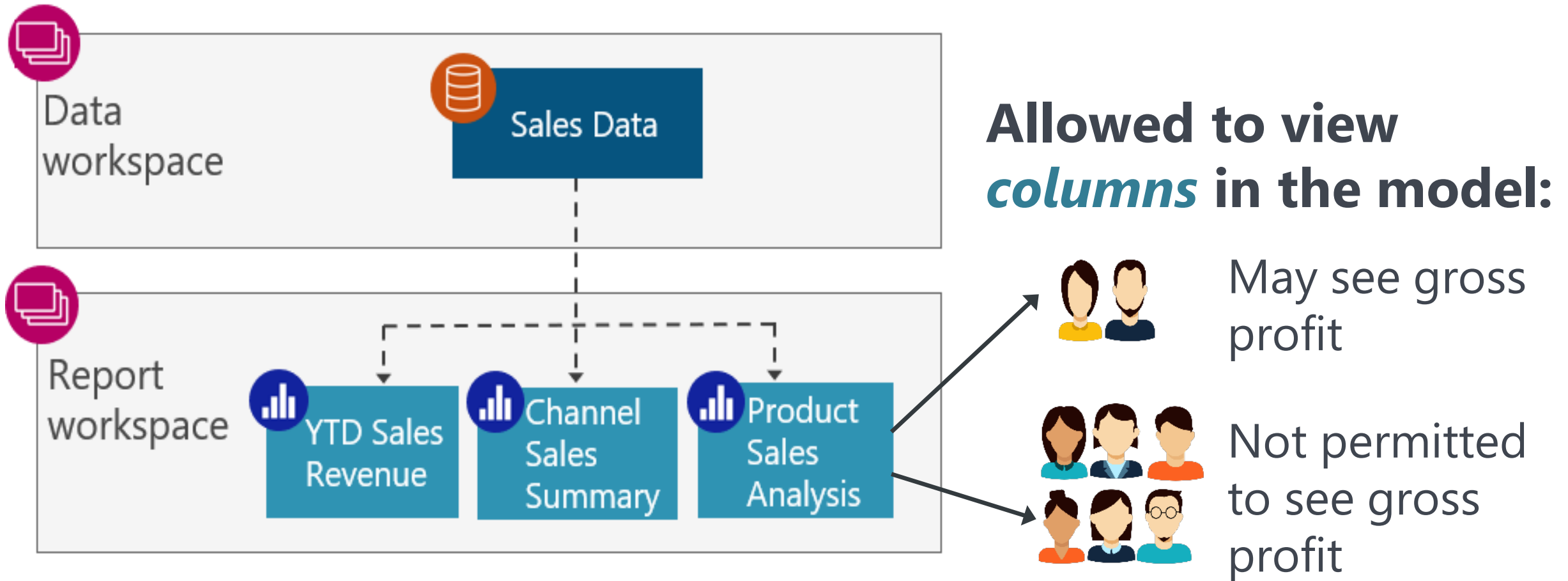
What if we want different users to see a subset of the data?





# Object-Level Security

What if we want different users to see a subset of the data?

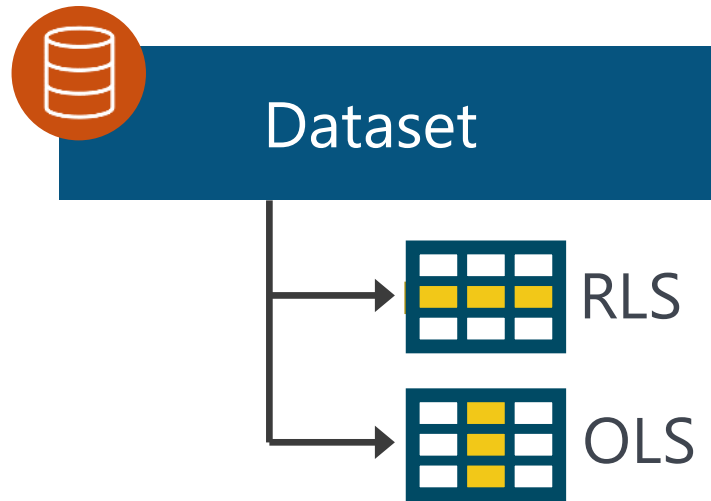


# Different Data Results Based on User Identity



**Row-level security:** Which *rows* a user sees

**Object-level security:** Which *columns* a user sees



RLS and OLS:

- Are defined on the dataset!
- Impacts what data is shown to consumers on reports & visuals
- Based on members assigned
- Only applicable to viewers



# Row-Level Security (simplified)

**1 Roles are defined to filter the model**

**2 Mappings between roles and which users/groups**

RLS role 1	Rule A
	Rule B

RLS role 2	Rule C
	Rule D

Role mappings "dataset security"	Group A
	Group B
	Group C
	User 1

**3 RLS rules are invoked for users with read-only permissions to the underlying dataset**

**Rule expressions:  
DAX expressions (static or dynamic) to filter the model.  
If true = user can see the row.**



# The Default User Experience Is Different



The presence of RLS changes the default experience for users!


***If at least one RLS role exists in a model:***

A user must be mapped to a role in order to see data. For this reason, RLS is thought of as a “second layer of defense.”




# RLS for Consumers

Consumers: Workspace viewers & dataset read permissions

  
Viewers see **all**  
of the data in  
Dataset1



  
Viewers see **none** of the  
data in Dataset2 unless  
they're in an RLS role



 **Contains no RLS roles**



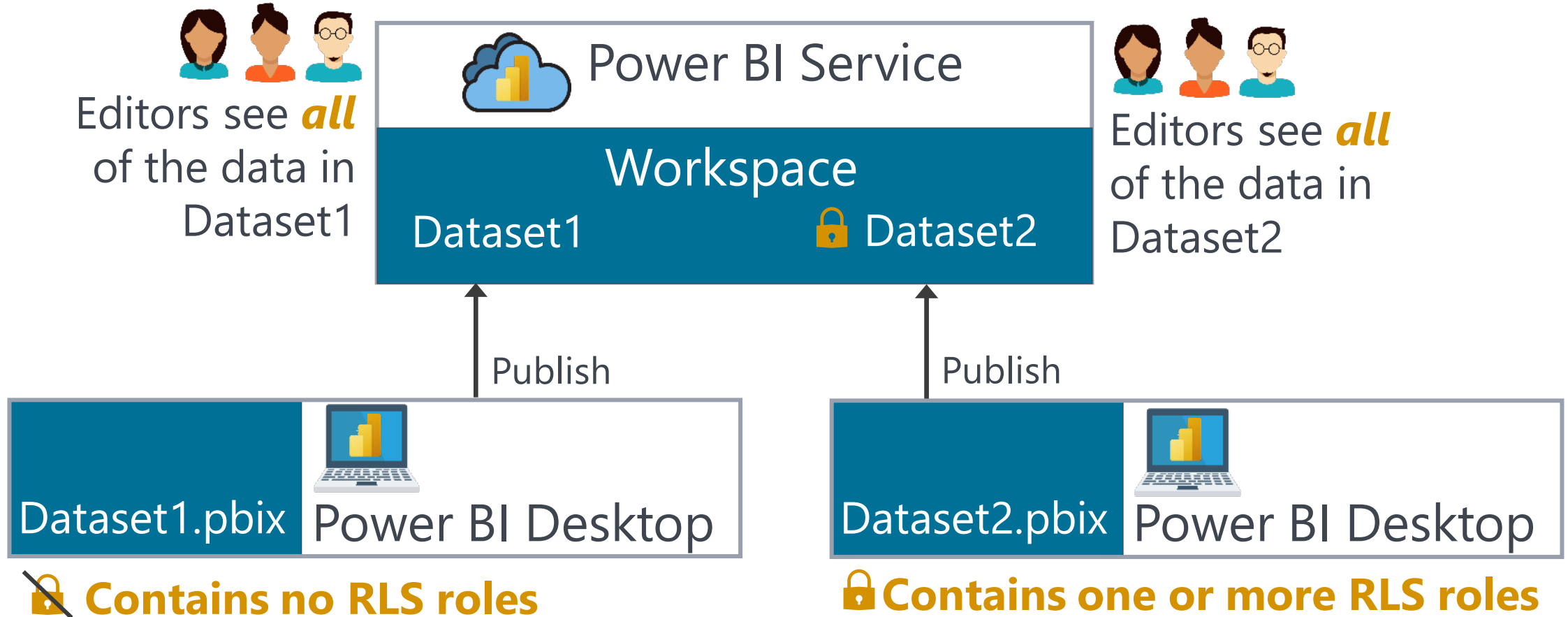
 **Contains one or more RLS roles**





# RLS for Content Creators

Creators: Workspace contributors/members/admins OR dataset write





# Row-Level Security: Watch Out For



RLS is *ignored* in Power BI Desktop.

RLS is *ignored* in the Power BI Service for users with edit permission to the dataset:

- Workspace contributors, members, and admins
- Dataset 'write' permission



# Row-Level Security: Watch Out For



To avoid a poor user experience, keep RLS role assignments the same as:

- Dataset read permissions and/or
- Workspace viewer permissions

*Tip:* You can think of RLS as a “second line of defense” for security. If someone is granted read access but shouldn’t have been, they won’t see anything if RLS is configured. But that’s not the best user experience.



# Row-Level Security: Watch Out For



If static RLS gets complicated to maintain, look into dynamic RLS to manage data-driven permissions.

Static rules: constants (ex: sales region = Midwest)

Dynamic rules: data-driven (DAX functions that return environmental variables: userprincipalname, customdata)

*Tip:* Create a database table, or a dataflow, for content creators to use as a single source for RLS rules.



# Security Strategies & Suggestions



# Multiple Layers of Security

## Permissions for a Collection of Items



Workspace Roles



App Permissions

## Per-Item Permissions



Datasets



Reports, Dashboards, etc.

## Data Access & Data Results Per User



Dataset & Datamart RLS & OLS



Data Sources & Gateways

# Content Creators vs. Consumers



## Workspace permissions for content creators



**Data**

**Authors**



**Report Authors**

Limit access to the workspace to those who are handling:

- Authoring
- Development
- Testing & data validations



## App permissions for consumers



**Viewers**

Provide access via an app for:

- Read-only consumers



# Ways to Provide Permissions to Consumers



## 1<sup>st</sup> choice: App permissions

Best user consumption experience for distributing a set of reports & dashboards. Audiences provide flexibility to mix & match.



## 2<sup>nd</sup> choice: Workspace viewer permissions

Suitable for small teams that don't need an app & when viewers are allowed to see everything in the workspace.



## 3<sup>rd</sup> choice: Per-item sharing

Links or direct access per item. Sharing is like an 'exception' to workspace roles and needs to be maintained for every item.



# Control Who Your Power BI Administrators Are

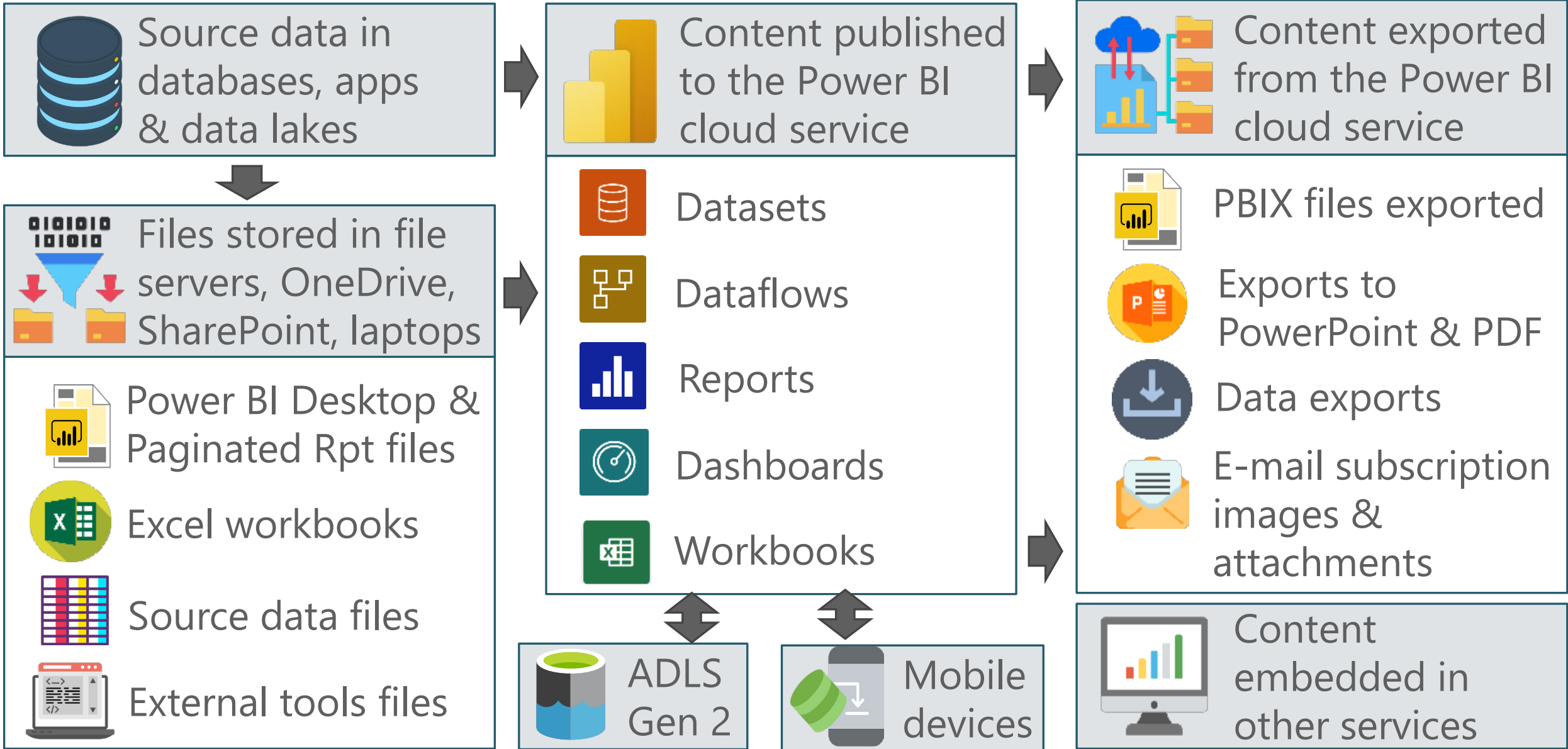


The Power BI administrator (service admin) is a very high privilege role.

Power BI administrators can:

- ✓ Update/delete workspace roles in the tenant
- ✓ Access personal workspaces
- ✓ Access all APIs and tenant-wide metadata
- ✓ Manage all tenant settings

# Don't Forget Data Stored Outside of the Service





# What's Your Data Culture?



Encourage a healthy data culture that:

- ✓ Understands that securing organizational data is everyone's responsibility.
- ✓ Values saying "yes and" rather than "no" as a default response.



**Open Q&A**

# More Information from Melissa Coates



**Slides:**

[CoatesDS.com/Presentations](https://CoatesDS.com/Presentations)



**Diagrams:**

[CoatesDS.com/Diagrams](https://CoatesDS.com/Diagrams)



**Power BI Governance Training:**

[CoatesDS.com/Training](https://CoatesDS.com/Training)



**Blog:**

[CoatesDS.com/Blog-Posts](https://CoatesDS.com/Blog-Posts)