



Options for Securely Sharing Power BI Content in Microsoft Fabric

Melissa Coates

Data Architect | Consultant | Trainer



Slides & recordings: CoatesDS.com/Presentations

Content last updated: June 27, 2023



Melissa Coates



Data architect specializing in Power BI governance & administration

Author of Microsoft guidance:

[Power BI Adoption Roadmap](#)

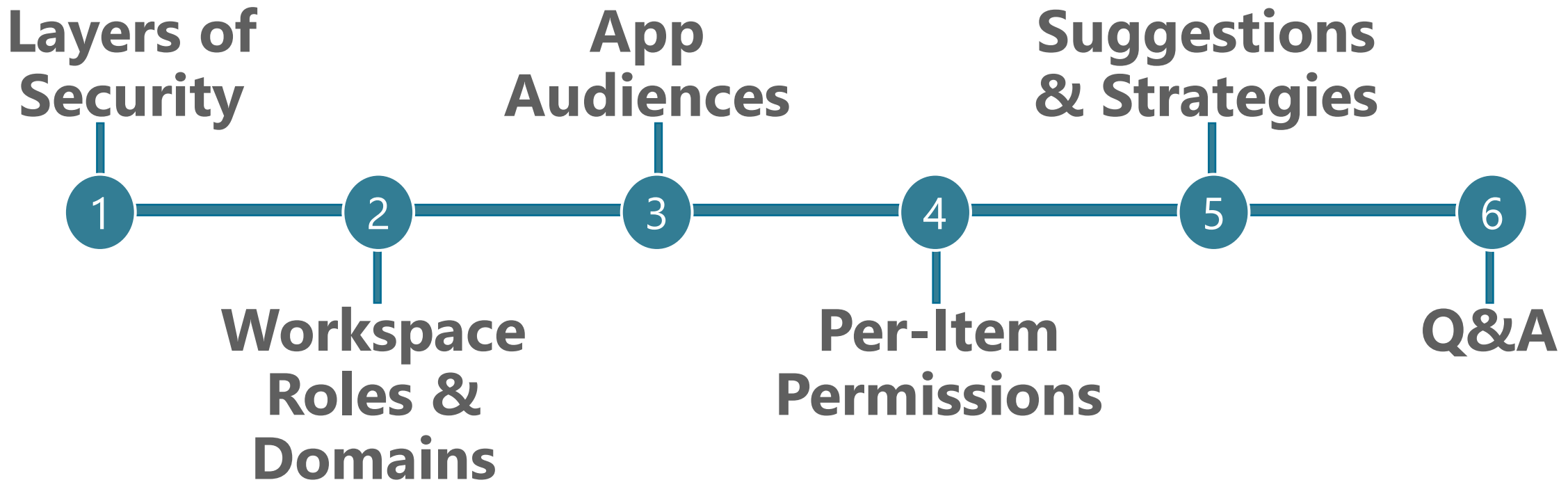
[Power BI Implementation Planning](#)

Original creator of the [Power BI Deployment & Governance](#) training course (now run by Mike Carlo)



Options for Securely Sharing Power BI Content in Microsoft Fabric

Agenda:



Slides & recordings: CoatesDS.com/Presentations




So Many Security Related Topics We Don't Have Time to Cover!

- Users vs. groups vs. service principals
- Request access workflow
- Row-level security & object-level security
- Dataflow & datamart permissions
- Scorecard & metric permissions
- Cross-tenant dataset sharing
- Strategies for external users
- E-mail subscriptions
- Information protection & data loss prevention
- Data discovery
- Gateway & data source security
- Azure Active Directory: identity management & authentication
- Networking: secure virtual networks & private links
- Power BI Report Server security options
- Power BI Embedded or content embedded in other applications
- Microsoft Purview integration & permissions

Other Presentations from Melissa

Related presentations you might also find helpful:



Increasing Trustworthiness of Power BI Content

Melissa Coates
Data Architect | Consultant | Trainer
CoatesDataStrategies.com
@SQLChick | @CoatesDS

Slides & recordings: CoatesDS.com/Presentations



Securing and Protecting Content in Power BI

Melissa Coates
Data Architect | Consultant | Trainer
CoatesDataStrategies.com

Slides & recordings: CoatesDS.com/Presentations

↑ A longer session that includes things we don't cover in this shorter session



Other Resources

[!\[\]\(5eb1325dfdc3f1cad8426726c0db51cd_img.jpg\) Power BI Implementation Planning: Security](#)



Also written
by Melissa

- Security overview
- Tenant-level planning
- Report consumer planning
- Content creator planning

[!\[\]\(5a132f13505a6571904d622757b7a8f0_img.jpg\) Power BI security whitepaper](#)

[!\[\]\(10f8862fc183b400327470ea85afe9ae_img.jpg\) Microsoft Fabric security documentation](#)

[!\[\]\(e1d6102fe77919492c04879c8450f1f5_img.jpg\) Azure security baseline for Power BI](#)



Layers of Security



Multiple Layers of Security

Collection of Items

Individual Items

Data Results Per User

Other

Multiple Layers of Security

Prior to OneLake Security
that's coming to Fabric



Collection of Items



Workspace Roles



App Permissions

Individual Items: Visuals



Reports
└ Charts



Dashboards



Paginated
Reports



Scorecards
└ Metrics



~~Workbooks~~

Individual Items: Data



Lakehouse



Warehouse



Datasets



Datamarts



~~Dataflows~~

Data Results
Per User



Row-Level Security



Object-Level Security

Other

Data Sources, Gateways,
Cross-Tenant Sharing etc...

Item crossed out = no per-item permissions available



Security Settings are Inherited

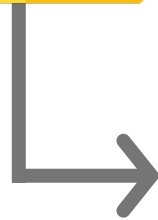
Conceptually – Power BI inheritance is the same idea as folders and file security:

Collection of Items

Individual Items



Folder



File

1



File

2



File

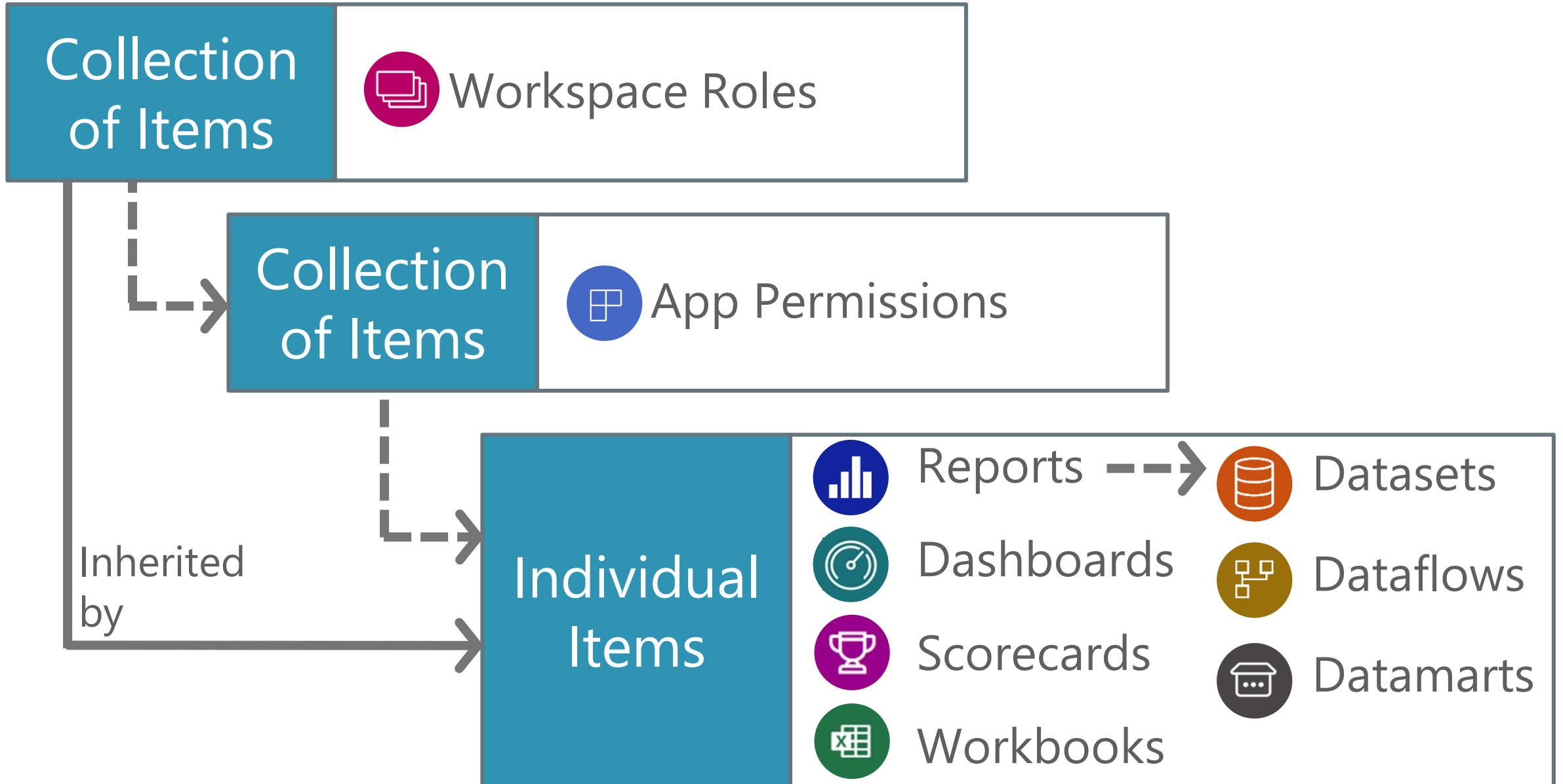
3



File

4

Security Settings are Inherited

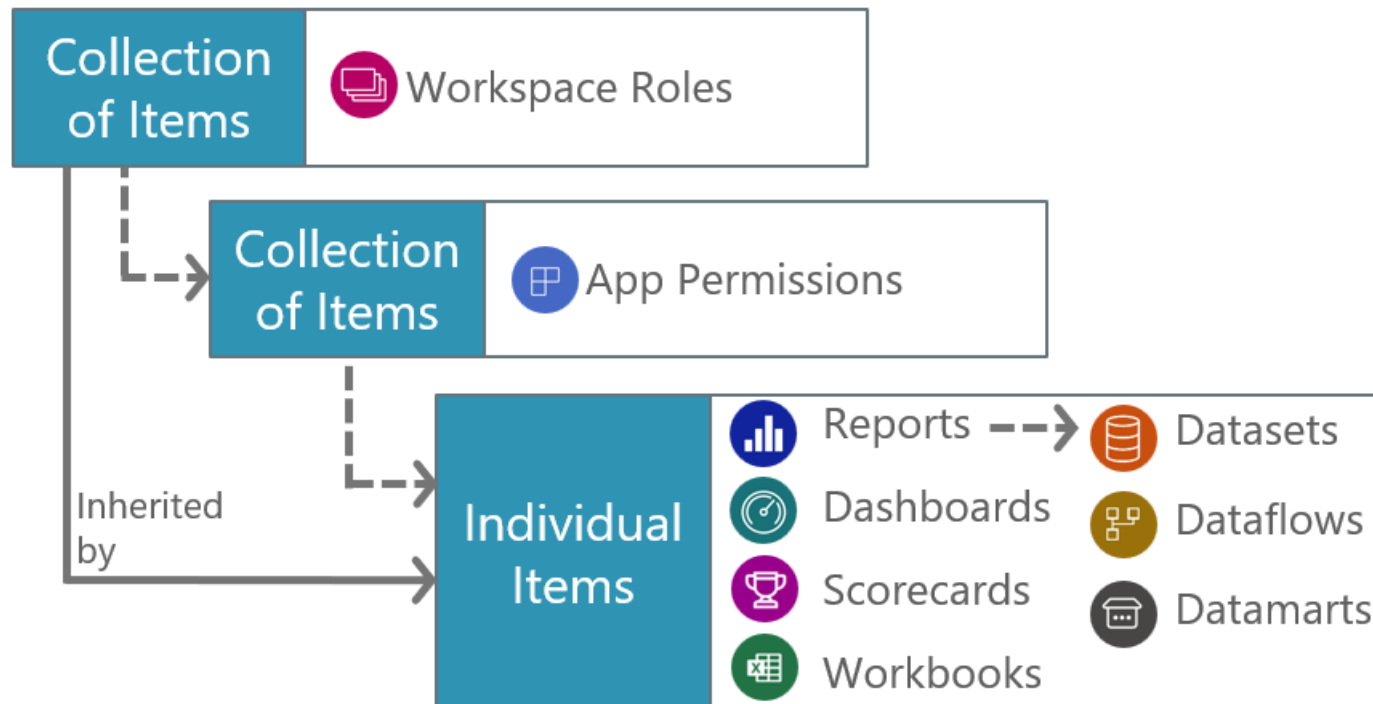




Key Takeaways

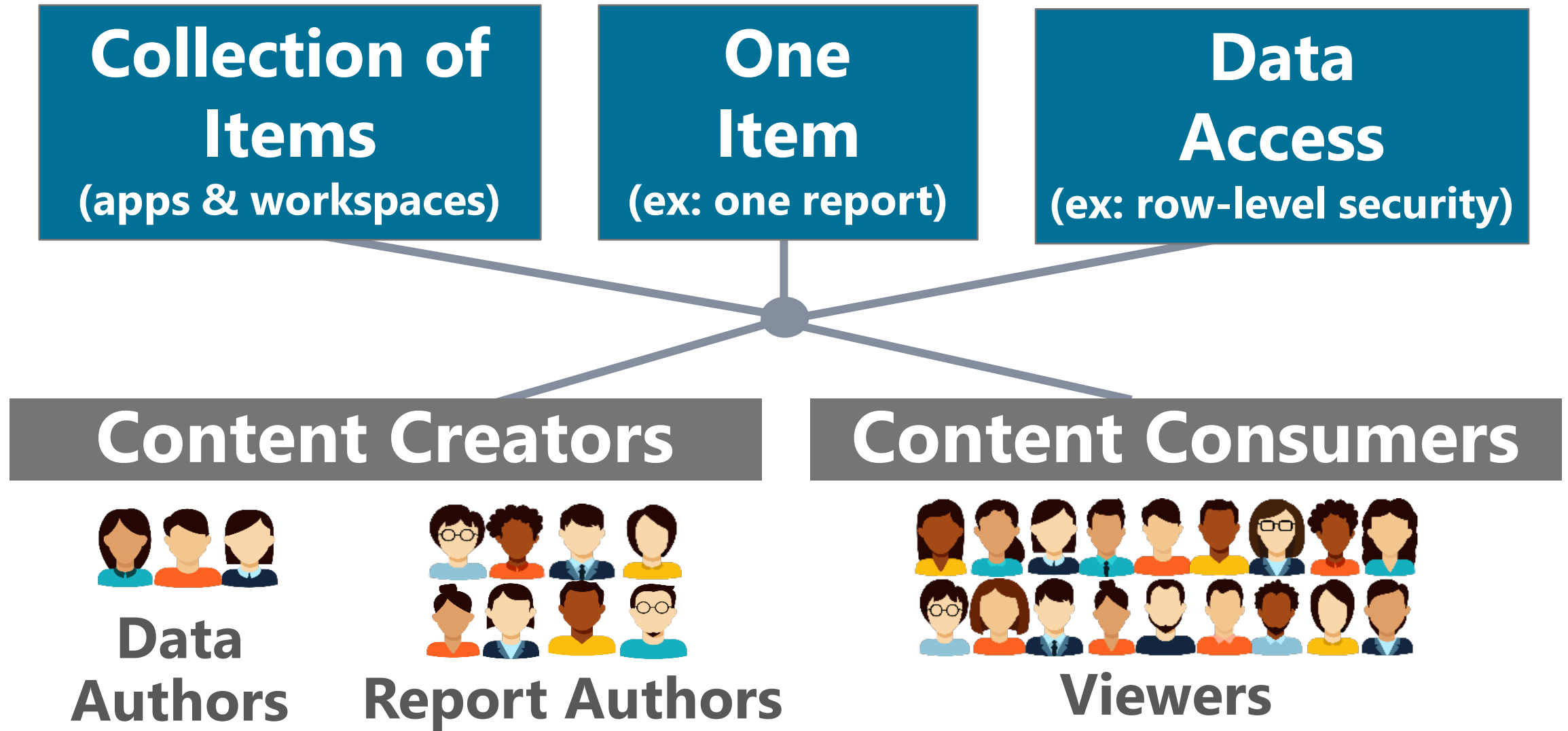


Individual items obtain their permissions one of several ways. Security can be inherited -OR- set directly.





Different Users Have Different Security Needs





It's a Balance

Try to use techniques that balance security needs.

- Follow the principle of least privilege
- Set permissions for a collection of items rather than individual items
- Use groups rather than individual users

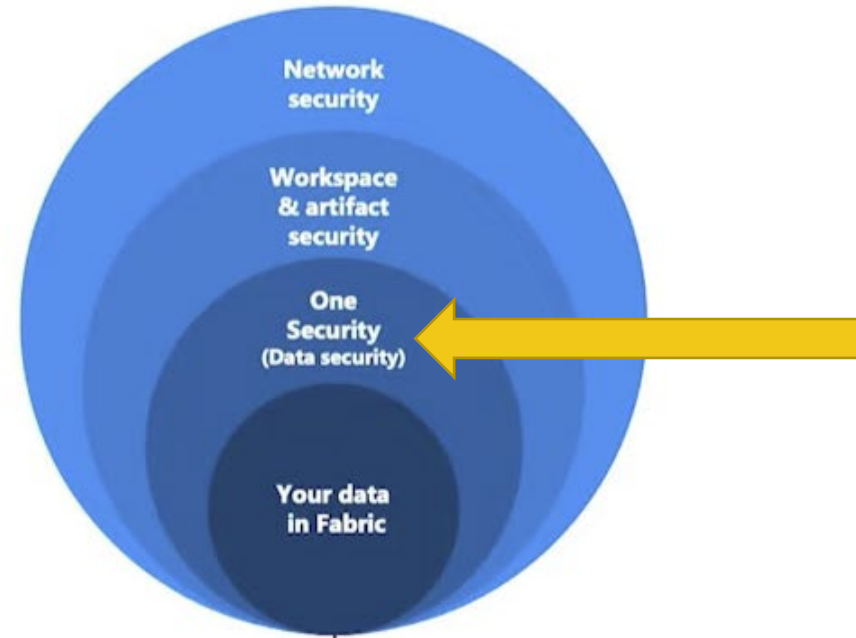




What About OneLake Security?

Pay attention to the OneLake security model announcements that are coming to Fabric. This will be a big deal.

- Define security once in OneLake (on the one copy of data)
- Enforce the same permissions across different data engines and compute workloads



[Image source](#)





Workspace Roles

Admin, Member, Contributor, Viewer
&

Workspace Domains

Admin, Contributor



Two Types of Workspaces



Personal workspace
"My workspace"



One owner



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



Workspace



Four workspace roles



A Fabric administrator can manage permissions for any workspace in the tenant



More Info

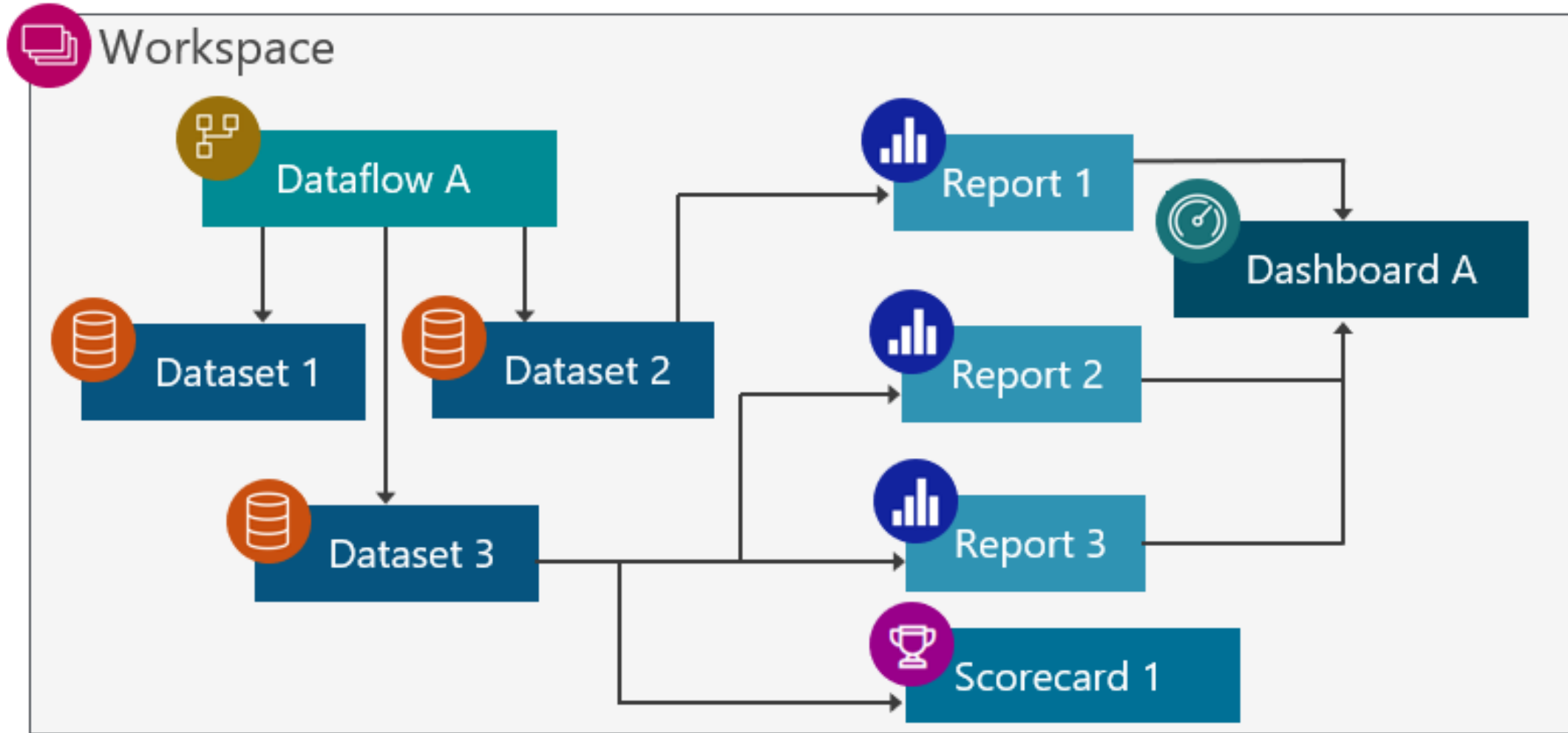
Power BI Implementation Planning: [Workspaces](#)

Melissa's Blog: [Workspace planning](#)



Purpose for Workspaces

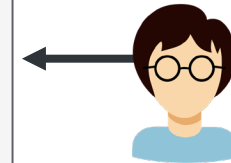
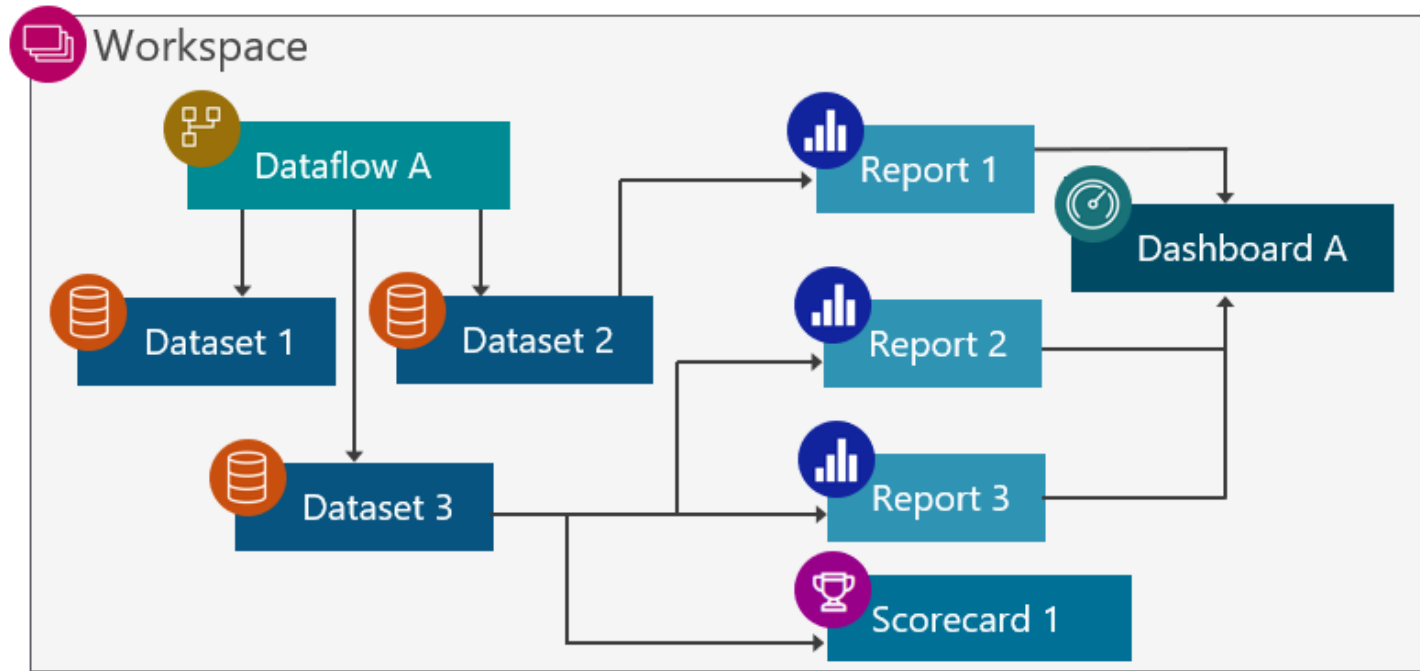
#1: Storage & organization of content





Purpose for Workspaces

#2: Collaboration on content



Tester
Data validation,
QA, UAT



Data model owner
Designs dataset &
manages refresh

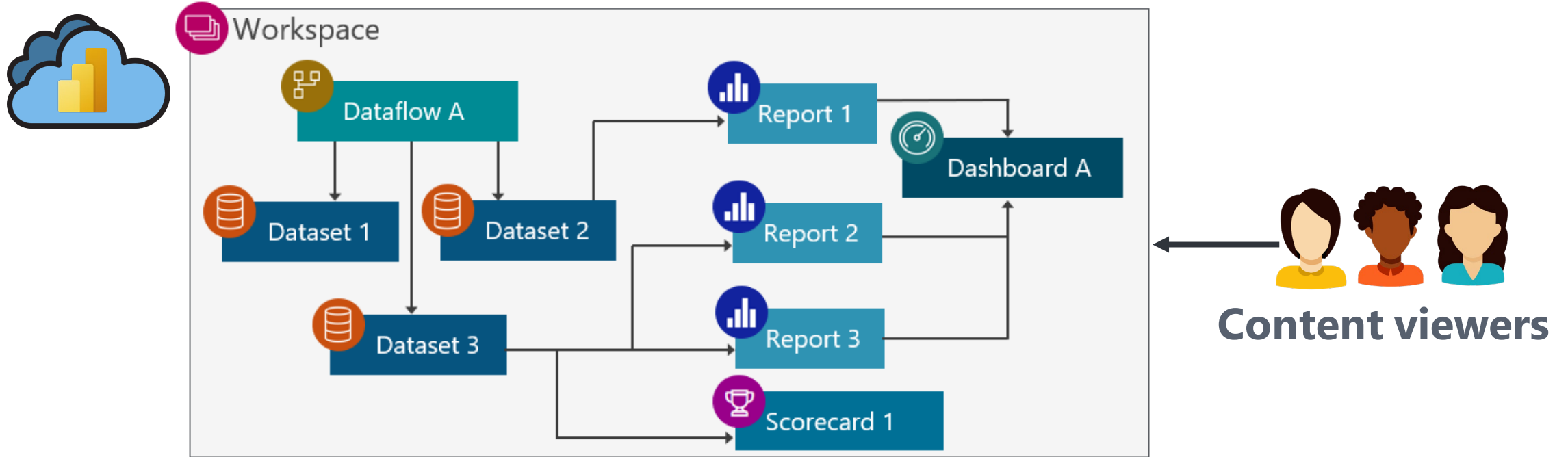


Report owner
Designs visuals



Purpose for Workspaces

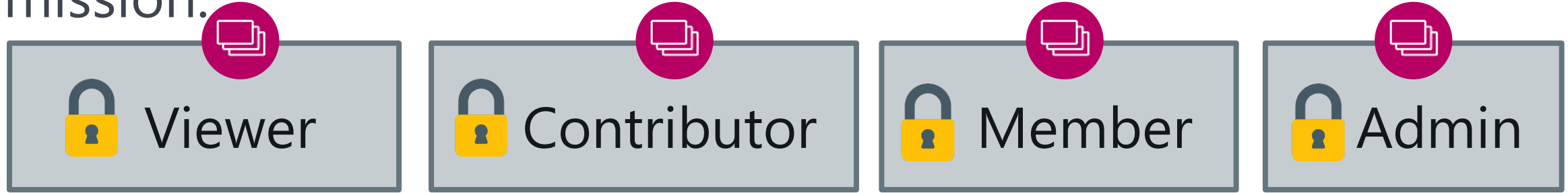
#3: Content distribution for small / informal teams





Four Workspace Roles

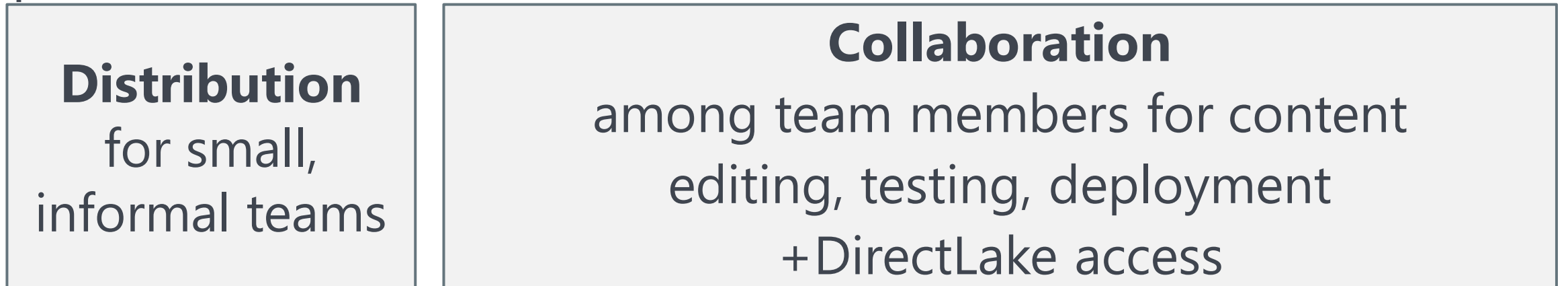
Permission:



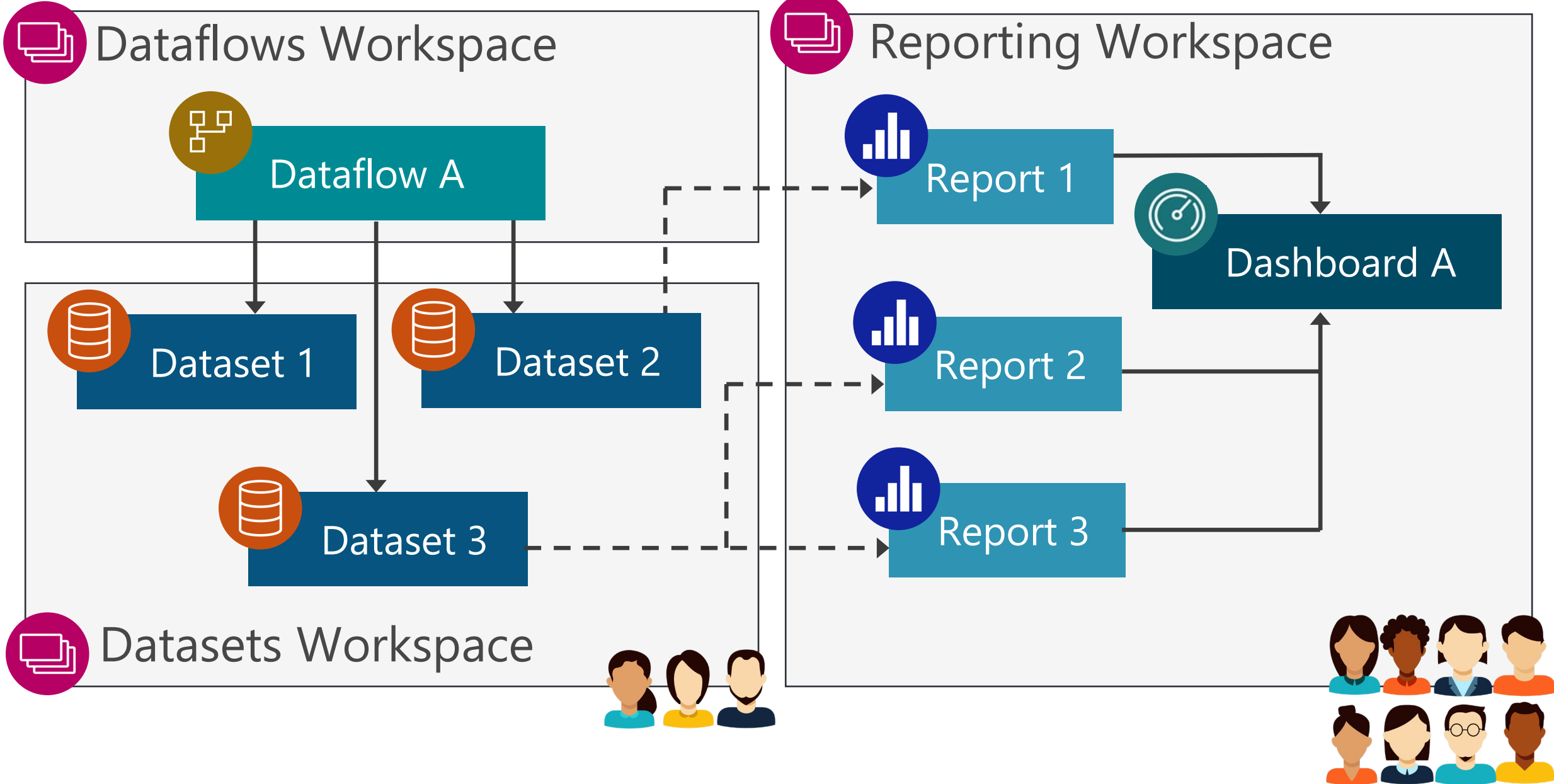
Targeted to:



Purpose:



Workspace Organization Affects Security



Dataset Author Permissions



Data workspace



Sales Data



Dataset authors:

Workspace role:
admin, member
or contributor
OR

The "write"
permission on
the individual
dataset



Report workspace



YTD Sales Revenue

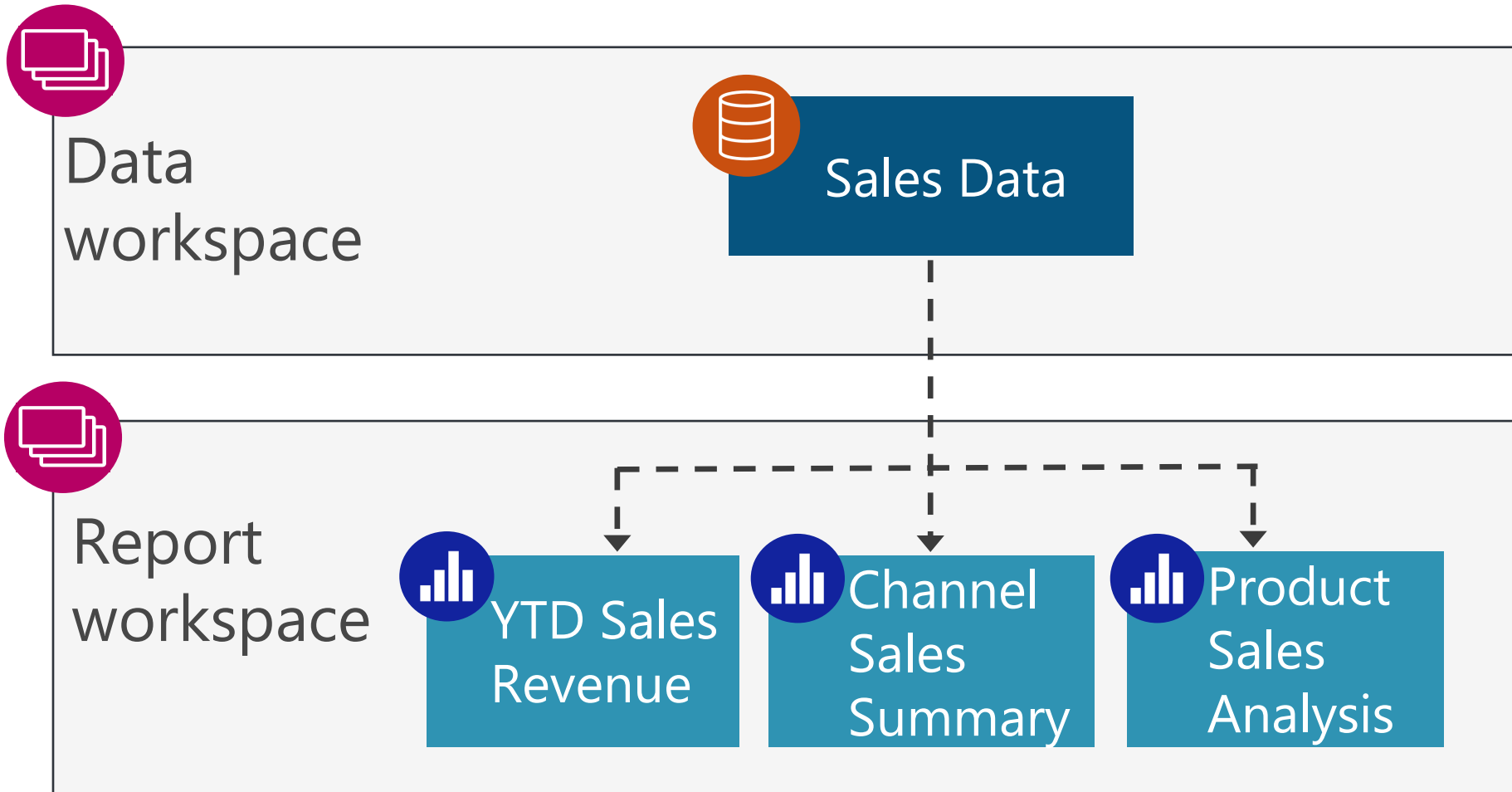


Channel Sales Summary



Product Sales Analysis

Report Author Permissions



Report authors:

Build on the dataset

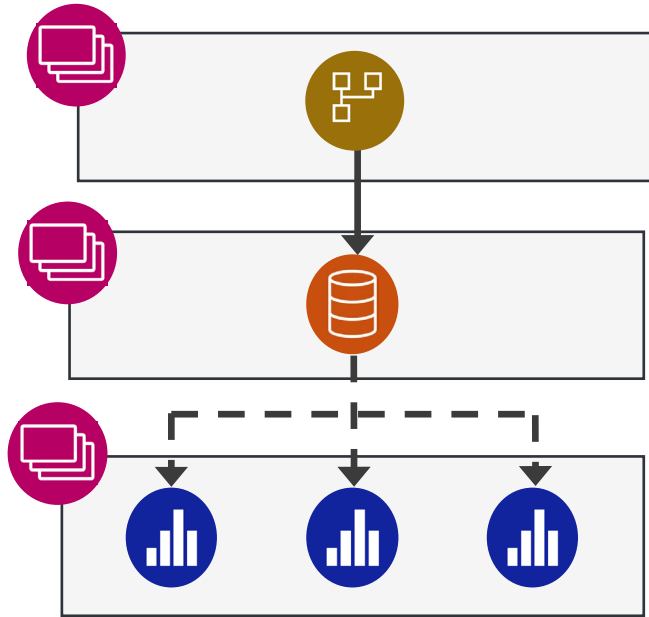


+

Workspace role:
admin, member
or contributor



Security Advantages of Separating Workspaces



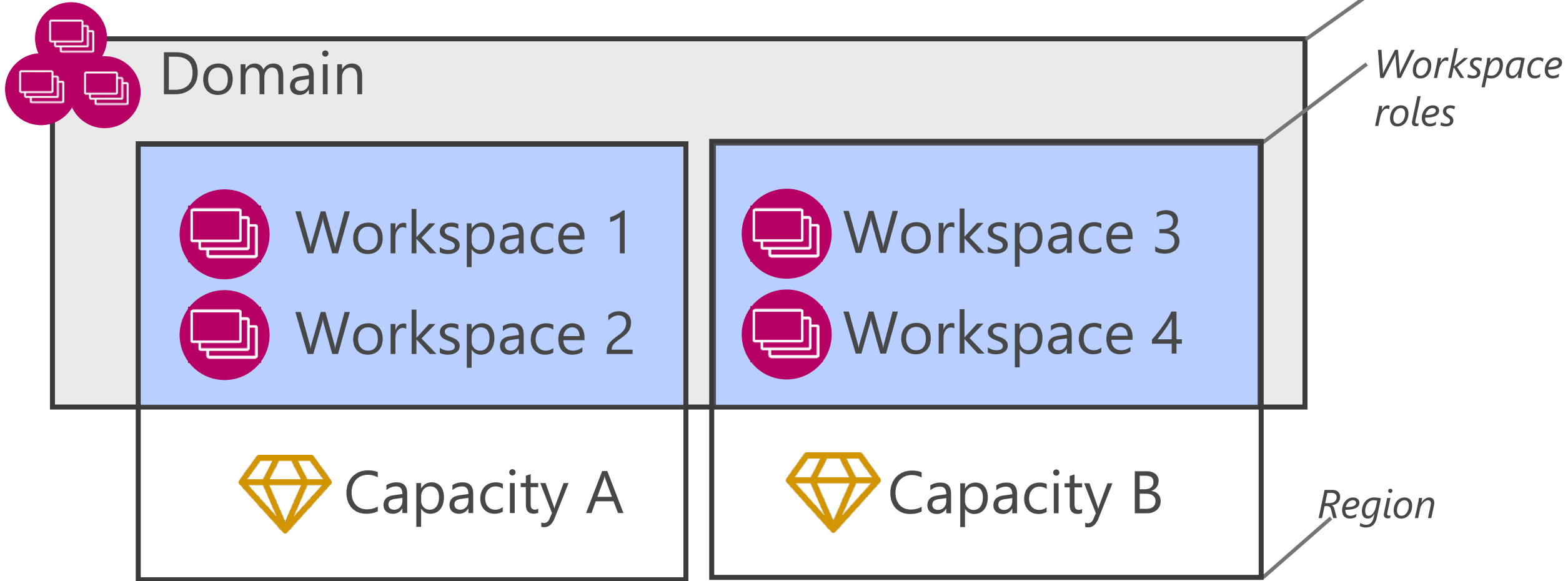
- Clarity on who may edit vs. view: helpful when separate people are responsible for data vs. reports (or dataflows vs. datasets)
- No over-provisioning of permissions; no reliance on the “honor system” for who may edit content
- Row-level and object-level security works for report authors who only have view permissions on the dataset

More info: CoatesDS.com/blog/5-tips-for-separating-power-bi-datasets-and-reports



Workspace Domains

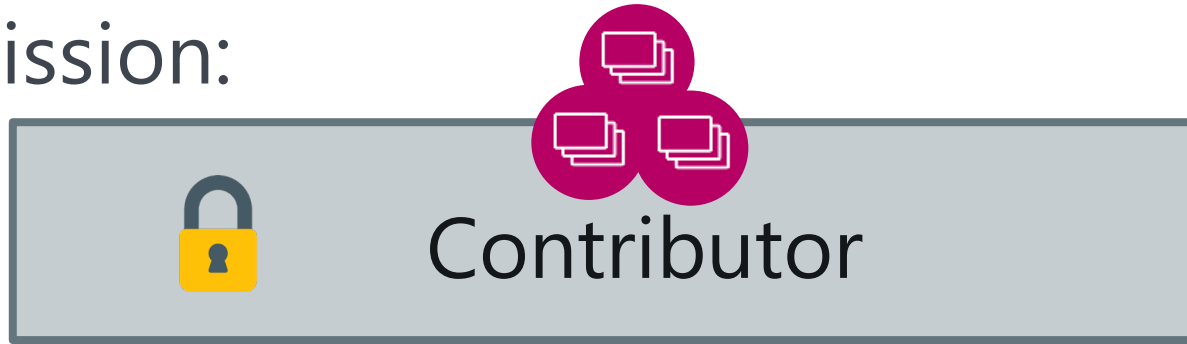
A logical grouping of Fabric workspaces





Two Domain Roles

Permission:



A grey rectangular box representing the Contributor role. On the left is a yellow padlock icon. In the center is the word "Contributor". Above the text are three overlapping pink circles, each containing a white icon of a document with a checkmark.



A grey rectangular box representing the Admin role. On the left is a yellow padlock icon. In the center is the word "Admin". Above the text are three overlapping pink circles, each containing a white icon of a document with a checkmark.

Targeted to:

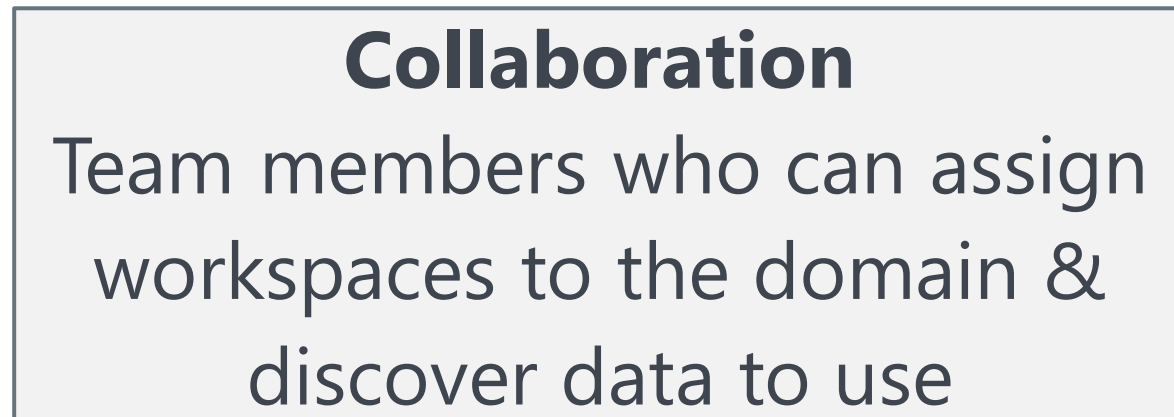


A teal rectangular box representing the target audience for the Contributor role. On the left is a small icon of a man's head and shoulders. In the center is the text "Content creators".

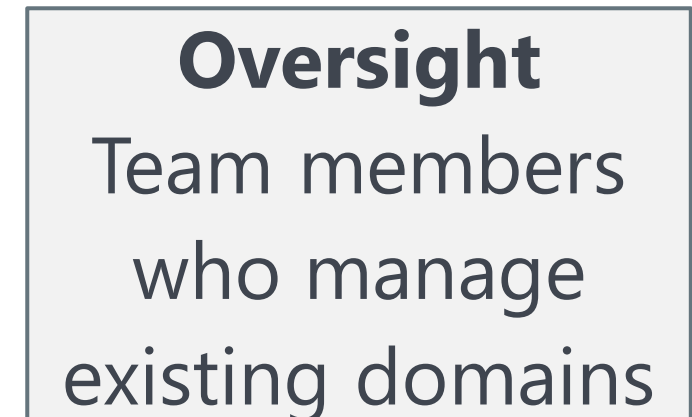


A purple rectangular box representing the target audience for the Admin role. On the left is a small icon of a woman's head and shoulders. In the center is the text "Content admins".

Purpose:



A light grey rectangular box representing the purpose of the Contributor role. It contains the word "Collaboration" in bold, followed by the text "Team members who can assign workspaces to the domain & discover data to use".



A light grey rectangular box representing the purpose of the Admin role. It contains the word "Oversight" in bold, followed by the text "Team members who manage existing domains".



Common Ways to Use Domains

Subject Areas:

Sales

Finance

Marketing

Responsibility/Ownership:

IT

Functional Area

Business Unit:

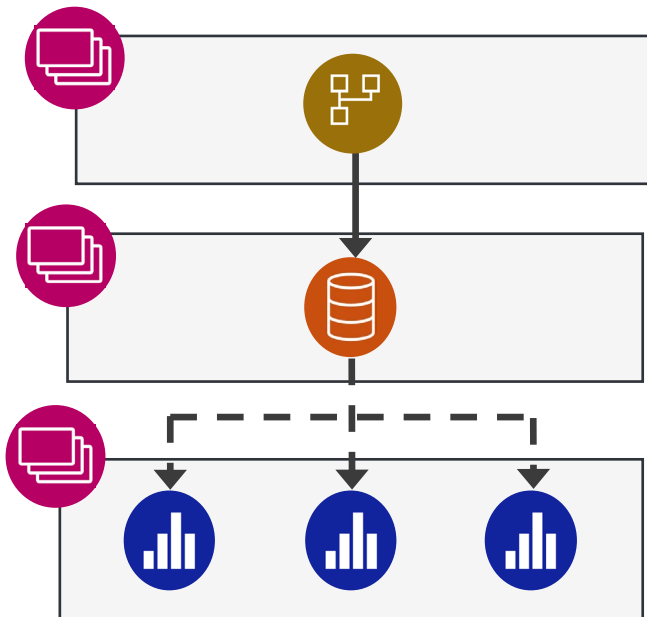
US Division

European Division



Key Takeaways

Workspace roles are inherited by everything else so it's critical to get them right.



Your ability to support different types of users, with different needs, starts with good workspace organization.



Key Takeaways



Don't store mission critical content in personal workspaces!



Use standard workspace roles for managing Team BI, Departmental BI, and Enterprise BI content.



App Audiences

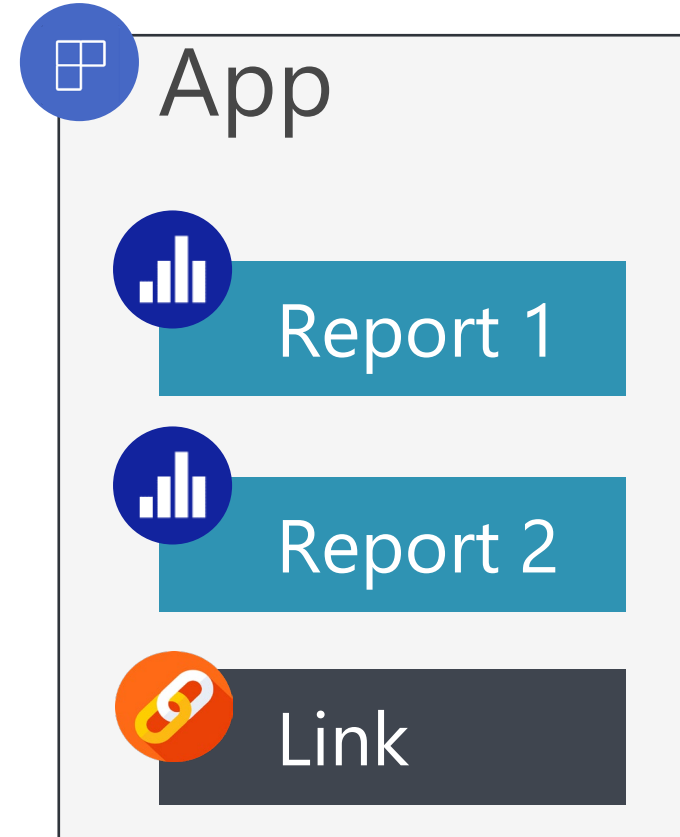
Permissions for organizational apps



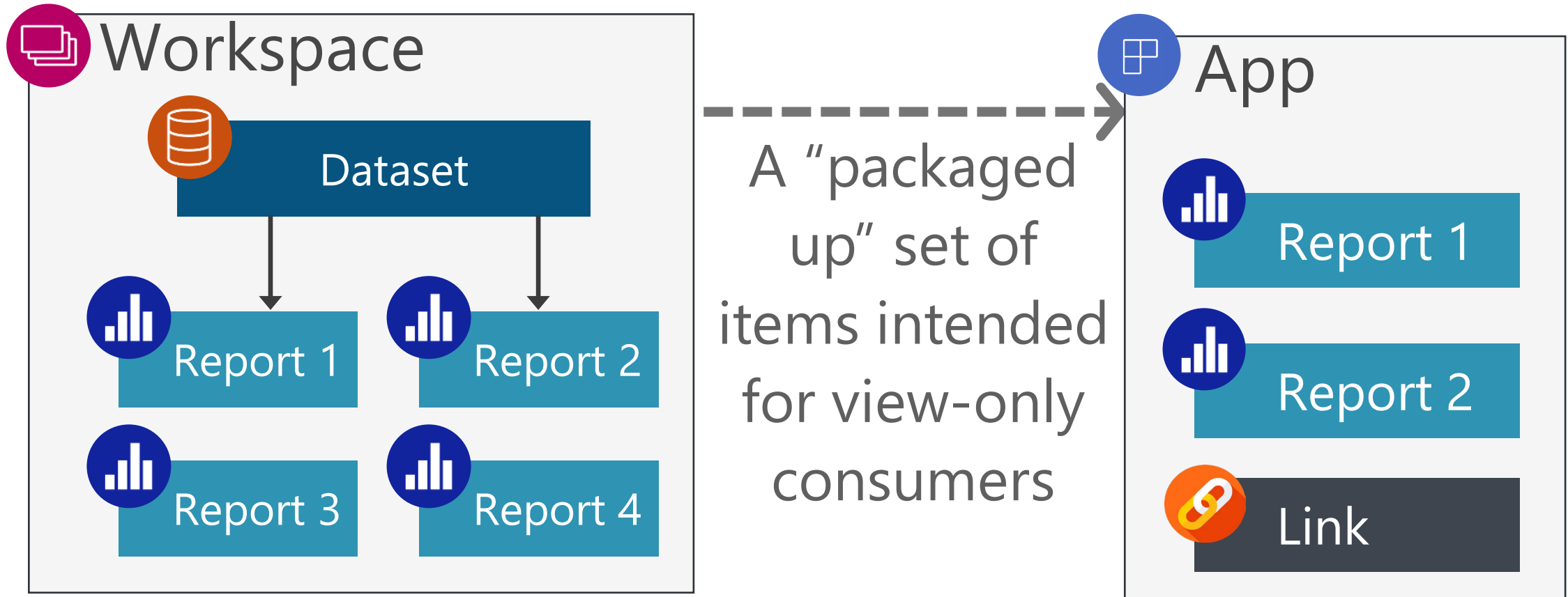
Purpose for Organizational Apps

Broad content distribution scenarios
to a large # of people

More formal content distribution
scenarios

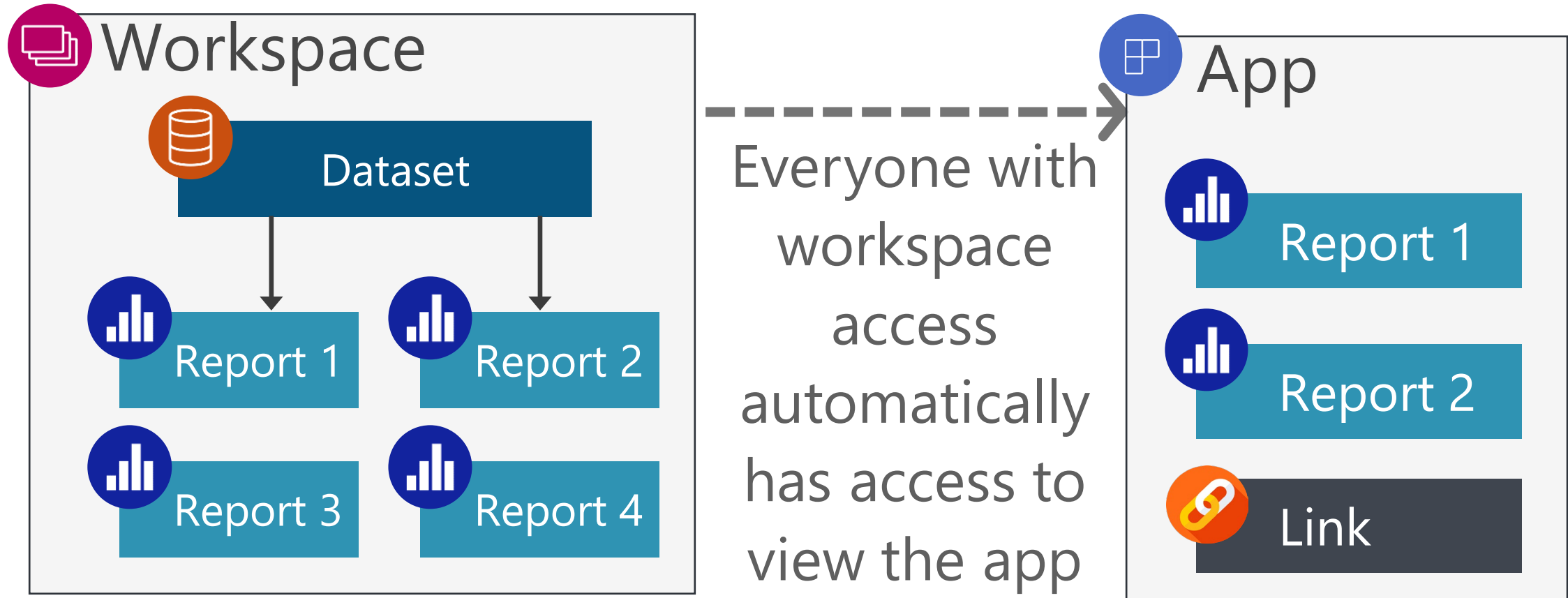


One App Exists Per Workspace

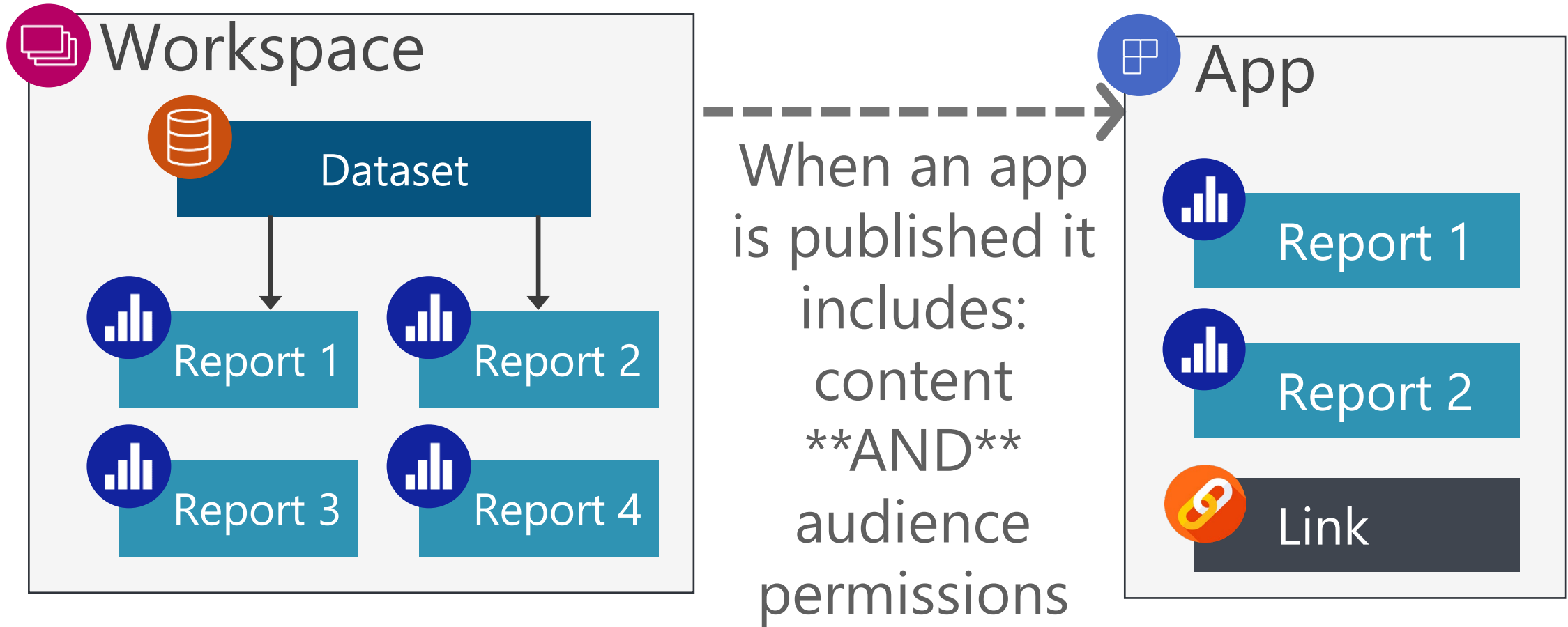




Workspace Roles are 'Sort Of' Inherited

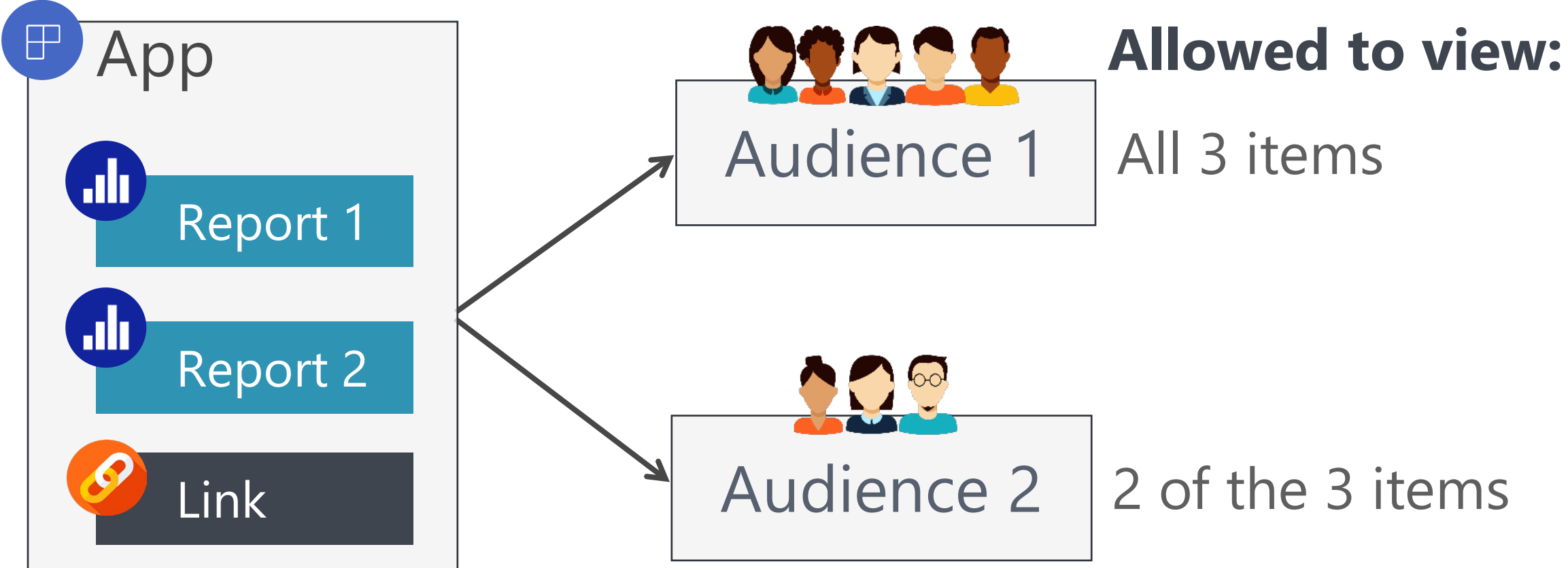


Permissions & Content are Deployed Together



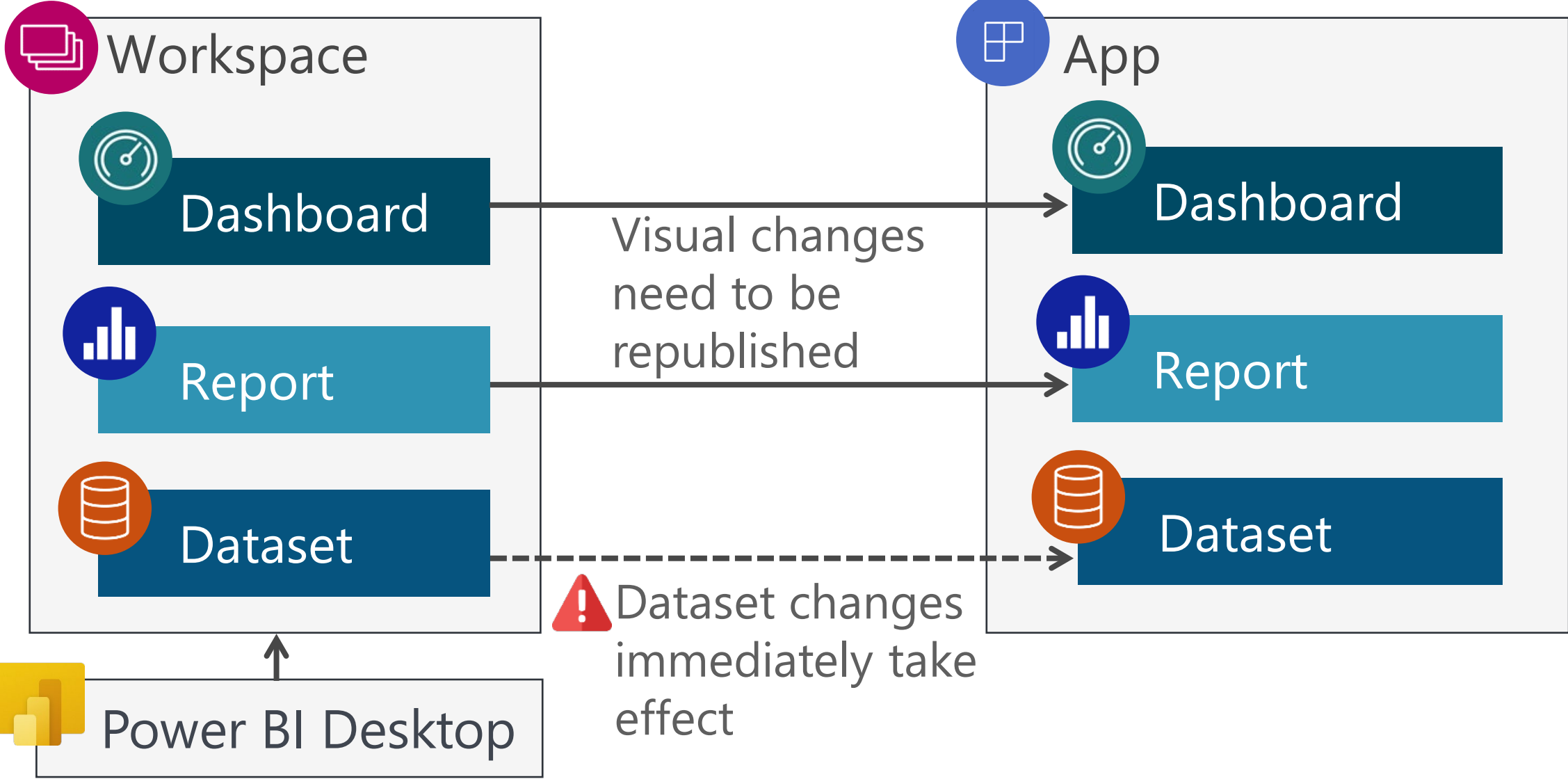


Audiences: Mix & Match Consumers & Content





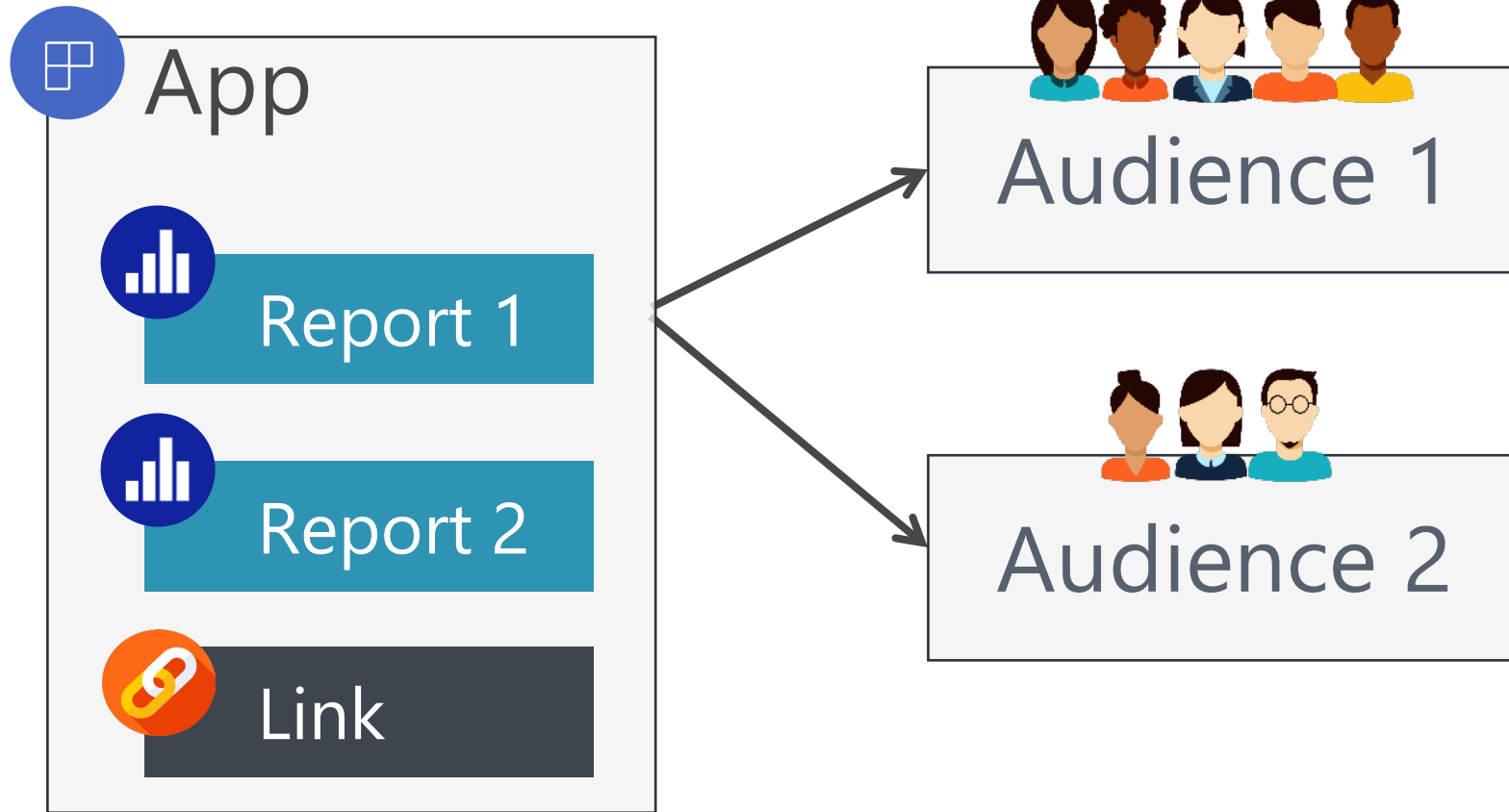
Apps: Watch Out For





Key Takeaways

Simplify workspace design. Use app audiences to “mix and match” who is allowed to view what content:

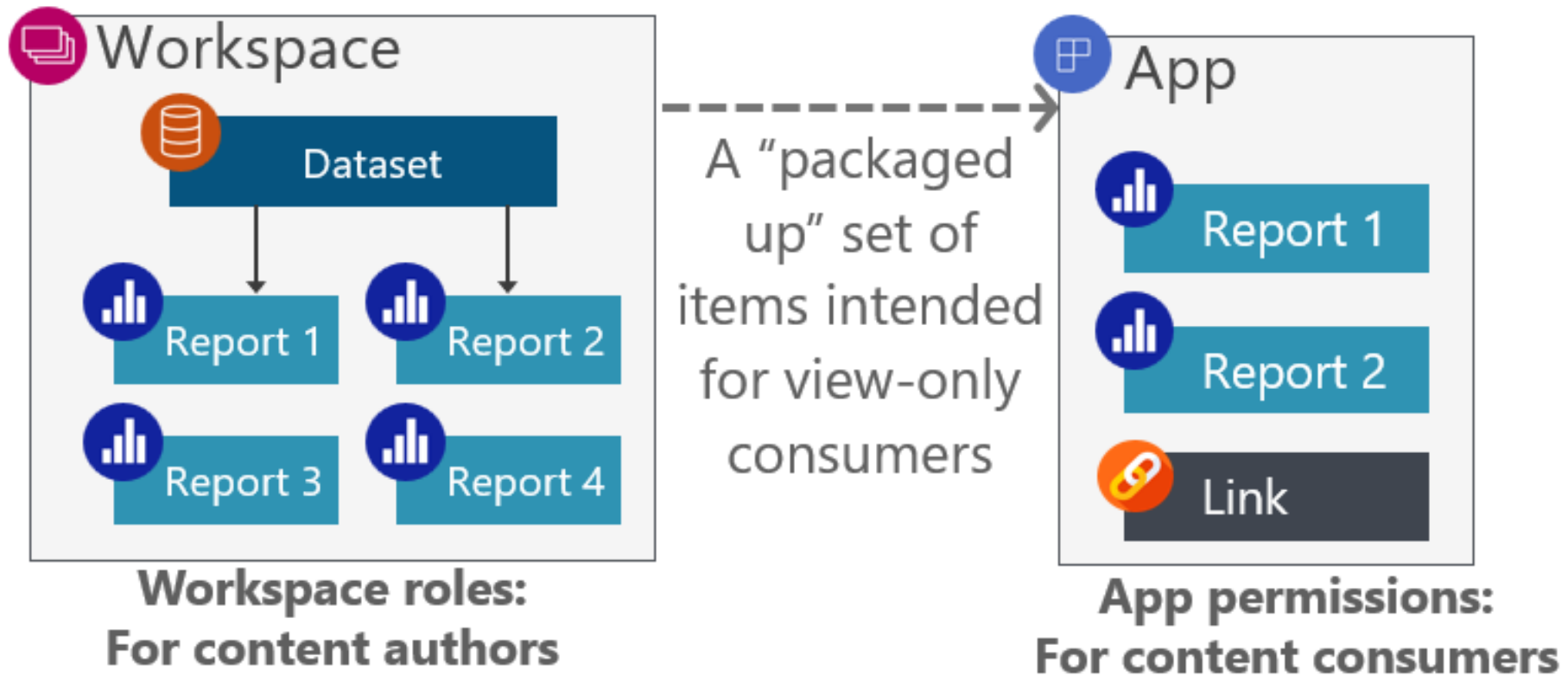


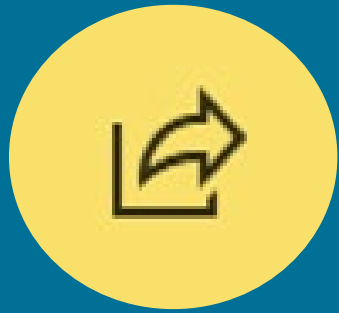


Key Takeaways

Use app audiences to provide security to content *consumers*.

Use workspace roles for content *creators*.












Per-Item Permissions

Sometimes called 'sharing'



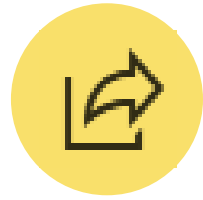
Purpose for Per-Item Permissions

Assign permissions directly to an individual item.

 Reports	 Datasets
 Dashboards	 Dataflows
 Scorecards	 Datamarts
 Workbooks	



When to Use Per-Item Permissions



Per-item permissions are most suitable when:

You want to provide access to only 1 item

BECAUSE

You *don't* want the recipient to view/edit everything in workspace

OR

You *don't* want the recipient to view everything in an app



Think of item permissions as an 'exception' to workspace roles



Per-item permissions: reports



Two Types of Report-Level Permissions

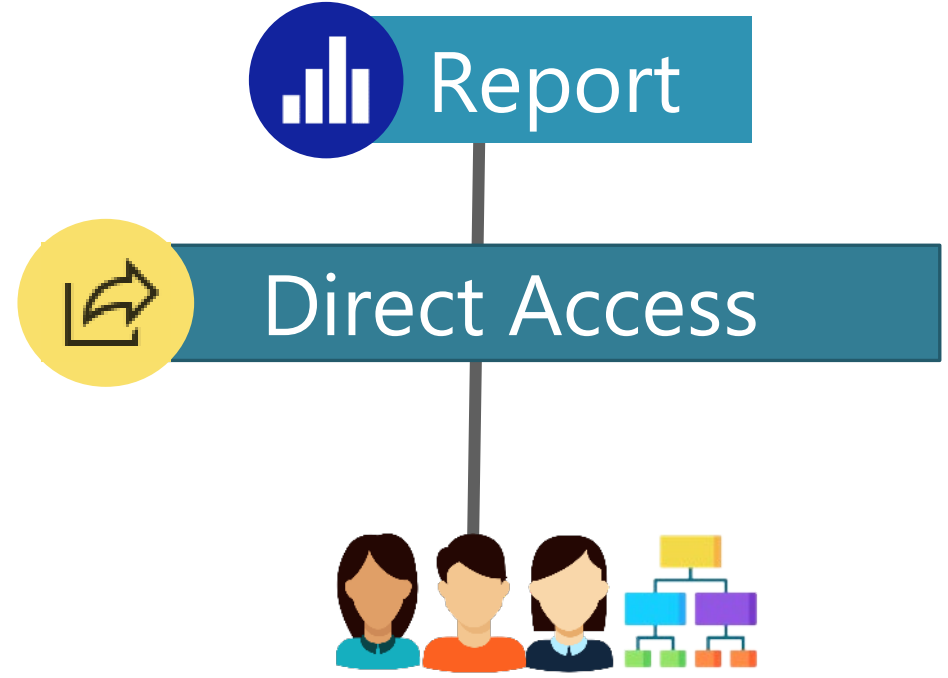
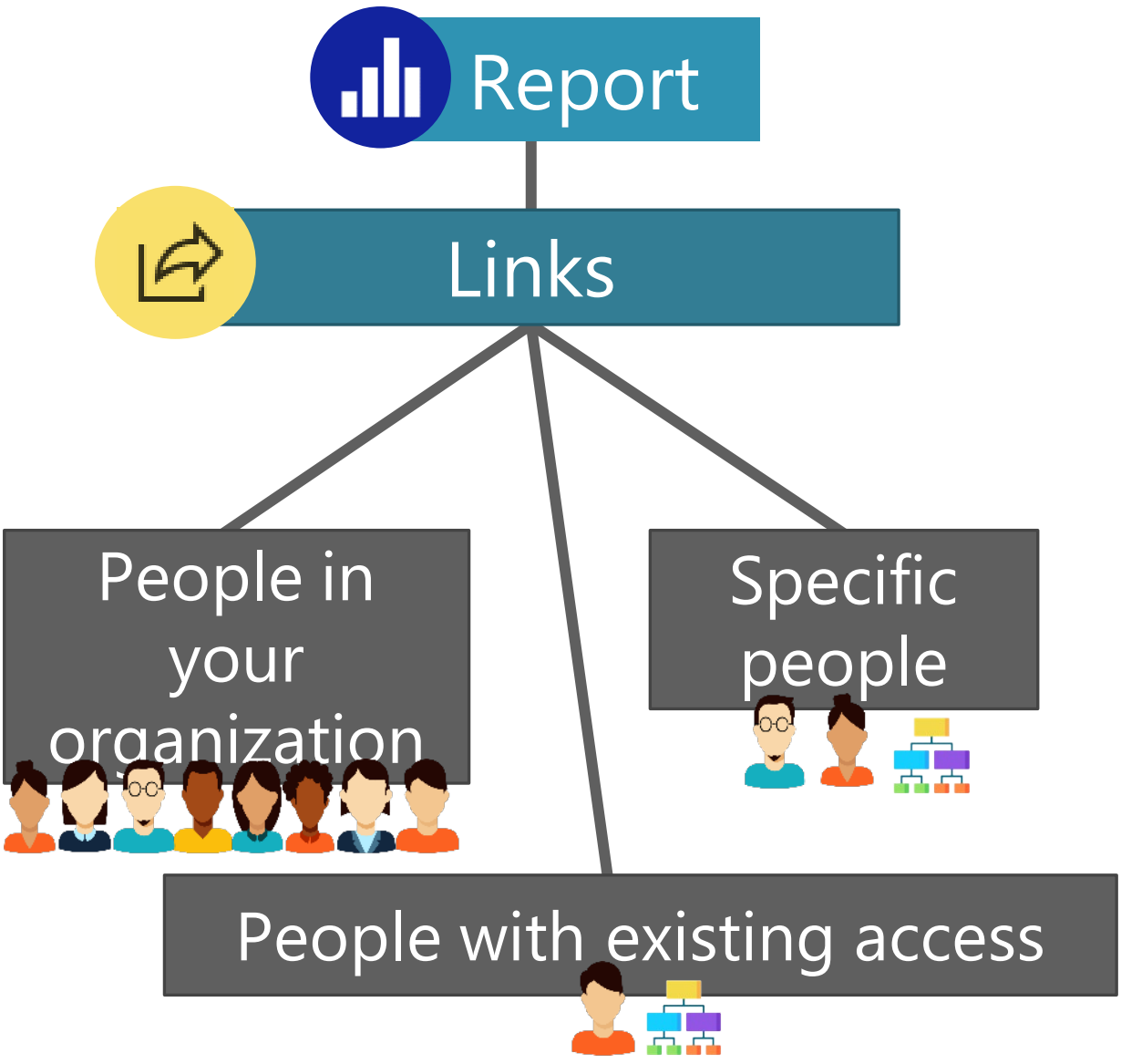


Chart Sharing



 Report

 Chart Sharing: Link to Selection

 Shared View

People with existing access






Per-Item Report Permissions

Permission:



 Read



 Reshare

Targeted to:



Report consumers



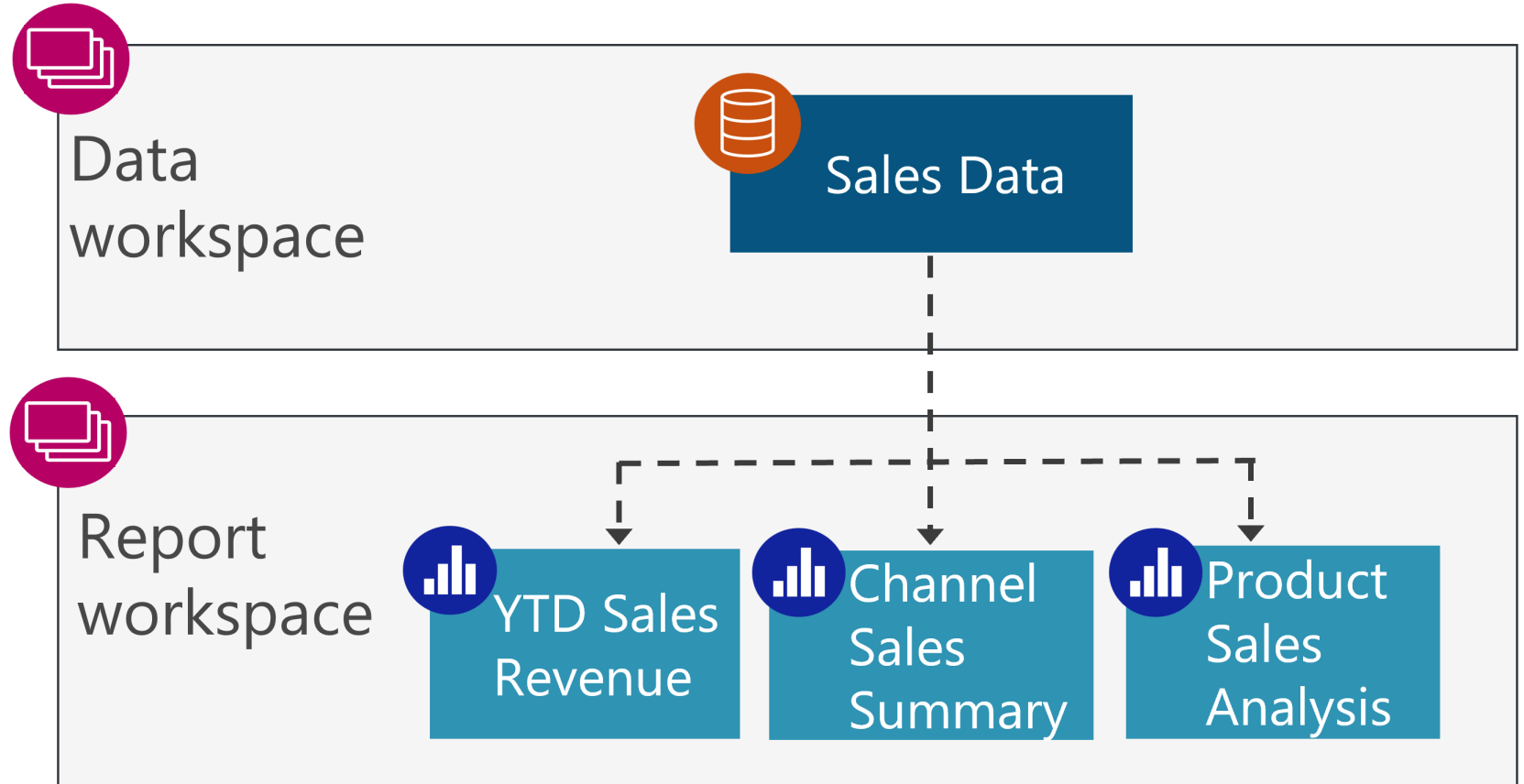
Report consumers allowed to freely reshare



Key Takeaways

Per-item *report* permissions focus on *consumers*.

To support *report authors*:
instead use
workspace
permissions for
the reports +
read/build
permissions for
the dataset





Per-item permissions:
datasets



Shared Datasets

Intended for reuse by reports & models



Shared dataset:



Live Connection

Analyze In Excel

DirectQuery
(Composite Model)



Reports & composite models:



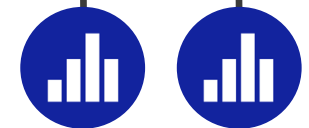
Power BI report



Paginated report



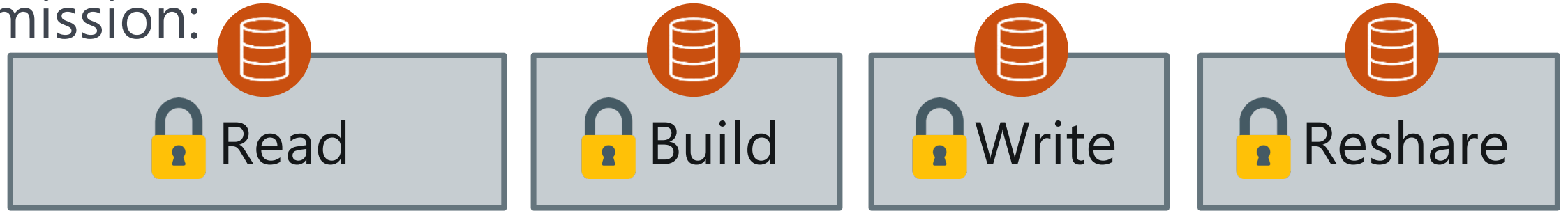
Excel report





Per-Item Dataset Permissions

Permission:



Targeted to:

 Report consumers

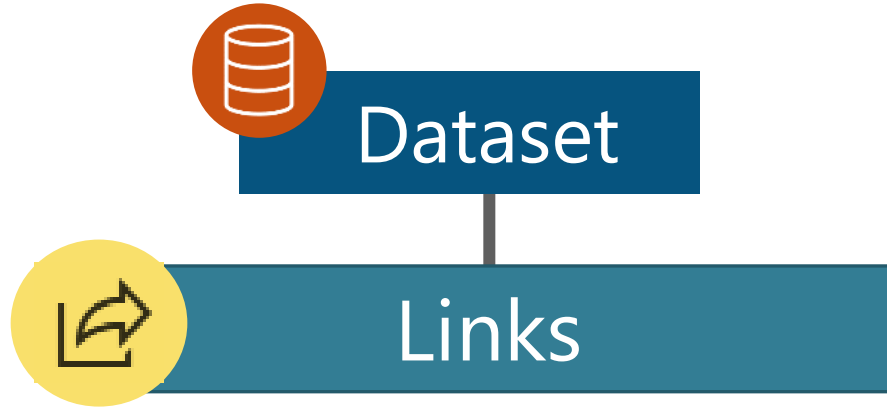
 Report creators

 Dataset creators

 Consumers & creators allowed to freely reshare the data

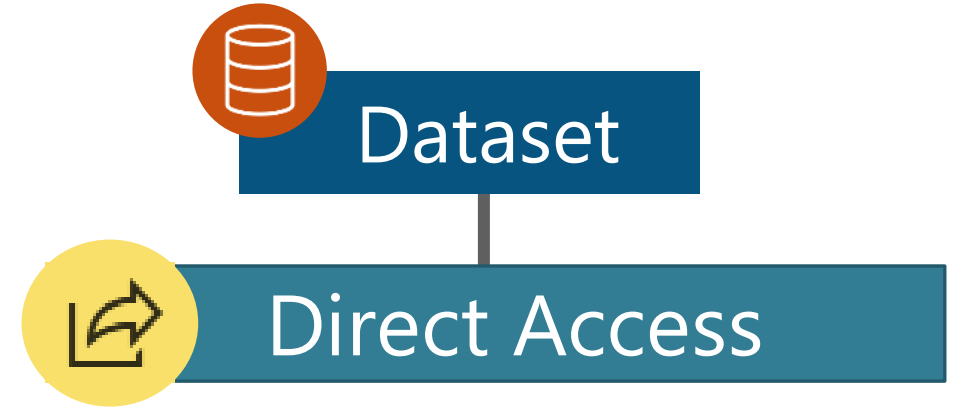


Two Types of Dataset-Level Permissions



Inherited only: links CANNOT be configured directly for a dataset

Stays 'tightly coupled'



Can be configured directly for a dataset

NOT 'tightly coupled'



Key Takeaways



Report



Dataset

For both *creators* and *consumers*, there are always multiple levels of permissions to account for.

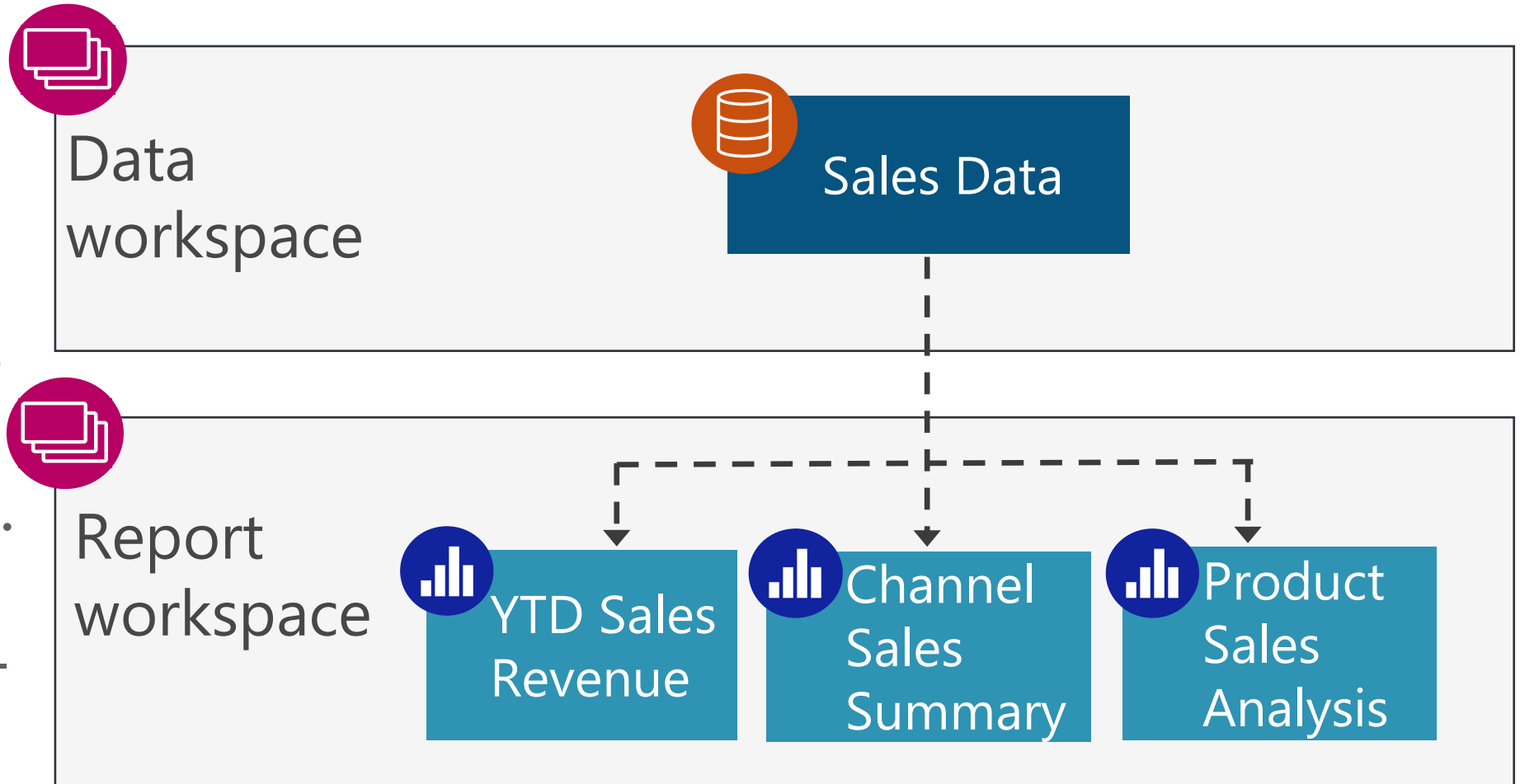
Sometimes report and dataset permissions are 'tightly coupled' and sometimes they're not.





Key Takeaways

To support *dataset authors*: workspace permissions are usually appropriate. There's also the dataset-level *write* permission.





Strategies & Suggestions

Multiple Layers of Security

Prior to OneLake Security
that's coming to Fabric



Collection of Items



Workspace Roles



App Permissions

Individual Items: Visuals



Reports
└ Charts



Dashboards



Paginated
Reports



Scorecards
└ Metrics



~~Workbooks~~

Individual Items: Data



Lakehouse



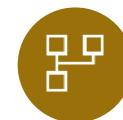
Warehouse



Datasets



Datamarts



~~Dataflows~~

Data Results
Per User



Row-Level Security



Object-Level Security

Other

Data Sources, Gateways,
Cross-Tenant Sharing etc...

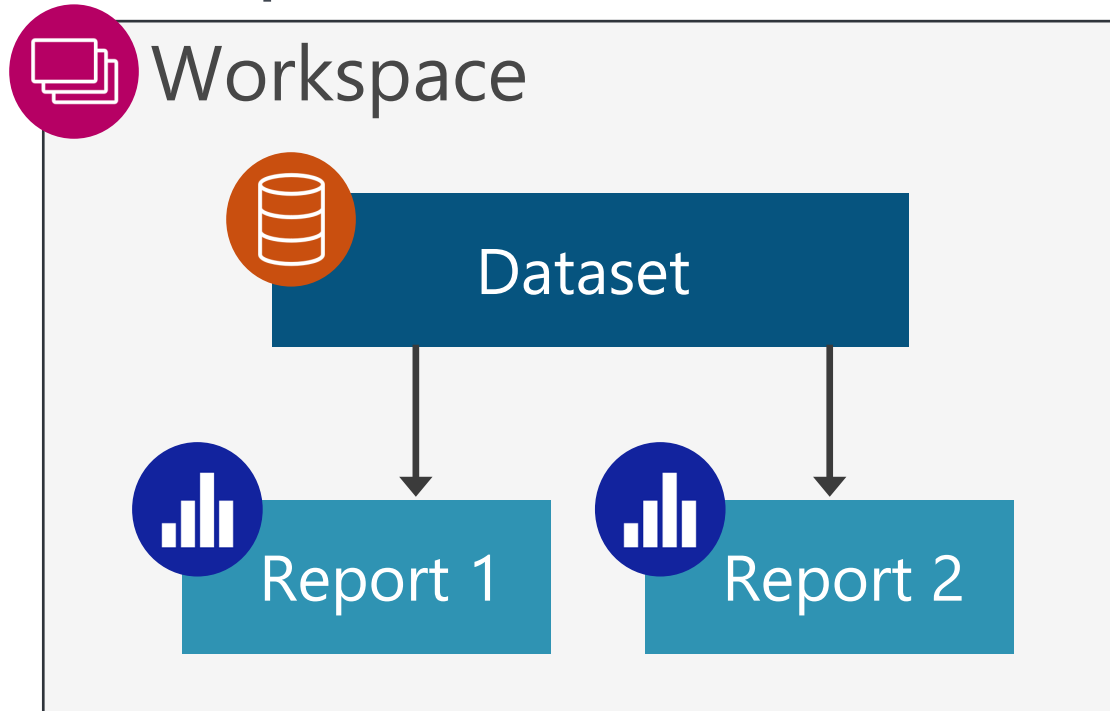
Item crossed out = no per-item permissions available



Multiple Layers of Security

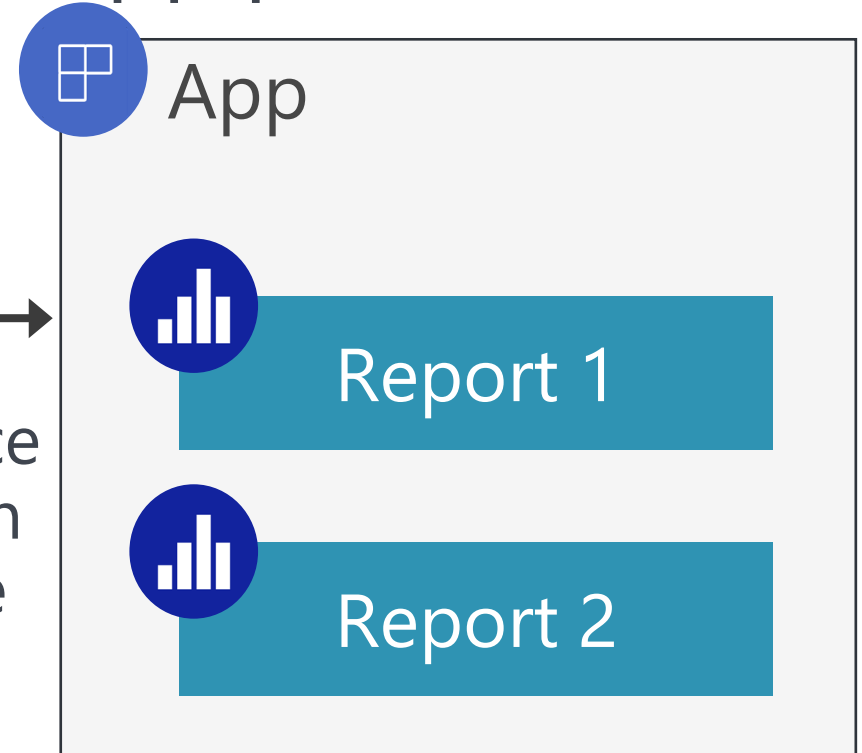
Permissions for a Collection of Items

Workspace roles:



Workspace roles: Admin, member, contributor, viewer

App permissions:

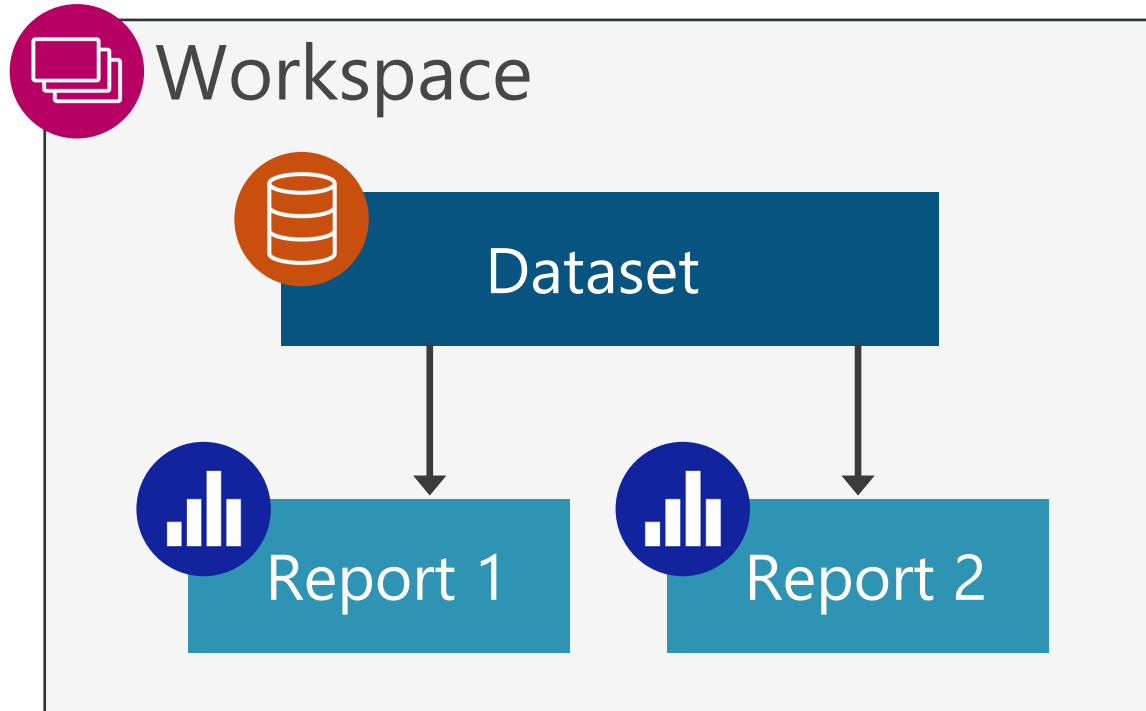


App permissions: Read (view only)

All workspace users can view the app

Multiple Layers of Security

Permissions for Individual Items



- Per-item permissions can be:
- Assigned to (most) items
 - Inherited from workspace roles and apps
 - Links or direct access

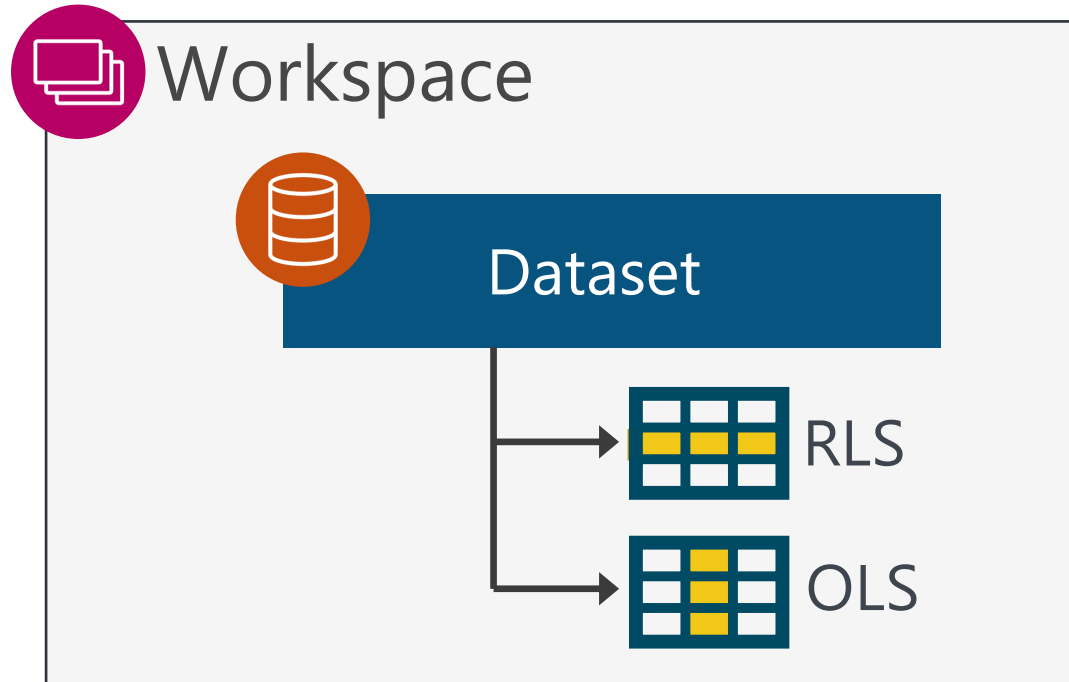


Multiple Layers of Security

Different Data Results Based on User Identity

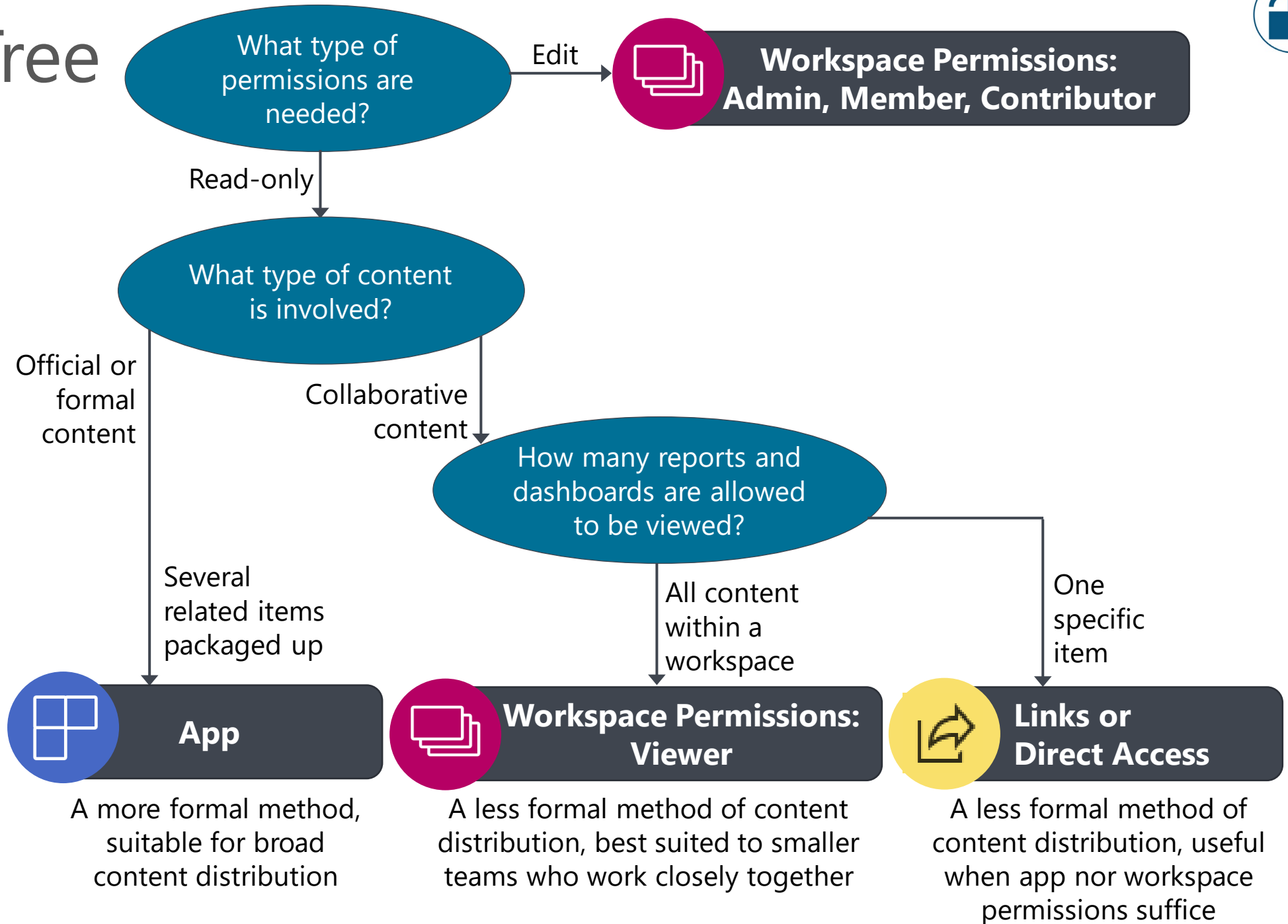
Row-level security: which rows a user sees

Object-level security: which columns a user sees



The presence of RLS changes the default behavior of what a user sees in a model: no data vs. all data

Decision Tree



Adapted from:
[Planning a Power BI Enterprise Deployment Whitepaper](#)

Co-authored by
Melissa Coates &
Chris Webb

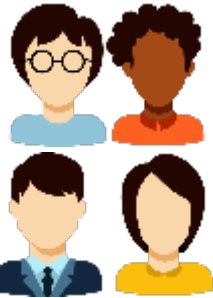


Permissions Based on Type of Audience



Large Teams and Broad Distribution

Apps are usually the best situation, especially for people who do not work closely together.



Small Teams

Either workspace or app.
Depends on if the additional layer of an app is desirable.



Per-Item Sharing

Valid option for small # of people if you don't want recipient to see everything in the workspace or the app.
Should be last option, not first.



Exact Audience Is Not Known

Template apps can work if you don't know audience.



When to Use Workspace & App Permissions



Workspace

Limit access to the workspace to those who are handling:

- Authoring
- Development
- Data validations
- Quality assurance (QA)
- User acceptance testing (UAT)



App

Provide access via an app for:

- Read-only consumers



Managing Permissions for Consumers



1st choice: App permissions

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



2nd choice: Workspace viewer permissions

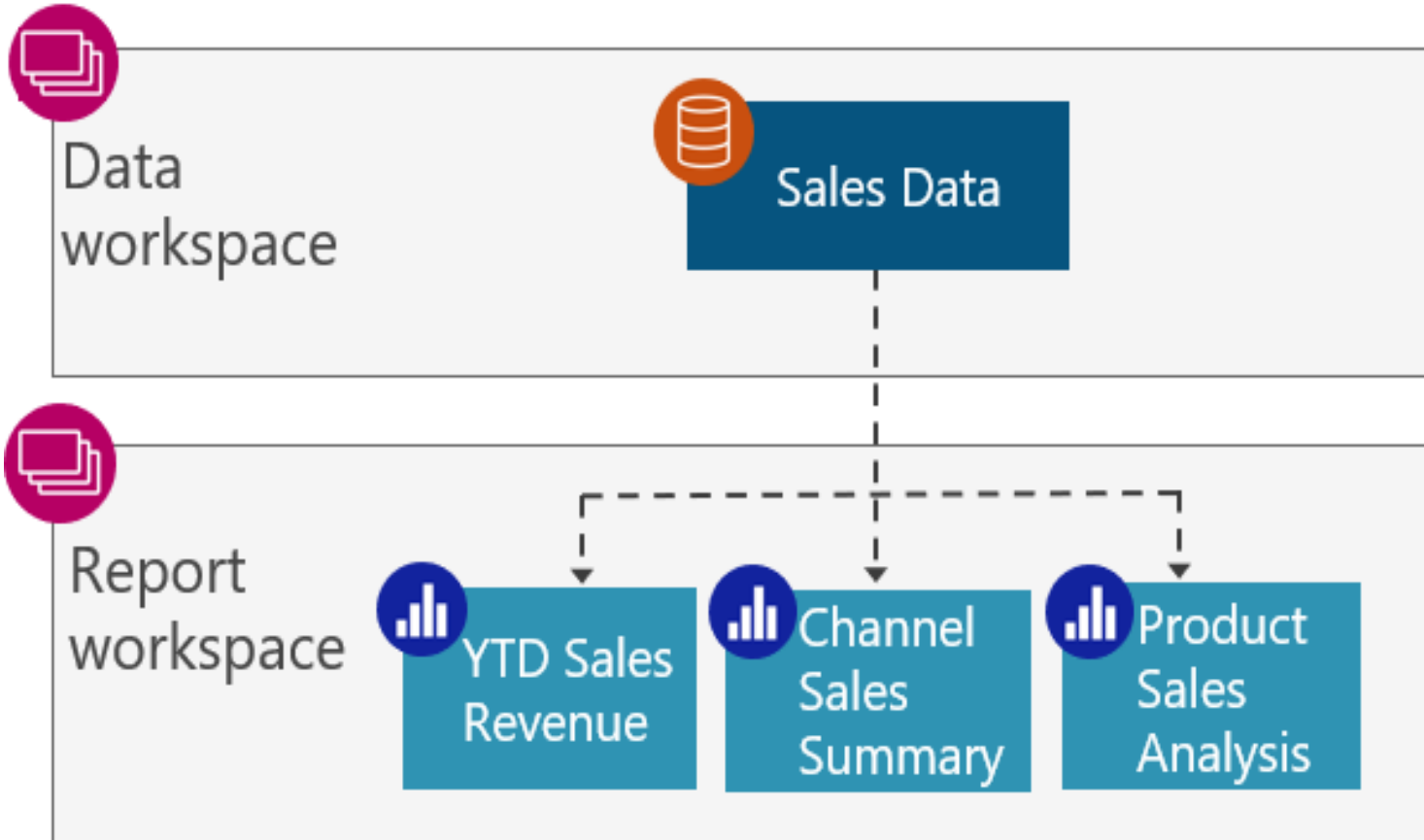
Suitable for small teams that don't need an app & when viewers are allowed to see everything in the workspace.



3rd choice: Per-item sharing

Links or direct access per individual item. Consider sharing to be an 'exception' to workspace roles since it's maintained for every item.

Managing Permissions for Content Creators



Dataset authors:

Workspace role (admin, member, contributor)
OR dataset write



Report authors:

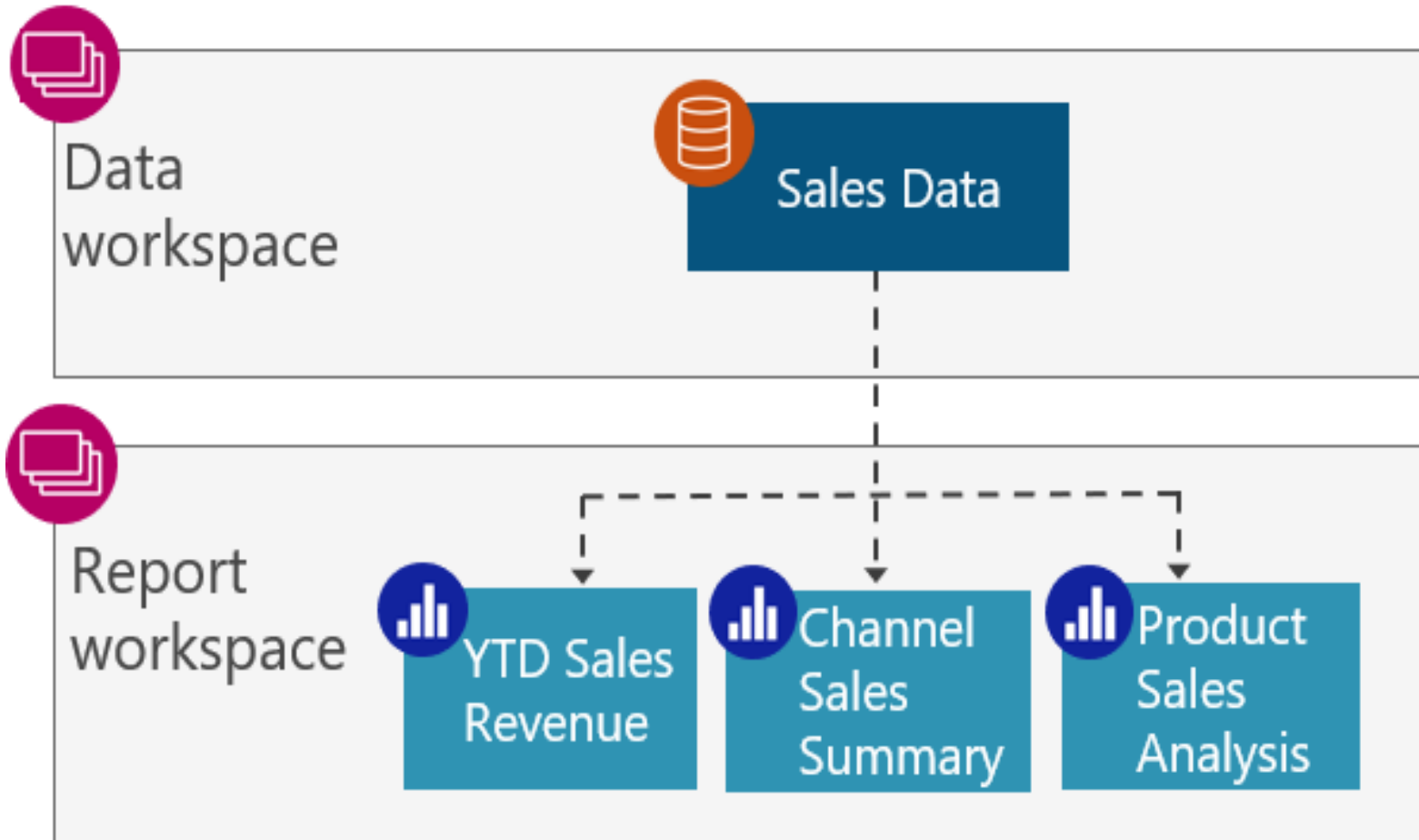
Build on the dataset
+

Workspace role (admin, member, contributor)





Managing Permissions for Content Creators

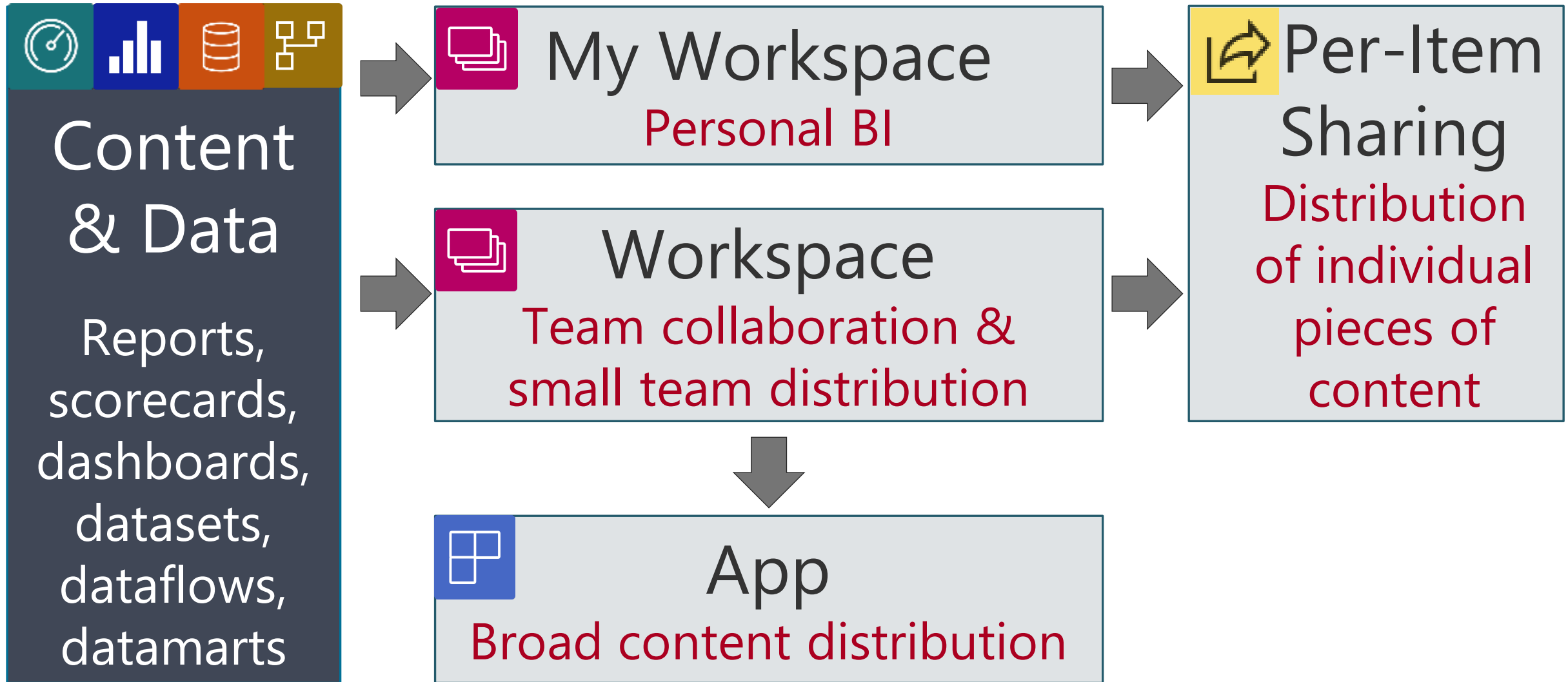


◀ **Build allows a user to:**
Create a new report*
Create a composite model**
Use Analyze in Excel
Query with XMLA endpoint

*Using that dataset in Live Connection mode

**Using that dataset in DirectQuery mode

Primary Purpose for Each





Q&A

More Information from Melissa Coates



Slides:

CoatesDS.com/Presentations



Diagrams:

CoatesDS.com/Diagrams



Power BI Governance Training:

CoatesDS.com/Training



Blog:

CoatesDS.com/Blog-Posts



YouTube:

YouTube.com/CoatesDataStrategies



Social Media:

[LinkedIn](#) | [Mastodon](#)