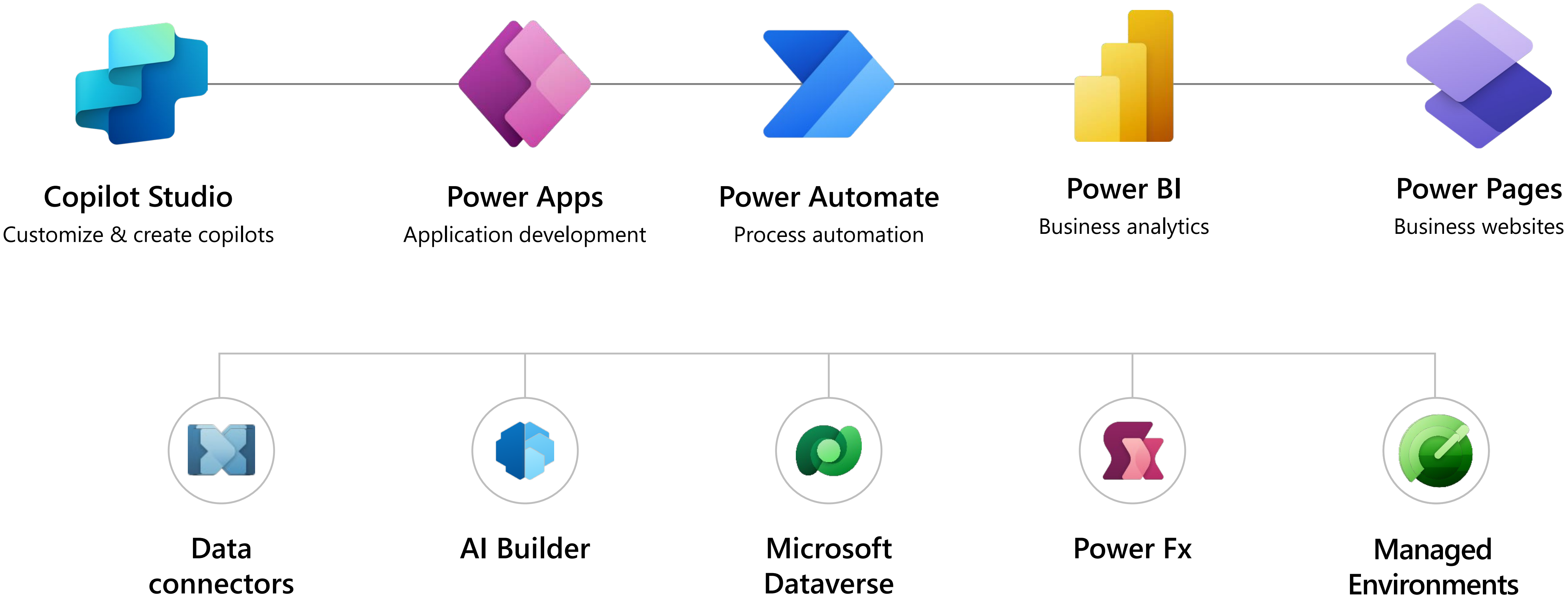
Dataverse Security

Learn how to safeguard your data in Dataverse with effective security practices

Microsoft Power Platform

The most complete low-code platform



Copilot Studio
Customize & create copilots

Power Apps
Application development

Power Automate
Process automation

Power BI
Business analytics

Power Pages
Business websites

Data connectors

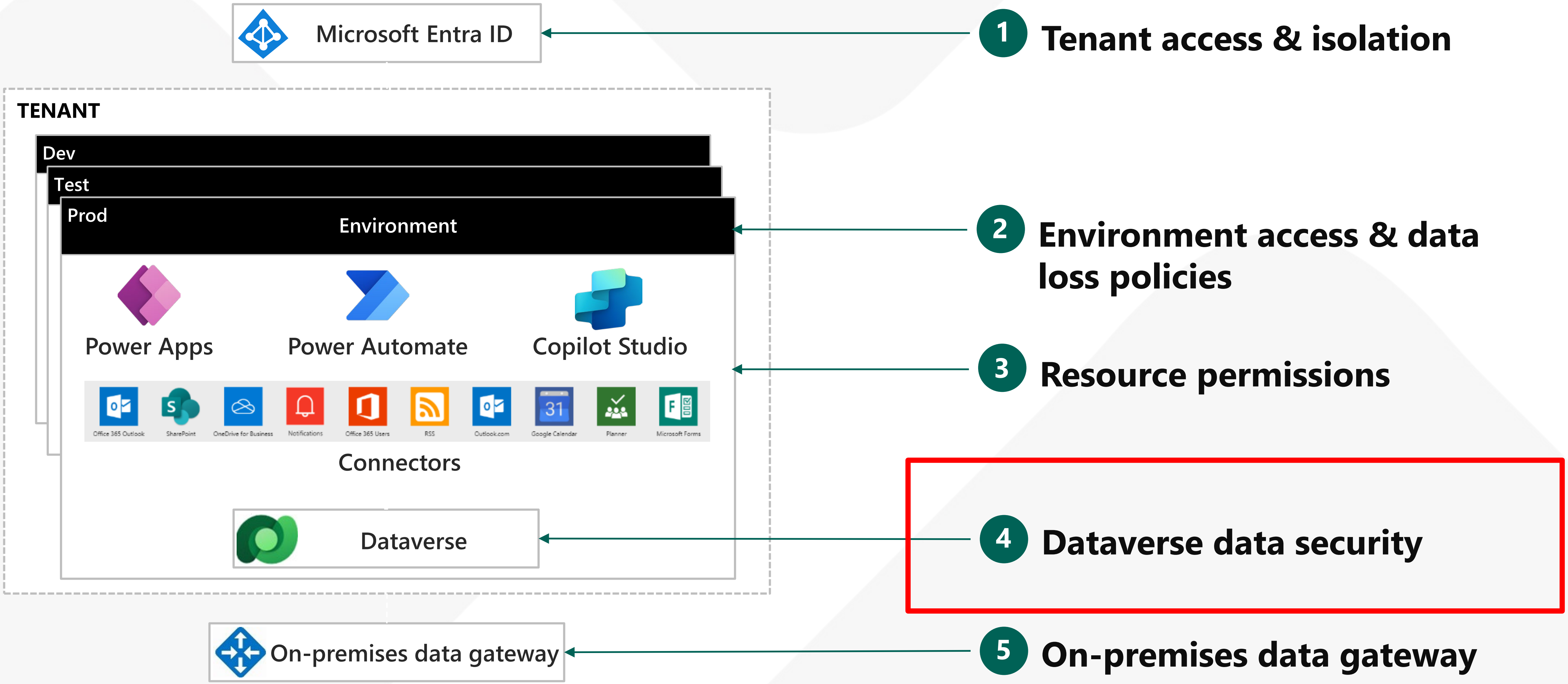
AI Builder

Microsoft Dataverse

Power Fx

Managed Environments

Security is built into every layer



Microsoft Entra ID

TENANT

Dev

Test

Prod

Environment

Power Apps

Power Automate

Copilot Studio

Connectors

Dataverse

On-premises data gateway

1 Tenant access & isolation

2 Environment access & data loss policies

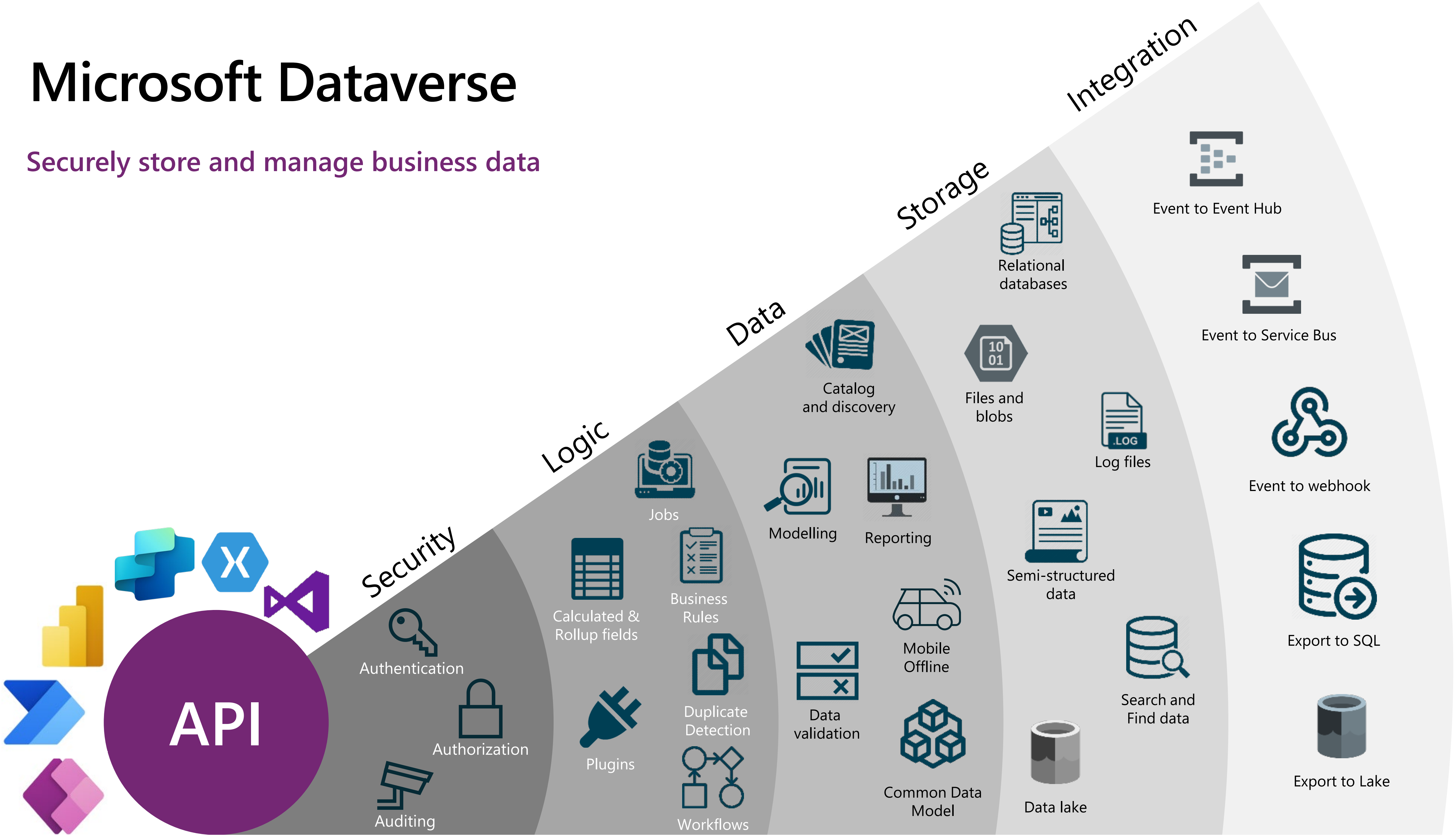
3 Resource permissions

4 Dataverse data security

5 On-premises data gateway

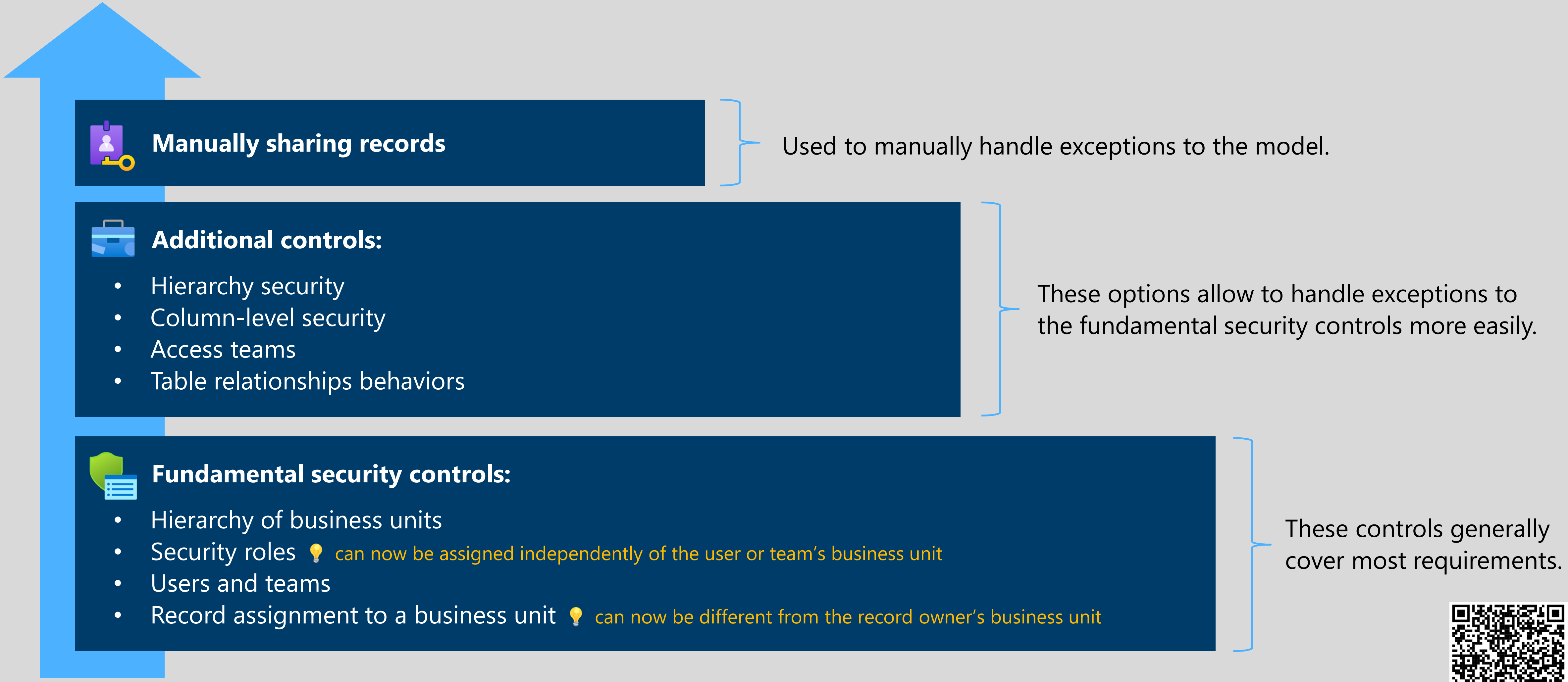
Microsoft Dataverse

Securely store and manage business data



Dataverse security controls overview

From fundamental security controls to exception management



Manually sharing records

Used to manually handle exceptions to the model.

Additional controls:

- Hierarchy security
- Column-level security
- Access teams
- Table relationships behaviors

These options allow to handle exceptions to the fundamental security controls more easily.

Fundamental security controls:

- Hierarchy of business units
- Security roles 💡 can now be assigned independently of the user or team’s business unit
- Users and teams
- Record assignment to a business unit 💡 can now be different from the record owner’s business unit

These controls generally cover most requirements.

Learn more on Dataverse security concepts: https://docs.microsoft.com/power-platform/admin/wp-security-cds

Approaching a security model design

Shortly after defining personas and scopes, it’s important to define how users, teams and records will be organized around the hierarchy of business units.

Define what data you’re trying to secure

Reflect on the required granularity between organizational and confidential data.

Consider splitting data into separate tables when there is a mix of company and commercial data.

Define the hierarchy of business units

Business units shouldn’t necessarily reflect an internal organization: they define the hierarchical structure of users, teams, and records. They work in conjunction with security roles to grant access to data for specific scopes.

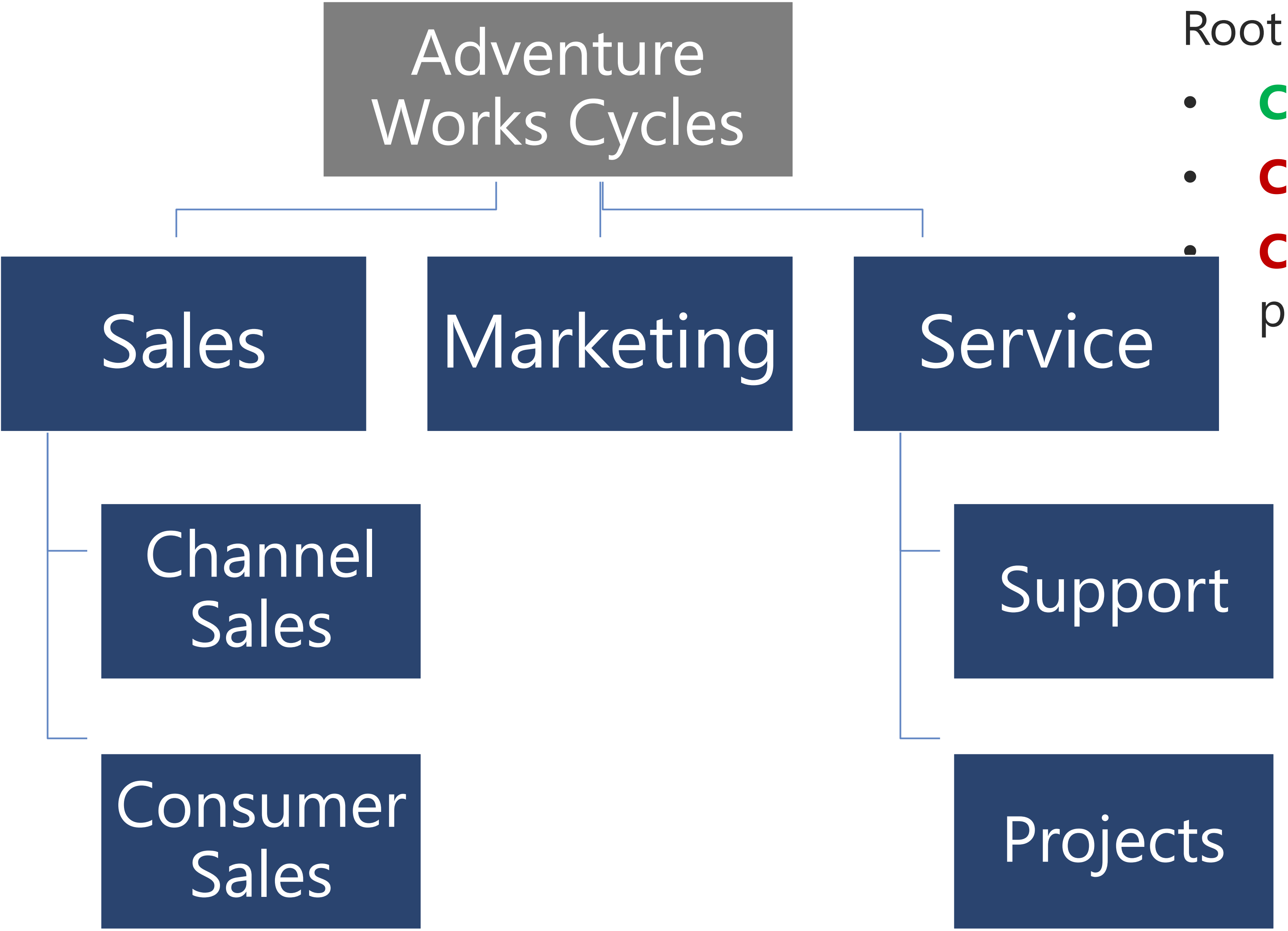
Define how users and teams are organized in the hierarchy of business units

In some situations, users can remain at the root business unit level while security roles scoped to other business units allow to tailor access rights to another business unit. Security roles inherited from teams also allow rich setups.

Define how records are organized in the hierarchy of business units

By default, records belong to their owner’s business unit. This can be overridden by changing the “Owning Business Unit” column of a table, so that records can be assigned to a business unit irrespective of their owner’s.

Business Unit Hierarchy



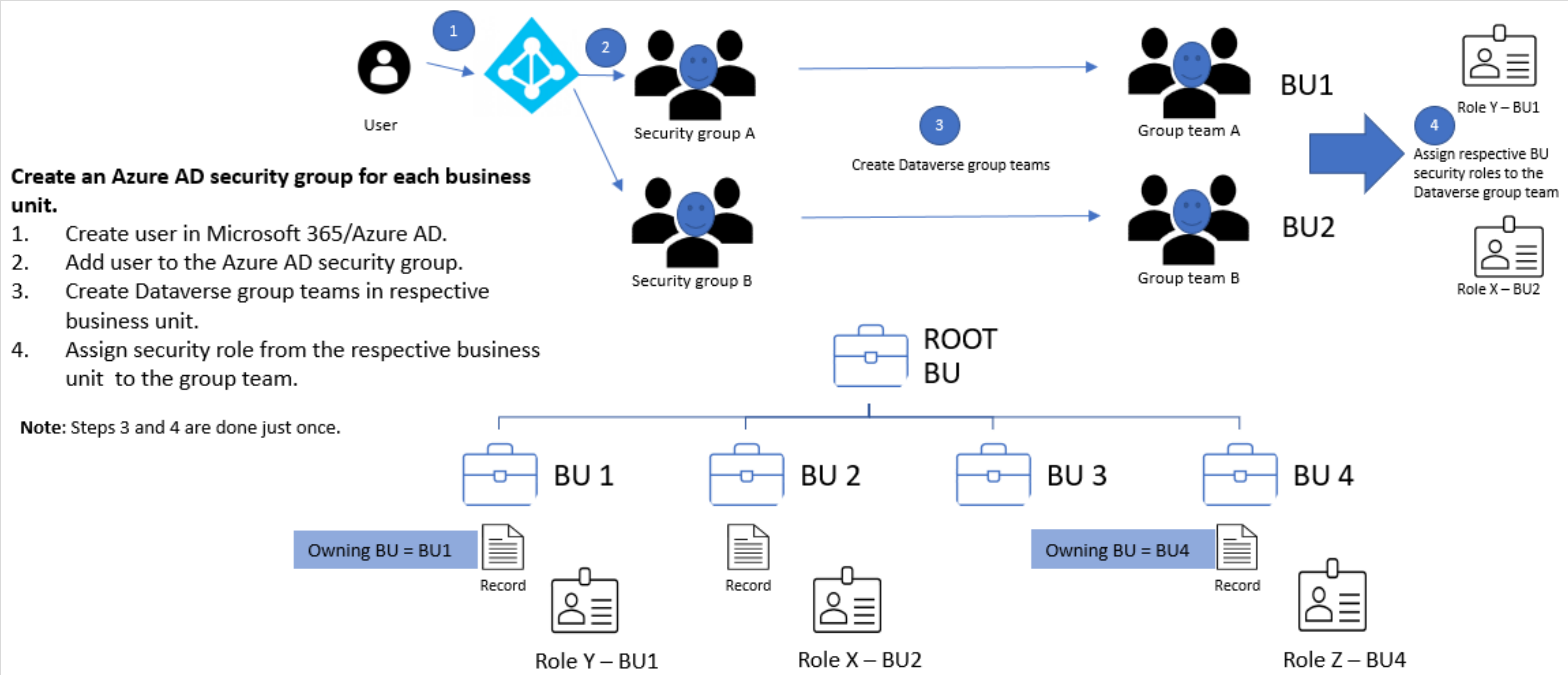
Root Business Unit

- **Can** be renamed
- **Cannot** be disabled or deleted
- **Cannot** be moved to have a parent business unit

Child Business Units

- **Can** be renamed
- **Can** be disabled then deleted
- **Can** be moved under a new parent Business Unit

Business Unit Hierarchy



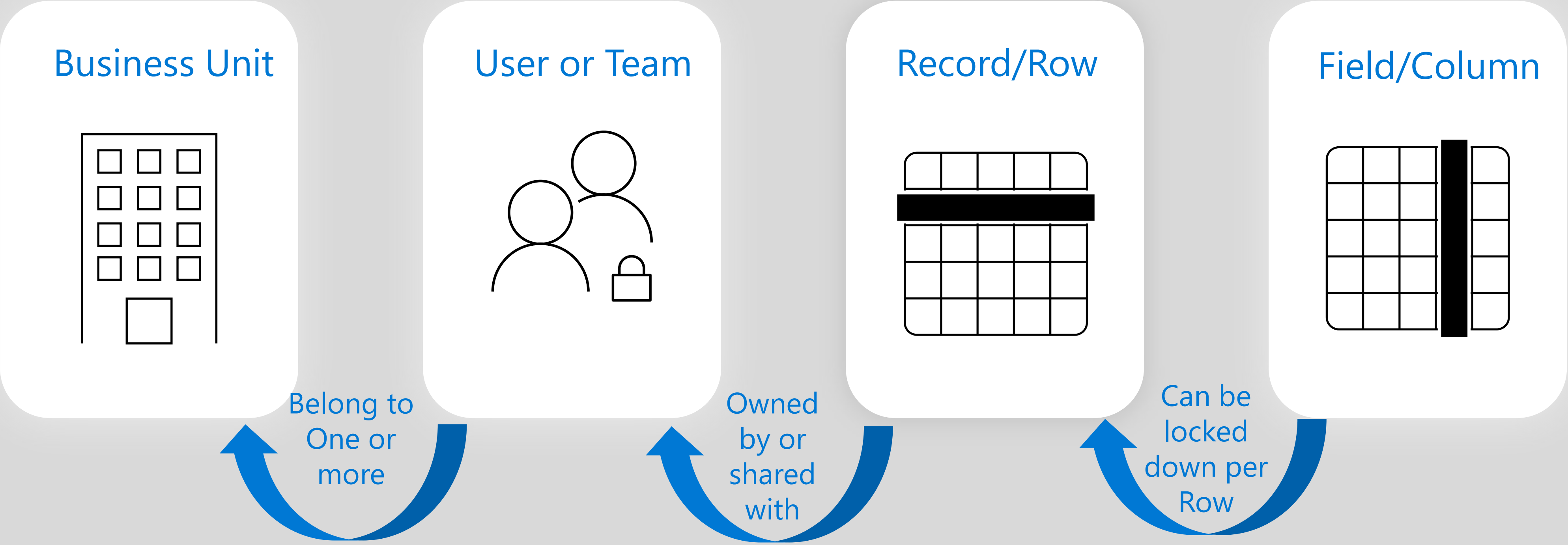
Create an Azure AD security group for each business unit.

1. Create user in Microsoft 365/Azure AD.
2. Add user to the Azure AD security group.
3. Create Dataverse group teams in respective business unit.
4. Assign security role from the respective business unit to the group team.

Note: Steps 3 and 4 are done just once.

Dataverse Security Structures

Fine-grained control using privileges



Business Unit

User or Team

Record/Row

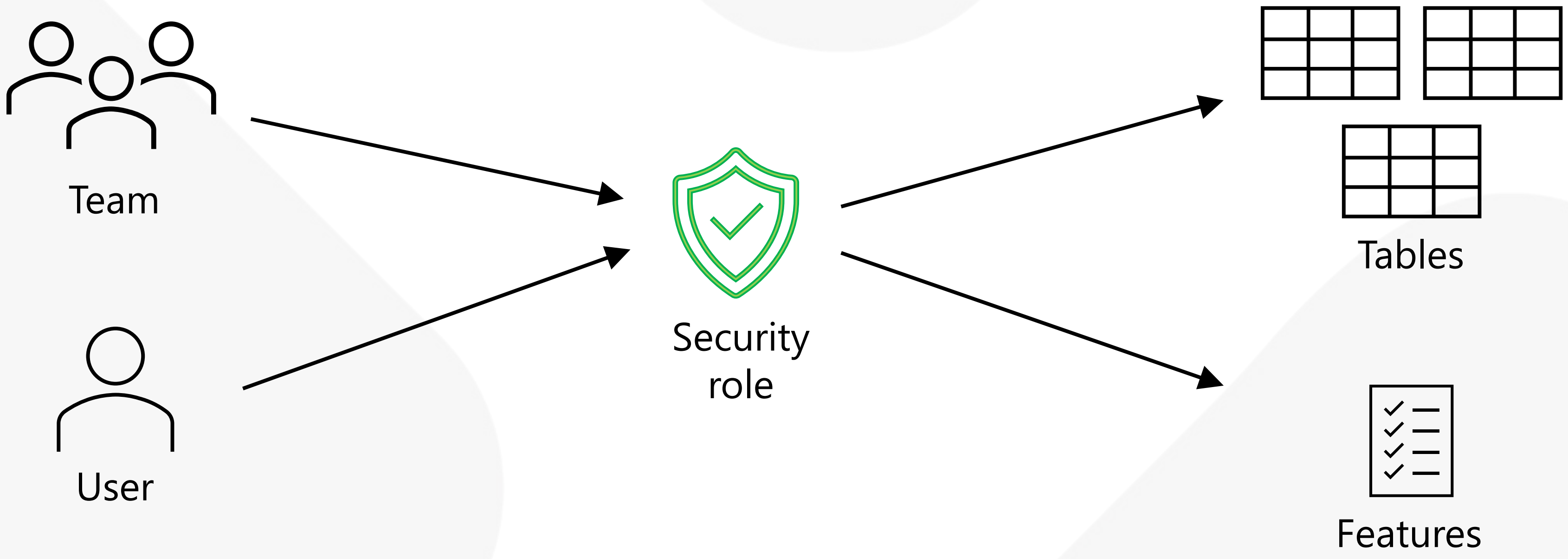
Field/Column

Belong to One or more

Owned by or shared with

Can be locked down per Row

- create
- read
- write
- delete
- append
- append to
- assign
- share



Team

User

Security role

Tables

Features

create

read

write

delete

append

append to

assign

share

Security Roles and Privileges

Roles:

- Define how different users access different types of records
- Contain a set of privileges
- Users can be assigned to multiple security roles
- Security role privileges are cumulative

Privileges:

- Record-level privileges
- Action/Task-based privileges
    - Ex: Publish articles.
- Different level of accesses:
    - Global
    - Deep
    - Local
    - Basic

Security roles development best practices

Defining security roles for your applications

Implement a least privilege strategy when designing your security roles

Consider only providing users with what is necessary (just-enough-access – JEA) to accomplish their job by reducing read/write privileges to a user or business unit scope and avoid granting delete privileges by favoring deactivating records instead.

When possible, drive security roles assignment through Azure AD groups

Managing user roles through Azure AD group teams greatly reduces administration effort and risks of error.

Start from a copy of existing security roles and create them at the root business unit

This allows better control over the new security roles and avoids conflicts with first-party updates.

Security roles at the root business level can be included in solutions and deployed to other environments.

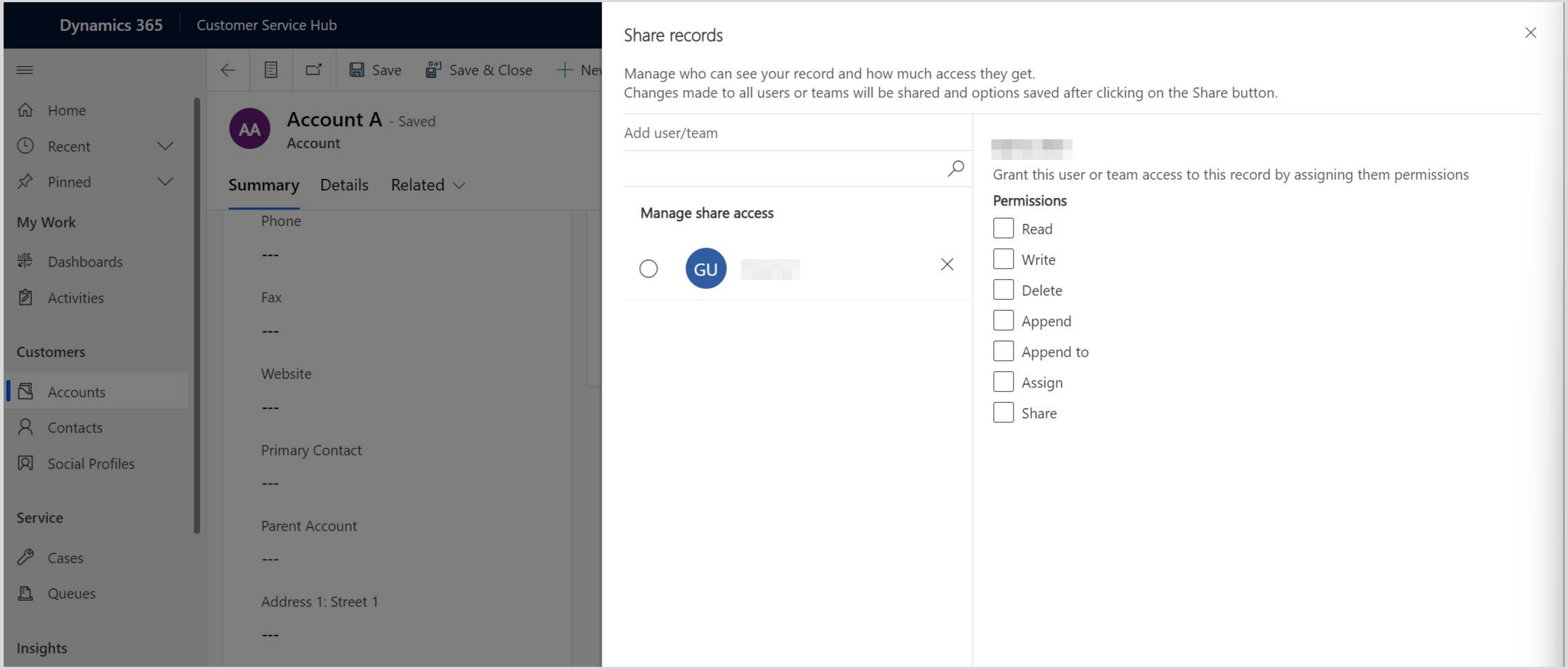
Be mindful of privileges potentially leading to elevated permissions

E.g., "Promote User to Microsoft Dynamics 365 Administrator Role"

Combine similar roles for easier management

You rarely need as many security roles as there are job titles.

Record Sharing



Share records

Manage who can see your record and how much access they get.
Changes made to all users or teams will be shared and options saved after clicking on the Share button.

Add user/team

Manage share access

○ GU [redacted]

[redacted]

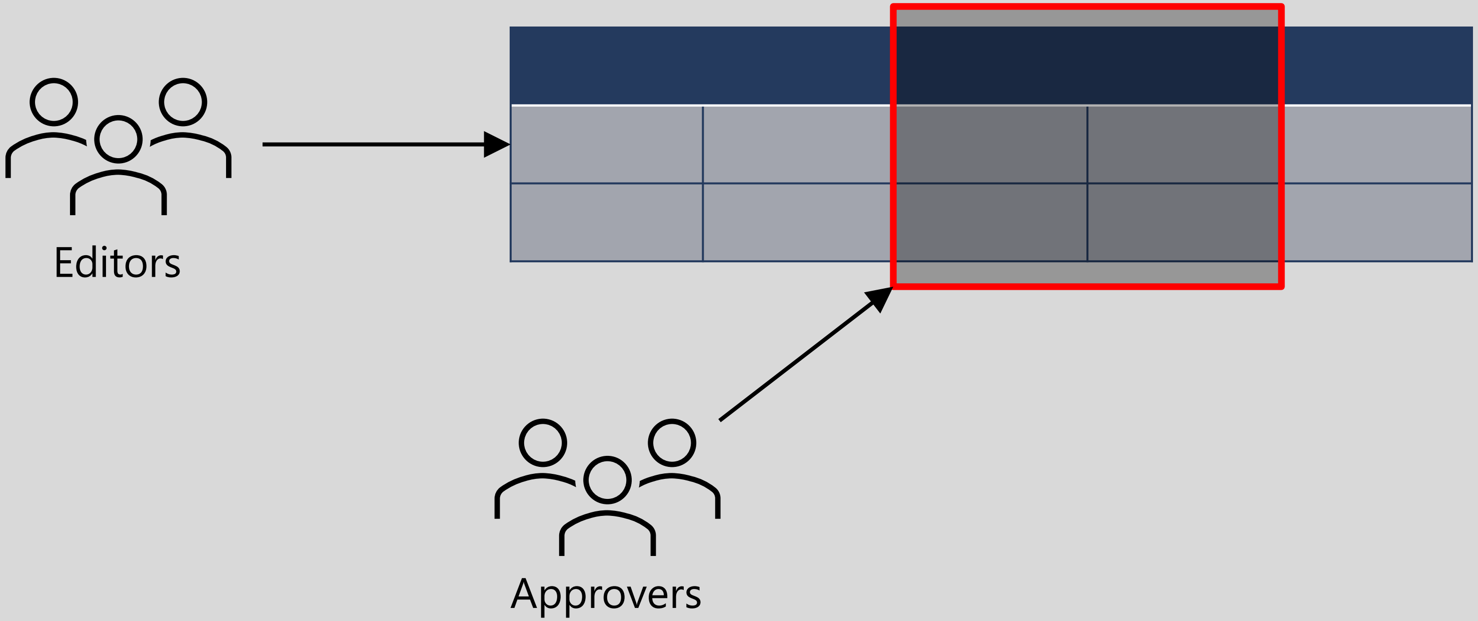
Grant this user or team access to this record by assigning them permissions

Permissions

- □ Read
- □ Write
- □ Delete
- □ Append
- □ Append to
- □ Assign
- □ Share

Column-level Security

- Restrict access to specific columns in a table
- Column-level security profile defines permissions
- Overlapping security profiles are permissive



What is the risk associated with your Dataverse security model?

How do you assess the risk associated with various table privileges at varied level within a Security role?

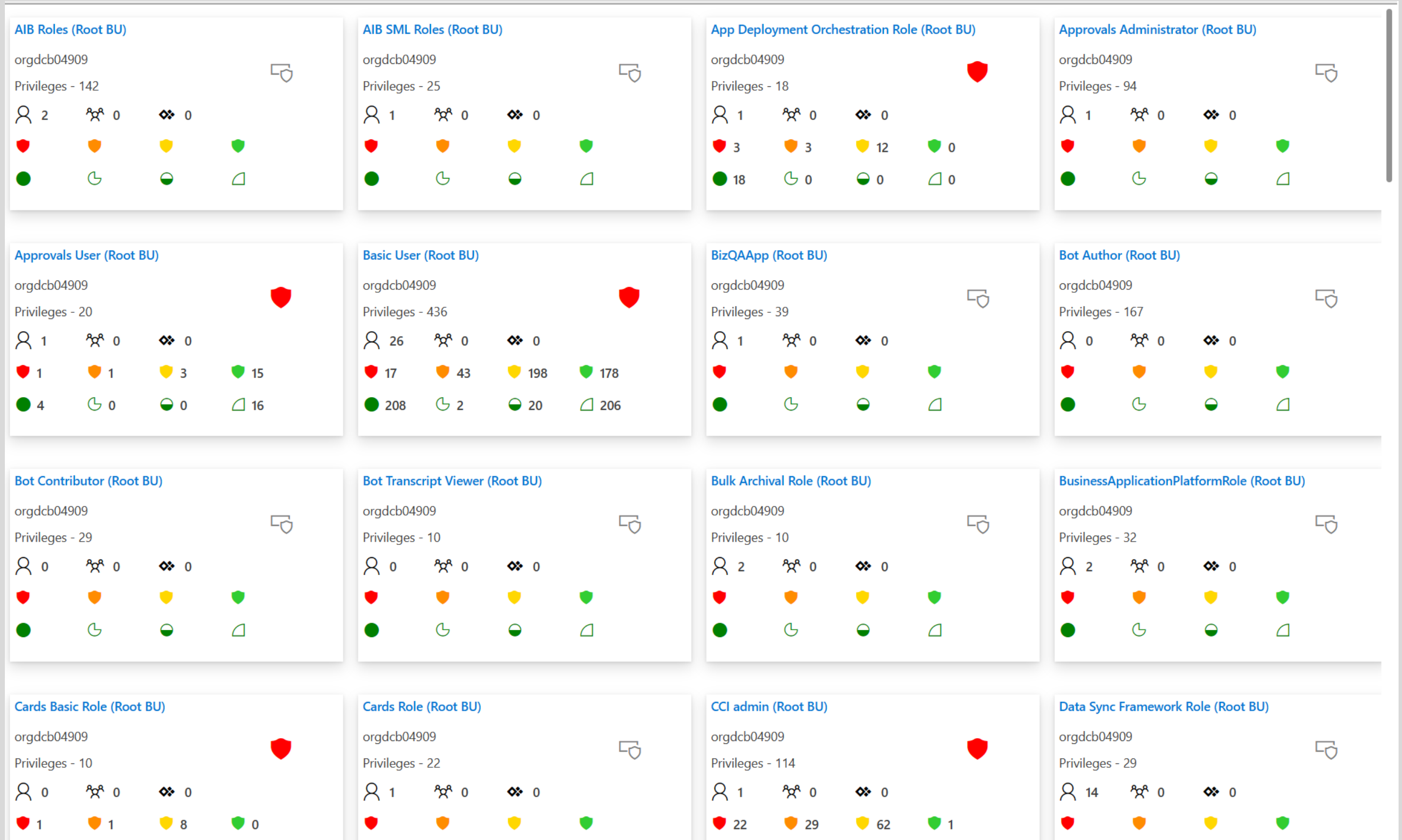
Security Role Risk Assessment

Key Features and Benefits

- Reduce Misconfigurations
- Prevent Over-Permissioned Roles
- Proactive Solution
- Enhanced Security Management

Addressing User Challenges

- Complexity of Security Roles System
- Steep Learning Curve



AIB Roles (Root BU)
orgdcb04909
Privileges - 142
2 0 0

AIB SML Roles (Root BU)
orgdcb04909
Privileges - 25
1 0 0

App Deployment Orchestration Role (Root BU)
orgdcb04909
Privileges - 18
1 0 0
3 3 12 0
18 0 0 0

Approvals Administrator (Root BU)
orgdcb04909
Privileges - 94
1 0 0

Approvals User (Root BU)
orgdcb04909
Privileges - 20
1 0 0
1 1 3 15
4 0 0 16

Basic User (Root BU)
orgdcb04909
Privileges - 436
26 0 0
17 43 198 178
208 2 20 206

BizQAApp (Root BU)
orgdcb04909
Privileges - 39
1 0 0

Bot Author (Root BU)
orgdcb04909
Privileges - 167
0 0 0

Bot Contributor (Root BU)
orgdcb04909
Privileges - 29
0 0 0

Bot Transcript Viewer (Root BU)
orgdcb04909
Privileges - 10
0 0 0

Bulk Archival Role (Root BU)
orgdcb04909
Privileges - 10
2 0 0

BusinessApplicationPlatformRole (Root BU)
orgdcb04909
Privileges - 32
2 0 0

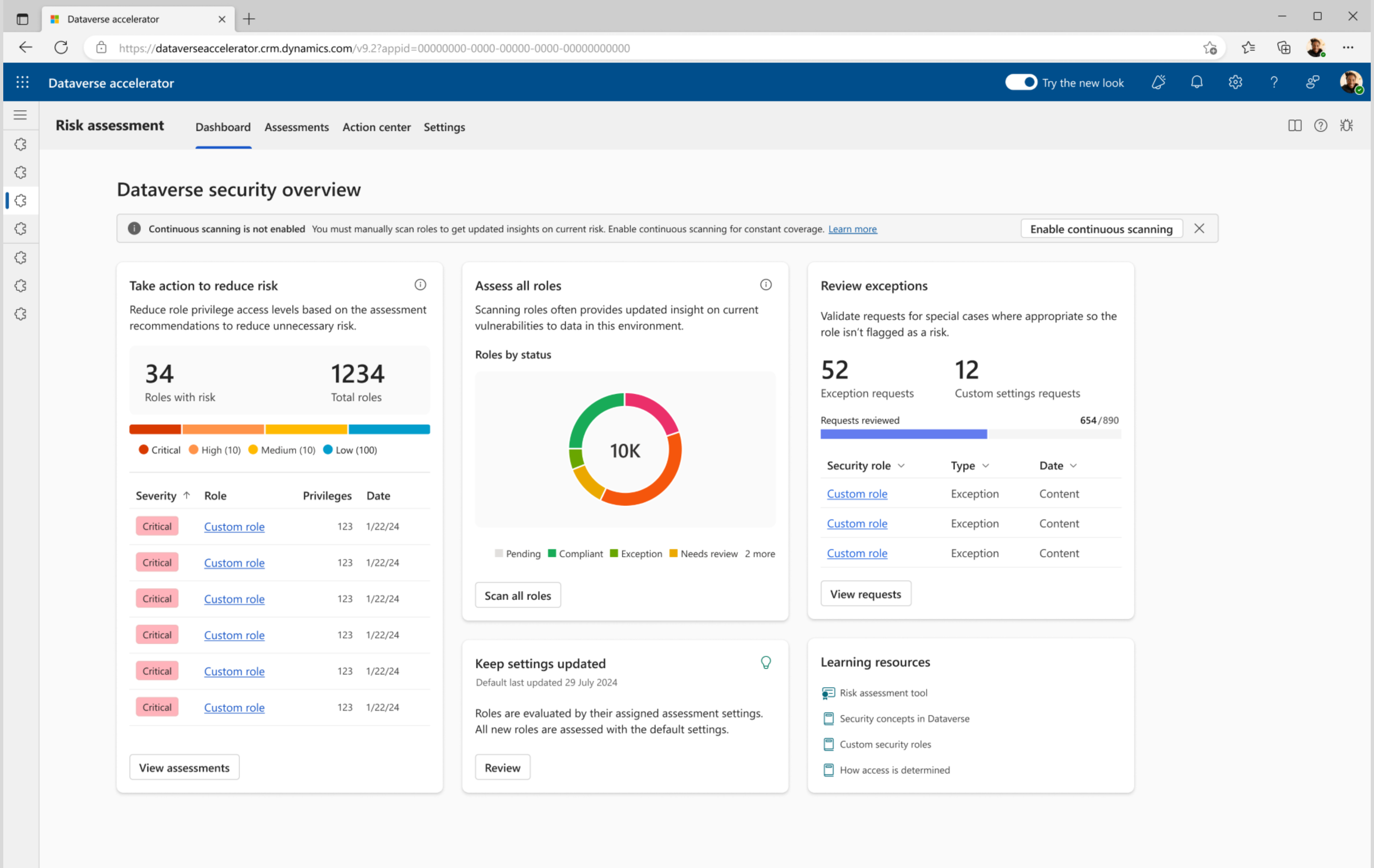
Cards Basic Role (Root BU)
orgdcb04909
Privileges - 10
0 0 0
1 1 8 0

Cards Role (Root BU)
orgdcb04909
Privileges - 22
1 0 0

CCI admin (Root BU)
orgdcb04909
Privileges - 114
1 0 0
22 29 62 1

Data Sync Framework Role (Root BU)
orgdcb04909
Privileges - 29
14 0 0

https://aka.ms/pcattools/dvsecurityriskapp



Dataverse accelerator
https://dataverseaccelerator.crm.dynamics.com/v9.2?appid=00000000-0000-00000-0000-00000000000
Dataverse accelerator
Try the new look

Risk assessment

Dashboard Assessments Action center Settings

Dataverse security overview

Continuous scanning is not enabled You must manually scan roles to get updated insights on current risk. Enable continuous scanning for constant coverage. Learn more

Enable continuous scanning

Take action to reduce risk

Reduce role privilege access levels based on the assessment recommendations to reduce unnecessary risk.

34
Roles with risk

1234
Total roles

● Critical ● High (10) ● Medium (10) ● Low (100)

Severity ↑	Role	Privileges	Date
Critical	Custom role	123	1/22/24
Critical	Custom role	123	1/22/24
Critical	Custom role	123	1/22/24
Critical	Custom role	123	1/22/24
Critical	Custom role	123	1/22/24
Critical	Custom role	123	1/22/24

View assessments

Assess all roles

Scanning roles often provides updated insight on current vulnerabilities to data in this environment.

Roles by status

10K

■ Pending ■ Compliant ■ Exception ■ Needs review 2 more

Scan all roles

Review exceptions

Validate requests for special cases where appropriate so the role isn't flagged as a risk.

52
Exception requests

12
Custom settings requests

Requests reviewed 654/890

Security role	Type	Date
Custom role	Exception	Content
Custom role	Exception	Content
Custom role	Exception	Content

View requests

Keep settings updated

Default last updated 29 July 2024

Roles are evaluated by their assigned assessment settings. All new roles are assessed with the default settings.

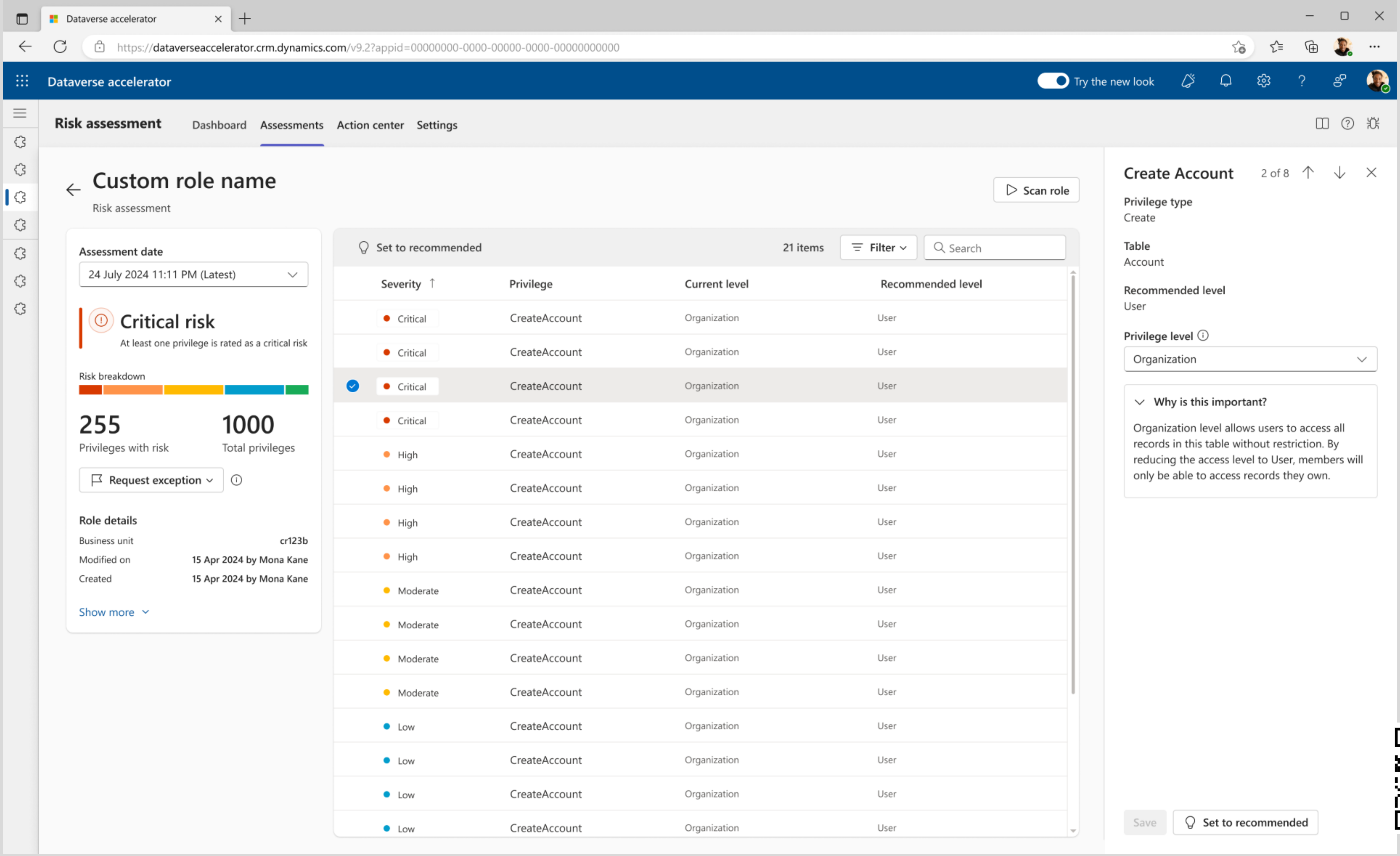
Review

Learning resources

- Risk assessment tool
- Security concepts in Dataverse
- Custom security roles
- How access is determined

https://aka.ms/dvacc/riskassess/preview

ETA is November 2024



Custom role name

Risk assessment

Assessment date

24 July 2024 11:11 PM (Latest)

Critical risk

At least one privilege is rated as a critical risk

Risk breakdown

255 Privileges with risk

1000 Total privileges

Role details

Business unit	cr123b
Modified on	15 Apr 2024 by Mona Kane
Created	15 Apr 2024 by Mona Kane

Severity ↑	Privilege	Current level	Recommended level
● Critical	CreateAccount	Organization	User
● Critical	CreateAccount	Organization	User
● Critical	CreateAccount	Organization	User
● Critical	CreateAccount	Organization	User
● High	CreateAccount	Organization	User
● High	CreateAccount	Organization	User
● High	CreateAccount	Organization	User
● High	CreateAccount	Organization	User
● Moderate	CreateAccount	Organization	User
● Moderate	CreateAccount	Organization	User
● Moderate	CreateAccount	Organization	User
● Moderate	CreateAccount	Organization	User
● Low	CreateAccount	Organization	User
● Low	CreateAccount	Organization	User
● Low	CreateAccount	Organization	User
● Low	CreateAccount	Organization	User

Create Account 2 of 8

Privilege type
Create

Table
Account

Recommended level
User

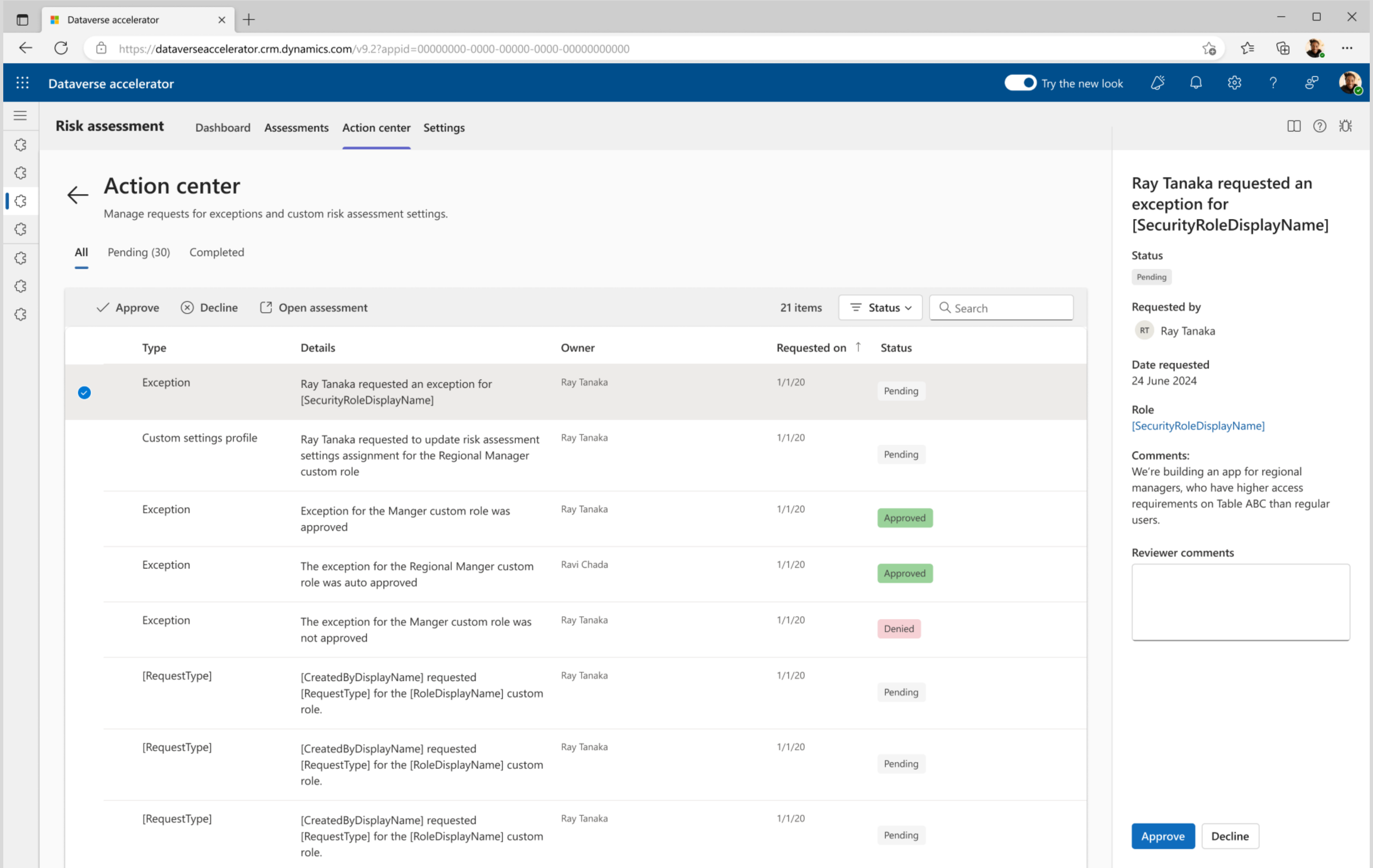
Privilege level
Organization

Why is this important?

Organization level allows users to access all records in this table without restriction. By reducing the access level to User, members will only be able to access records they own.

https://aka.ms/dvacc/riskassess/preview

ETA is November 2024



Action center

Manage requests for exceptions and custom risk assessment settings.

Type	Details	Owner	Requested on ↑	Status
Exception	Ray Tanaka requested an exception for [SecurityRoleDisplayName]	Ray Tanaka	1/1/20	Pending
Custom settings profile	Ray Tanaka requested to update risk assessment settings assignment for the Regional Manager custom role	Ray Tanaka	1/1/20	Pending
Exception	Exception for the Manger custom role was approved	Ray Tanaka	1/1/20	Approved
Exception	The exception for the Regional Manger custom role was auto approved	Ravi Chada	1/1/20	Approved
Exception	The exception for the Manger custom role was not approved	Ray Tanaka	1/1/20	Denied
[RequestType]	[CreatedByDisplayName] requested [RequestType] for the [RoleDisplayName] custom role.	Ray Tanaka	1/1/20	Pending
[RequestType]	[CreatedByDisplayName] requested [RequestType] for the [RoleDisplayName] custom role.	Ray Tanaka	1/1/20	Pending
[RequestType]	[CreatedByDisplayName] requested [RequestType] for the [RoleDisplayName] custom role.	Ray Tanaka	1/1/20	Pending

Ray Tanaka requested an exception for [SecurityRoleDisplayName]

Status
Pending

Requested by
RT Ray Tanaka

Date requested
24 June 2024

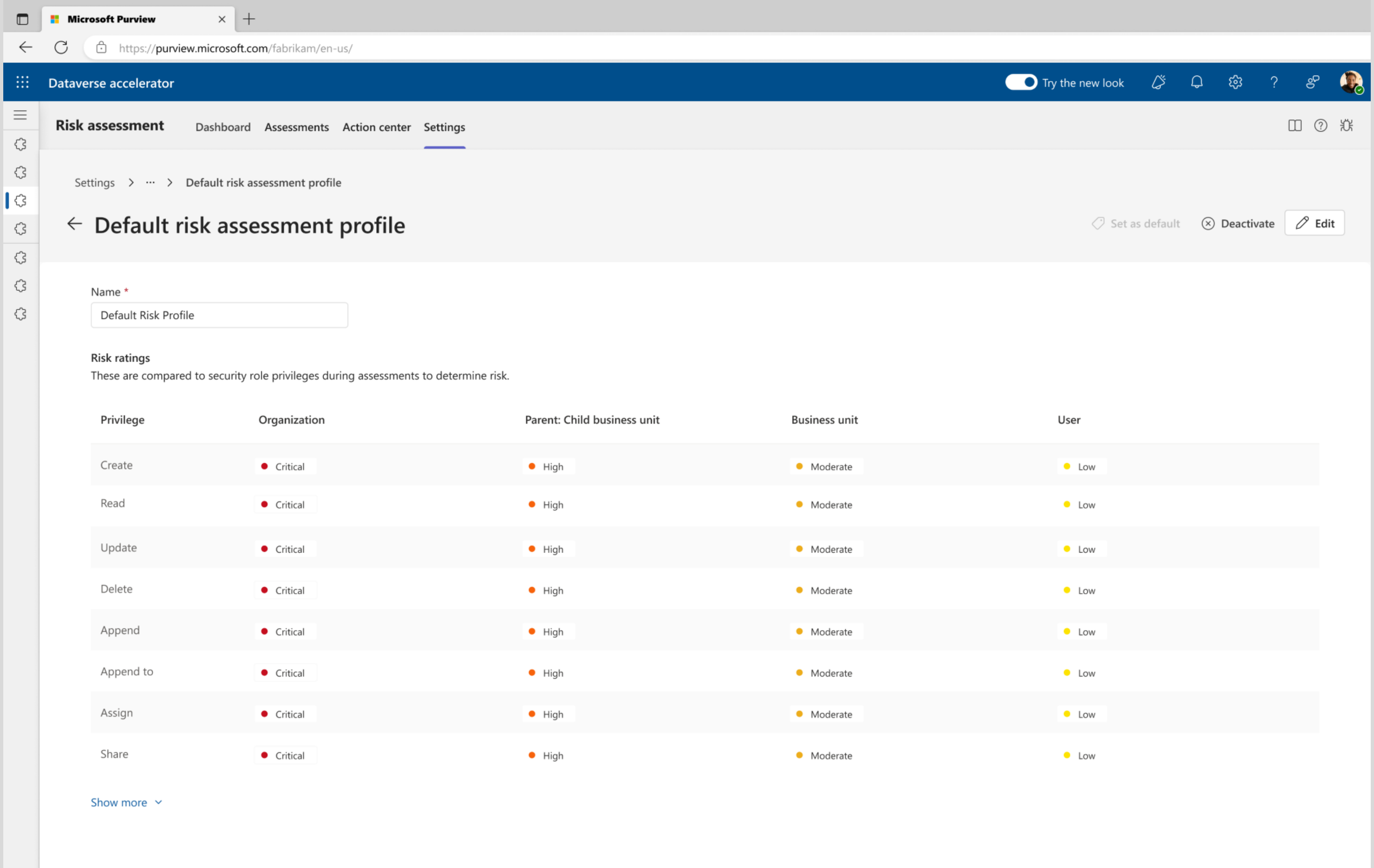
Role
[SecurityRoleDisplayName]

Comments:
We're building an app for regional managers, who have higher access requirements on Table ABC than regular users.

Reviewer comments

https://aka.ms/dvacc/riskassess/preview

ETA is November 2024



Default risk assessment profile

Name *

Default Risk Profile

Risk ratings

These are compared to security role privileges during assessments to determine risk.

Privilege	Organization	Parent: Child business unit	Business unit	User
Create	● Critical	● High	● Moderate	● Low
Read	● Critical	● High	● Moderate	● Low
Update	● Critical	● High	● Moderate	● Low
Delete	● Critical	● High	● Moderate	● Low
Append	● Critical	● High	● Moderate	● Low
Append to	● Critical	● High	● Moderate	● Low
Assign	● Critical	● High	● Moderate	● Low
Share	● Critical	● High	● Moderate	● Low

Show more

https://aka.ms/dvacc/riskassess/preview

ETA is November 2024

Security model best practices

Defining your Dataverse security model

Keep your model simple and have the future in mind

Be mindful of the required effort to maintain the security model.
Anticipate the impact of reorganizations, user onboarding, user leaving or user changing roles.
Try to limit the number of security patterns, security roles, business units (and their depth) and teams.

Avoid unhealthy patterns

Automated sharing at scale is never easy to maintain and can introduce scalability and performance issues. Try to cover as many scenarios as possible with simple patterns, and only resort to sharing for exceptions to the model.

Plug-ins firing on Retrieve and RetrieveMultiple events also have caveat and impact performances negatively.

Understand that customization of the user interface is different from securing data

When a user has update privileges on a record, just because a field is set as read-only on a form doesn't mean the data can't be updated through other means. True security resides server-side.
Hiding the "Export to Excel" button doesn't mean users can't export the data with other tools.

That being said, security roles can and should also be leveraged to create simple role-based UX.

Assess security impacts in related applications and/or features

Evaluate access rights in satellite apps and services (e.g., Customer Insights, SharePoint, Teams, Portals, Power BI, etc.).

Additional considerations

Processes & guidelines

Consider reporting to simplify a security model

If managers only need an overview of business (e.g., territory pipeline forecast), instead of defining a complex model on individual records, consider an anonymized report with limited access to the underlying raw data.

Monitor customizations being deployed to production

By being source control-centric and with a gated Application Lifecycle Management (ALM) approach – with code reviews and approvals of pull requests – reduce risk of deploying malicious or unsecure customizations.

Have a secure process to handle changes to data involved in sensitive operations

E.g., updating a customer phone number used for verification, should it be approved, audited?
Should the customer be warned?

Consider security checks and trainings for employees accessing confidential data

Reduce risks by performing security checks and providing security trainings.

Don’t use Dataverse as a vault for highly sensitive information such as credit cards

Compliant tools and solutions should be considered instead.

Thank You

Ravi Chada

Principal Program Manager