
5th
POWER PLATFORM
BOOTCAMP
5 tips to secure your #PowerPlatform #ecosystem
POWER PLATFORM
BOOTCAMP
upzoids
Microsoft Solutions, Tailored for You
Microsoft
#GlobalPowerPlatformBootcamp
#GPPB2024

5 tips to secure your Power Platform ecosystem

Trust built in at every level

Aroh Shukla

POWER PLATFORM BOOTCAMP

upzoids
Microsoft Solutions, Tailored for You

Microsoft

#GlobalPowerPlatformBootcamp
#GPPB2024

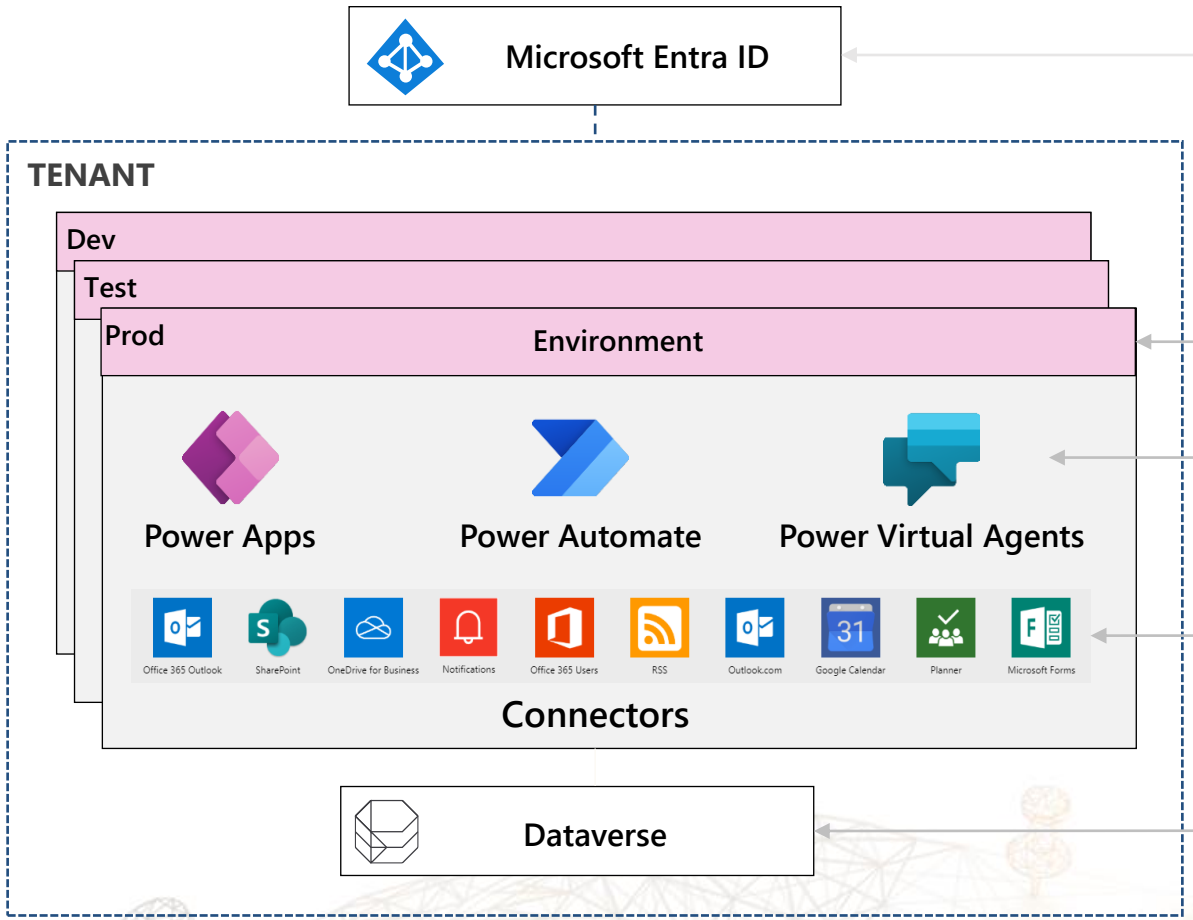
Aroh Shukla

- Regional Microsoft Cloud Architect (Health Care Industry)
- Microsoft MVP Alumni (Biz Apps & Data Platform)
- Love learning and Sharing

Agenda

1. Tenant access & isolation
2. Environment access & strategy
3. Resource permissions
4. Data polices (DLP Polices)
5. Dataverse Security
6. DEMOS

POWER PLATFORM SECURITY LAYERS



1 **Tenant access & isolation**

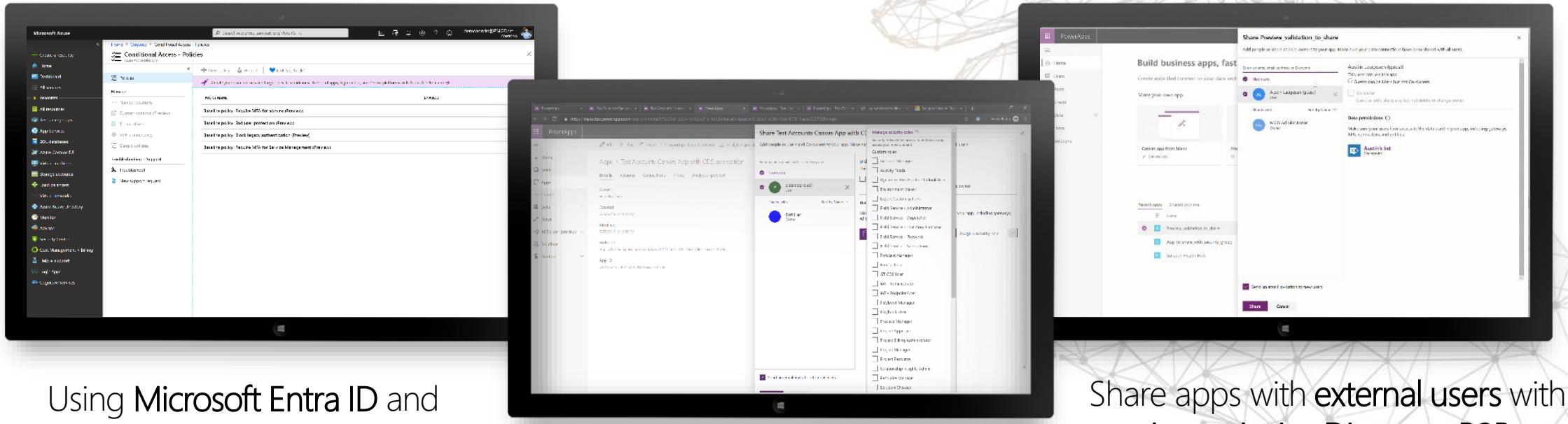
2 Environment access & strategy

3 Resource permissions

4 Connector access and data loss policies

5 Dataverse security

IDENTITY MANAGEMENT WITH MICROSOFT ENTRA ID



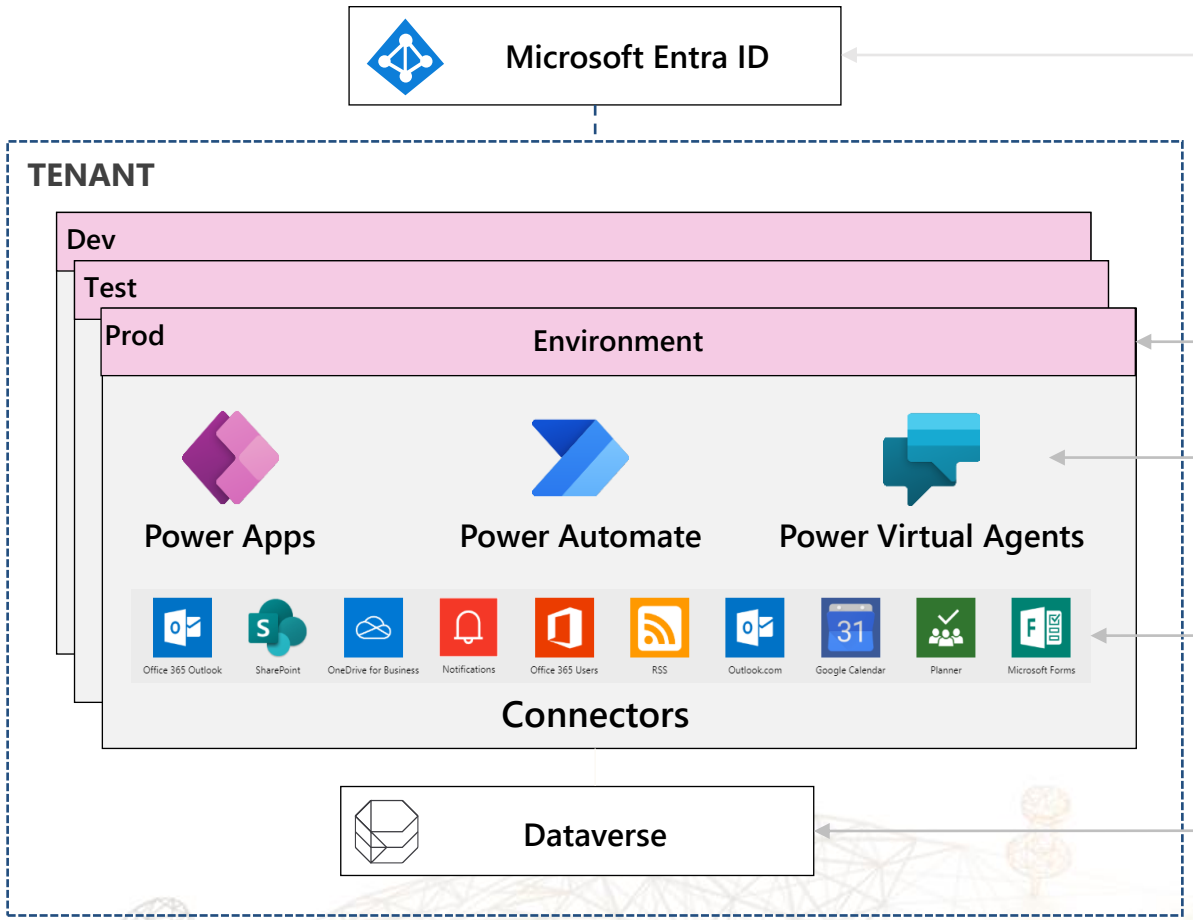
Using **Microsoft Entra ID** and **conditional access policies** to manage timeout and access requirements.

Use Azure Active Directory groups to **manage/share apps** and **data access**.

Share apps with **external users** with **Azure Active Directory** B2B collaboration.

DEMO 1
TENANT LEVEL ACCESS

ENVIRONMENT SECURITY



1 Tenant Access & Isolation

2 **Environment access & strategy**

3 Resource permissions

4 Connector access and data loss policies

5 Dataverse security

KEY FACTS ABOUT ENVIRONMENTS

POWER PLATFORM'S UNIT OF ORGANIZATION

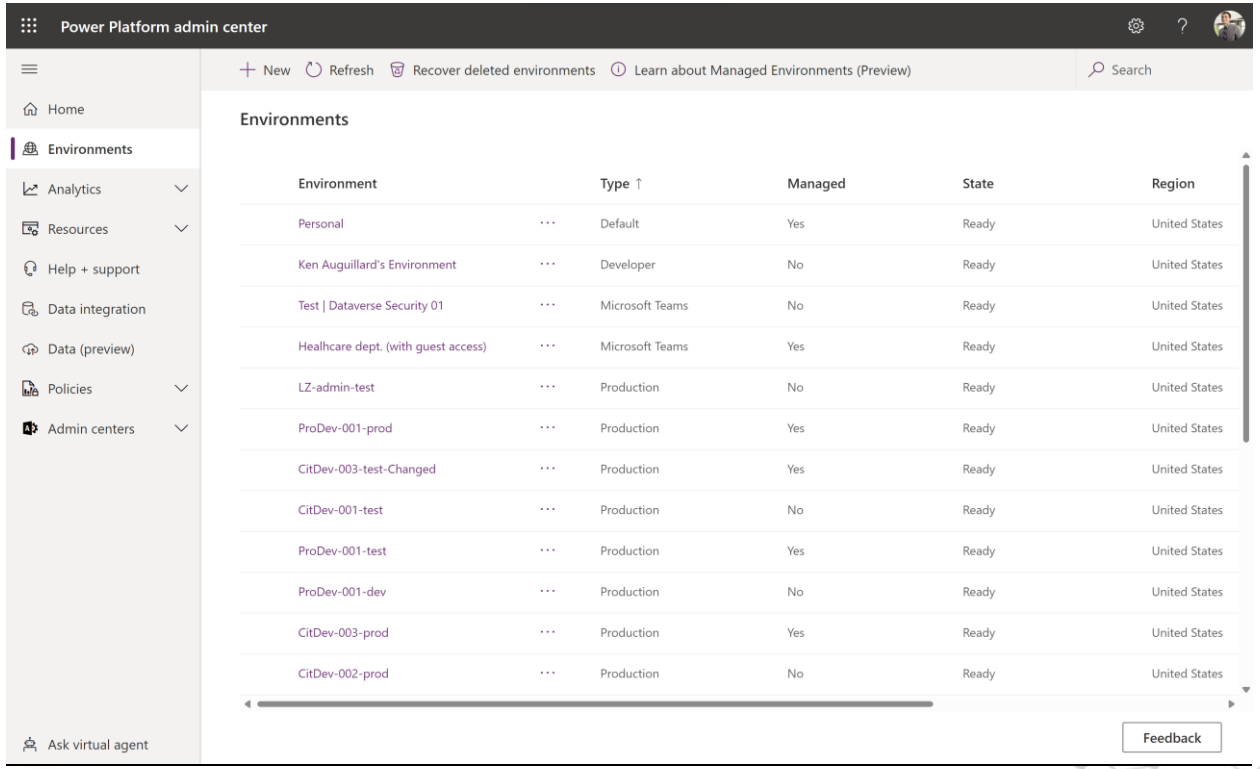
It is a container to separate resources that have different roles, security

Every tenant has a default environment where all licensed users can create apps, flows

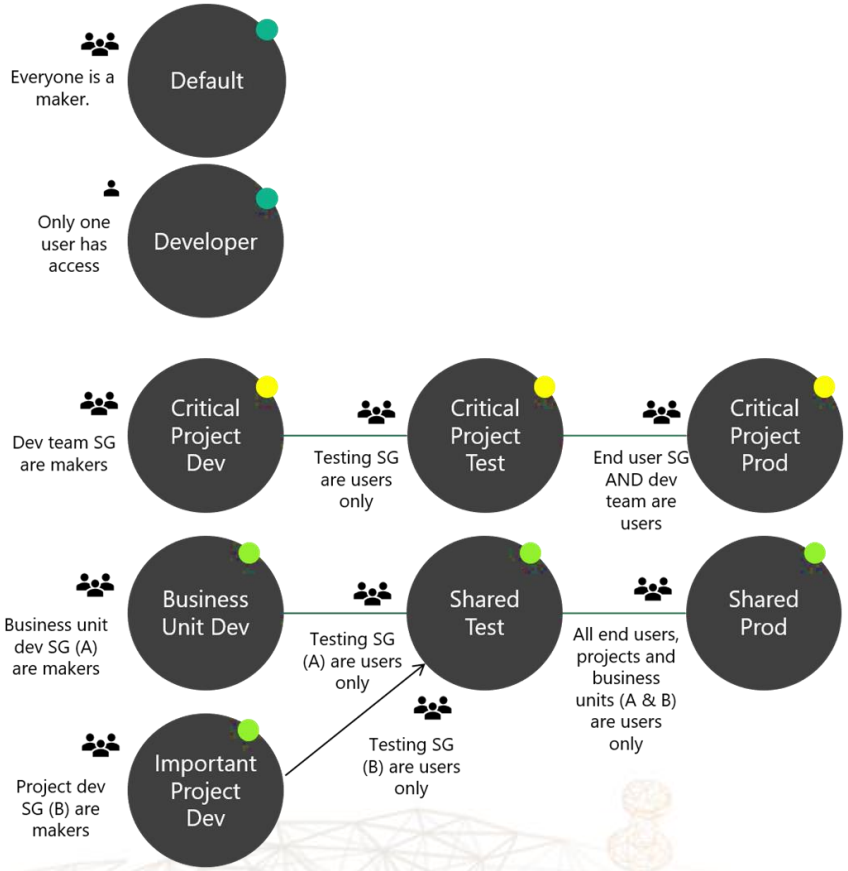
It is bound to a geography so that apps, flows, etc. are routed only to datacenters in

Dataverse is available to securely store and manage data that's used by business applications

Control who can create environments in the Power Platform admin center. (**Governance**)



ENVIRONMENT STRATEGY



Communicate with everyone that **Default** is not for development of critical apps.

Developer environments are completely locked for any other user except the user who subscribed to the community plan. Applications can be moved out of the environment if needed.

Dedicated dev/test/prod environments for each critical application. Developers have Environment Maker access in the dev environment, but only user access in test and prod. End users only have end user access to the production solution so no one can modify the applications.

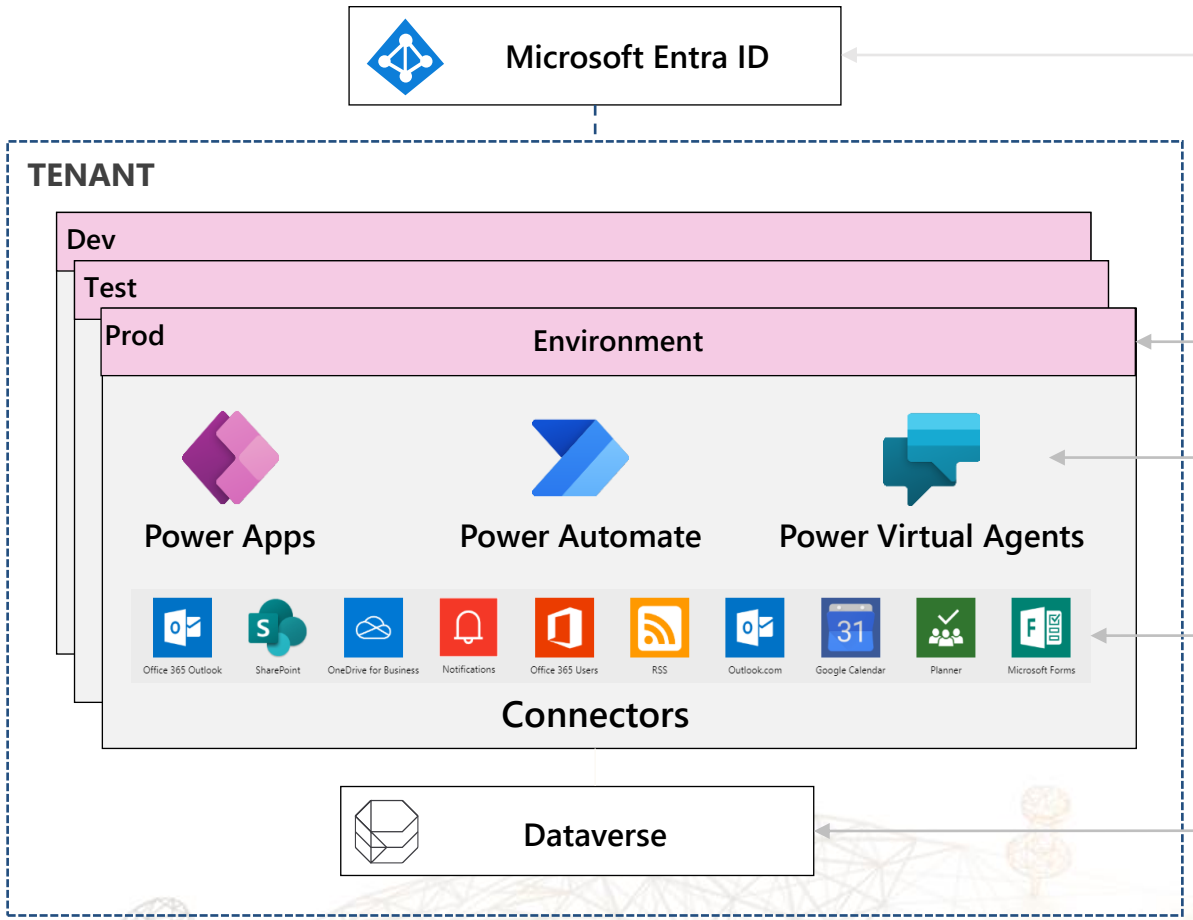
Shared test/prod environments for important but medium complex apps can be shared between multiple projects or business units.
Individual projects and business units should always have their own development environment to protect data. End users only have basic user access to solutions and data in production environments.

- Critical project
- Individual project
- Personal productivity apps

SG = Security Group

DEMO 2
ENVIRONMENT ACCESS

RESOURCE PERMISSIONS



1 Tenant access & isolation

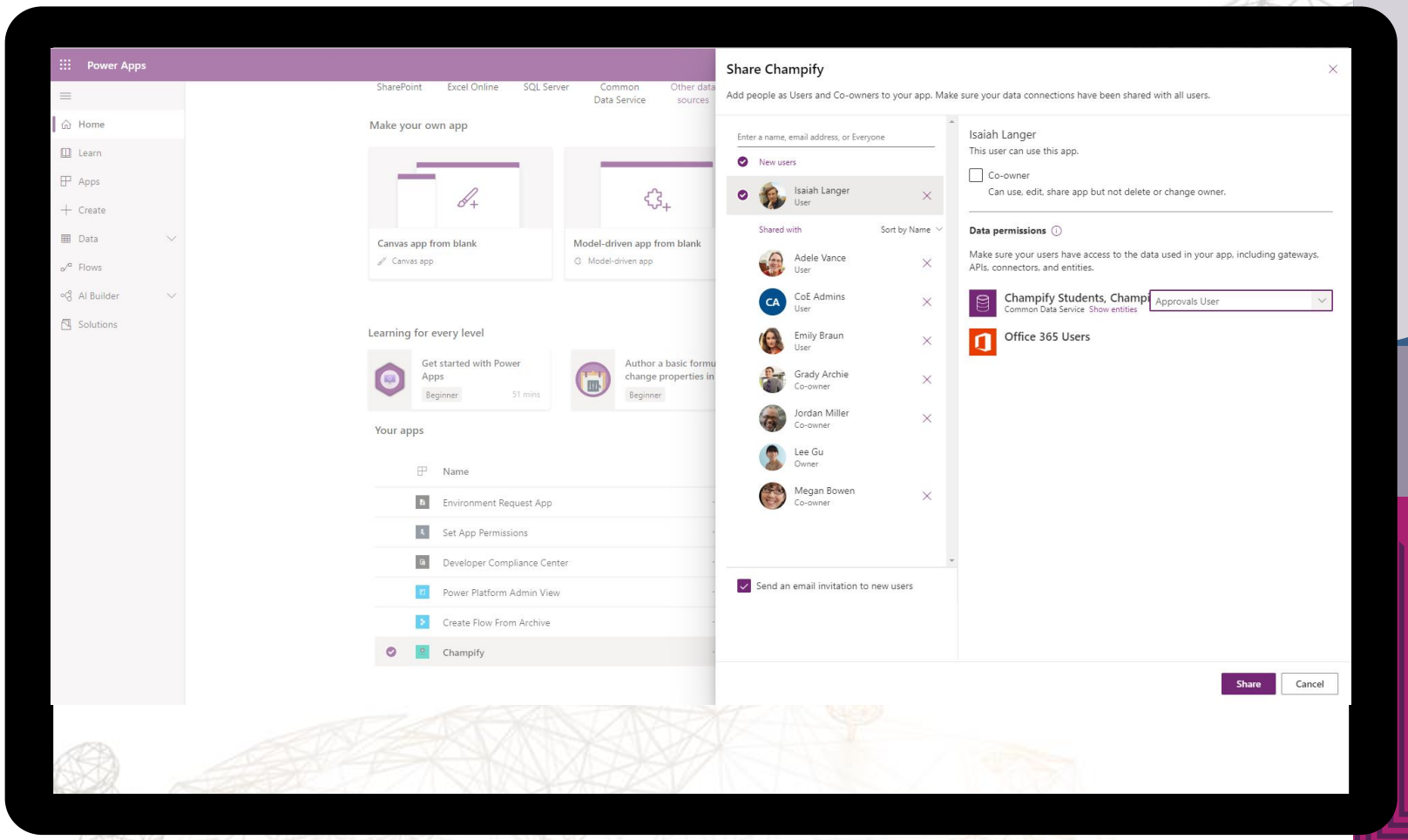
2 Environment access & strategy

3 **Resource permissions**

4 Connector access and data loss policies

5 Dataverse security

SHARING COMPONENT AND GRANTING DATA ACCESS



POWER PLATFORM BOOTCAMP

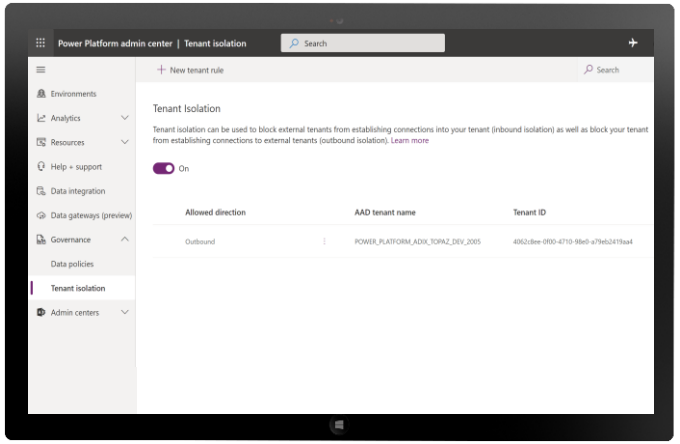
upzoids
Microsoft Solutions, Tailored for You

Microsoft

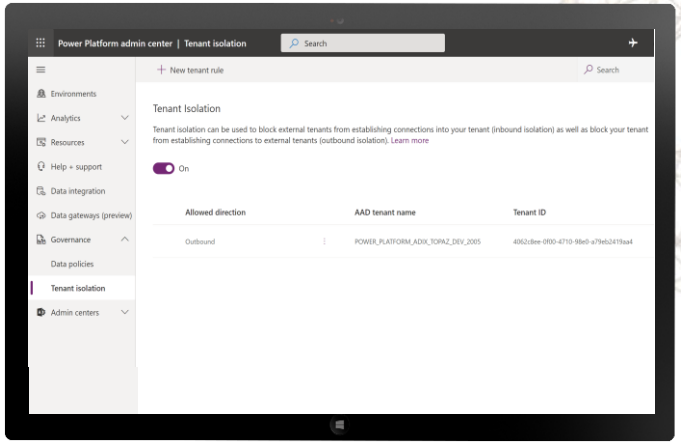
#GlobalPowerPlatformBootcamp
#GPPB2024

RESOURCE LEVEL ACCESS

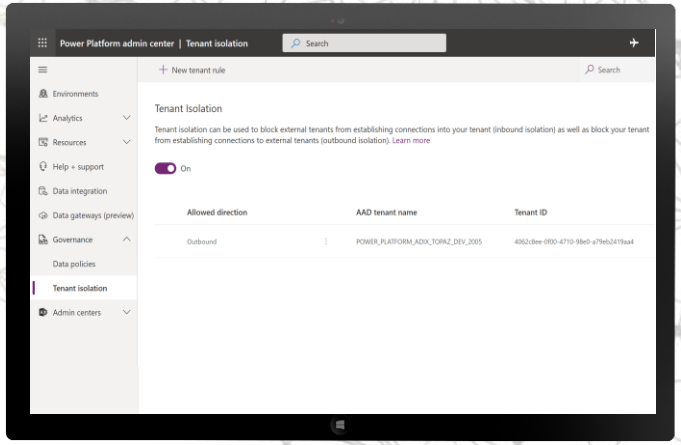
- Access to co-own components – edit, share, use
- Flow co-ownership sharing also shares connections in the flow implicitly with owners
- Access to run components – use only



Power Automate



Power Apps



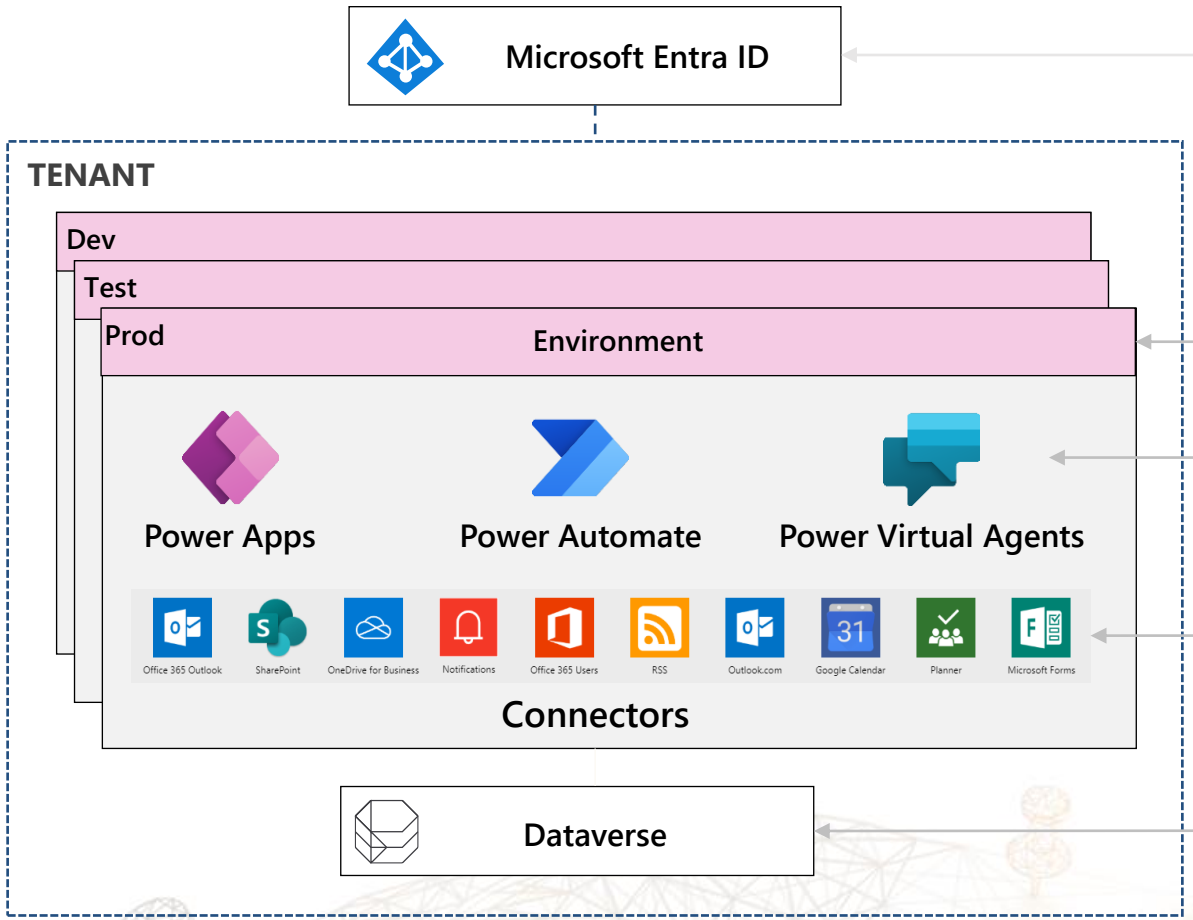
Copilot Studio

Important:

Power Apps, Power Automate, and Copilot ***do not provide*** users access to **any data assets** that they don't already have access to.

DEMO 3
SHARING ACCESS

DATA POLICIES (DLP)



1 Tenant access & isolation

2 Environment access & strategy

3 Resource permissions

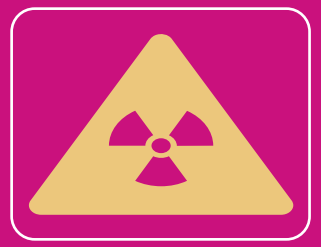
4 **Connector access and data loss policies**

5 Dataverse security

DATA POLICIES (DLP) CATEGORIES

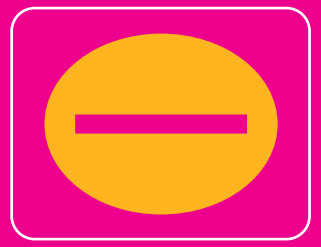
Business

- Connectors for **sensitive** data
- Connectors in this group can't share data with connectors in other groups.



Non-Business

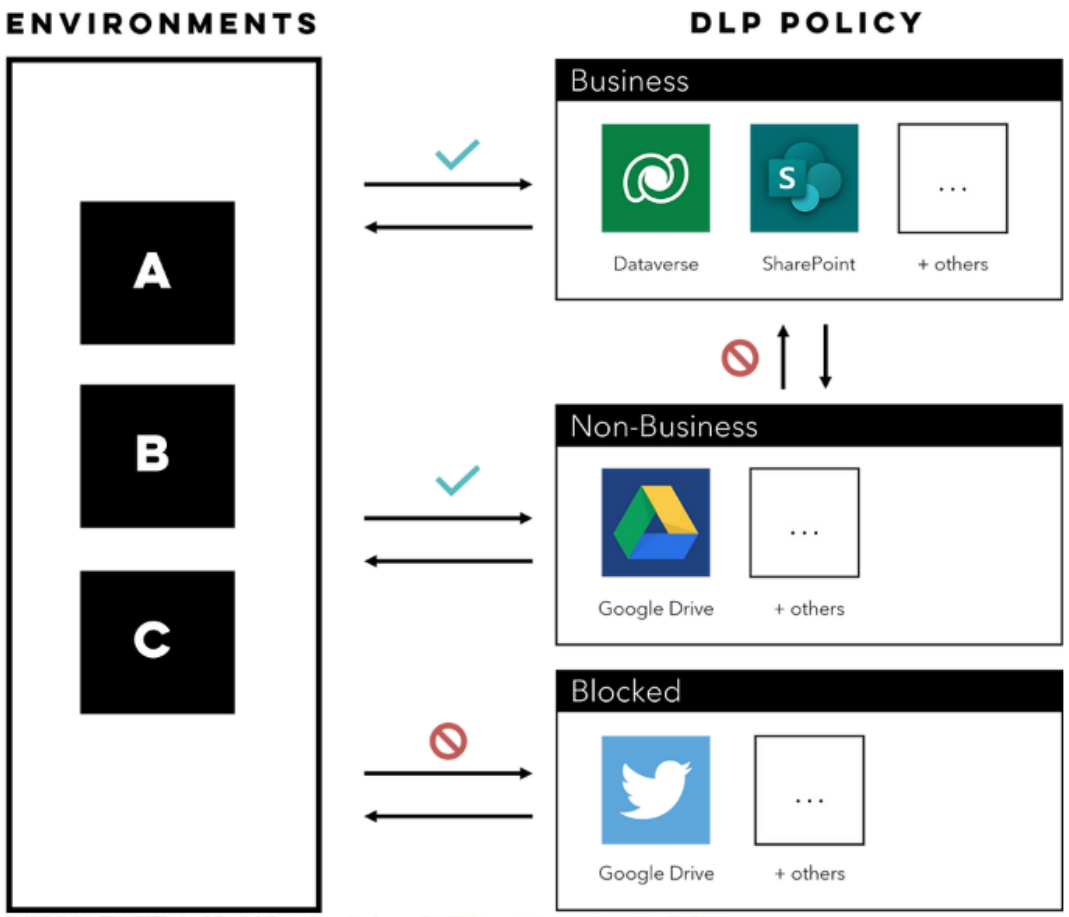
- Connectors for **non-sensitive** data
- Connectors in this group can't share data with connectors in other groups.
- Unassigned connectors will show up here **by default**.



Blocked

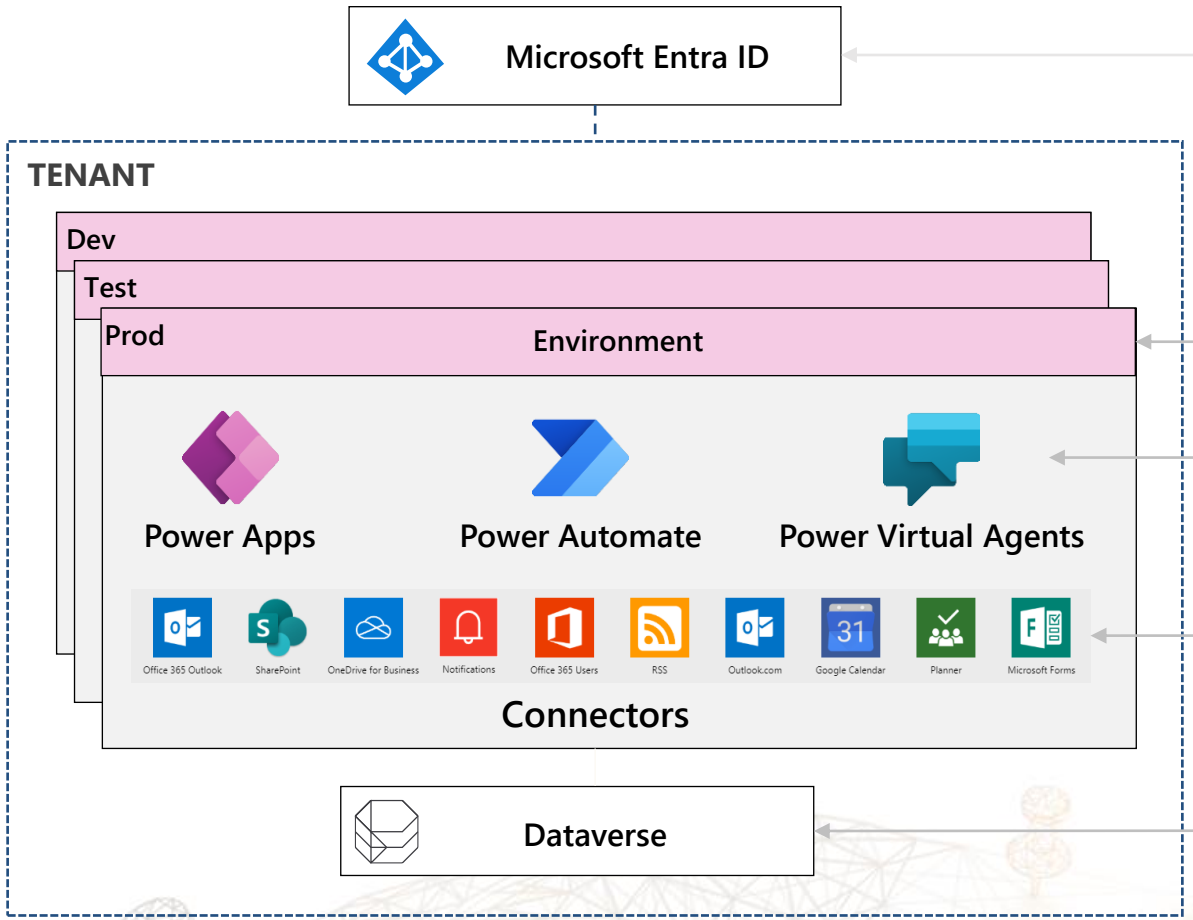
- Blocked connectors can't be used where this policy is applied.
- Sysmex users cannot use in their flows and apps.

EXAMPLE OF CONNECTOR GROUPS FOR



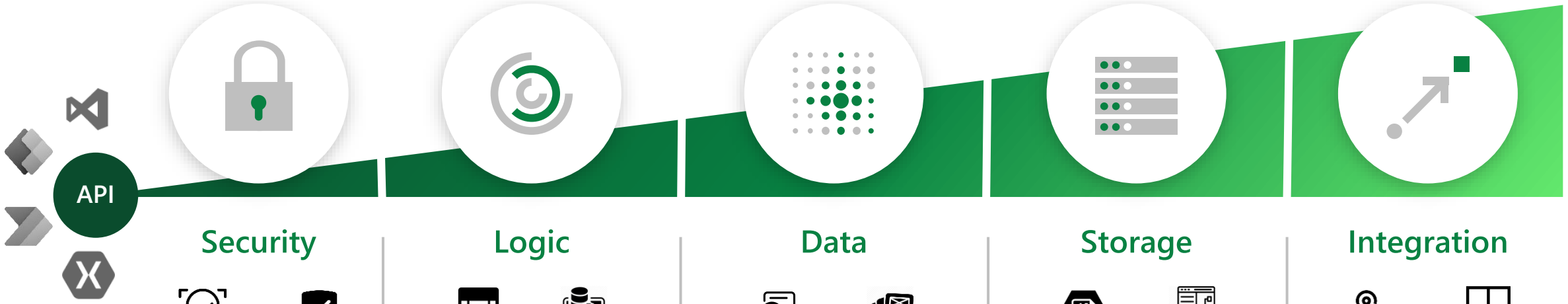
DEMO 4
DLP POLICES

DATA POLICIES (DLP)



1. Tenant access & isolation
2. Environment access & strategy
3. Resource permissions
4. Connector access and data loss policies
5. **Dataverse security**

MICROSOFT DATAVERSE – WHAT'S IN THE BOX?



Security

- Authentication
- Authorization
- Role-based security
- Auditing

Logic

- Calculated & Rollup fields
- Jobs
- Plugins
- Business Rules
- Duplicate Detection
- Workflows

Data

- Modelling
- Catalog and discovery
- Reporting
- Data validation
- Common Data Model
- Multi-language Multi-currency

Storage

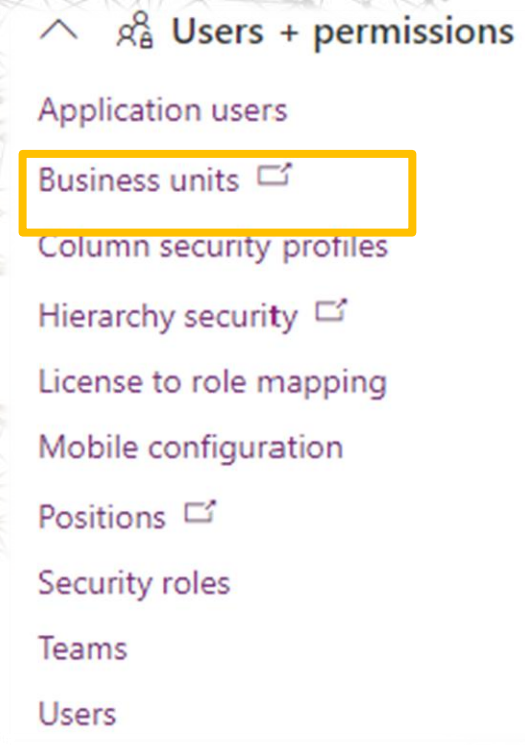
- Files and blobs
- Relational databases
- Semi-structured data
- Log files
- Relevance Search & Find data

Integration

- Webhooks
- ALM
- Azure DevOps
- Azure Synapse Analytics
- GitHub
- Data export

BUSINESS UNITS

- **Business units** work with **security roles** to determine the effective security that a user has.
- You can **create child business units** to help further segment your users and data.
- **Every user assigned to an environment** will belong to a business unit.



TEAMS

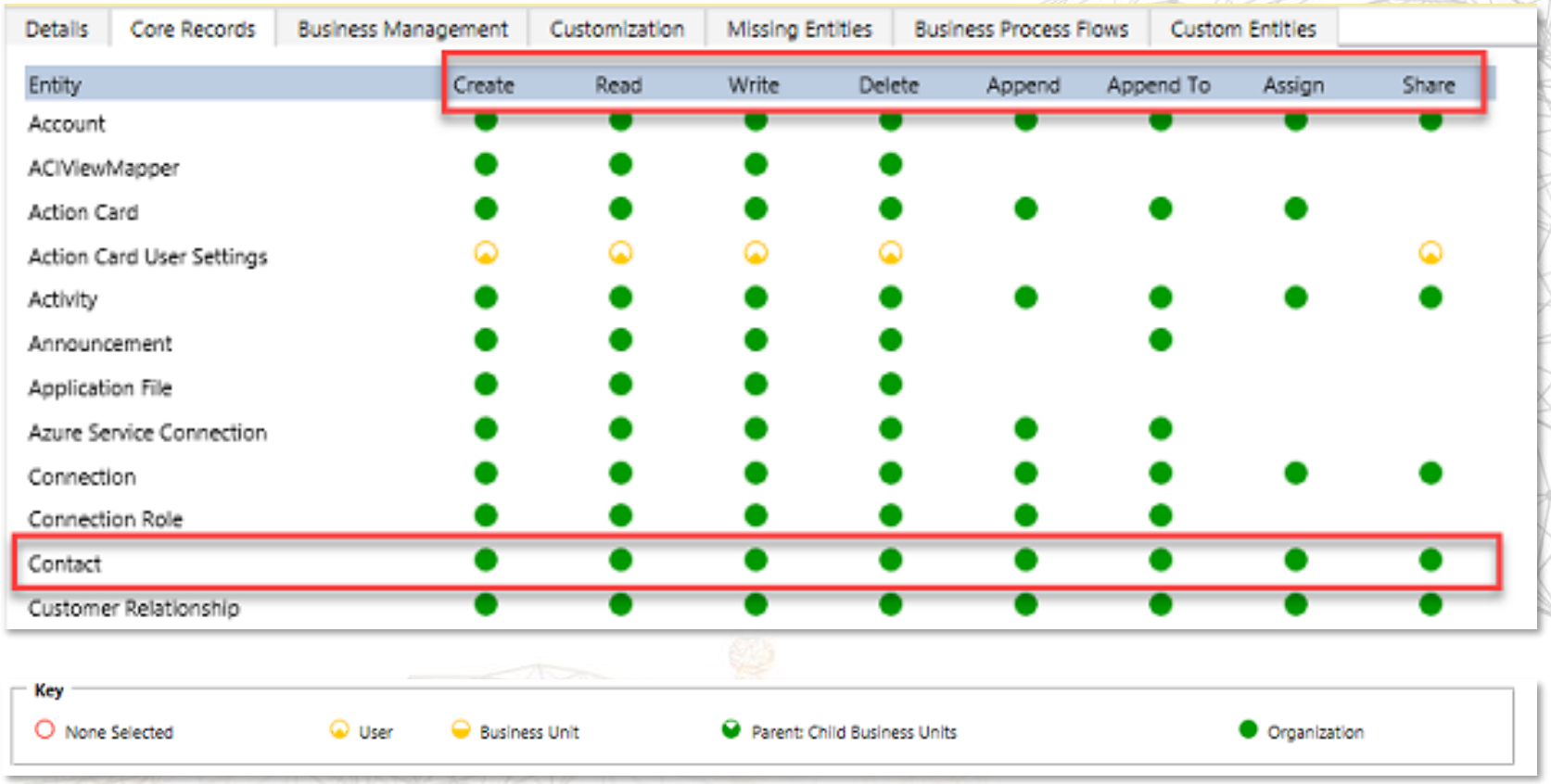
- Associate a **business unit** with an **Azure AD security group**
- Use **an Azure AD security group to map your business unit** for streamlining your user administration **and role assignment.**

SECURITY ROLES

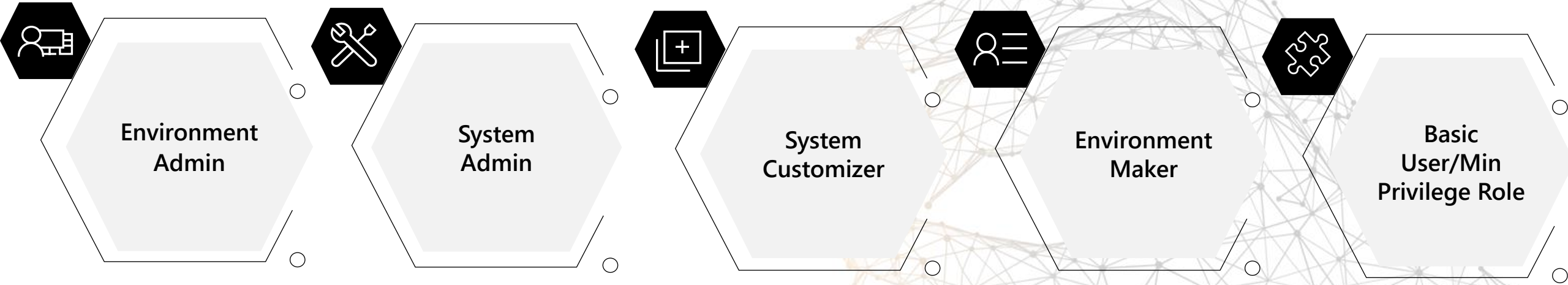
- **Security roles** can be **associated directly to users**, or they can be associated with **Dataverse teams** and **business units**.
- All users associated with the team will benefit from the role.

SECURITY ROLES – PRIVILEGES

- You can **either add more privileges** in an existing **security role or create a custom security role**.



KEY OUT-OF-BOX SECURITY ROLES YOU NEED TO KNOW



Perform all environment level **administrator tasks** – User mgmt., Dataverse provisioning, Resource mgmt., DLP mgmt etc

Customize or administer the **environment**, including creating, modifying, and assigning security roles. View all data in the environment (if licensed).

Customize the environment. View records for environment entities that they create.

Resource creation – apps, connections, custom APIs, gateways, and flows

Resource consumption by **end users for standard entities**

DEMO 5
DATAVERSE SECURITY

Any Questions?

Please fill out the survey!
& Win Swags!!

https://bit.ly/GPPBSurvey

Powered By upzids
Microsoft Solutions, Tailored for You

POWER PLATFORM BOOTCAMP

upzids
Microsoft Solutions, Tailored for You

Microsoft

#GlobalPowerPlatformBootcamp
#GPPB2024

Thanks To Our Sponsor's

Platinum Sponsor

Microsoft

upzoids
Microsoft Solutions, Tailored for You

Local Sponsors

THANK YOU

Resources: