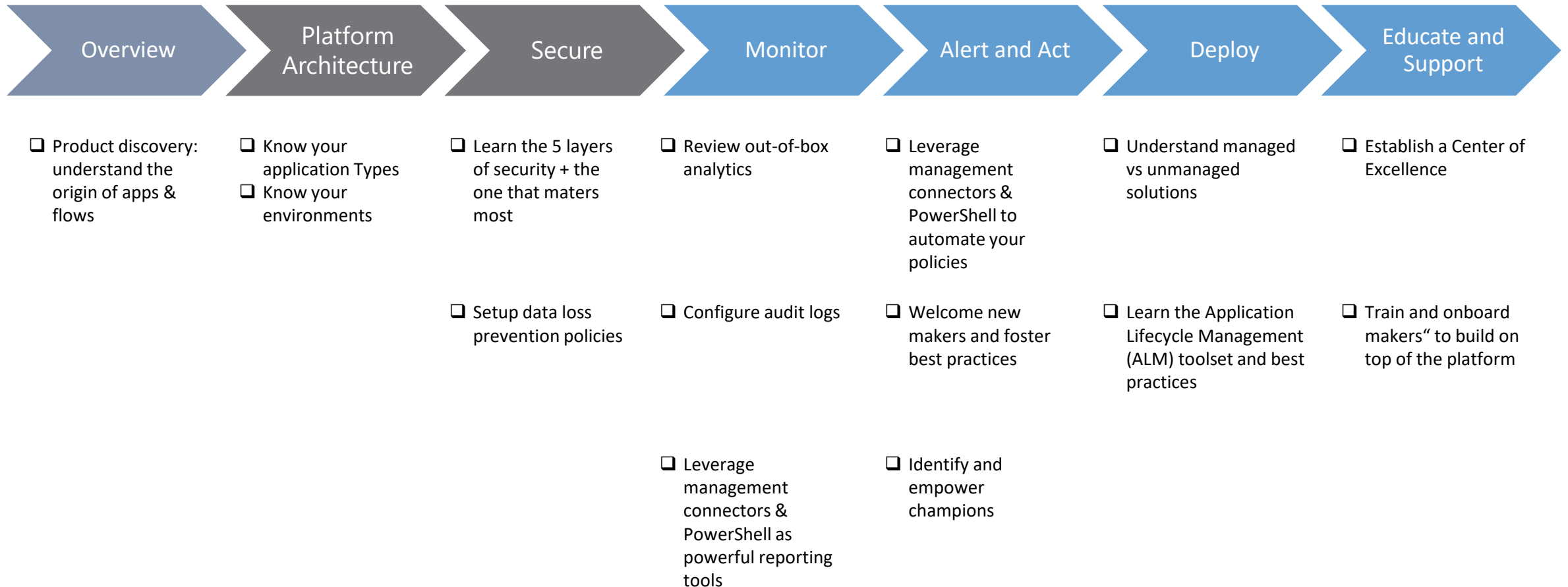


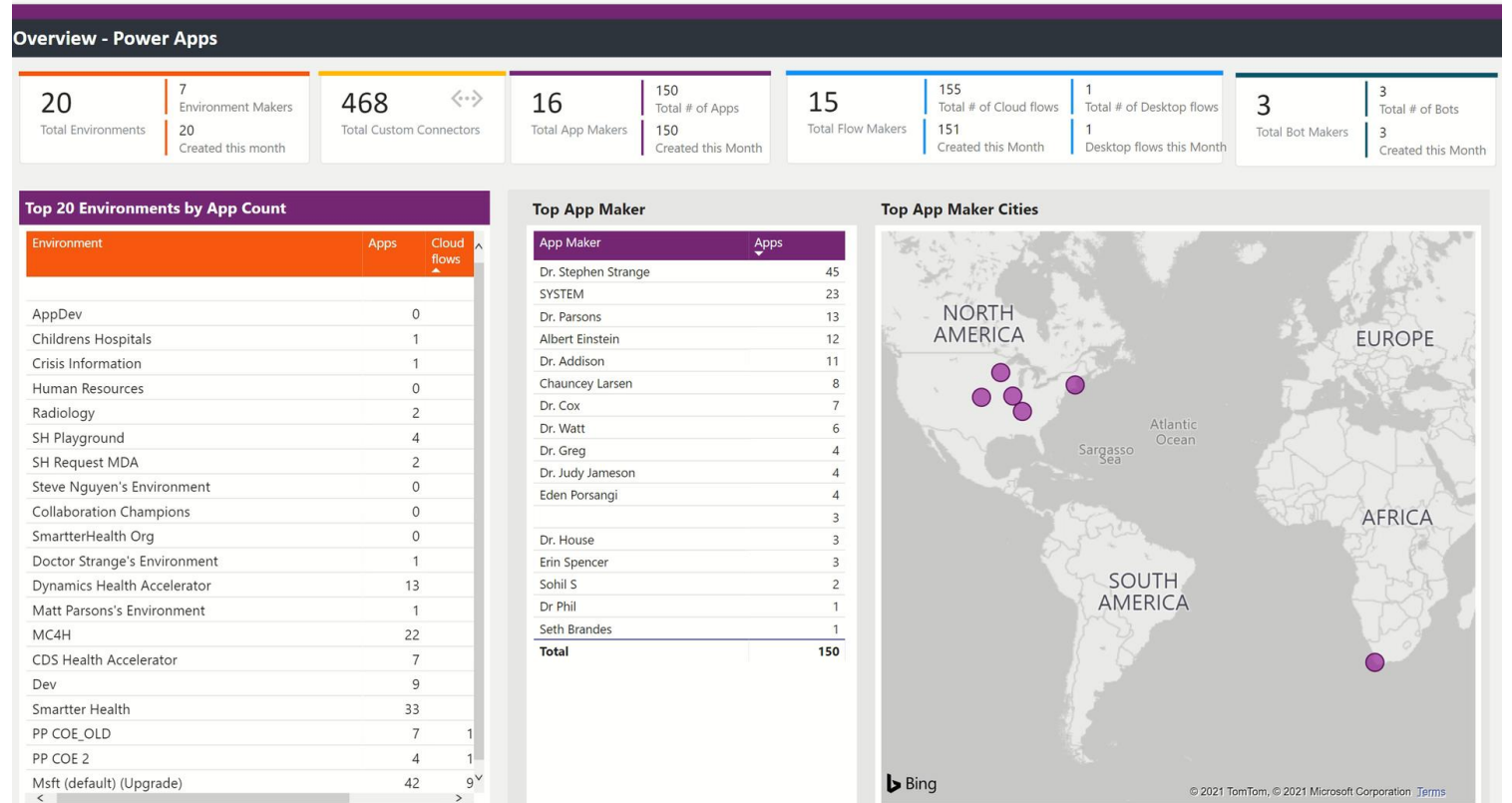
Governance – How to get started?

What's out of the box, what's in the CoE starter kit?

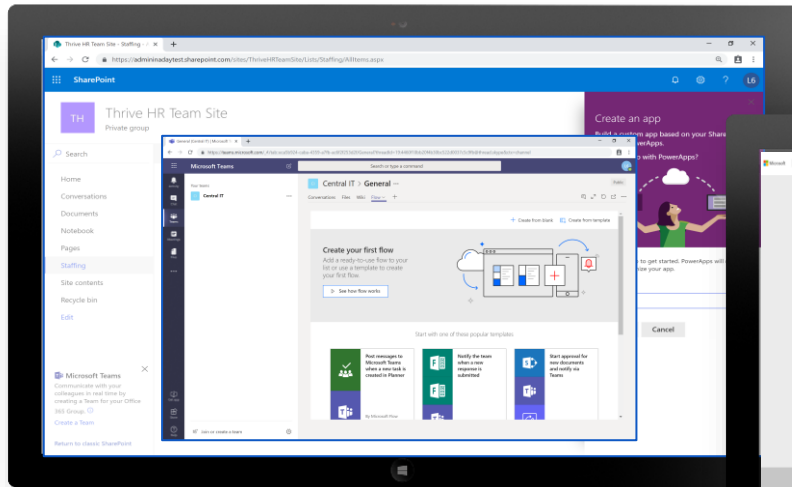


Product Discovery

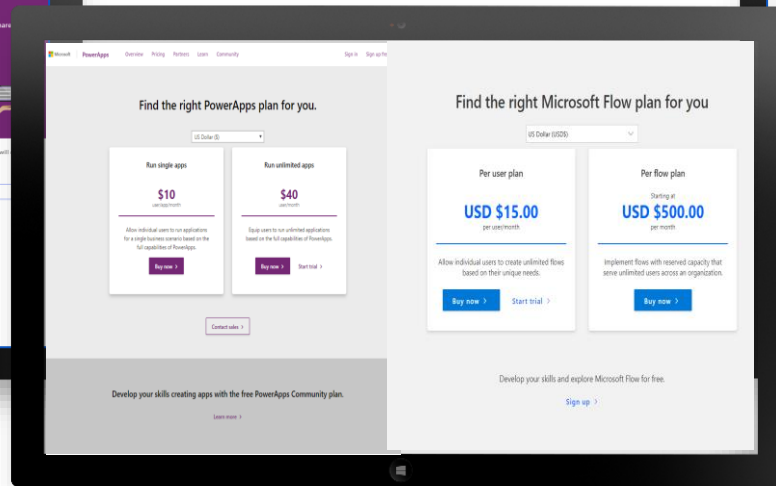
understand the origin of apps & flows



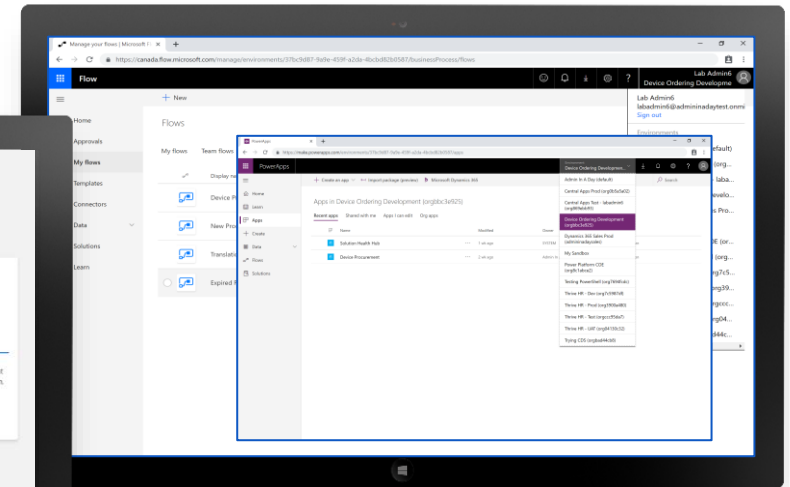
And where do apps and flows come from?



Power Apps and Power Automate provide customization for Office 365 and Dynamics 365



Individuals can sign-up to learn and test out: Power Automate or Power Apps community plan



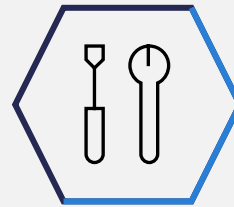
Power Apps and Power Automate paid licenses give users the ability to build stand-alone apps and flows

Define Organizational Admin Roles



Global Admin

Full administration to all services in tenant



Power Platform Admin

Dynamics 365 Admin

Power Platform Admin role



Delegated Admin

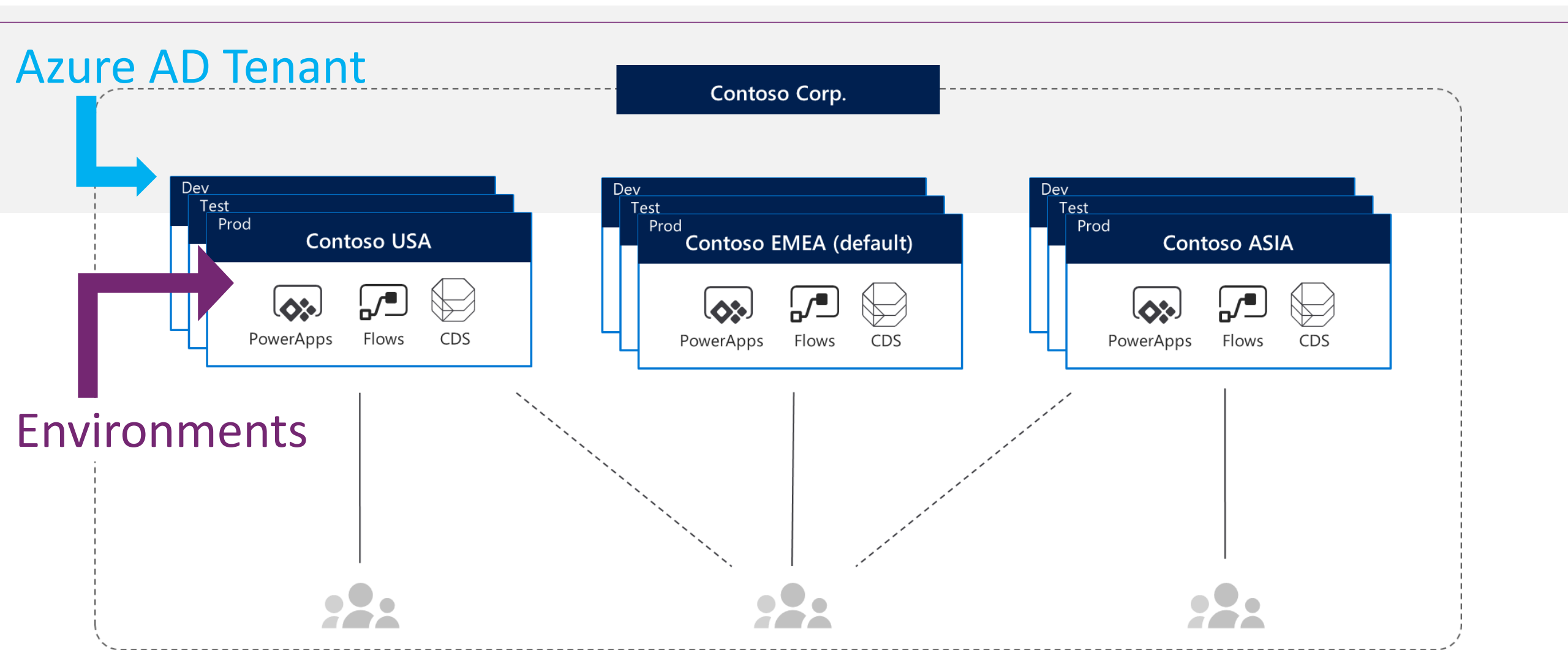
Full administration to all services in tenant

Used for partners to provide support to customers

Full support for Power Platform

Environments

Environments are containers that administrators can use to manage apps, flows, connections, and other assets; along with permissions to allow organization users to use the resources



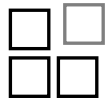
Environment – Key facts



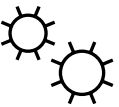
Environments are tied to a geographic location that is configured at the time the environment is created.



Environments can be used to target different audiences and/or for different purposes such as dev, test and production.

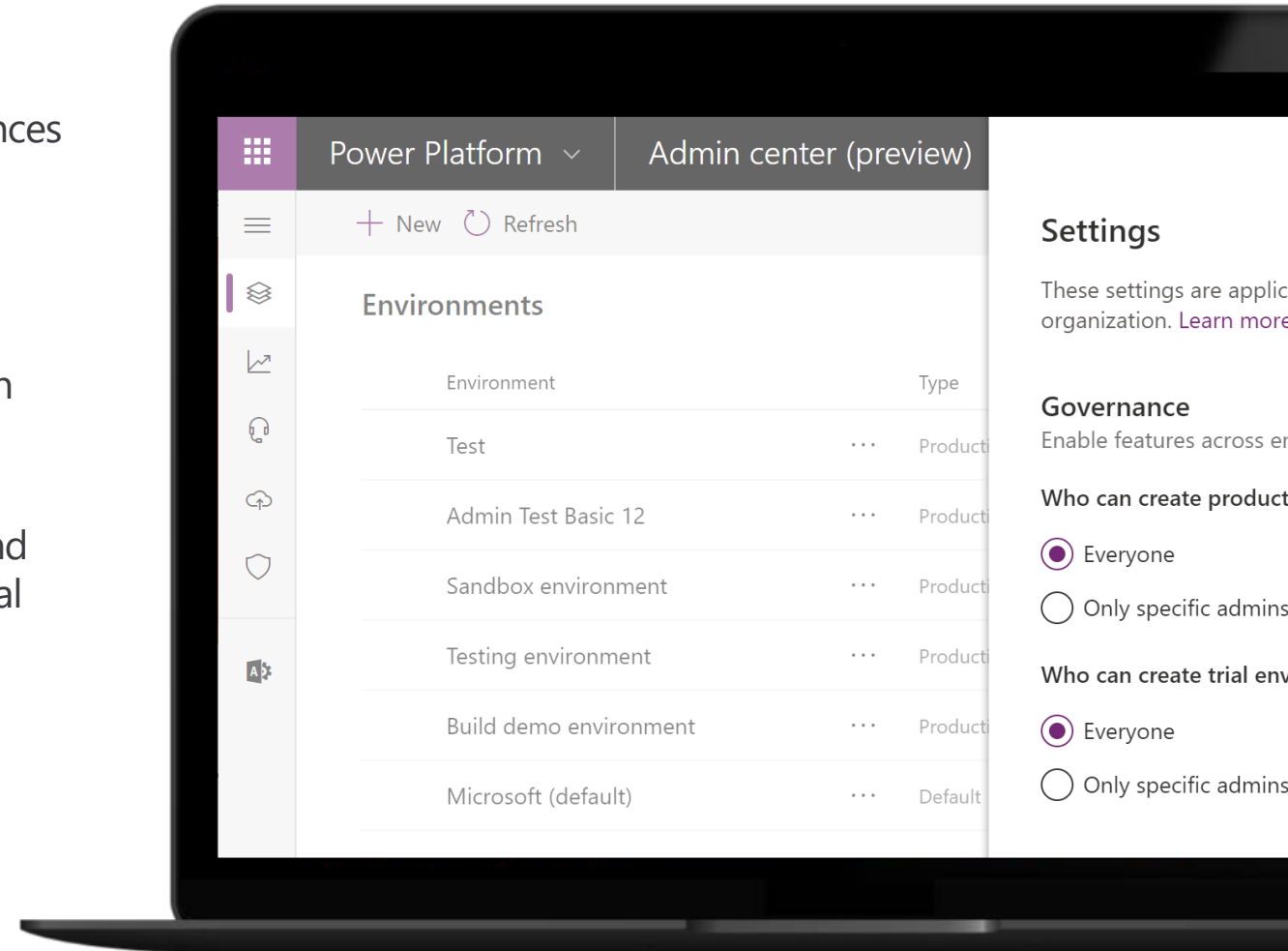


Every tenant has a Default environment where all licensed Power Apps and Power Automate users can create apps & flows.

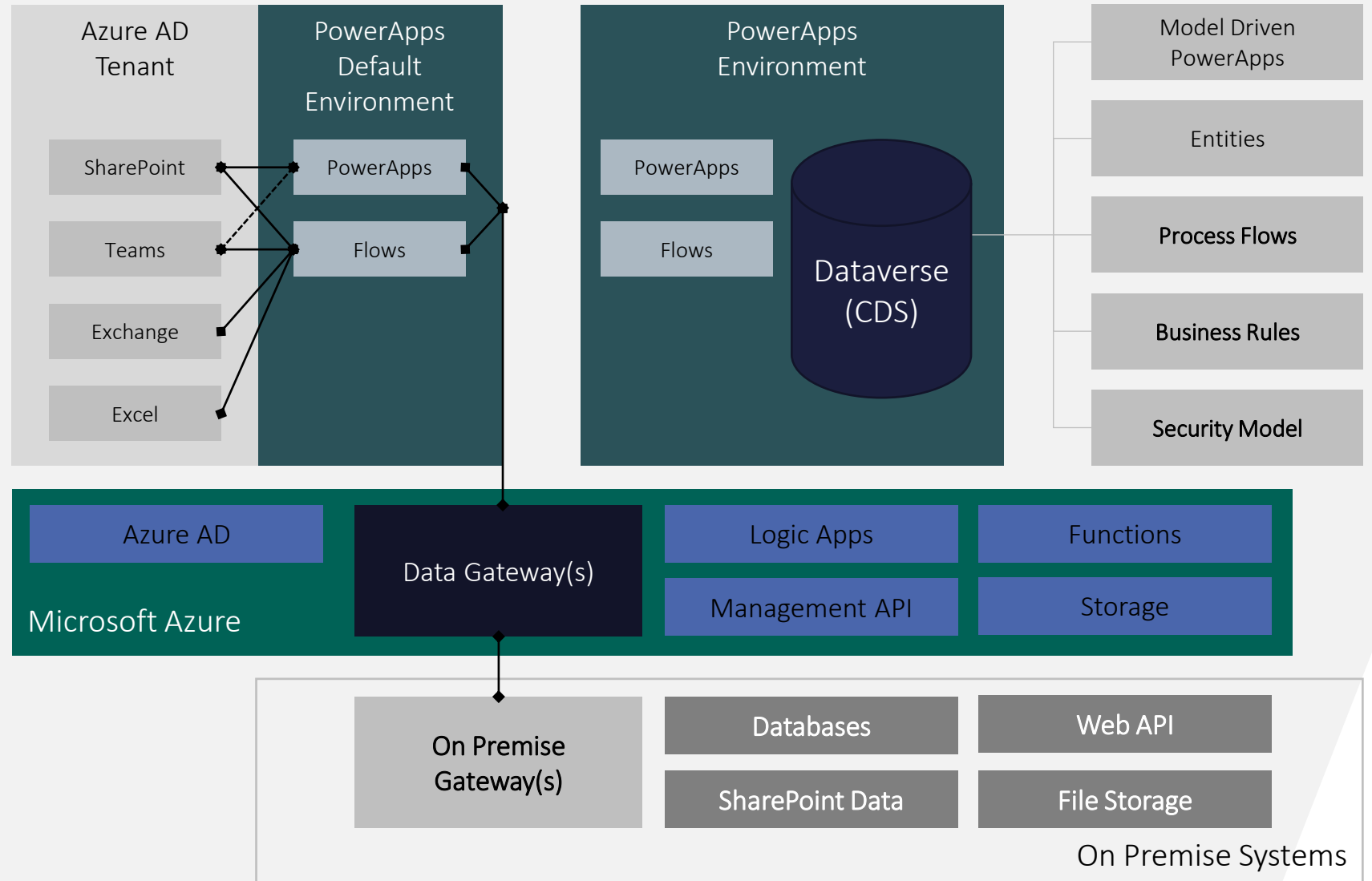


Non-default environments offer more control around permissions. Creation can be restricted to only global and service admins from the Power Platform admin center: <https://aka.ms/ppac>

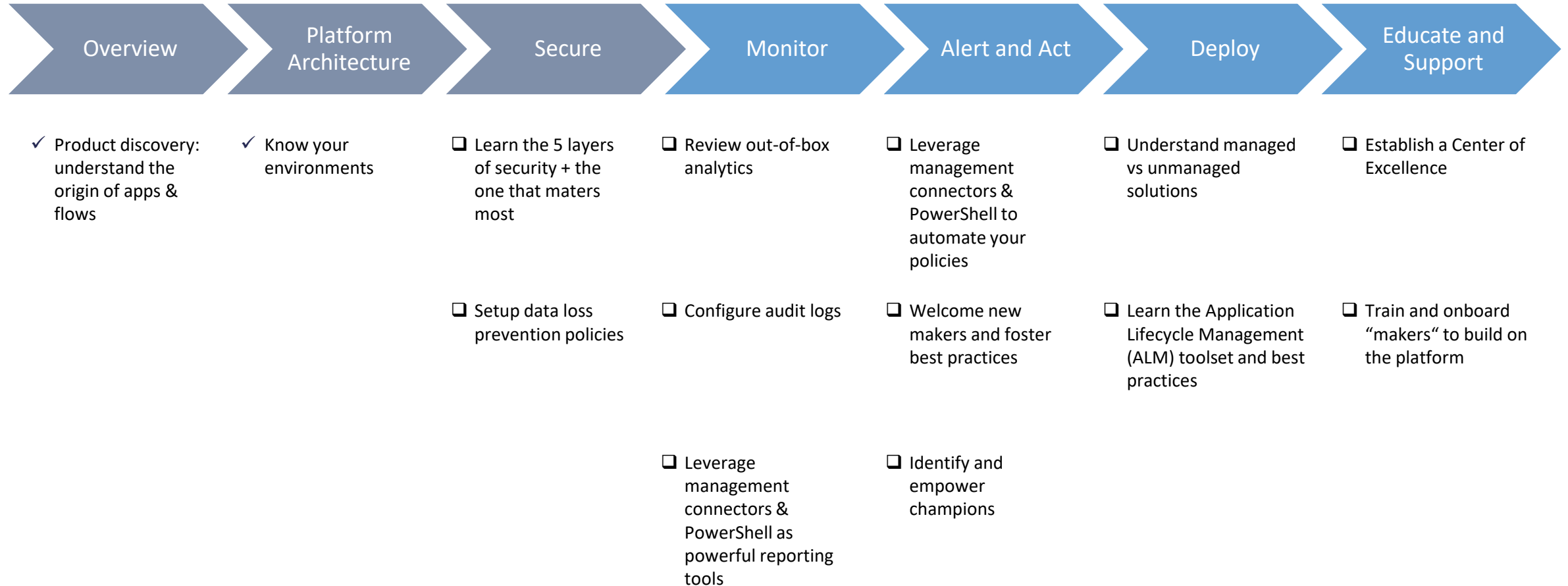
Automatically created with first user in the region closest to the Azure AD tenant



Looking inside environments



Governance – How to get started?



The 5 layers of security + the one that matters most

Less code. More Power. Faster Innovation.



Tenant level

Azure AD
Conditional Access



Environment level

Environments have two built-in roles that provide access to permissions within an environment



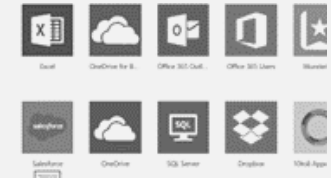
Resource level

Resource permissions for apps, flows, custom connectors...



Common Data Service

Assigned Common Data Service security roles



Cross Tenant level

Cross-tenant inbound & outbound restrictions to the 300+ connectors to cloud services, content services, DBs, APIs, etc..

Secure your data at rest

- There is no such thing as security through obscurity
- Power Apps & Power Automate do not provide users with access to any data assets that they don't already have access to.
- Users should only have access to data that they really require access to.

Conditional service access

Azure AD Premium required

Scenario coverage

Grant/block access based upon



User/Group



Device



Location

The screenshot displays the Azure AD Conditional Access configuration interface. It is divided into three main sections:

- New:** Contains an 'Info' section with a name field. Below are 'Assignments' for 'Users and groups' (1 user included), 'Cloud apps' (0 cloud apps selected), and 'Conditions' (0 conditions selected). Under 'Access controls', there are sections for 'Grant' (0 controls selected) and 'Session' (0 controls selected).
- Cloud apps:** Features 'Include' and 'Exclude' buttons, radio buttons for 'None', 'All cloud apps', and 'Select apps', and a 'Select None' button.
- Select:** A list of applications is shown, with 'Power Automate' highlighted in a red box. Other applications include Microsoft Azure Information Protection, Microsoft Azure Management, Microsoft Cloud App Security, Microsoft Demos, Microsoft Forms, Microsoft Intune Enrollment, and Microsoft Power BI.