Microsoft

Module 4

Data Loss Prevention Policies

Microsoft Customer Success Unit

CONDITIONS AND TERMS OF USE:

Introduction

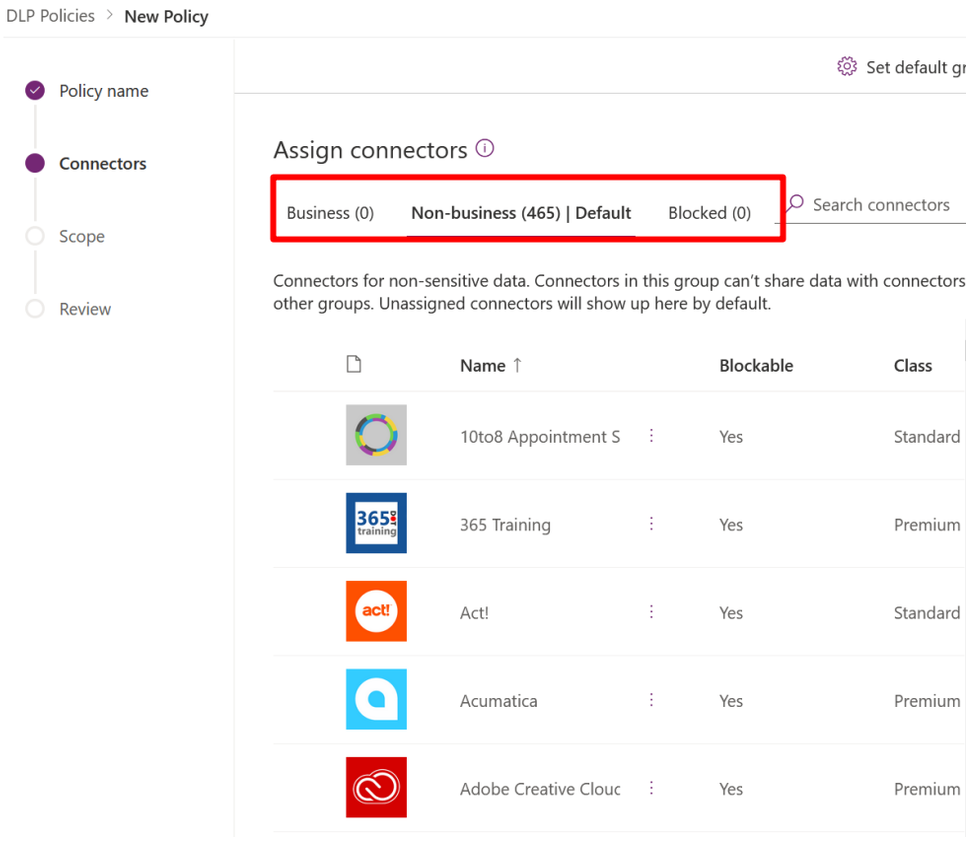
In this lesson, you will learn the following:

- Understand Data Loss Prevention Policies.
- DLP Policies Scope.
- How to Create a DLP Policy.
- How to Manage a DLP Policy.

Data Loss Prevention Policies

Data Loss Prevention Policies

- Power Platform DLP policies allow you to control data flows across data connectors when used within Power Apps and Power Automate
- Simply put, DLP enables admins to isolate business data from personal use data within Power Platform
- Able to classify Power Platform connectors across business and non-business groups and additionally choose to block certain connectors
- As you see on the user interface here the DLP policy allows admins to segregate connectors across three different buckets – **Business**, **Non-business** and **Blocked**



Connectors Classification

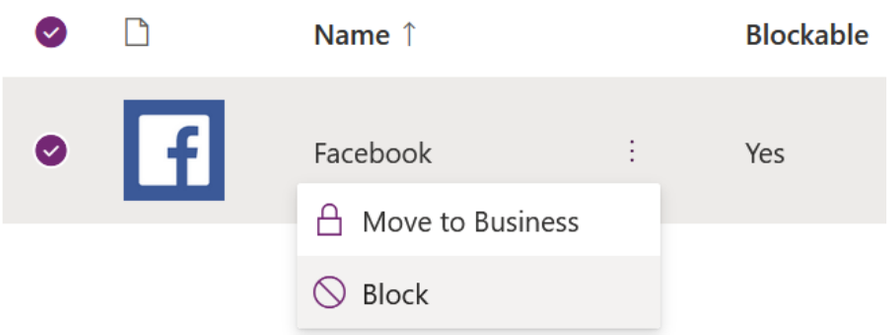
Business	Non-business	Blocked
A given Power App or Power Automate resource can use one or more connectors from Business group	A given Power App or Power Automate resource can use one or more connectors from **Non-business** group	Any Power App or Power Automate resource cannot use any connector from **Blocked** group
If a Power App or Power Automate resource uses a **Business** connector, it cannot use any **Non-business** connector	If a Power App or Power Automate resource uses a **Non-business** connector, it cannot use any **Business** connector	All Microsoft owned premium connectors and third-party connectors (standard and premium) can be blocked
		All Microsoft owned standard connectors and Microsoft Dataverse cannot be blocked

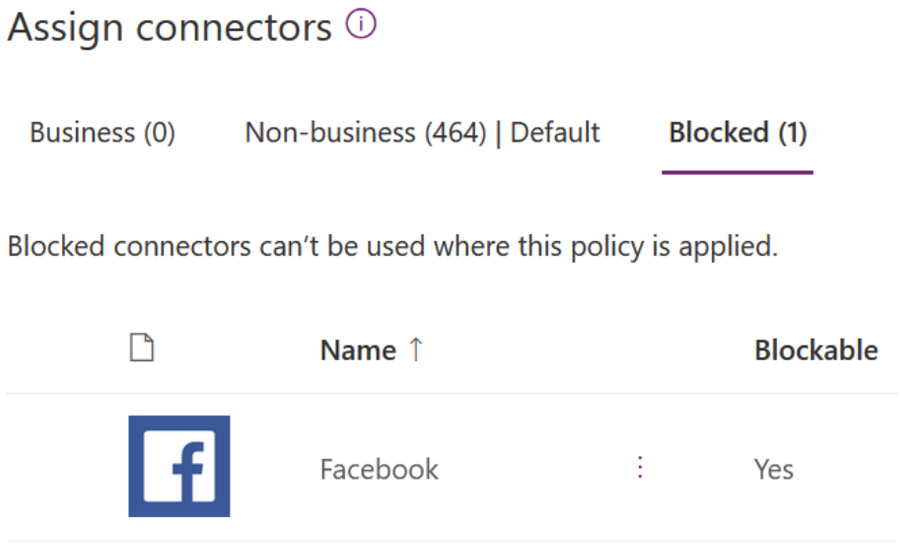
How Data is Shared among Data Groups?

- Data **can't** be shared among connectors that are located in different groups.
- For example, if you place **SharePoint** and **Salesforce** connectors in the Business group and you place **Gmail** in the Non-Business group, makers can't create an app or flow that uses both the SharePoint and Gmail connectors.
- This in turn restricts data flows between these two services in Microsoft Power Platform.
- Although data can't be shared among services in different groups, it can be shared among services within a specific group.
- From the earlier example, because **SharePoint** and **Salesforce** were placed in the same data group, makers can create an app or flow that uses both SharePoint and Salesforce connectors together.
- This in turn allows data flows between these two services in Microsoft Power Platform.
- The key point is that connectors in the same group can share data in Microsoft Power Platform, whereas connectors in different groups can't share data.

Blocked Data Group

- Data flow to a specific service can be blocked by marking that connector as **Blocked** which restricts all data flows to this service in Microsoft Power Platform.
- For example, if you place Facebook in the Blocked group, makers can't create an app or flow that uses the Facebook connector.
- All third-party and Microsoft-owned Premium (except Dataverse) connectors can be blocked.
- All connectors driving core Power Platform functionality like Dataverse and Approvals as well as connectors enabling core Office customization scenarios like Microsoft Enterprise Plan standard connectors will remain non-blockable to ensure core user scenarios remain fully functional.
- These non-blockable connectors can be classified into Business or Non-Business data groups.





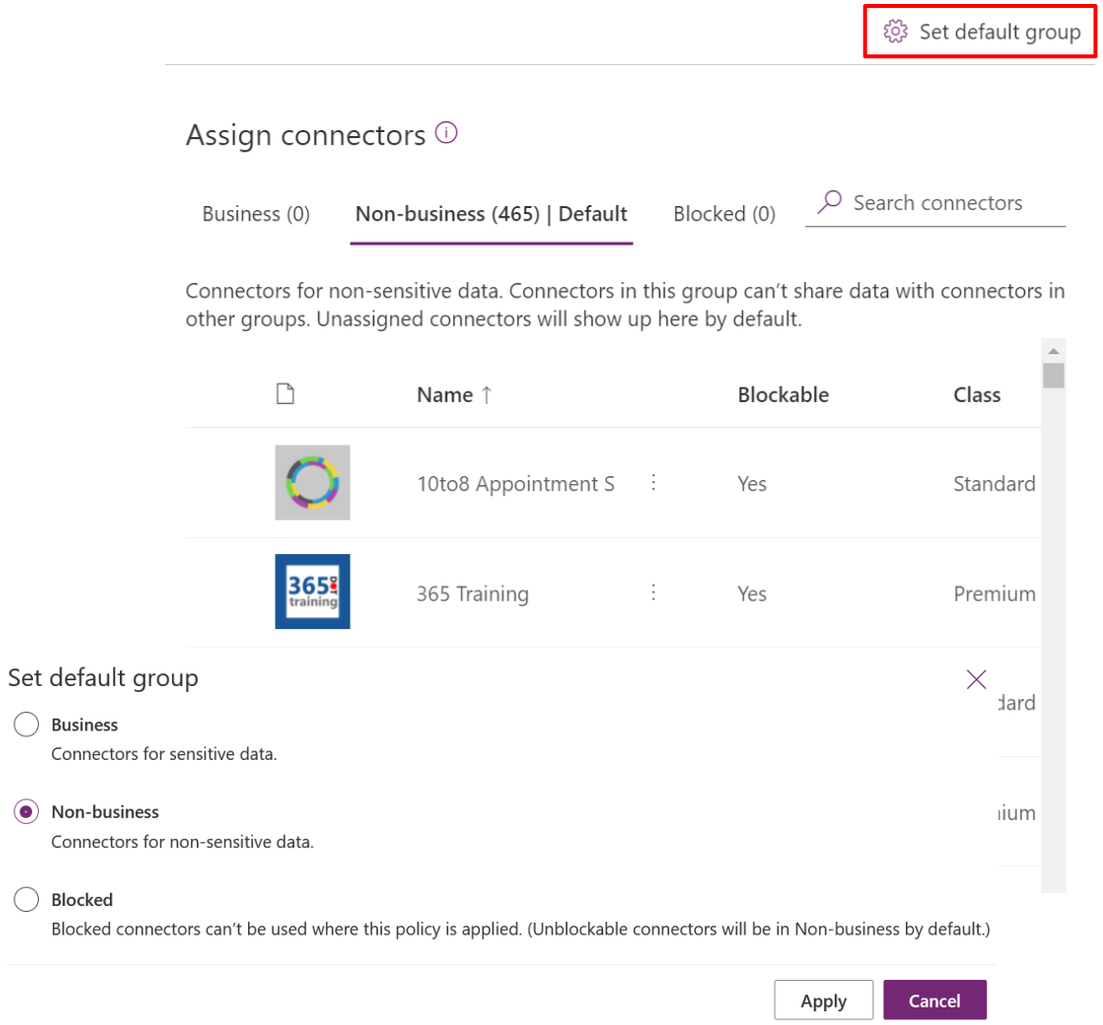
Custom Connector Classification

- At the moment custom connectors aren't part of the standard configuration capabilities of DLP policies in the **Power Platform admin center**.
- You have to use PowerShell commands to set and manage custom connectors in DLP policies PowerShell commands to set them up into Business, Non-Business, and Blocked groups.
- As custom connectors are **environment level** resources you <u>can</u> use them only in environment level policies
- By using PowerShell, you can configure DLP policy to include these connectors.

Default Data Group for New Connectors

Following grouping logic is applied to new connectors added to Power Platform:

- Power Platform connector ecosystem keeps evolving and adding new connectors
- If connectors are added after DLP policy creation, admins have not had a chance to explicitly categorize them.
- These new connectors are automatically added to 'default connector' group identified for them
- Admins can set the 'default connector' group for new connectors in a DLP policy to – Business or Non-business or Blocked
- Admins can review these new connectors retrospectively and classify them explicitly as appropriate



Policy Scope

Tenant policies have three scope settings

All environments

By default, tenant level policies will be applied to all environments created in the tenant

All except selected environments

Tenant admins can choose to exclude specific environments to apply the policy

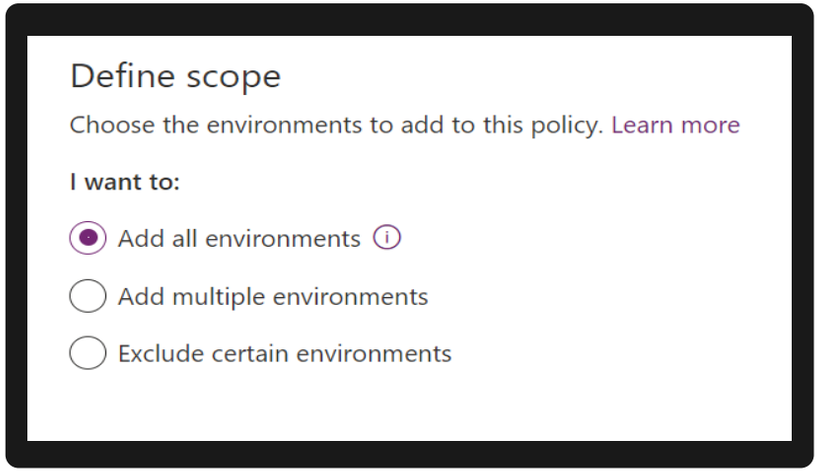
Only selected environments

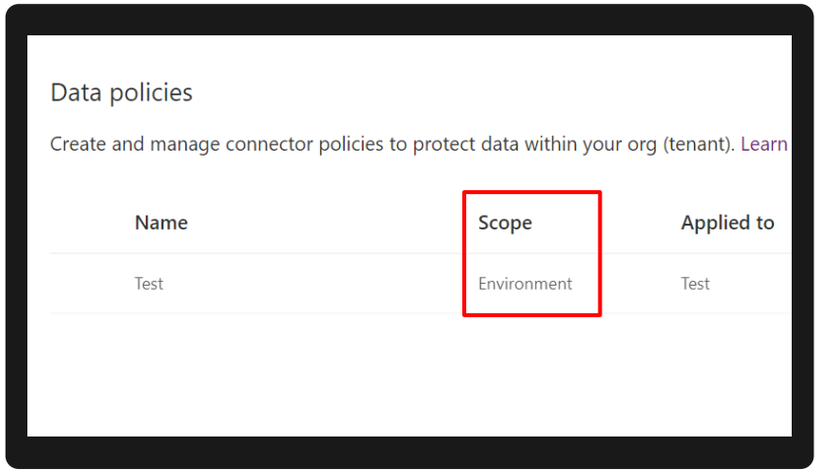
Tenant admins can choose to include only specific environments to apply the policy

Environment policies have one setting

One environment only

Environment admins can choose to apply the policy on one environment at a time

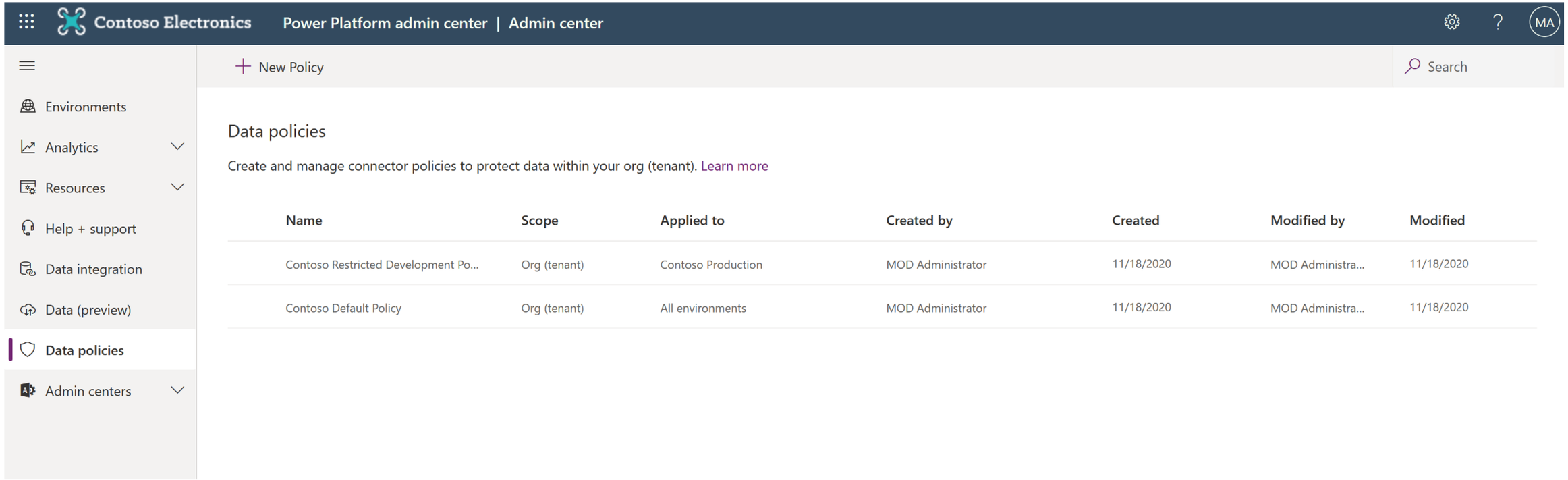




View DLP Policies

Using the view policy feature, environment admins can view tenant-level policies and policies within environments that the admin has access to, at an individual policy level.

Non-admins can also view tenant-level policies using this feature.



Combining DLP Policies Impact

Blocked connectors

- If a connector is marked as ‘blocked’ in any one DLP policy applied to the environment, then the net outcome is that this connector is blocked from usage within the environment
- It doesn’t matter if other DLP policies applied to the environment mark it as business or non-business

Business/Non-Business connectors

If all DLP policies applied to the environment mark certain set of connectors as business or non-business, then the most **restrictive** groupings define what connectors can be used together vs. not

For example –

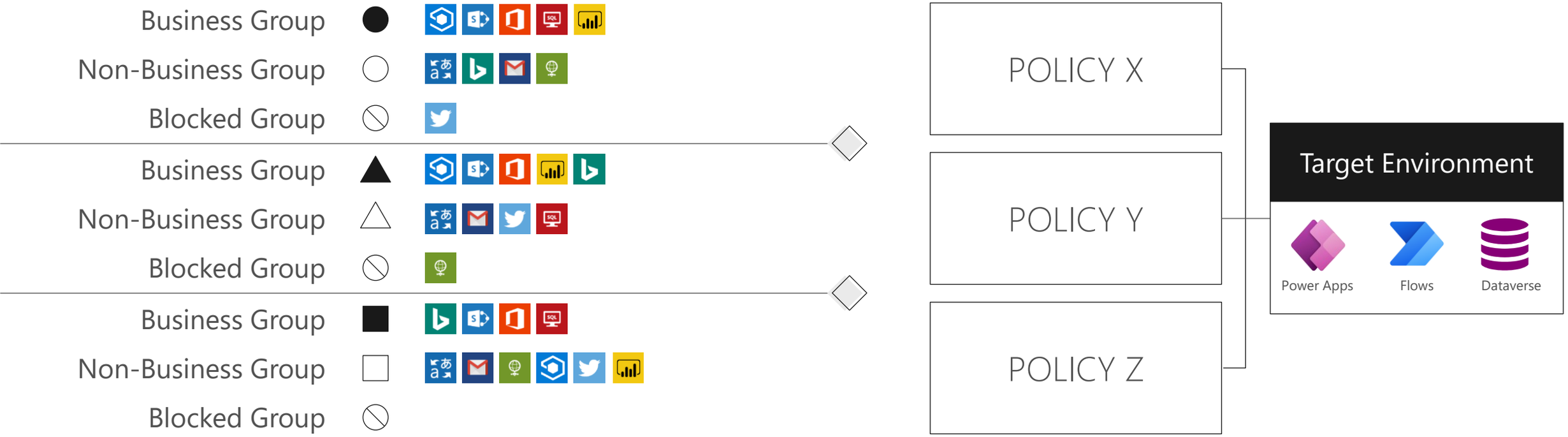
Policy X = B {1,2,3} NB {4,5} ; Policy Y = B {3,4,5} NB {1,2}

Then –

Net outcome : {1,2} {3} {4,5}

Power Platform Multiple DLP Policy –

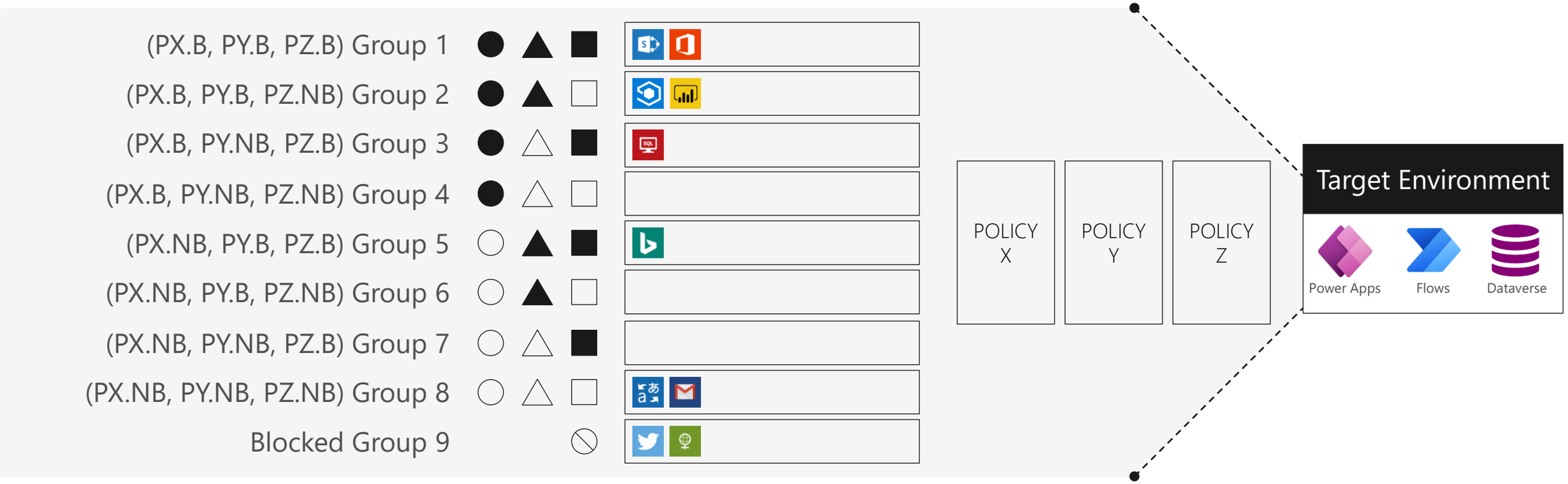
Example Scenario



Multiple DLP policies applied to the same environment grouping connectors across Business/Non-business/Blocked. This set up makes the outcome of what connectors can be used together – Fragmented and hard to predict

Power Platform Multiple DLP Policy –

Net Outcome



All blocked connectors map to blocked. For business/non-business - 3 policies will fragment connector grouping outcome into as many as 3^2 = 8 different sets. For predictable outcomes use minimal number of DLP policies per environment

DLP Policy Enforcement

Design-time

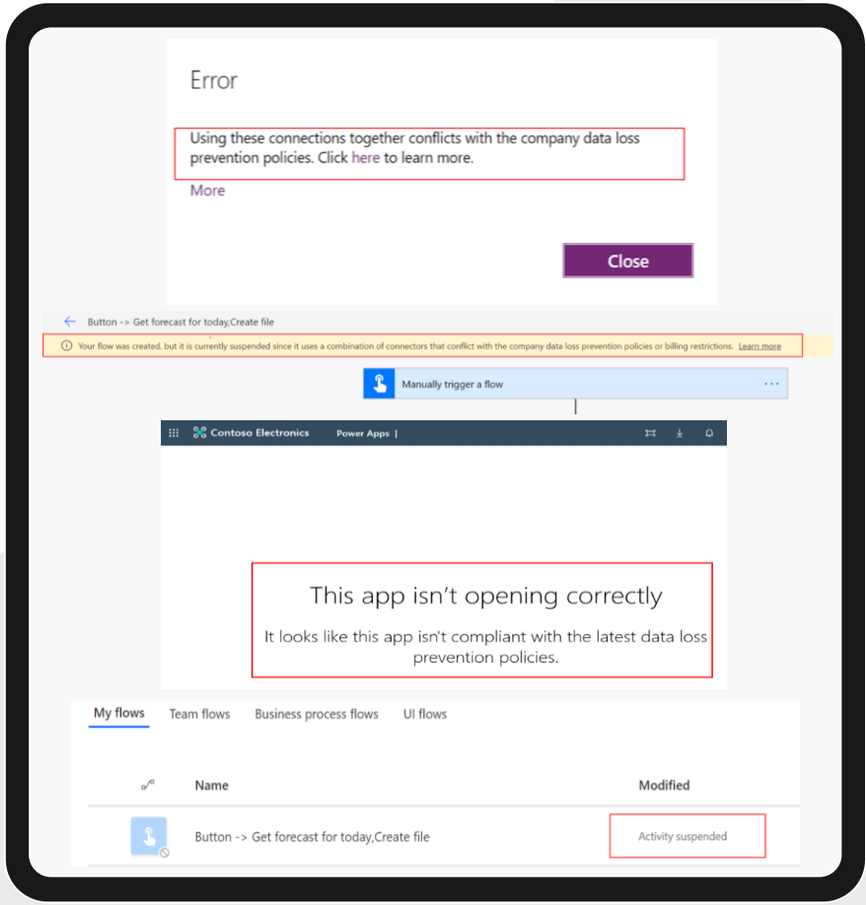
Power Apps makers see an error upon using connectors that don't belong together or are blocked using DLP policies. Apps violating DLP policies cannot be saved at design time unless DLP violation is resolved.

Power Automate makers see a warning while saving a flow using connectors that don't below together or are blocked using DLP policies Flow will be saved but marked as 'Suspended' and will not execute unless DLP violation is resolved.

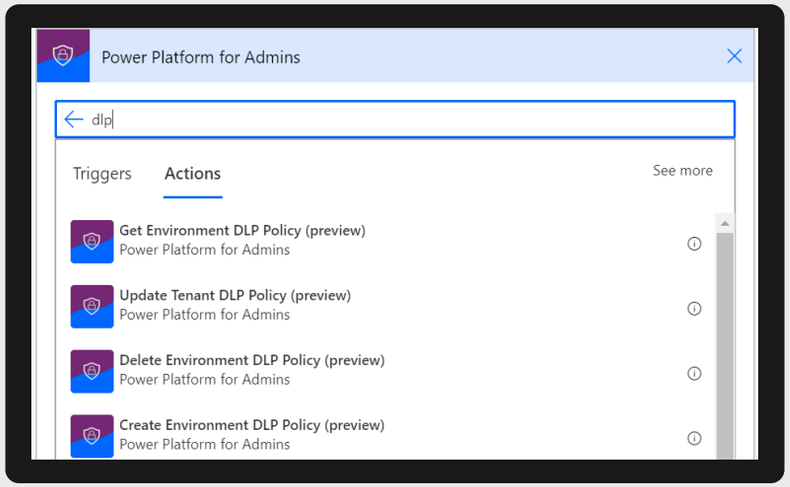
Run-time

If DLP policy changes impact an existing Power App negatively and it becomes non-compliant then users are no longer able to launch it and get an error.

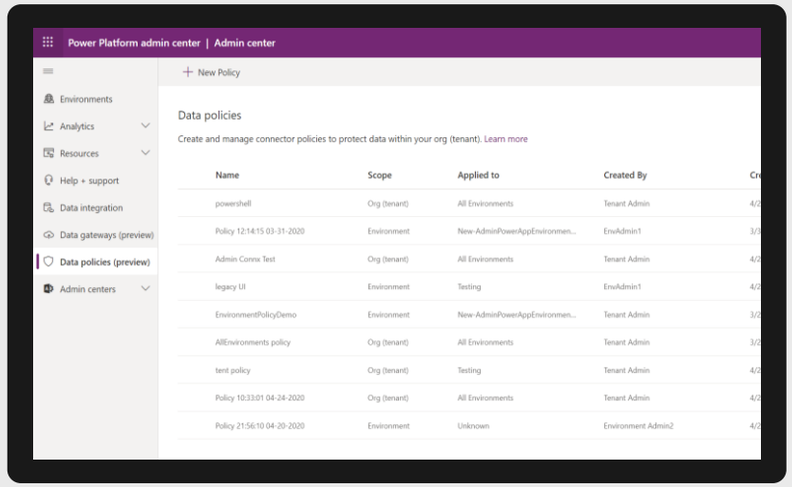
If DLP policy changes impact an existing Power Automate negatively and it becomes non-compliant then it is automatically marked as suspended users are no longer able to execute it. Power Automate suspension may take ~5 mins to come into effect after policy changes.



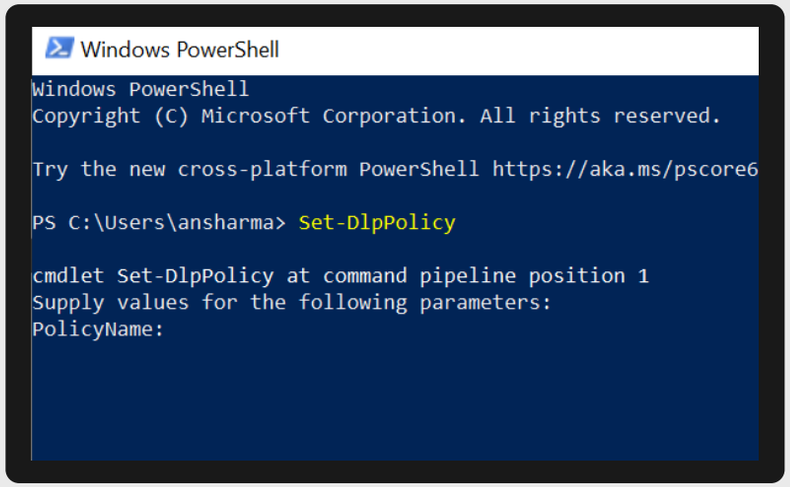
DLP Management Interfaces



Power Platform for Admins Connector



Power Platform Admin Center



Power Apps PowerShell

Labs: Module 4

1. Create DLP Policy Using UI
2. Create DLP Policy using PowerShell

Microsoft