





Thibault JOUBERT

WAVESTONE

(2016 – 2021)



Depuis Novembre 2021



<https://www.thijoubert.com/>



<https://fr.linkedin.com/in/thijoubert>



@thijoubert/

Au programme

- PARTIE 1 : Quels risques pour la Power Platform ?
- PARTIE 2 : Quelles mesures concrètes pour assurer un niveau minimal de sécurité ?



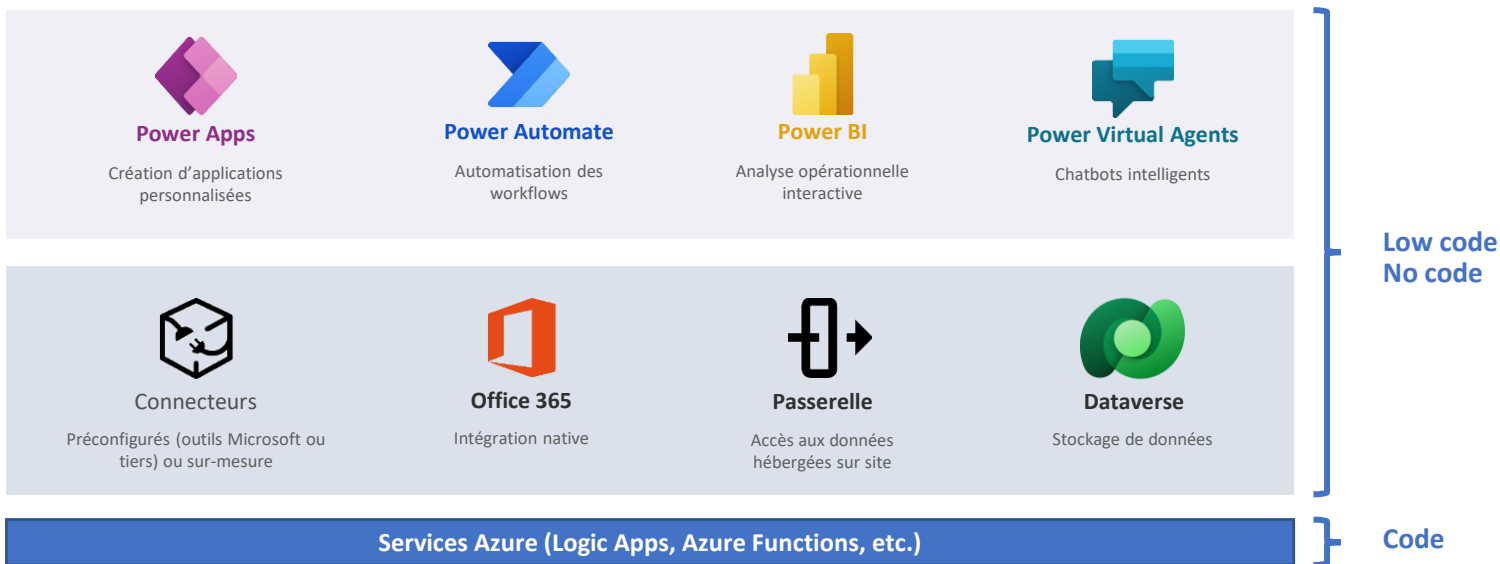
PARTIE 1

Quels risques pour la Power Platform ?



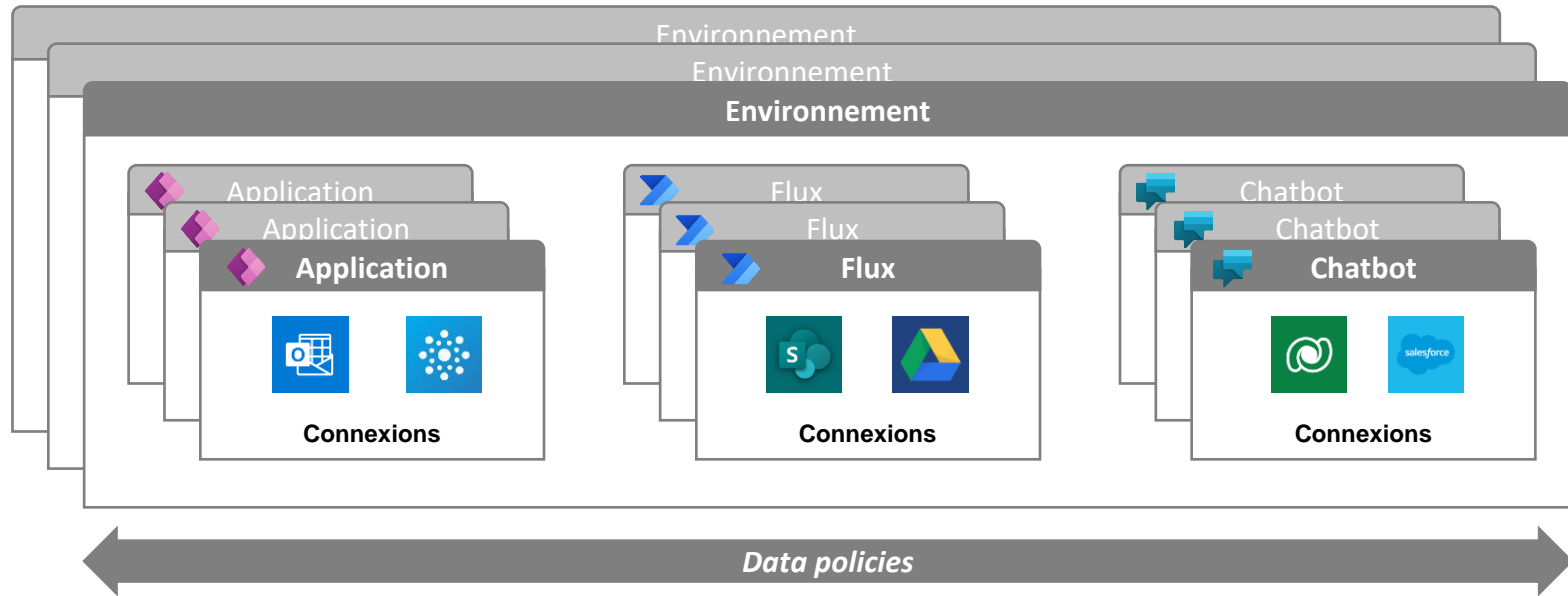
Rappel sur le low / no code et la Power Platform

- Le **Low code / no code** désigne les outils permettant **aux utilisateurs non IT** de **créer des applications** avec des composants préconstruits, **souvent intégrées à leurs outils de productivité habituels (Office 365)**
- « **Power Platform** » est la **plateforme low code / no code de Microsoft** regroupant quatre produits permettant de **visualiser et recueillir** des données, **automatiser** des processus et **interagir** avec des utilisateurs.





Architecture Power Platform



- **Connecteur** : proxy / wrapper générique autour de webservices
- **Connexions** : instantiation du connecteur au sein d'une application ou d'un flux pour un utilisateur



Pourquoi la Power Platform un sujet pour les entreprises ?

- Low code / no code : Opportunité pour les métiers (pénurie de développeurs, réponse rapide à des problèmes simples)
- Power Platform : Inclus dans les licences Microsoft
- Gartner : 65% des applications en 2024 (2019)
- Forrester : 40% des futures applications vers 2025 (2019)
- Et ça c'était avant la COVID-19...
- Plusieurs grands comptes ont lancé des plans pour déployer largement le Power Platform ou une autre plateforme



Pourquoi la Power Platform est (vraiment) un sujet pour les équipes sécurité ?

- La Power Platform est en plein essor, les programmes d'adoption se lancent et les utilisateurs commencent à jouer avec dans l'environnement Default, mais les équipes sécurité ne sont pas embarquées dans la démarche...

Manque de connaissance

Manque de recul

- ... Alors que si non maîtrisés, les services de la Power Platform peuvent présenter des **NOMBREUX RISQUES**



Phishing Externe : Partage d'une application Power Apps



Phishing Interne : Partage d'une application ou d'un flow (co-propriétaire)

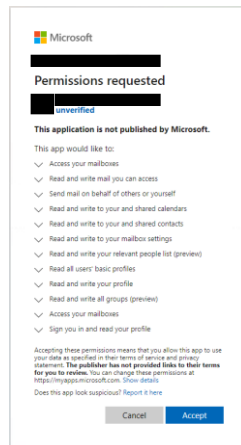


Persistance en cas d'intrusion : Création de connexion



Action malveillante ou erreur

- Extraction de données
- Ransomware / Destruction de données
- Exposition de données





« Je ne me sens pas concerné »

- **Mais je n'ai pas de licence Premium ...**

→ Les connecteurs standards Office 365 sont « largement suffisants » pour poser des risques



- **Mais je n'ai déployé que Teams et SharePoint**

→ Les licences Office 365 E1, E3 et E5 incluent nativement Power Apps for Office 365 ou Power Automate for Office 365

- **Mais je n'ai pas donné de licences Power Apps ou Power Automate for Office 365 ...**








→ Par défaut, un utilisateur peut s'octroyer une licence gratuite, prendre une licence développeur ou souscrire à une plan premium payant

- **Mais je n'ai pas donné d'accès ou de droits à un environnement Power Apps**

→ L'environnement « Default » est accessible par tous les utilisateurs avec un rôle de maker

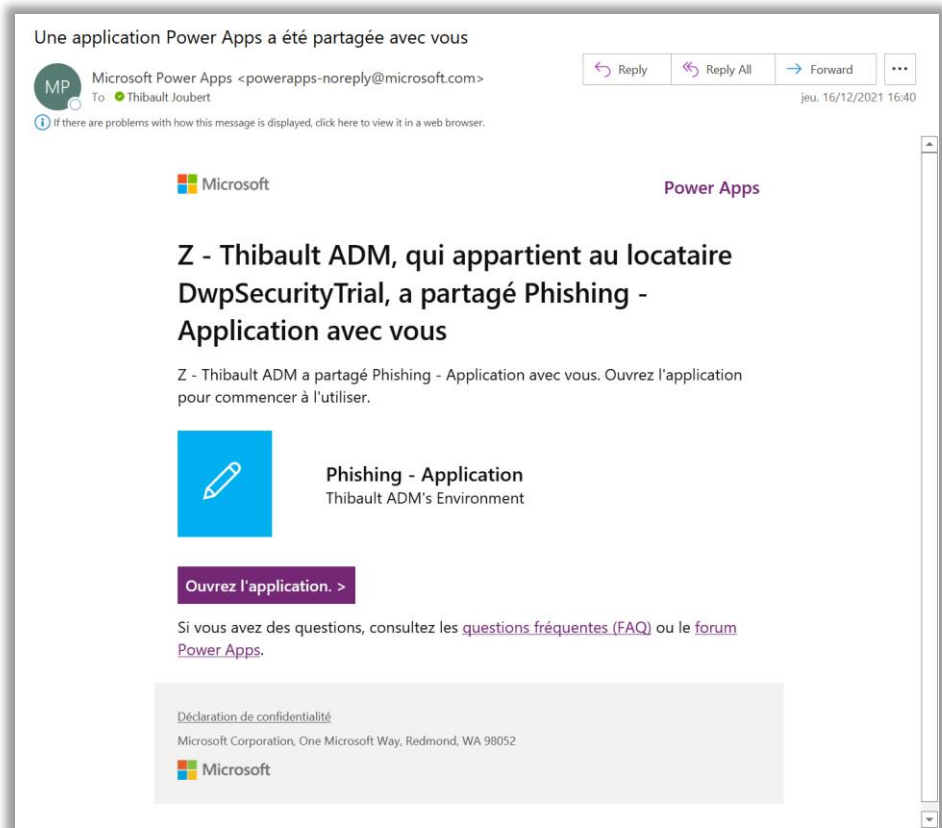


Risques liés aux connecteurs standards Office 365

	Connecteurs	Exemples d'actions	Atteinte à la donnée	Usurpation d'identité	Automatisation et multiplication d'actions
	SharePoint Online	<ul style="list-style-type: none">Grant access of share items or filesModify items or filesSend an HTTP request to SharePoint	✓		✓
	Office 365 Users	<ul style="list-style-type: none">Get user profileGet manager	✓		✓
	Outlook	<ul style="list-style-type: none">Get or Export emailsSend a new mailCreate or modify events	✓	✓	✓
	Microsoft Teams	<ul style="list-style-type: none">Create a teamAdd or delete a memberGet or post messages within chat		✓	✓
	OneDrive for Business	<ul style="list-style-type: none">Create sharing linkCreate, Modify or Delete files	✓		✓
	Excel	<ul style="list-style-type: none">Get, Create or Modify worksheetsSame things for Word and PowerPoint	✓		✓
	Office 365 Groups	<ul style="list-style-type: none">Send an HTTP request (preview)Add or Remove a member to groupList groups that I own and belong to	✓		✓

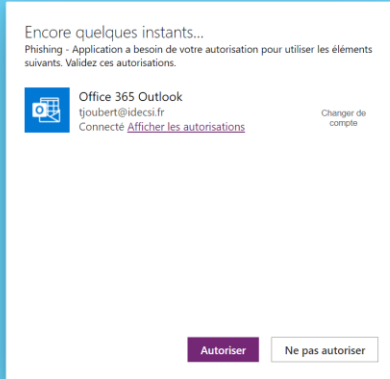


Exemple 1 : Phishing via une application





Exemple 1 : Phishing via une application



[Déclaration de confidentialité](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



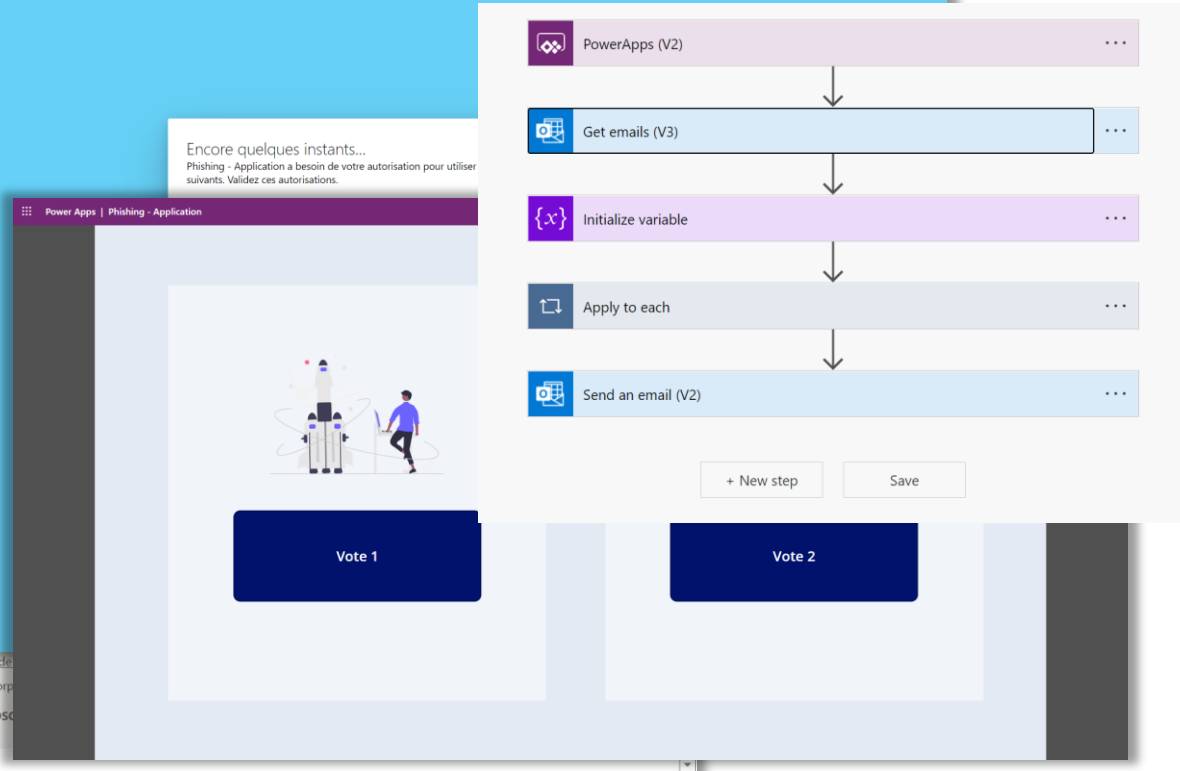


Exemple 1 : Phishing via une application





Exemple 1 : Phishing via une application





Exemple 1 : Phishing via une application

Encore quelques instants...

Phishing - Application a besoin de votre autorisation pour utiliser suivants. Validez ces autorisations.

Power Apps | Phishing - Application

Vote 1

PowerApps (V2)

Get emails (V3)

Initialize variable

Apply to

Send an email

Got phished

This message was sent with Low importance

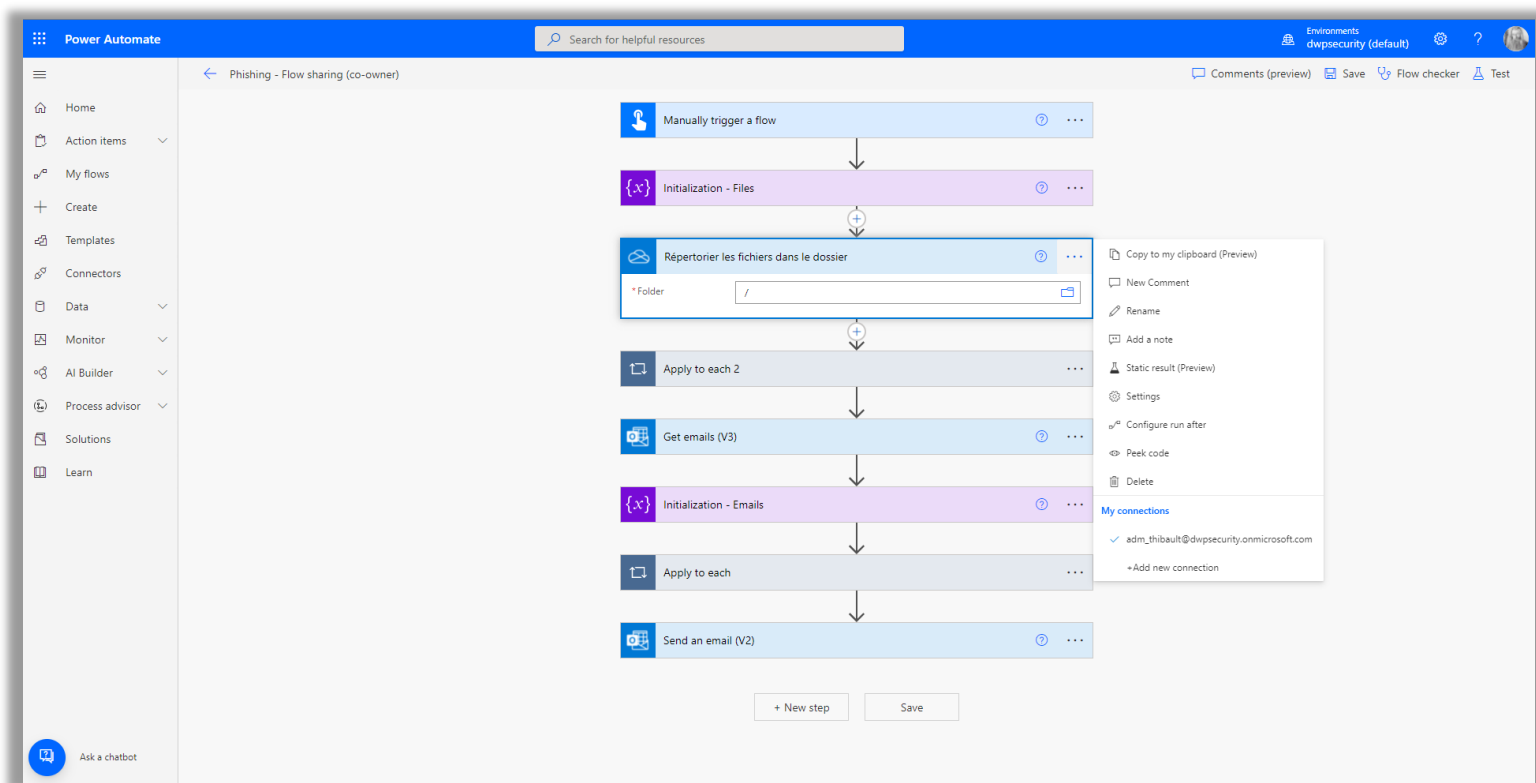
Z - Thibault JOUBERT
Wed 12/15/2021 4:12 PM
To: Z - Thibault JOUBERT

Got phished
Got phished
Got phished
An app is ready to use in IRM - Case 001
Azure AD Identity Protection Weekly Digest
Companies and customers win with Okta—here's how
Notification: Test3-Doc3
You've joined the MG - DLP - Test 3 group
You've joined the MG - DLP - Test 2 group
You've joined the MG - DLP - Test 1 group

Reply | Forward



Exemple 2 : Phishing via un flux (*co-owner*)





Exemple 2 : Phishing via un flux (*co-owner*)

The screenshot shows the Microsoft Power Automate web interface. The left sidebar contains navigation options: Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area displays the 'Phishing - Flow sharing (co-owner)' flow. A modal dialog box titled 'Connections Used' is open in the center. The dialog contains the following text:

Connections Used

Owners of the flow will have full access to all connections in the flow and the content within the connected accounts. Owners are not required to add connections to their own accounts, and can take any actions in existing connections and their content.

adm_thibault@dwpssecurity.onmicrosoft.com
Office 365 Outlook

Owners with access to this connection can:

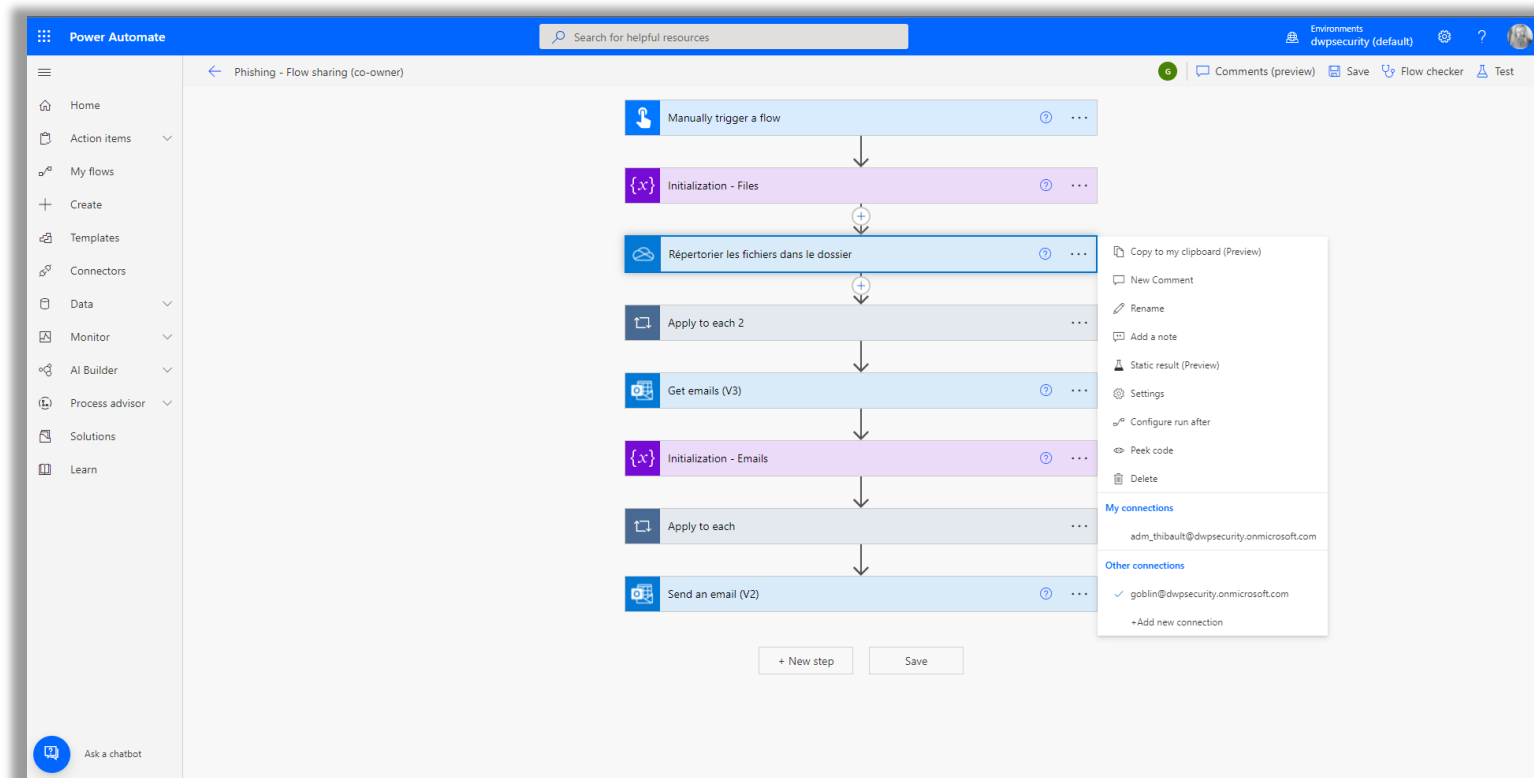
- Read your user profile
- Read, update, and delete your mails
- Send mail as signed in user (you)
- Create, read, update, and delete events
- Create, read, update, and delete contacts

Only add owners to a flow if you wish to share full access to all connections and the content within them. If you want to have someone else edit a flow offline without granting access to connections, you can export your flow. [Learn more](#)

At the bottom of the dialog are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

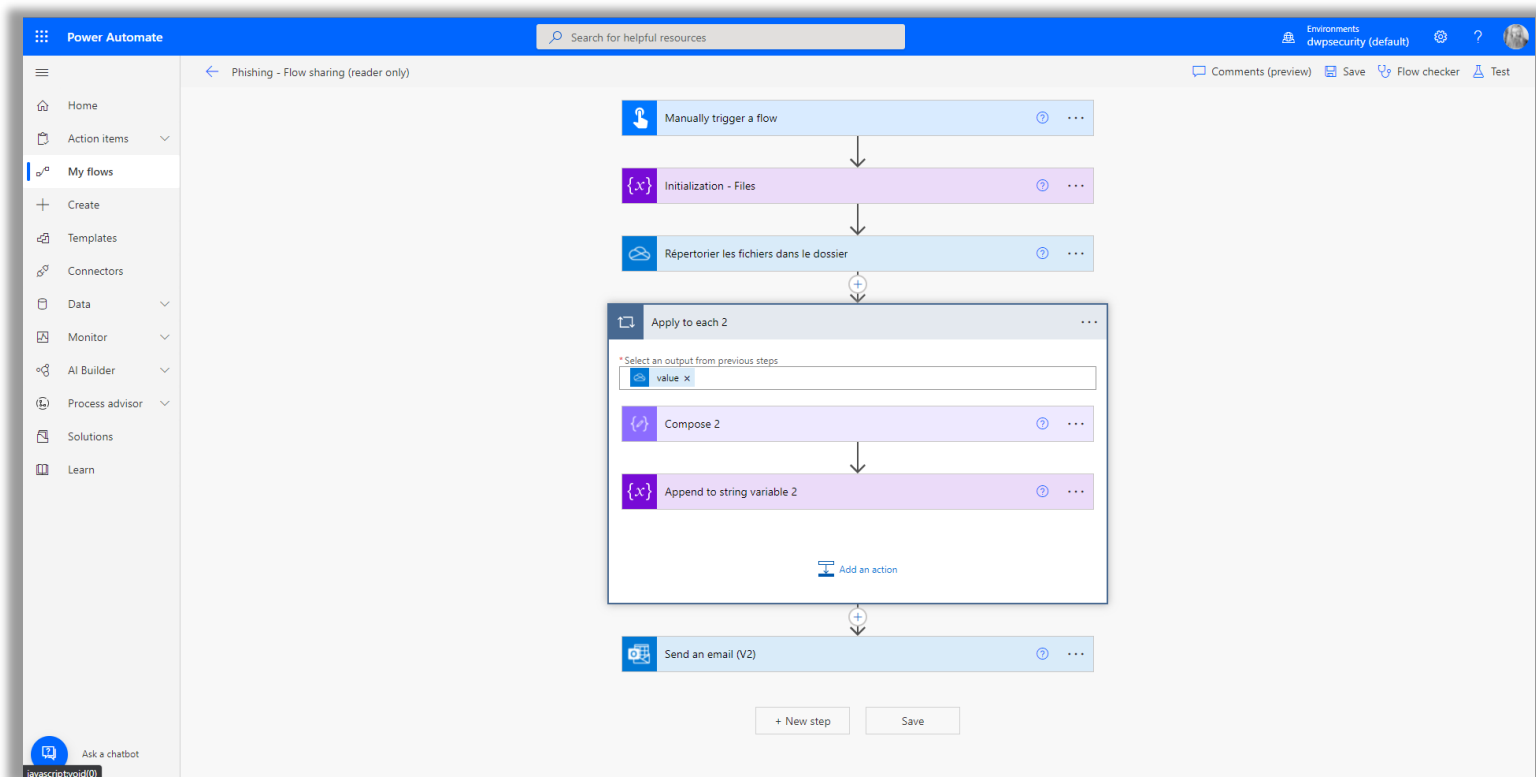


Exemple 2 : Phishing via un flux (*co-owner*)





Exemple 3 : Phishing via un flux (*read only*)





Exemple 3 : Phishing via un flux (*read only*)

The screenshot displays the Microsoft Power Automate interface. The left sidebar shows the navigation menu with options like Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area shows the details of a flow named "Phishing - Flow sharing (reader only)".

Details:

Flow	Status
Phishing - Flow sharing (reader only)	On

Owner	Created
Z - Thibault JOUBERT	Dec 15, 03:50 PM

Modified	Type
Dec 15, 03:51 PM	Instant

Plan
Per-user plan

28-day run history [All runs](#)

Your flow hasn't been run yet. Select Run to see it work.

Manage run-only permissions

Invite users or groups
Let others run this flow and see the results, but not edit in any way.

Enter names, emails, or user groups

Owners
Gobin
gobin@dwpscurity.onmicrosoft...

Currently shared with
This flow has not been shared with any users. Add a person and see their name here.

Connections Used
These connections will provide the users listed here to have run-only access to this flow. Unless providing their own connection, run-only users will not have access to these connections outside this flow.

Run only

Your flow

Office 365 Outlook
Access to this connection is provided by the owner of the flow.

Use this connection (adm_thibault@dwpscurity.onmicrosoft.com)

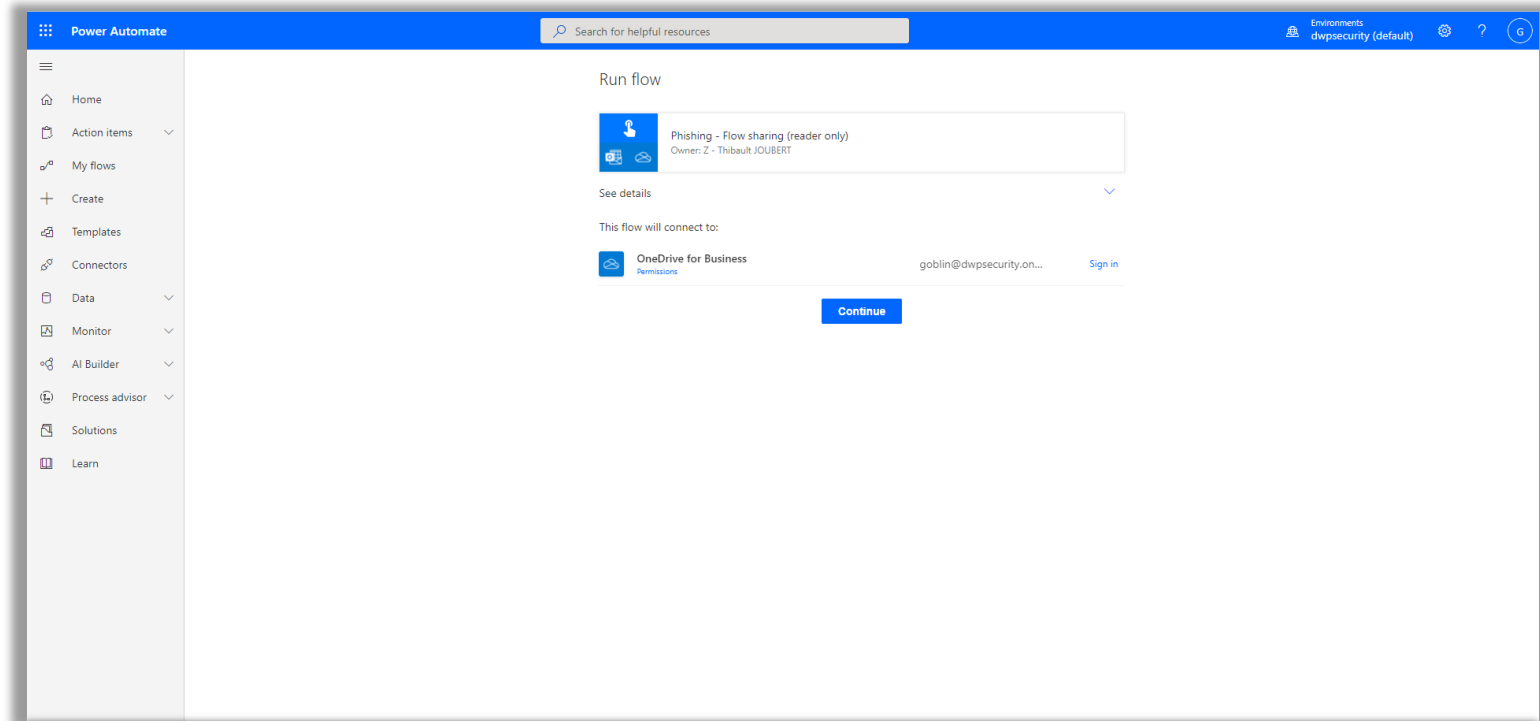
OneDrive for Business
Run-only users will be asked to provide their own connection to this connector.

Provided by run-only user

Save **Cancel**

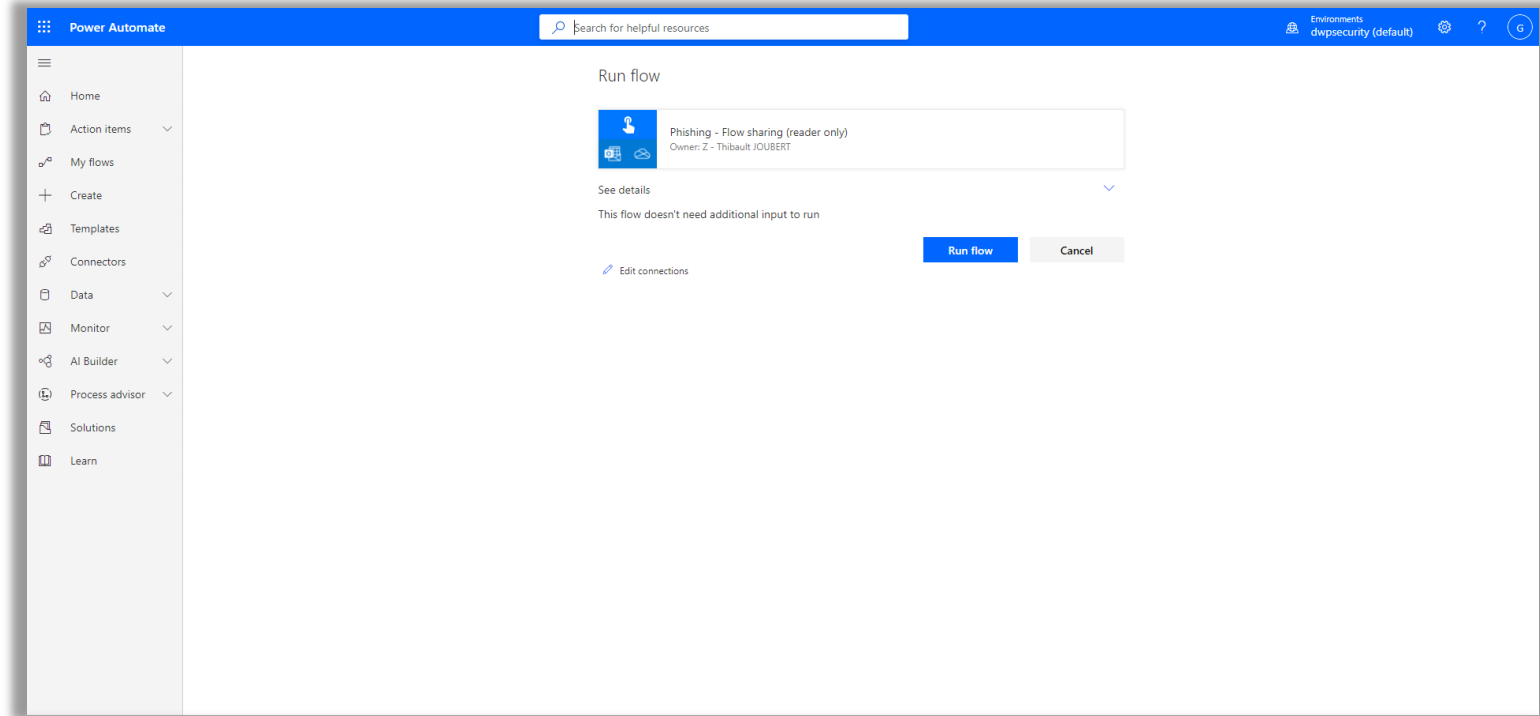


Exemple 3 : Phishing via un flux (*read only*)





Exemple 3 : Phishing via un flux (*read only*)



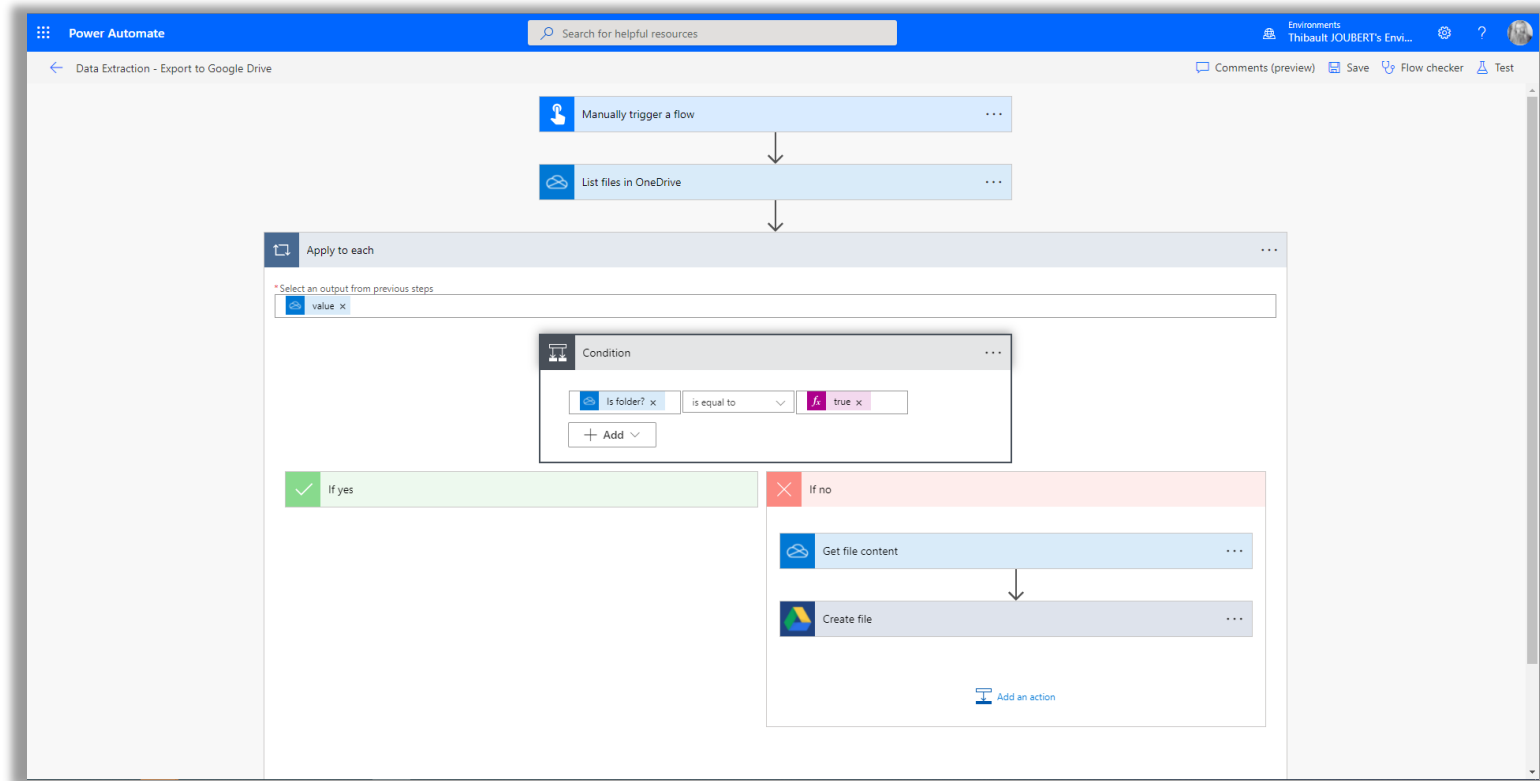


Exemple 4 : Transfert automatique des mails

The screenshot displays the Microsoft Power Automate web interface. At the top, the header bar includes the 'Power Automate' logo, a search bar, and user information for 'Environments Thibault JOUBERT's Envi...'. The main workspace shows a flow titled 'Data - Forward email'. The flow begins with a trigger step 'When a new email arrives (V3)'. An arrow points down to an 'Apply to each' loop. Inside this loop, the first step is 'Attachments', which is used to select the output for the subsequent 'Send an email (V2)' step. The 'Send an email (V2)' step is configured with the following fields: 'To' is set to 'Goblin' with a dynamic content icon; 'Subject' is set to 'Subject'; 'Body' is set to 'Body'; 'From (Send as)' is a text field with a placeholder; 'CC' and 'BCC' are text fields with placeholders; 'Attachments Name - 1' is set to 'Attachments N...'; 'Attachments Content - 1' is set to 'Attachments C...'; 'Sensitivity' is set to 'Sensitivity'; and 'Reply To' is set to 'The email addresses to use when replying'. The interface also shows options for 'Comments (preview)', 'Save', 'Flow checker', and 'Test'.

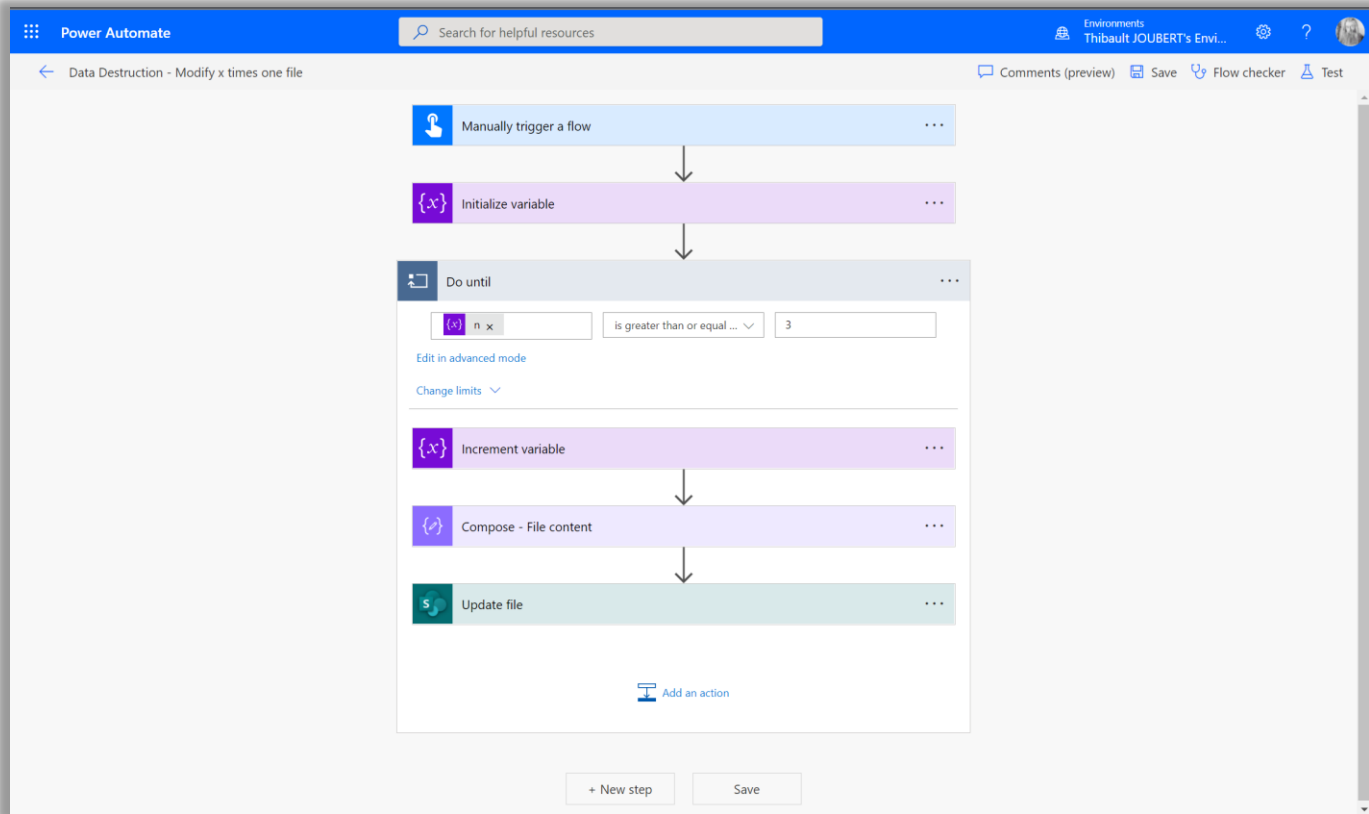


Exemple 5 : Extraction de données



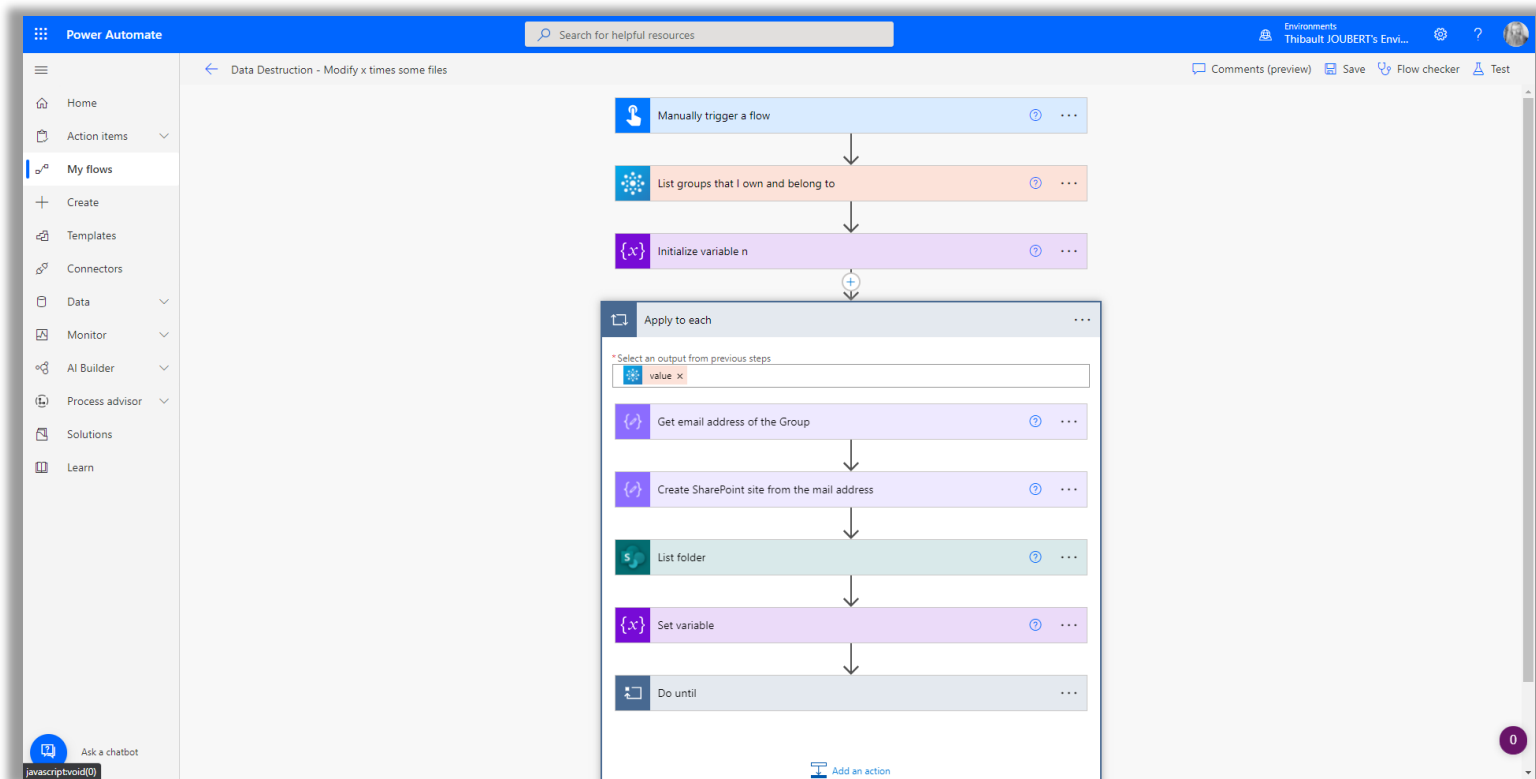


Exemple 6 : Destruction des données (1/2)





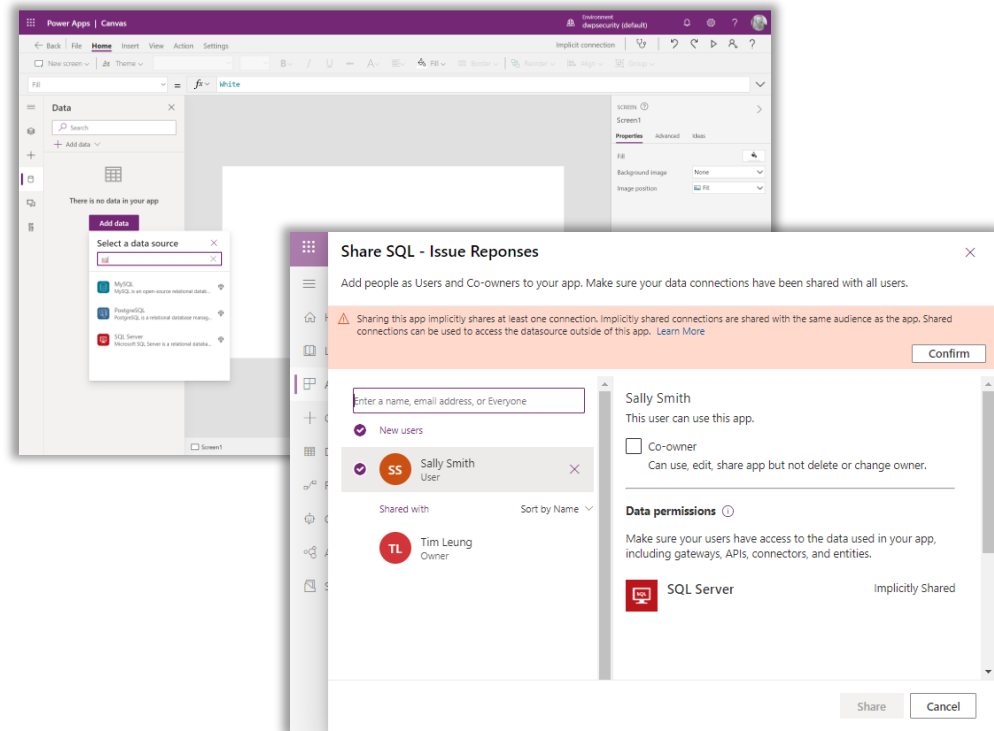
Exemple 7 : Destruction des données (2/2)





Exemple 8 : Exposition de données via une connexion implicite

- Certaines applications Power Apps peuvent s'appuyer sur des connexions ne dépendant pas du contexte utilisateur
- Le partage de l'application **expose ainsi les données sous-jacentes**



PARTIE 2

Quelles mesures concrètes pour assurer un niveau minimal de sécurité ?



Les mesures de vont s'ajouter aux couches de sécurité déjà existantes

Plusieurs rôles
peuvent être définis au
sein d'une application

Gestion des permissions
au sein de l'application

- Selon l'application
- Accès conditionnel par application (preview)

Le durcissement fixe
le champs des
possibles

Sécurité et Gouvernance
de la Power Platform

- **Configuration Power Platform**
- **Data Policies & Tenant isolation**
- **Suivi et Supervision**

Un utilisateur ne
pourra pas faire plus
de choses que ce qu'il
ne peut déjà faire

Accès aux données

- Permissions SharePoint, Teams, liens de partage directs
- Gestion des droits DataVerse
- Classification, Chiffrement, DLP, etc.

Sécurisation du tenant

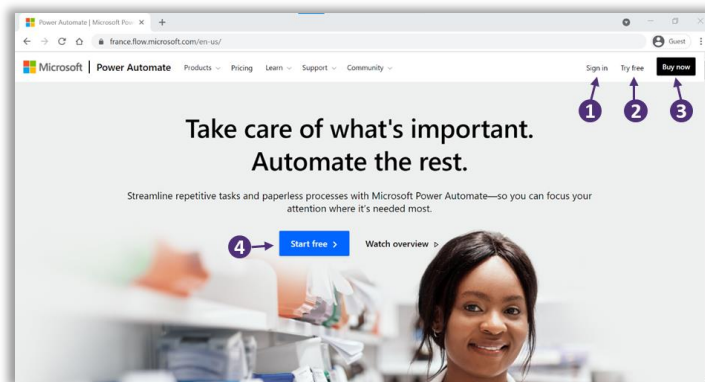
- Gestion des accès aux services
- Authentification & Accès conditionnel
- Audit, Supervision, etc.



1 – Définir qui peut accéder aux services

Par défaut, un utilisateur peut accéder à Power Automate ou Power Platform, car il s'agit d'un service gratuit :

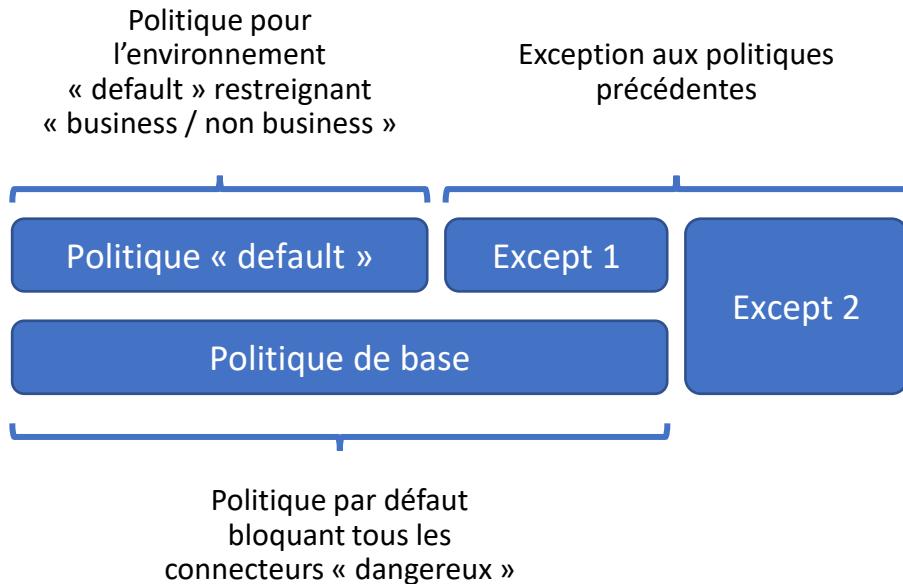
- Bloquer la souscription de licences *free* au niveau du tenant (*Set-MsolCompanySettings -AllowAdHocSubscriptions \$false*)
- Bloquer la souscription de licences *trial* ou *developer* (*Remove-AllowedConsentPlans -Types @"Internal", "Viral"*)
- Bloquer la souscription de licences payantes (*Get-MSCommerceProductPolicies -PolicyId AllowSelfServicePurchase | ? {\$_.PolicyValue -eq "Enabled"} | ForEach {Update-MSCommerceProductPolicy -PolicyId AllowSelfServicePurchase -ProductId \$_.ProductId -Enabled \$False}*)





2 – Mettre en place les *Data Policies*

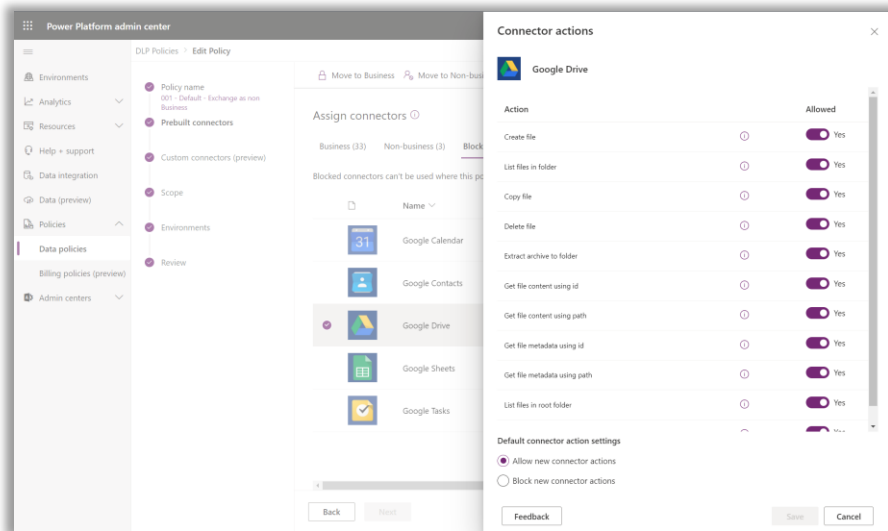
- Il existe trois catégories de connecteurs :
 - « Business »
 - « Non Business »
 - « Blocked »
- Une application ou un **flux ne peut pas utiliser un connecteur « business » ET un « non business »**
- Une *Data policy* peut s'appliquer à tous les environnements, à tous sauf, ou uniquement à
- En cas de politiques concurrentes, **l'intersection est retenue**
- A noter : les **connecteurs standards Microsoft ne peuvent pas être bloqués**





2 – *Data policies* : Contrôles granulaires

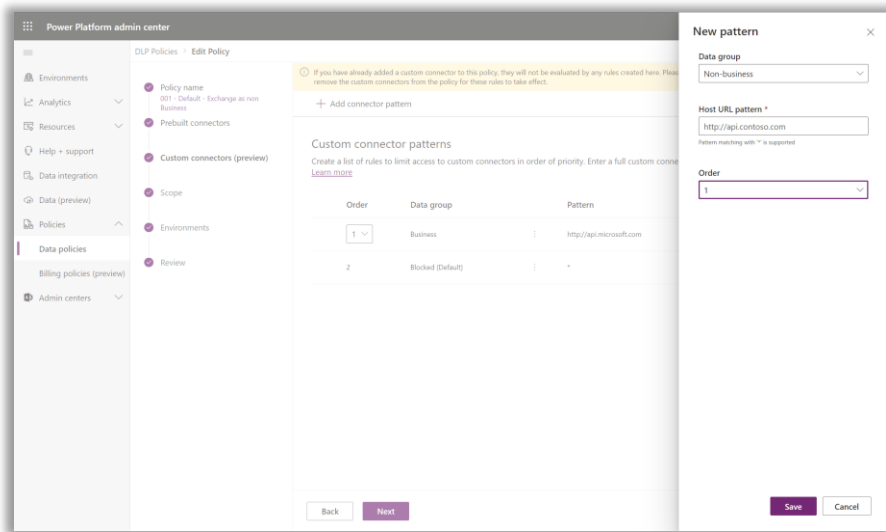
- Au-delà des catégories « business », « non business » et « blocked », il est désormais de limiter les actions possibles pour certains connecteurs :
 - Endpoint : HTTP, HTTP with Azure AD, HTTP Webhook, SQL Server, SMTP et Azure Blob Storage
 - Actions
- A date, la fonctionnalité est encore en preview, tous les contrôles ne sont disponibles





2 – *Data policies* : Connecteurs personnalisés

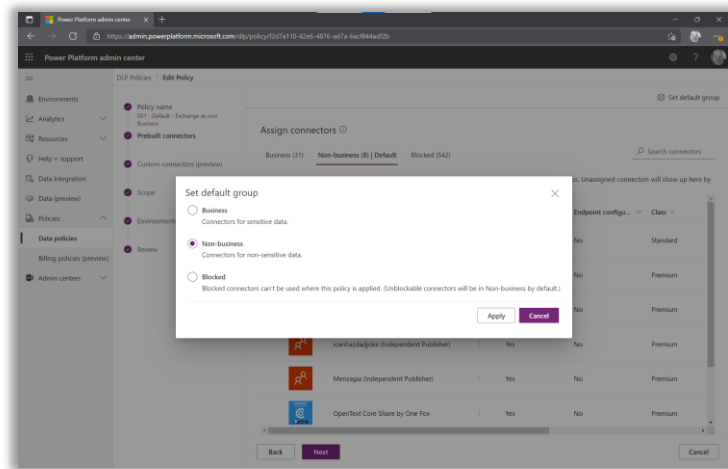
- Depuis 2021, les **connecteurs personnalisés** (*custom connectors*) peuvent être gérés dans l'UI avec les connecteurs natifs (encore en preview)
- Il est possible de **définir les endpoint autorisés**
- Un data group « **Default** » permet de couvrir tous les nouveaux connecteurs





2 – Data policies : Focus sur le Default Group

- Il est possible de choisir **un groupe où seront automatiquement placés les nouveaux connecteurs**
- Recommandation : « blocked »
- A noter : Une application « non blocable » sera automatiquement mise dans le groupe « non business »



```
PS C:\Users\tjoubert> # Initialization
$policyName = "f2d7a110-42e6-4876-ad7a-6ac644adf2b"
$policyDisplayName = "00b-Test"
$apiVersion = "2016-11-01"
$route = "https://api.bap.microsoft.com/providers/Microsoft.BusinessAppPlatform/scopes/admin/api/policies/$($policyName)?api-version=$($apiVersion)"

# Set a new value for the default group setting
$defaultApiGroup = "Blocked" #b1, blocked
$policy.properties.definition.defaultApiGroup = $defaultApiGroup
Invoke-ApI -Method PUT -Route $route -Body $policy -ApiVersion $apiVersion

# Get the default group
$policy = Invoke-ApI -Method GET -Route $route -ApiVersion $apiVersion
Write-Host
Write-Host "New default group is:" $policy.properties.definition.defaultApiGroup

Statuscode      : 412
StatusDescription : Precondition failed
Headers          : {If-Range: Strict-Transport-Security, x-ms-request-id, x-ms-correlation-request-id, ...}
Error            : #code=DLPPolicyetagMismatch; message=The DLP policy 'f2d7a110-42e6-4876-ad7a-6ac644adf2b' etag mismatch in the tenant '5eb0364a-1e47-4d89-8af8-ef88abfa199c'.
Message          : The DLP policy 'f2d7a110-42e6-4876-ad7a-6ac644adf2b' etag mismatch in the tenant '5eb0364a-1e47-4d89-8af8-ef88abfa199c'.
Internal         : System.Net.HttpWebResponse

New default group is: blocked
```



2 – *Data policies* : Nouveaux environnements

- Il est possible de **restreindre la création de nouveaux environnements** aux administrateurs
- Les nouveaux environnements doivent être couverts par la politique de base ou Recommandation : « blocked »

The screenshot displays the Power Platform admin center interface. On the left, a navigation pane lists various sections: Environments, Analytics, Resources, Help + support, Data integration, Data (preview), Policies, and Admin centers. The main area shows a table of environments with columns for Environment, Type, State, and Region. A green notification banner at the top indicates that a new environment 'IRM - Case 001' has been successfully created. On the right, the 'Power Platform settings' panel is open, showing options for governance, who can create production and sandbox environments, who can create trial environments, and analytics settings. The 'Who can create production and sandbox environments' and 'Who can create trial environments' sections both have 'Everyone' selected. The 'Analytics' section has 'Enable tenant-level analytics' turned off. 'Save' and 'Cancel' buttons are at the bottom right of the settings panel.

Environment	Type	State	Region
IRM - Case 001	Microsoft Teams	Ready	France
MG - Center of Excellence	Microsoft Teams	Ready	France
Thibault JOUBERT's Environment	Developer	Ready	France
deprecurity (default)	Default	Ready	France



3 – Mettre sous contrôle l'environnement Default

- Pour rappel, **il n'est pas possible de bloquer la création et l'usage** de flux et d'applications pour un utilisateur dans l'environnement Default
- Définir une **Data Policy** pour l'environnement default
- **Selon les exigences une intersection entre plusieurs politiques pourra être pertinente :**
 - **Politique 1 : Exchange Online en « non business »**
 - **Politique 2 : Office 365 Groups en « non-business »**
- **Mettre en place un processus de justification *a posteriori*** pour les applications et les flux
- **Sensibiliser les utilisateurs lors de la création d'une nouvelle application, flux, connexion**
- **Sensibiliser les utilisateurs régulièrement** pour revoir les connexion en place
- **Bloquer le partage d'une application à toute l'organisation** (s'applique pour tous les environnements)
\$settings = Get-TenantSettings
\$settings.powerPlatform.powerApps.disableShareWithEveryone

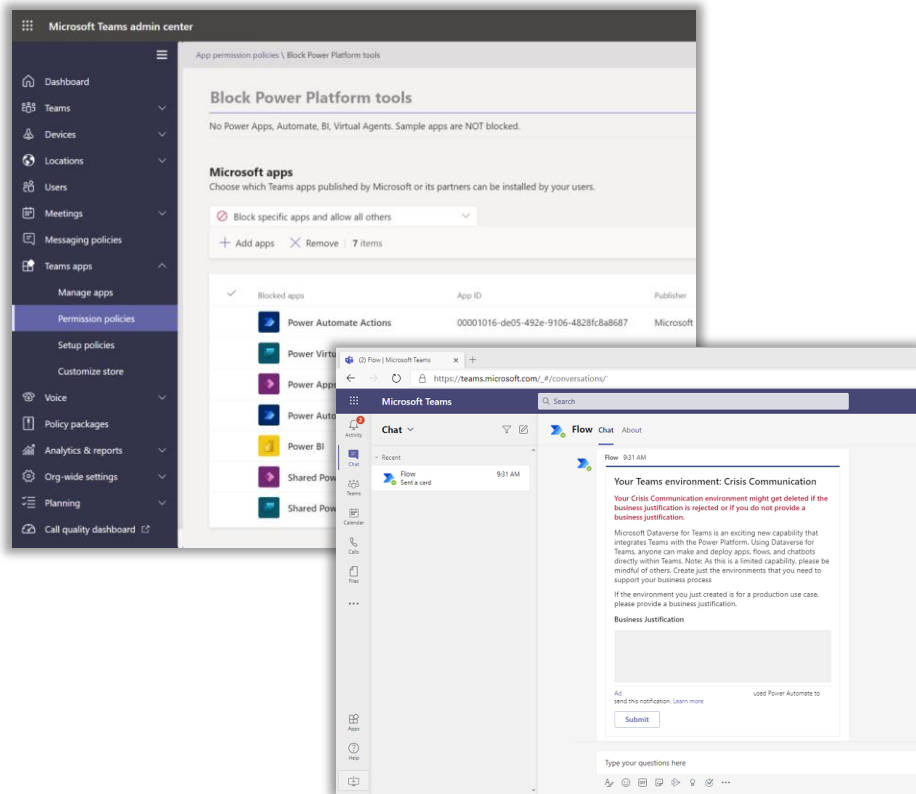
The screenshot shows the Power Automate interface with a sidebar on the left containing navigation options: Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area displays a table of connections for the 'dwpsecurity (default)' environment.

Name	Modified ↑	Status
RSS RSS	5 mo ago	Connected
adm_thibault@dwpsecurity.onmicrosoft.com Microsoft 365 message center (preview)	5 mo ago	Can't sign in. Fix connection
adm_thibault@dwpsecurity.onmicrosoft.com Office 365 Groups	5 mo ago	Can't sign in. Fix connection
Approvals Approvals	2 mo ago	Connected
[BaseResourceUrl] HTTP with Azure AD	3 wk ago	Can't sign in. Fix connection
adm_thibault@dwpsecurity.onmicrosoft.com Power Apps for Makers	3 d ago	Connected
adm_thibault@dwpsecurity.onmicrosoft.com Power Automate for Admins	3 d ago	Connected
adm_thibault@dwpsecurity.onmicrosoft.com Power Automate Management	3 d ago	Connected
adm_thibault@dwpsecurity.onmicrosoft.com Office 365 Users	3 d ago	Connected
adm_thibault@dwpsecurity.onmicrosoft.com Power Platform for Admins	3 d ago	Connected
adm_thibault@dwpsecurity.onmicrosoft.com Power Apps for Admins	3 d ago	Connected
adm_thibault@dwpsecurity.onmicrosoft.com HTTP with Azure AD	2 d ago	Connected



4 – Mettre sous contrôle les environnements Dataverse for Teams

- Préciser via les politiques Teams **qui peut ou non créer des nouvelles applications** (maker)
- Définir une **Data Policy pour tous les environnements Dataverse for Teams** et les ajouter automatiquement via Power Automate
- **Mettre en place un processus de justification a posteriori** de la création des environnements
- A noter : certaines applications Teams entraine la création d'un environnement Dataverse for Teams (même si l'utilisateur n'a pas de rôle de maker)





5 – Utiliser Office DLP pour bloquer la redirection de mail automatique

- Depuis 2020, un header indique dans un mail s'il a été envoyé depuis Power Automate
- La mise en place d'une règle Office DLP (ou ETR) permet de bloquer ces mails et sensibiliser l'utilisateur

The screenshot displays the Microsoft 365 compliance center interface. On the left, the 'Data loss prevention' section is active, showing a list of policy settings. The main area shows the 'Create rule' wizard. The 'Name' field is set to 'Block Power Automate mail'. The 'Description' field is empty. Under 'Conditions', the rule is configured to 'Header contains words or phrases', specifically detecting 'X-MS-Mail-Applica' and 'Microsoft Power Automate'. The 'Exceptions' section is currently empty. The 'Actions' section is also empty. At the bottom, there are 'Save' and 'Cancel' buttons.

Envoi depuis Power Automate

This message was sent with Low importance

Z - Thibault JOUBERT
Tue 12/14/2021 3:51 PM
To: Goblin

Hello there!!

Reply Forward

Message Header A...

Summary

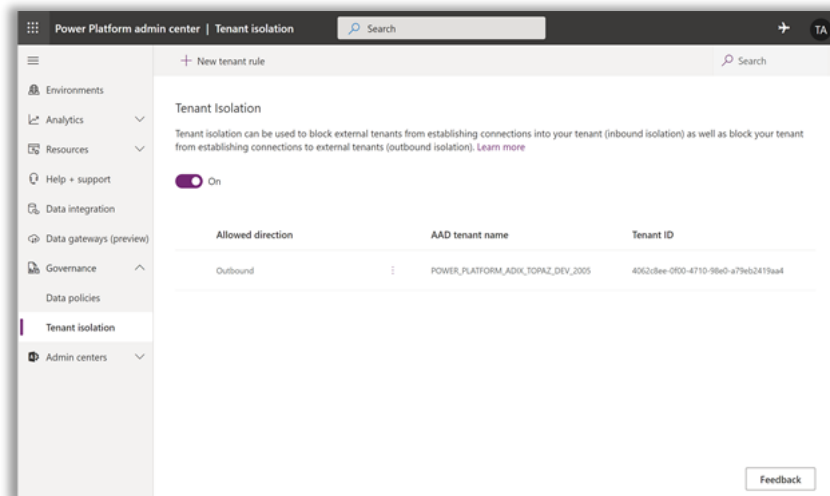
Original Headers

```
X-MS-Mail-Application: Microsoft Power Automate;  
User-Agent: Azure-Logic-Apps/1.0 (workflow  
2af43b0a1c844908c9a32c04b9f0); version  
085862133752637754) Microsoft-Flow/1.0  
X-MS-Mail-Operation-Type: Send  
X-MS-Mail-Environment-Id: default-5eb0364a-1e47-  
4d85-8af8-e788aef129c
```



6 – Implémenter le *tenant isolation*

- **Tout ce que l'on a vu précédemment ne sert à rien ...**
- ... Si l'utilisateur peut faire la même chose dans un environnement externe
- **Recommandation : activer le tenant isolation**
(nécessaire de passer par une demande support)
- A noter : l'accès conditionnel ne permet pas de bloquer la connexion (vu comme « App Services »)
- A noter : les autres plateformes de low code / no code utilisent les API, et donc le consentement, pour créer des connexions vers les données Office 365





7 – Sensibiliser les utilisateurs

SENSIBILISER

SENSIBILISER

SENSIBILISER

...



8 – Suivre les usages

Centre d'administration

- Liste des applications et des flux
- Statistiques sur les usages, les erreurs et le nombre d'exécution

PowerShell

- Scripts pour récupérer des informations
- Modification en masse des environnements, des applications
- Modification du propriétaire

Centre d'Excellence (CoE)

- *Starter Kit* mis à disposition par Microsoft
- Applications et flux prédéfinis pour gérer les environnements, les applications et les flux

Connecteurs Admin

- Création d'un portail admin personnalisé et automatisation (ex : création d'environnements)
- Alertes lors de la création d'évènements



Quel que soit le niveau d'adoption et la maturité de l'organisation, il est nécessaire d'arbitrer et mettre en place un certain nombre de mesures

- 1 [MUST HAVE] Définir qui peut accéder aux services : Licences, Licences de tests, Environnements développeurs
- 2 [MUST HAVE] Mettre en place les **Data Policies** : Catégories de connecteurs (standards / personnalisés), Environnements
- 3 [MUST HAVE] Mettre sous contrôle l'environnement **Default** : *Data policies* spécifiques, Sensibilisation utilisateurs
- 4 [MUST HAVE] Mettre sous contrôle **Dataverse for Teams** : *Data policies*, Sensibilisation, Politiques Teams
- 5 [MUST HAVE] Utiliser Office DLP pour bloquer la redirection de mail automatique
- 6 [MUST HAVE] Implémenter le **Tenant Isolation** : *Inbound isolation, Outbound isolation*
- 7 [NICE TO HAVE] Sensibiliser les utilisateurs : Nouvelles connexions, Forcer une revue des connexions
- 8 [NICE TO HAVE] Surveiller les usages : Centre d'administration, Centre d'Excellence, PowerShell

MERCI !



One more thing : Utilisation d'une liste SharePoint comme stockage de données pour une Power App

- Un utilisateur qui souhaite consulter ou modifier une liste SharePoint via une Power App doit avoir accès à la liste avec les droits requis.
 - ➔ Le risque est que **l'utilisateur puisse modifier directement la liste sans passer par l'application**
- **Plusieurs possibilités permettent de masquer la liste ...**
 - Modification des droits de l'entrée de la liste après création
 - Configuration de la vue SharePoint
 - Masquer l'affichage de la liste
 - Modifier les permissions de la liste pour ne permettre une modification que programmatiquement
 - Utilisation d'une liste temporaire
- **... Mais ce ne sont que des mesures d'obfuscation pas de protection**