Microsoft

BLUEHAT

SECURITY ABOVE ALL ELSE

Deprecating Azure AD Graph API is Easy and Other Lies We Tell Ourselves

Dr. Nestori Syynimaa

Agenda

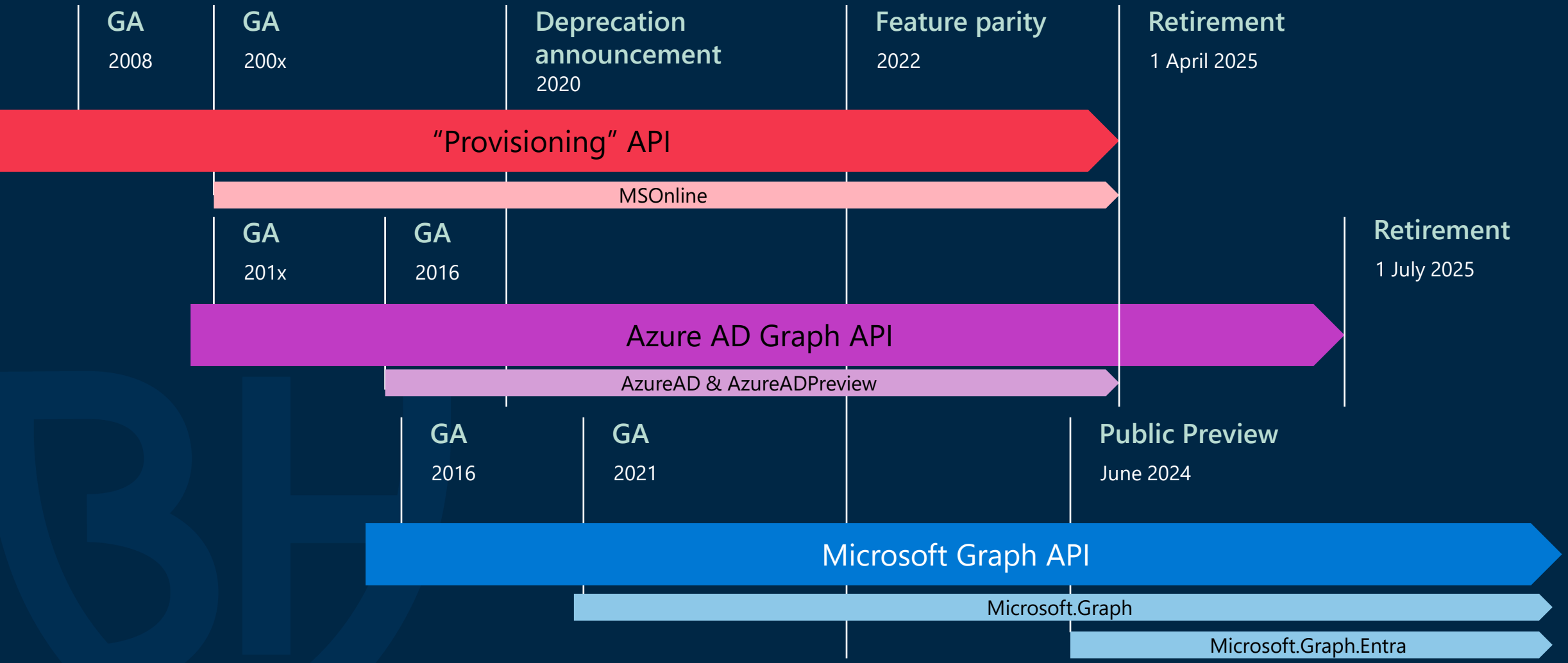
1. Introduction to ~~Azure AD~~ Entra ID APIs
2. Detecting API usage
3. Preventing API usage
4. What should I do?

Introduction to Entra ID APIs

~~Azure AD~~ Entra ID APIs & PowerShell modules

API	Uri	Content	PS modules
“Provisioning”	https://provisioningapi.microsoftonline.com	SOAP	MSOnline
Azure AD Graph	https://graph.windows.net	JSON	AzureAD AzureADPreview
Microsoft Graph	https://graph.microsoft.com	JSON	Microsoft.Graph *Microsoft.Graph.Entra* *Microsoft.Graph.Entra.Beta*

~~Azure AD~~ Entra ID APIs & PowerShell modules

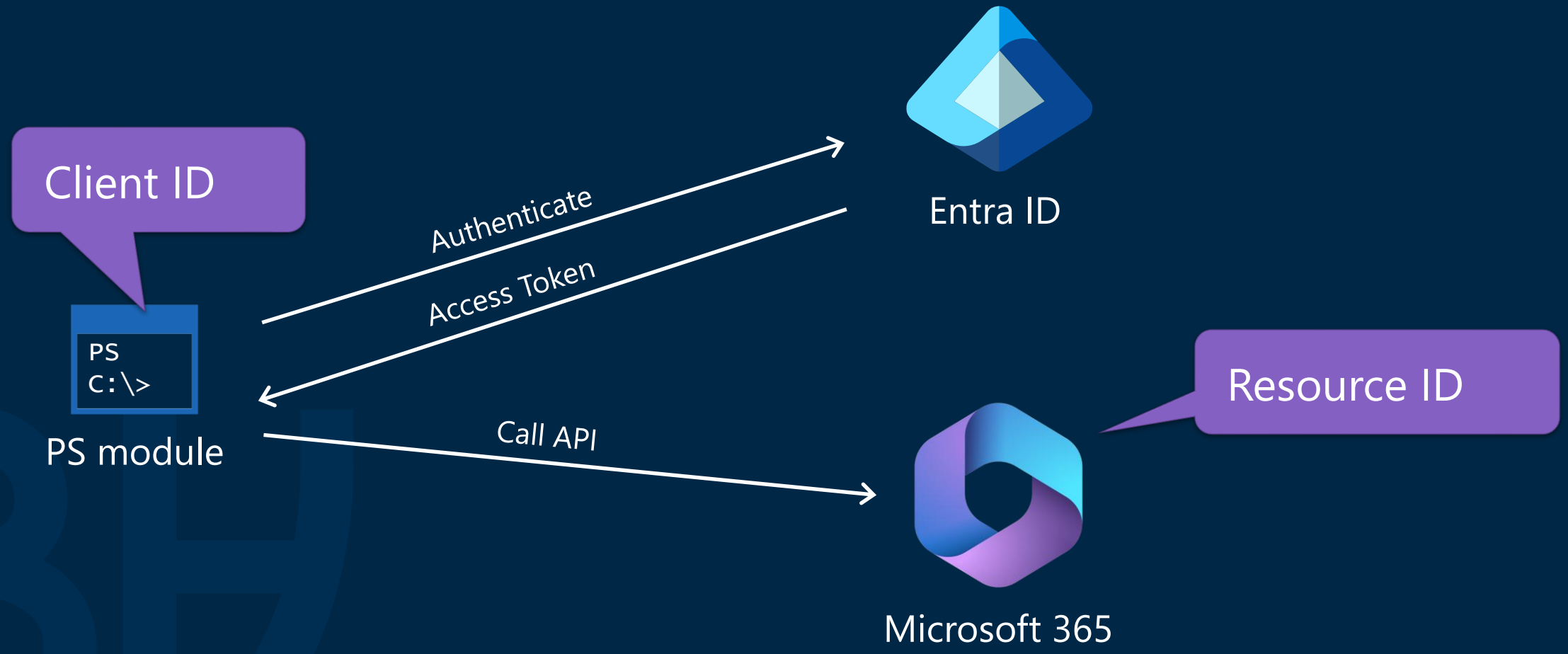


Why retirement have been so hard?

- Closing small number of feature parity gaps
- Some Microsoft Apps have not completed migration and require customer updates
- Active usage by customers

Detecting API usage

Recap: How cloud works



Detecting Azure AD Entra ID APIs & PowerShell module usage

API	Authentication	API calls
“Provisioning”	N/A	N/A
Azure AD Graph	Sign-in log	N/A
Microsoft Graph	Sign-in log	MS Graph Activity Log

- Entra ID recommendations enable detection of apps that use Azure AD Graph *

* https://learn.microsoft.com/en-us/entra/identity/monitoring-health/recommendation-migrate-to-microsoft-graph-api

~~Azure AD~~ Entra ID API resource & PowerShell client IDs

API	Name	Resource ID
“Provisioning”	N/A	N/A
Azure AD Graph	Windows Azure Active Directory	00000002-0000-0000-c000-000000000000
Microsoft Graph	Microsoft Graph	00000003-0000-0000-c000-000000000000

Module	Name	Client ID
MSOnline	Azure Active Directory PowerShell	1b730954-1685-4b74-9bfd-dac224a7b894
AzureAD	Azure Active Directory PowerShell	1b730954-1685-4b74-9bfd-dac224a7b894
Microsoft.Graph	Microsoft Graph Command Line Tools	14d82eec-204b-4c2f-b7e8-296a70dab67e

Preventing API usage

Preventing ~~Azure AD~~ Entra ID APIs & PowerShell clients

API	Prevention	Setting
“Provisioning”	Update authorizationPolicy[1]	blockMsolPowerShell
Azure AD Graph	N/A	N/A
Microsoft Graph	N/A	N/A

Module	Prevention	Client ID
MSOnline	Require role assignment[2]	1b730954-1685-4b74-9bfd-dac224a7b894
AzureAD		
Microsoft.Graph	Conditional Access Policy	14d82eec-204b-4c2f-b7e8-296a70dab67e

1. https://learn.microsoft.com/en-us/graph/api/authorizationpolicy-update
2. https://github.com/OfficeDev/O365-EDU-Tools/blob/master/SDS%20Scripts/Block%20PowerShell/Block-PowerShell_for_everyone_except_me.ps1

What should I do?

Microsoft Apps

- Microsoft services using Azure AD Graph: Don’t worry, we got you covered ☺
- Microsoft Public Clients calling Azure AD Graph:
  - AzureAD PowerShell: Migrate to **Microsoft.Graph** module
  - Az CLI/Az PowerShell: Upgrade to latest version
  - Other apps with MS Graph versions (VS 2022, M365 admin, etc): Upgrade!
  - Few apps that have not release MS Graph versions (VS 2019, MS Office, Intune Windows Agent): Stay tuned and upgrade when new version available

Migrating scripts from AzureAD to Microsoft.Graph

- Migrate scripts to use **Microsoft.Graph** commands[1]
- Migrate scripts to use the new **Microsoft.Graph.Entra** module OR use it with **Enable-EntraAzureADAlias**[2]

```
PS C:\Users\Nestori> Enable-EntraAzureADAlias

PS C:\Users\Nestori> Get-AzureADUser
```

1. https://learn.microsoft.com/en-us/powershell/microsoftgraph/migration-steps
2. https://techcommunity.microsoft.com/t5/microsoft-entra-blog/introducing-the-microsoft-entra-powershell-module/ba-p/4173546

Microsoft

BLUEHAT

SECURITY ABOVE ALL ELSE