



black hat[®]
EUROPE 2021

november 10-11, 2021

ARSENAL



black hat[®]
EUROPE 2021

november 10-11, 2021

ARSENAL

AADInternals

The Swiss Army Knife for Azure AD & Microsoft 365

Who am I?

- Dr. Nestori Syynimaa ([@DrAzureAD](#))
- Senior Principal Security Researcher at Secureworks CTU-SO
- Author of [AADInternals](#)
- <https://o365blog.com>
- Microsoft MVP
- Microsoft MVSR



AADInternals

PowerShell module

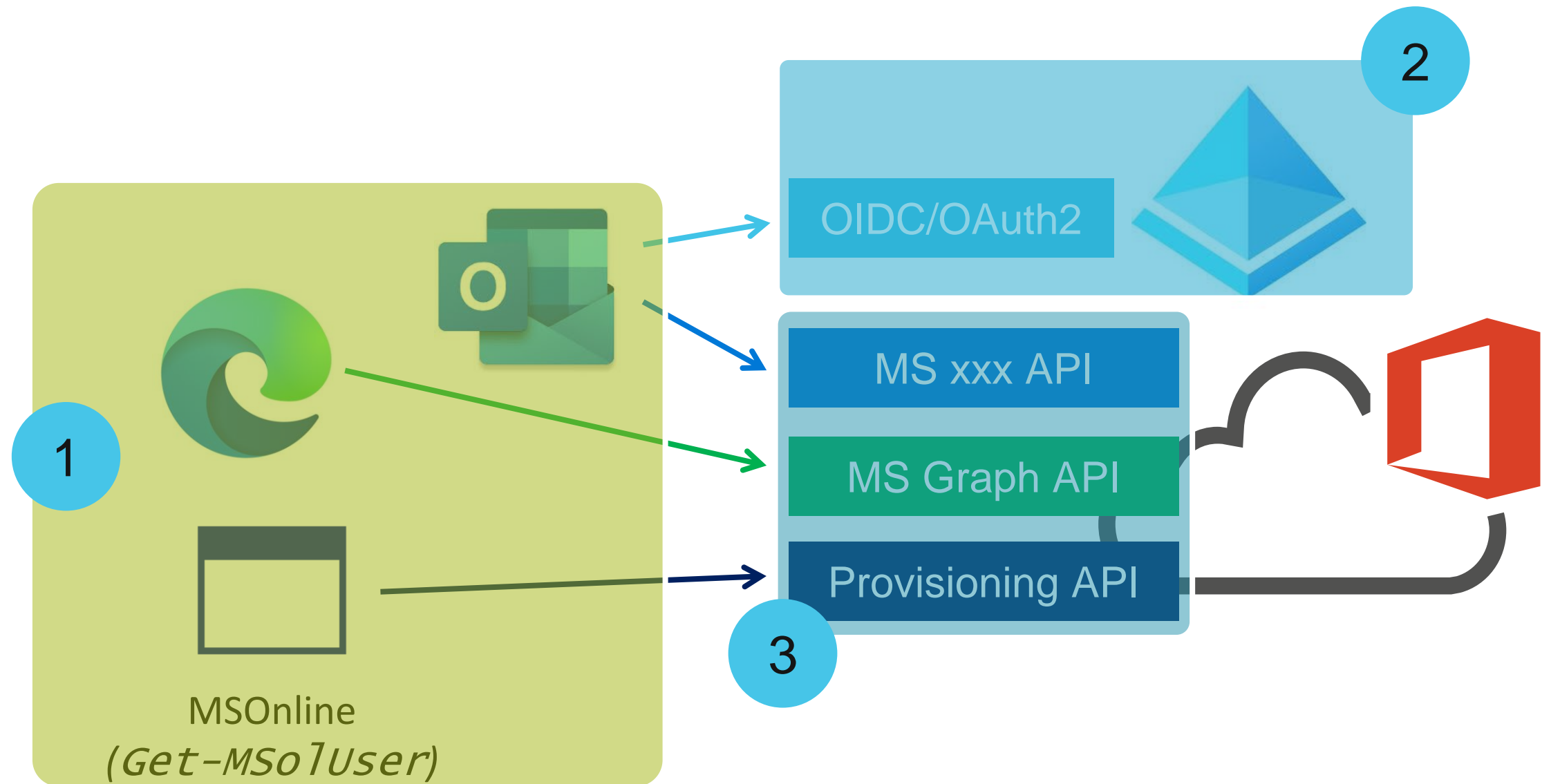
- Utilises (mostly) administrative REST APIs
- Reveal "hidden" information
- Create backdoors
- Bypass security features (e.g. MFA)

Available at:

- <https://o365blog.com/aadinternals>
- <https://github.com/Gerenios/AADInternals>
- PS C:\>Install-Module AADInternals

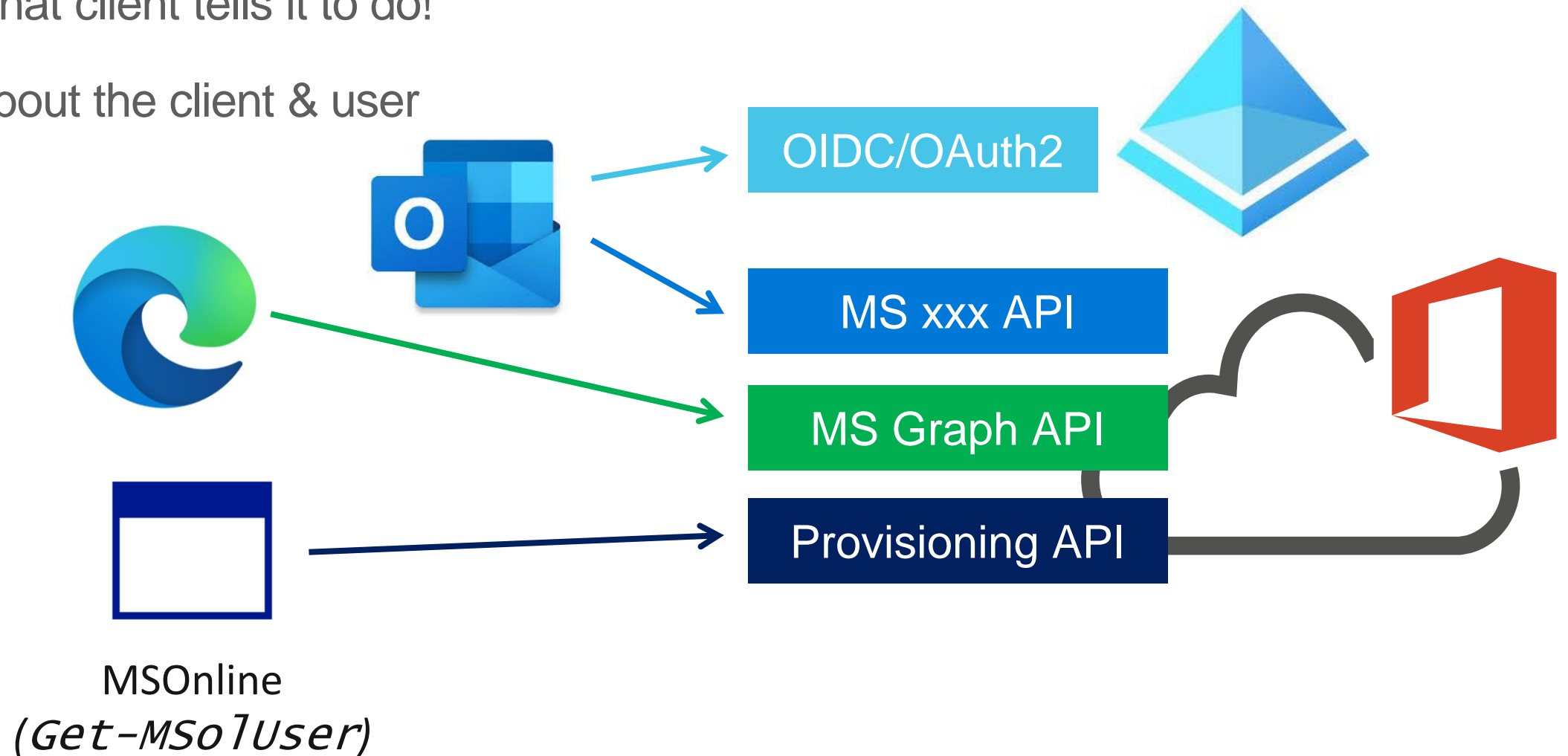
How the cloud works 1/2

1. Clients
2. Authentication
3. APIs

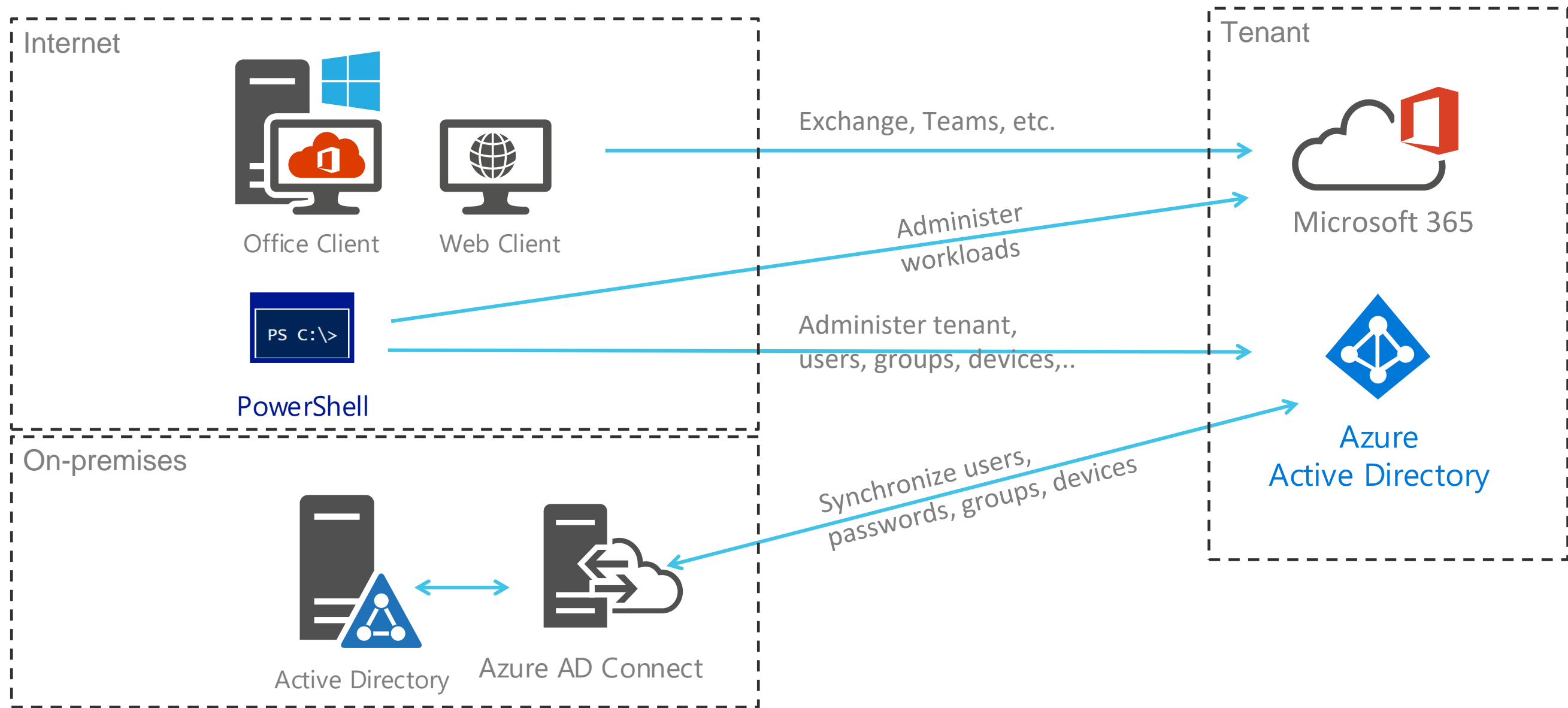


How the cloud works 2/2

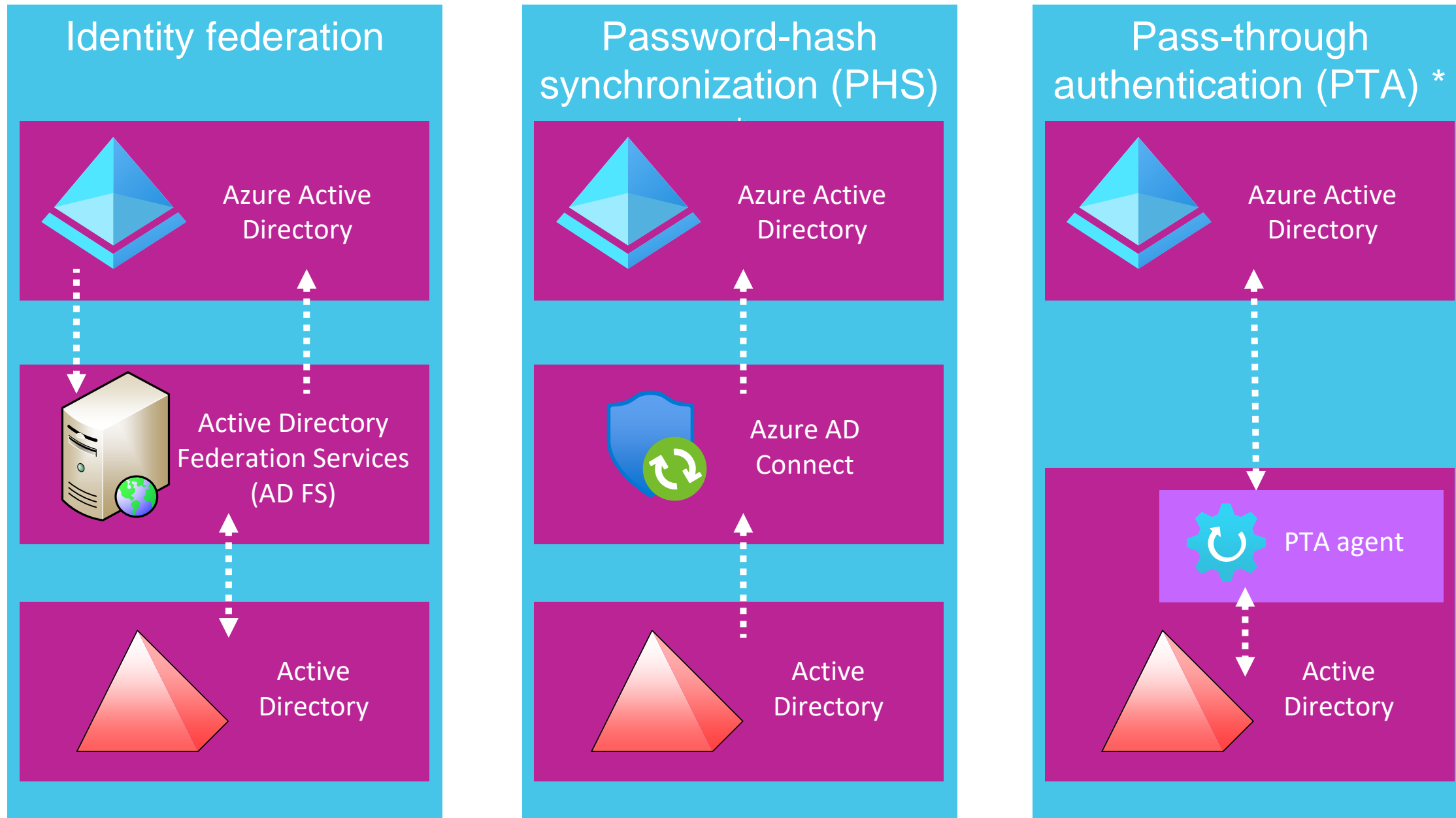
1. Cloud (only) does what client tells it to do!
2. Cloud only knows about the client & user what it is told to!



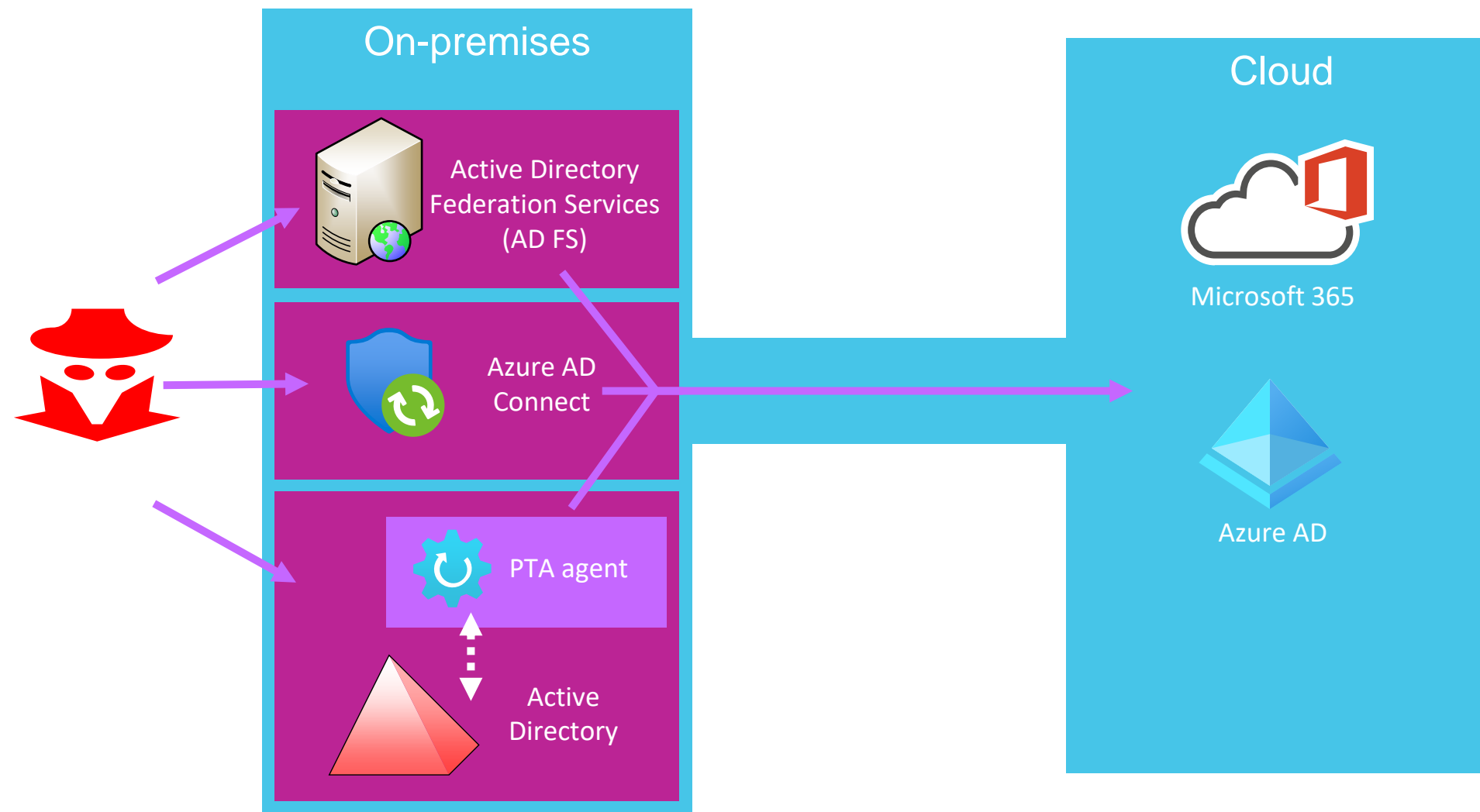
Microsoft 365 / Azure AD concepts



Hybrid authentication options



Hybrid security





Azure AD and Microsoft 365 kill chain

	Recon	Compromise	Persistence	Actions on Intent
Outsider	Get-AADIntTenantDomains Get-AADIntOpenIDConfiguration Get-AADIntLoginInformation Invoke-AADIntReconAsOutsider Invoke-AADIntUserEnumerationAsOutsider	Invoke-AADIntPhishing		
Guest	Get-AADIntAzureTenants Get-AADIntAzureInformation Get-AADIntSPOSiteUsers Get-AADIntSPOSiteGroups Invoke-AADIntReconAsGuest Invoke-AADIntUserEnumerationAsGuest			
User	Get-AADIntTenantDetails Get-AADIntGlobalAdmins Get-AADIntSyncConfiguration Get-AADIntCompanyInformation Get-AADIntSPOServiceInformation Invoke-AADIntReconAsInsider Invoke-AADIntUserEnumerationAsInsider			New-AADIntBulkPRTToken Join-AADIntDeviceToAzureAD Join-AADIntDeviceToTune
Admin	Get-AADIntAzureSubscriptions	Grant-AADIntAzureUserAccessAdminRole Set-AADIntAzureRoleAssignment Invoke-AADIntAzureVMScript Register-AADIntPTAAgent Set-UserMFA Set-UserMFAApps	ConvertTo-AADIntBackdoor Set-AADIntPassThroughAuthentication	New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal
On-prem admin		Export-AADIntADFSSigningCertificate Get-AADIntSyncCredentials Set-AADIntUserPassword Install-AADIntPTASpy		New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal

Demo

Thank you!

Follow me on Twitter: @DrAzureAD