



#AzureEvent  
#BuildWithAzure

# Azure Workshop GDPR, Security and Privacy features for cloud applications

Ben Roscorla, Mike Ormond, Robin Lester

*[vipazure@microsoft.com](mailto:vipazure@microsoft.com)*



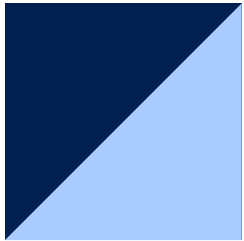
# Securing your applications



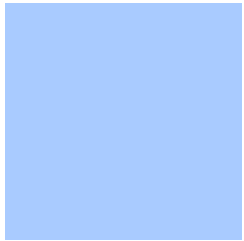
# Shared Responsibility



Customer management of risk  
Data Classification and data accountability



Shared management of risk  
Identity & access management | End Point Devices



Provider management of risk  
Physical | Networking



Cloud Customer



Cloud Provider

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host Infrastructure				
Physical Security				

<http://aka.ms/sharedresponsibility>

Security Imperative



Securing Investment

Securing Infrastructure

Securing Data

Securing Applications




Monitoring & Ops






JIT VM Access

Security Center

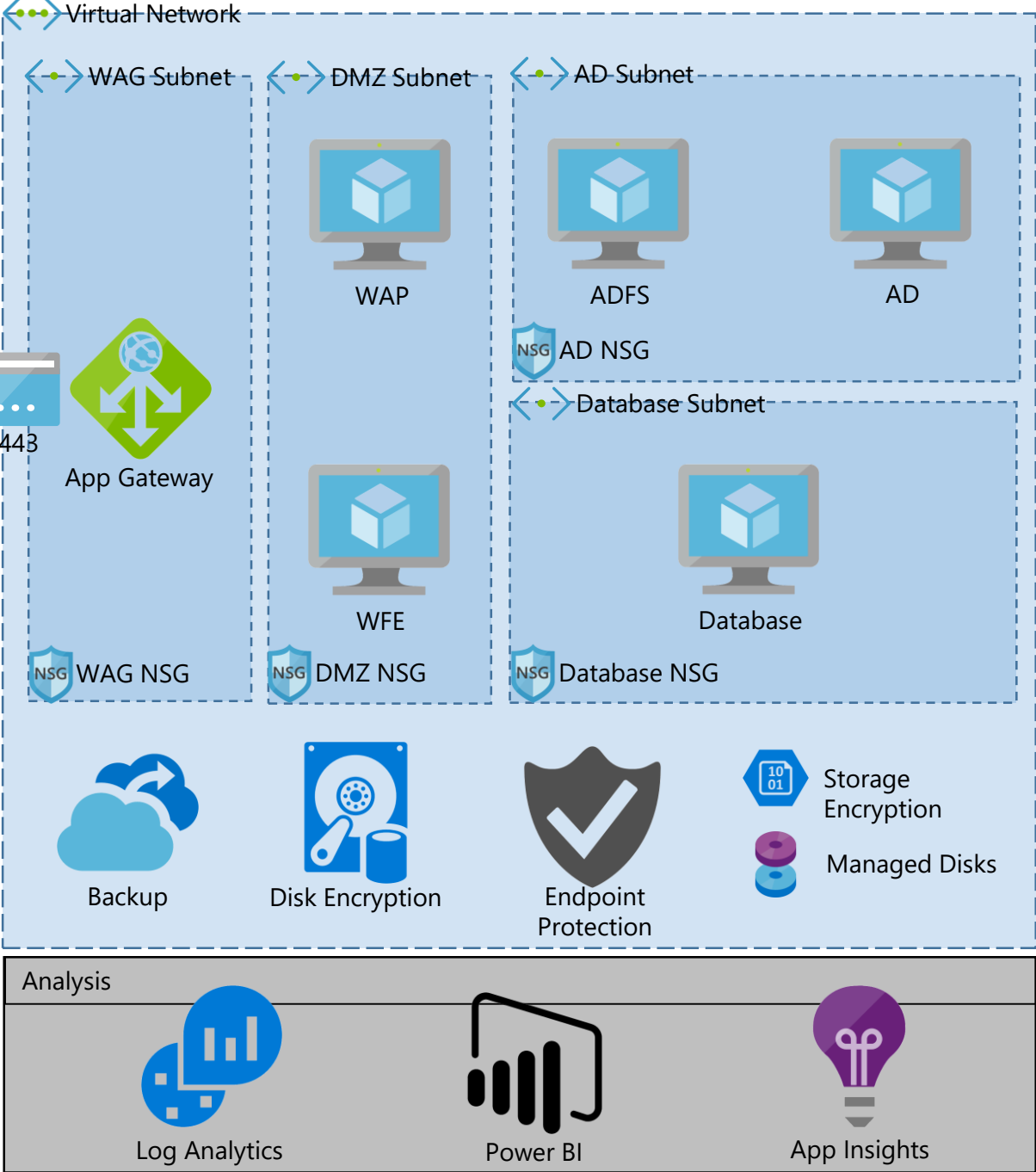
Identity











Key Vault




Deployment






Development

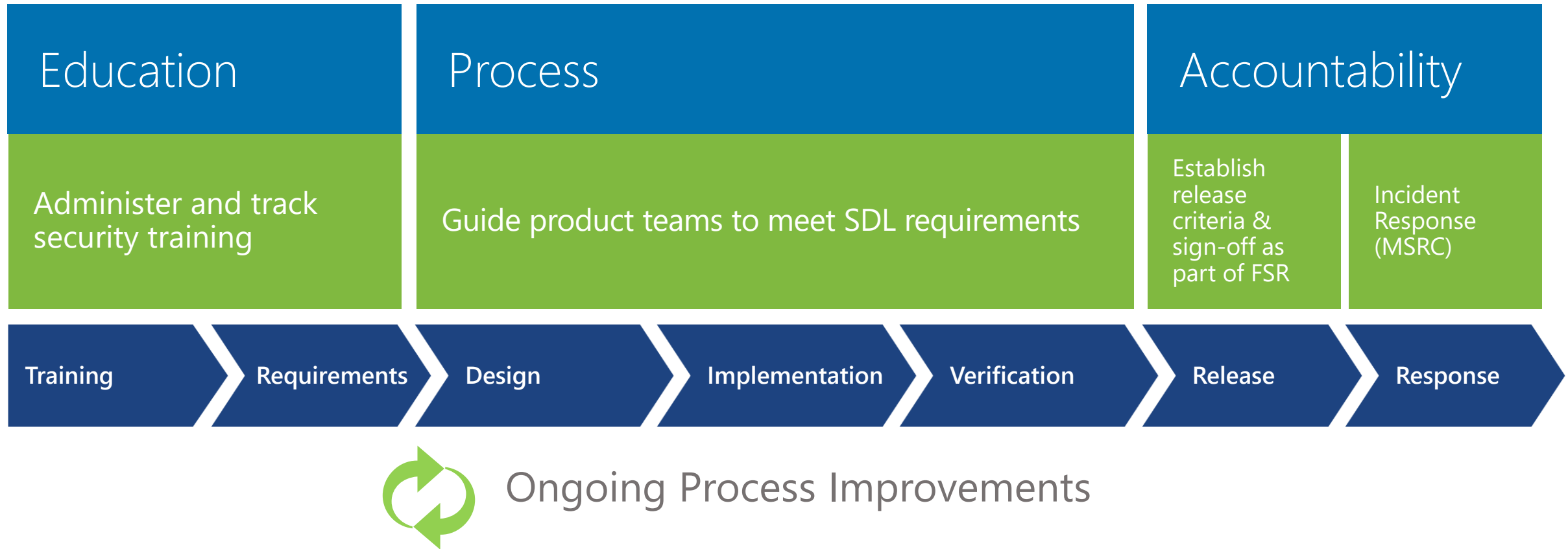






Management

# The Team - Security Development Lifecycle



<https://www.microsoft.com/en-us/sdl/>

Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

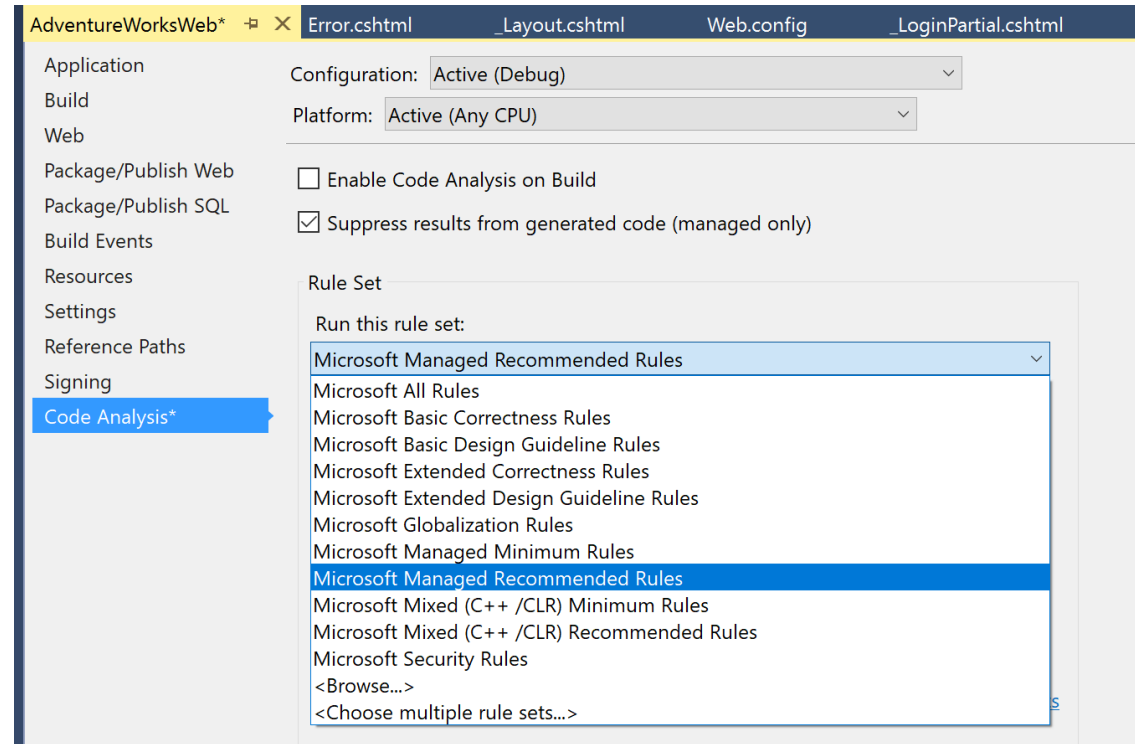
Securing Applications

Monitoring & Ops

# The Tools – Visual Studio and VSTS

## Source Code Analysis Tools

- Code Analysis
- Style Cop – Consistency is good
- VS Extensions
- VSTS Extensions
- Other 3<sup>rd</sup> Party tools – i.e. Sonarqube



<https://marketplace.visualstudio.com/search?term=security&target=VS&category=All categories&vsVersion=&sortBy=Relevance>

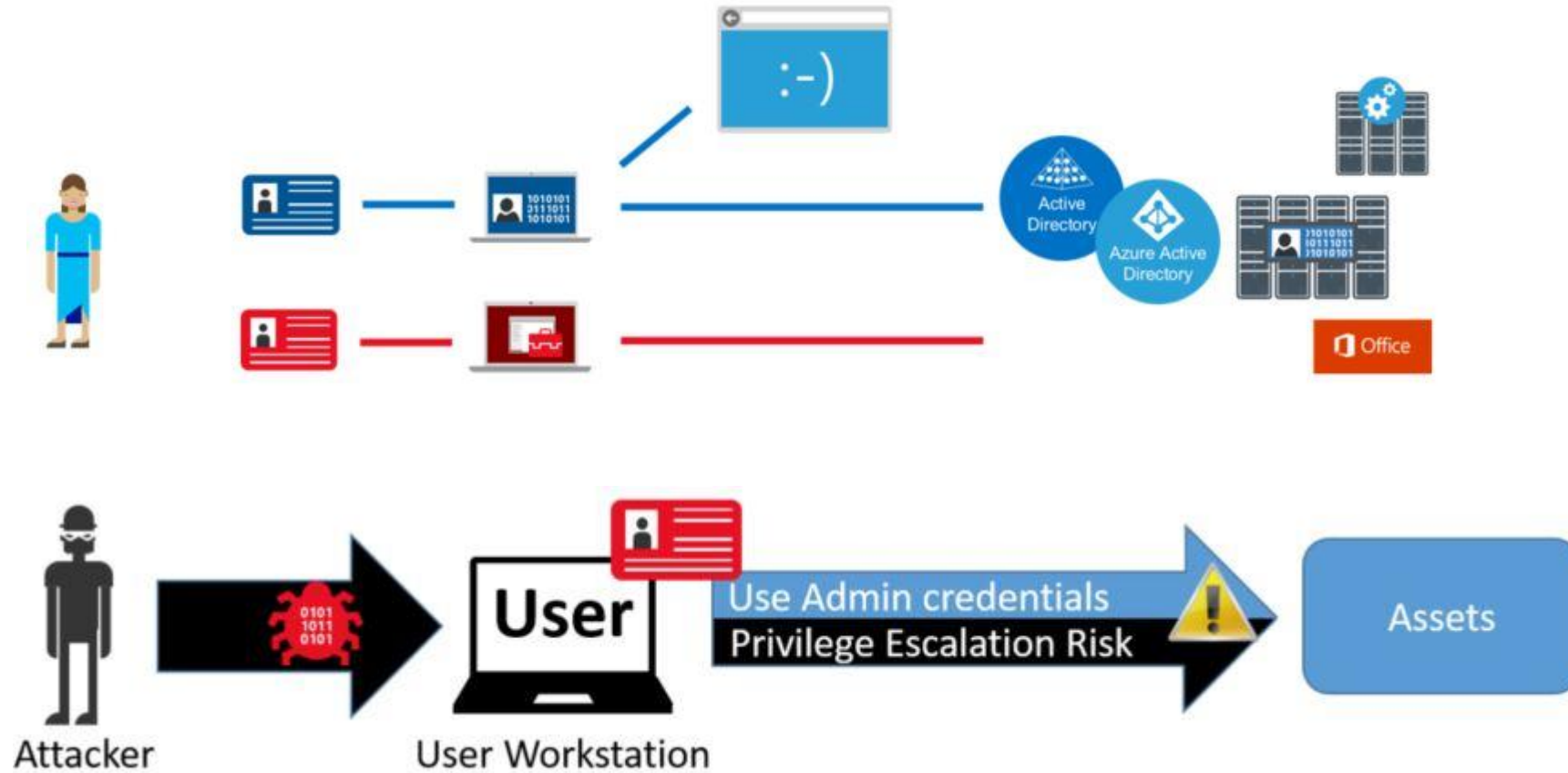
<https://marketplace.visualstudio.com/search?term=security&target=VSTS&category=Build and release&sortBy=Relevance>

[https://www.owasp.org/index.php/Source\\_Code\\_Analysis\\_Tools](https://www.owasp.org/index.php/Source_Code_Analysis_Tools)

<https://marketplace.visualstudio.com/items?itemName=VisualStudioPlatformTeam.MicrosoftCodeAnalysis2017>

<https://github.com/StyleCop/StyleCop>

# The Workstations - PAW



<https://docs.microsoft.com/en-gb/windows-server/identity/securing-privileged-access/privileged-access-workstations>

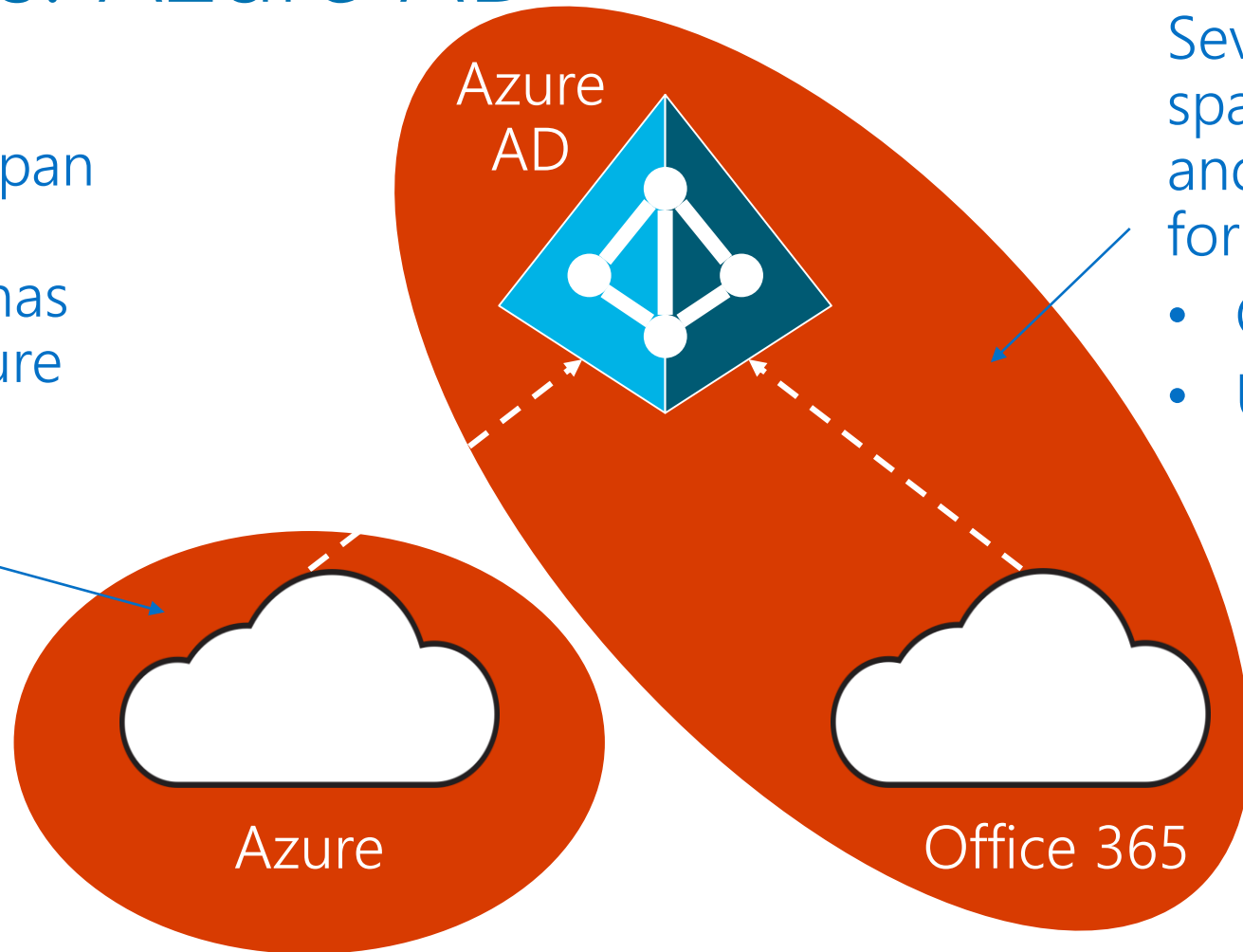
<https://gallery.technet.microsoft.com/Privileged-Access-3d072563>

# Identity & Access: Azure AD

By default, roles do not span Azure AD and Azure.  
Azure AD Global admin has no default access\* to Azure subscriptions

Several roles span Azure AD and Office 365, for example:

- Global admin
- User admin



\* Except if <https://portal.azure.com>  
→ Azure AD → Properties

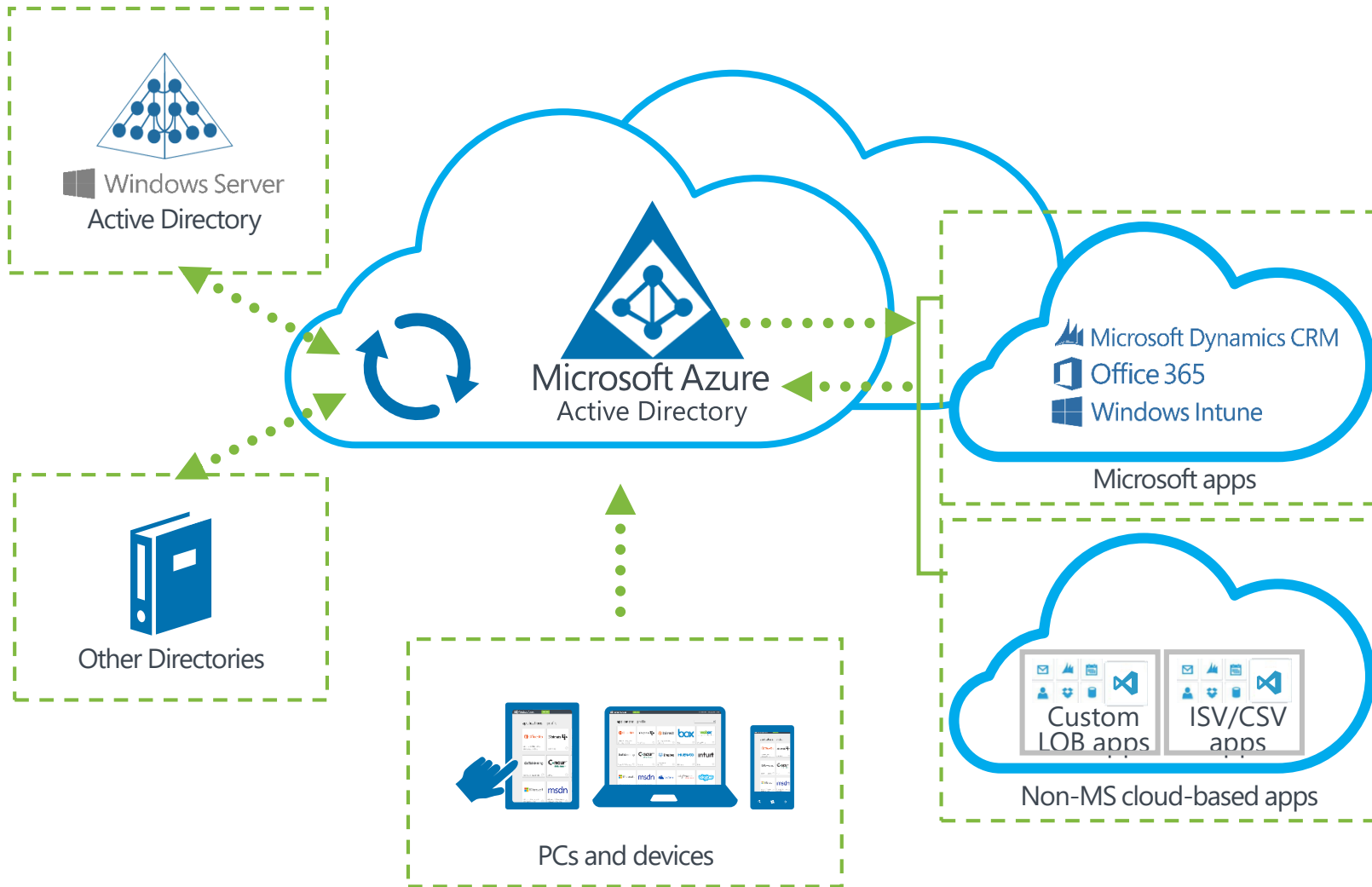
Global admin can manage Azure Subscriptions

Yes

No

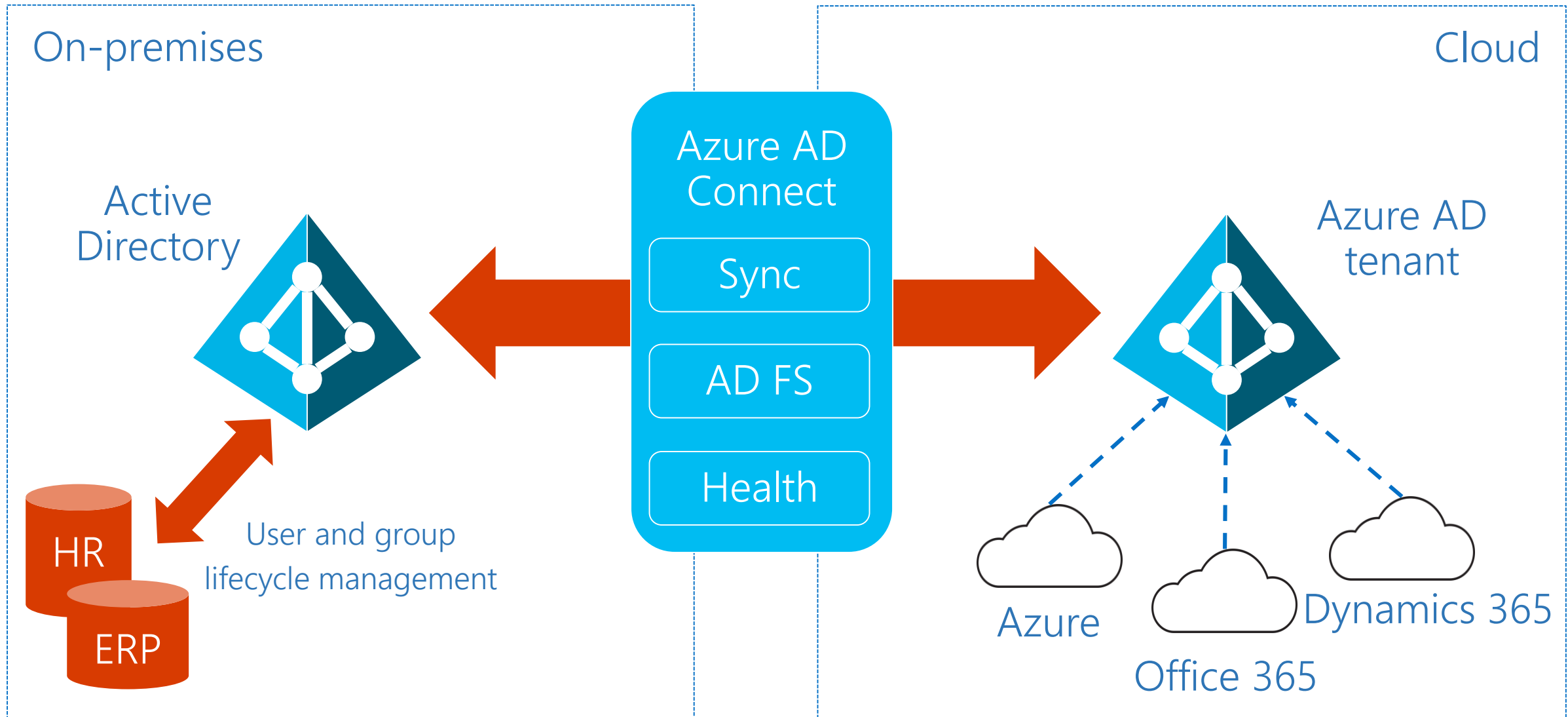


# Identity & Access: Single Sign On



- ✓ Review reports and mitigate potential threats
- ✓ Can enable Multi-Factor Authentication

# Connection to On-Premises



# Sign-in Options

Separate passwords on-premises and cloud

## Password sync

- Same password sign-in
- Hashed passwords stored in cloud

## Pass-through authentication

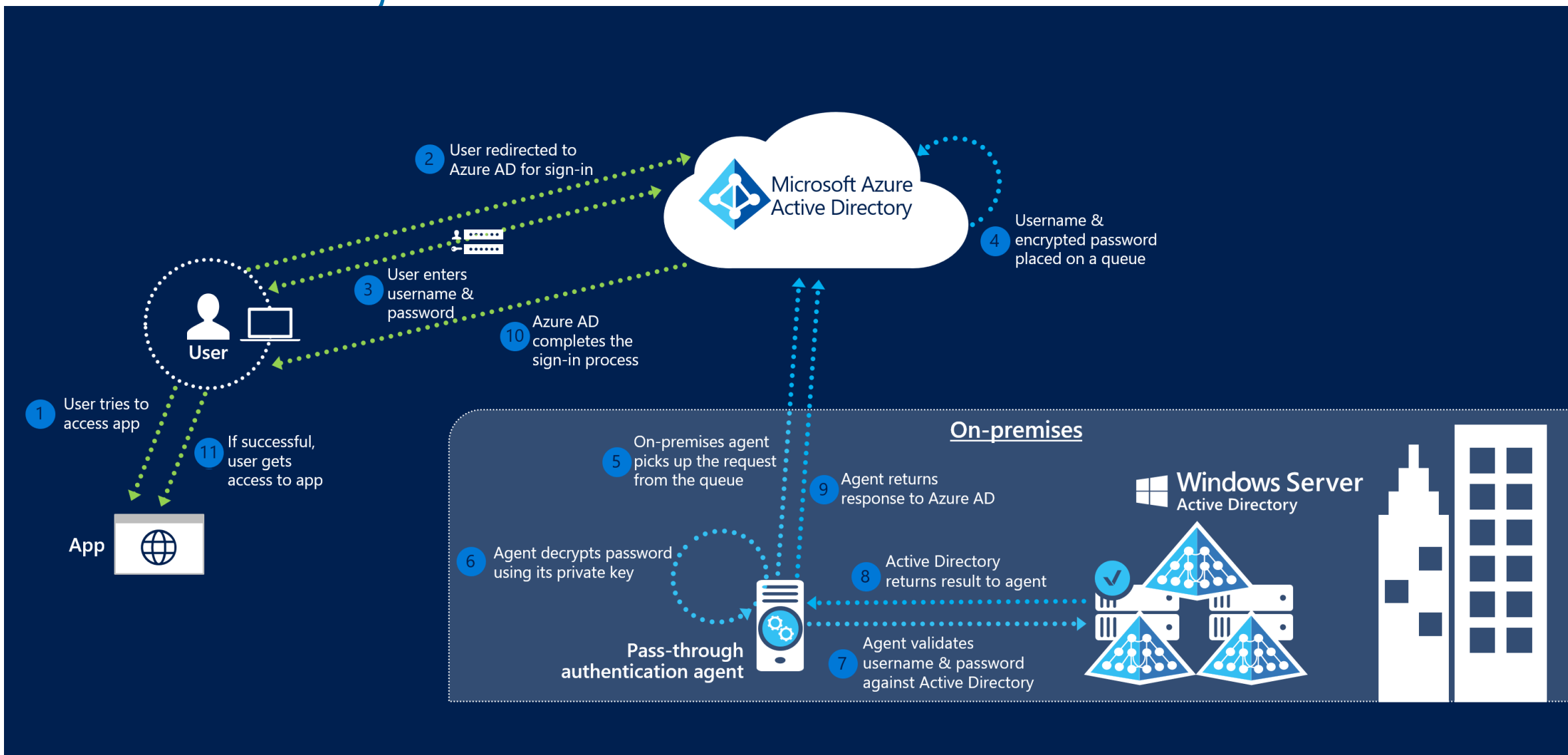
- Same password sign-in
- Password check done on-premises

## Federation with AD FS

- Single Sign On (SSO)
- Passwords never visible to cloud

The screenshot shows the 'Microsoft Azure Active Directory Connect' window, specifically the 'User sign-in' configuration page. On the left is a navigation pane with the following items: 'Welcome', 'Express Settings', 'Required Components', 'User Sign-In' (which is highlighted), 'Connect to Azure AD', 'Sync', 'Connect Directories', 'Azure AD sign-in', 'Domain/OU Filtering', 'Identifying users', 'Filtering', 'Optional Features', and 'Configure'. The main content area is titled 'User sign-in' and contains the instruction 'Select the Sign On method.' Below this are four radio button options: 'Password Synchronization' (selected), 'Pass-through authentication (Preview)', 'Federation with AD FS', and 'Do not configure'. Each option has a help icon. Below these options is another instruction: 'Select this option to enable single sign on for your corporate desktop users:', followed by a checkbox labeled 'Enable single sign on (Preview)'. At the bottom right of the window are two buttons: 'Previous' and 'Next'.

# Pass-Through Authentication



<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-how-it-works>

# Demo

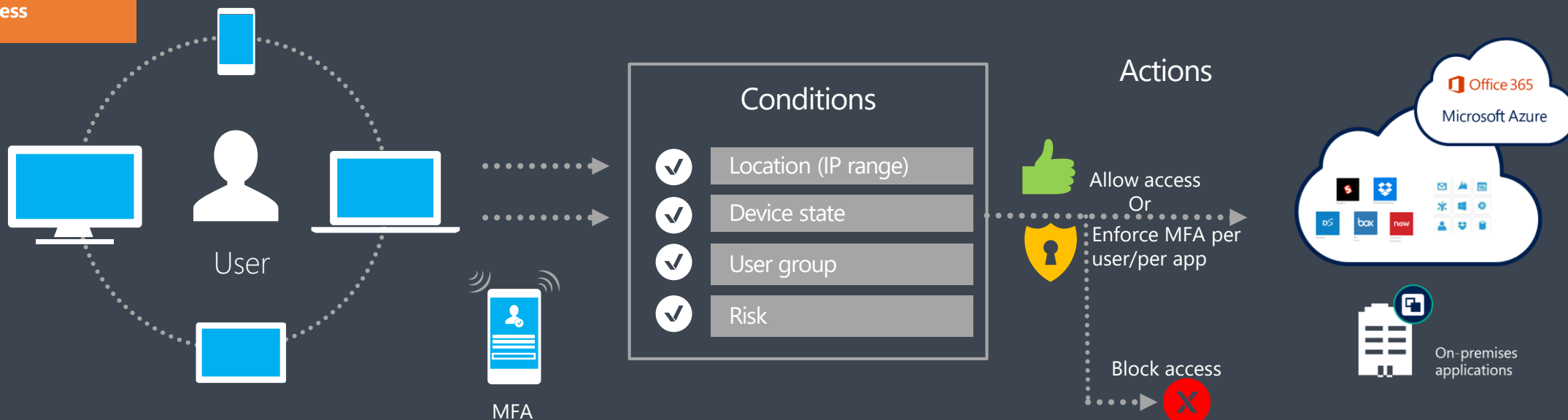
## Application Login



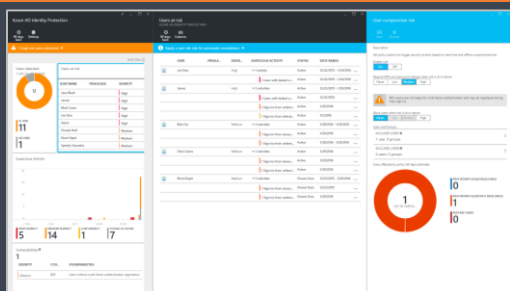
# Identity-driven security

Cloud IaaS/PaaS & On-Premise

## Conditional Access



## Azure AD Identity Protection

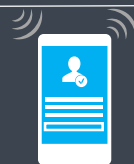


- ⚡ Brute force attacks
- ! Leaked credentials
- ! Suspicious sign-in activities
- 🚩 Infected devices
- 📋 Configuration vulnerabilities



- Consolidated view to examine suspicious user activities and configuration vulnerabilities
- Remediation recommendations
- Risk severity calculation
- Risk-based policies for protection for future threats

## PRIVILEGED IDENTITY MANAGEMENT



MFA

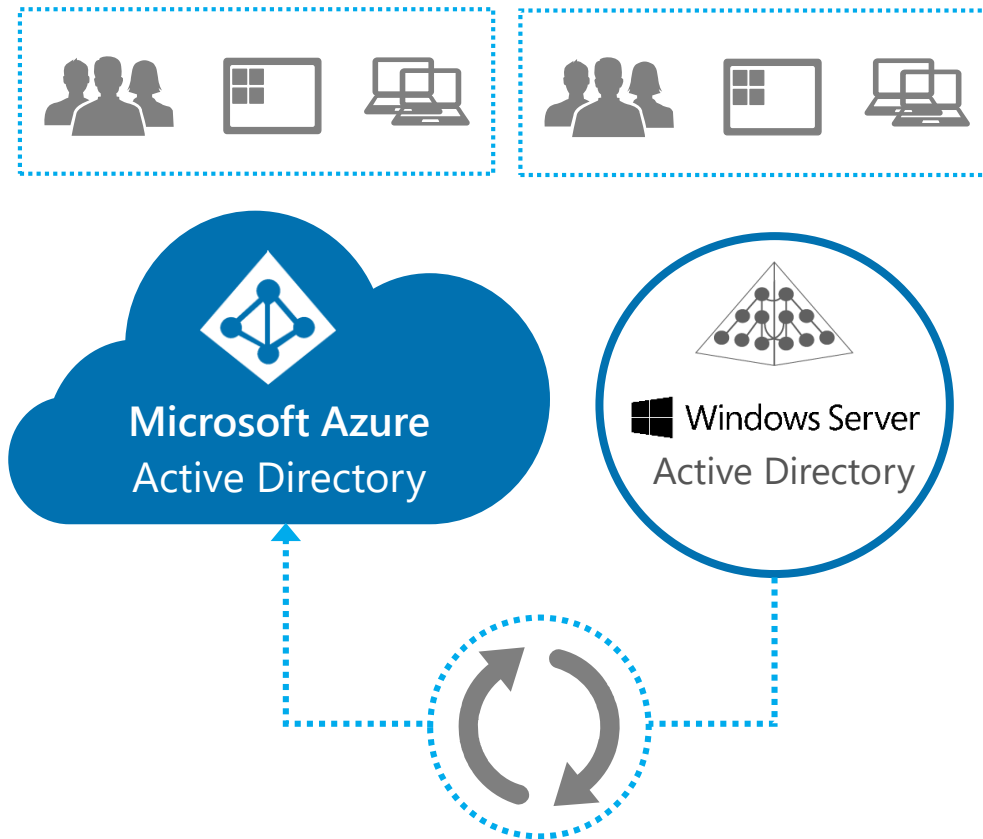


Block access



Time Based

# Identity & Access: Multi Factor Authentication



- ✓ Protect sensitive data and applications both on-premises and in the cloud with Multi Factor Authentication
- ✓ Can use Active Directory (on-premises) with Azure Active Directory (in cloud) to enable single sign-on, a single directory, and centralized identity management
- ✓ Multi Factor Authentication can be implemented with Phone Factor or with AD on-premises

# Per-User MFA versus Conditional Access

## Per-User MFA

Require MFA always, for all applications

Free of charge for all Azure AD admins and all Azure admins

### Additional security verification App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. View video to know how to secure your account

what's your preferred option?

We'll use this verification option by default.

Text code to my authentication p ▼

how would you like to respond?

Set up one or more of these options. Learn more

<input type="checkbox"/> Authentication phone	Select your country or region ▼	
<input type="checkbox"/> Office phone	Select your country or region ▼	Extension
<input type="checkbox"/> Alternate authentication phone	Select your country or region ▼	
<input type="checkbox"/> Authenticator app	Configure	

Save cancel

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

## Conditional Access

Require MFA under specific conditions

- For a specific app e.g. Azure
- When not on work network
- When sign-in considered high risk

Azure AD Premium feature

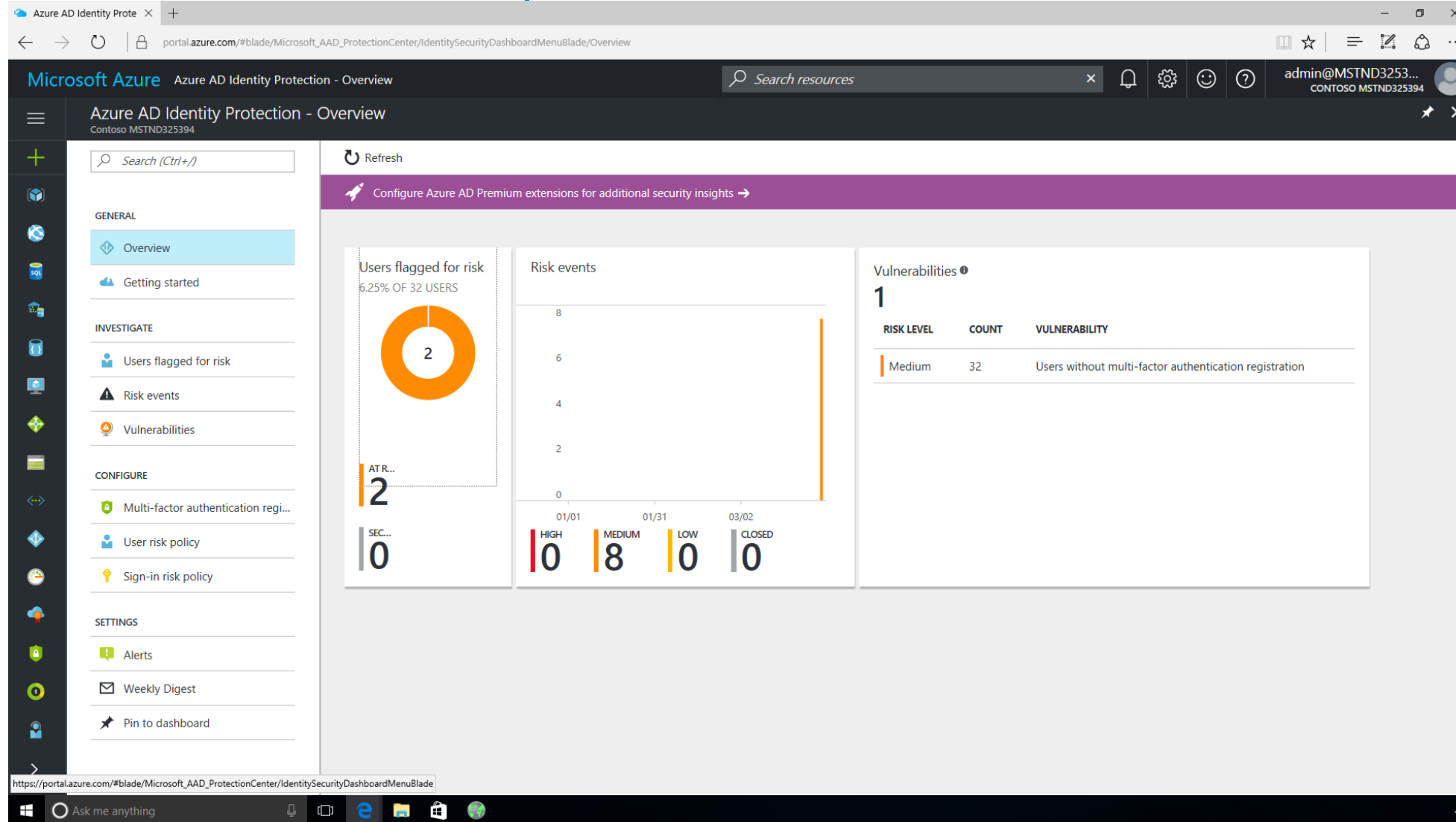
- P1 SKU
- Licenses needed for users who are affected by policy



# Best Current MFA Option: Windows Hello

- Formula:
  - Windows 10 workstation
  - Azure AD-joined
  - Windows Hello protected by biometric or PIN
  - Microsoft Edge browser and not in In-Private mode
- Result: Sign-in via TPM-protected asymmetric key

# Azure AD Identity Protection



<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection>

Security Imperative

Securing Investment

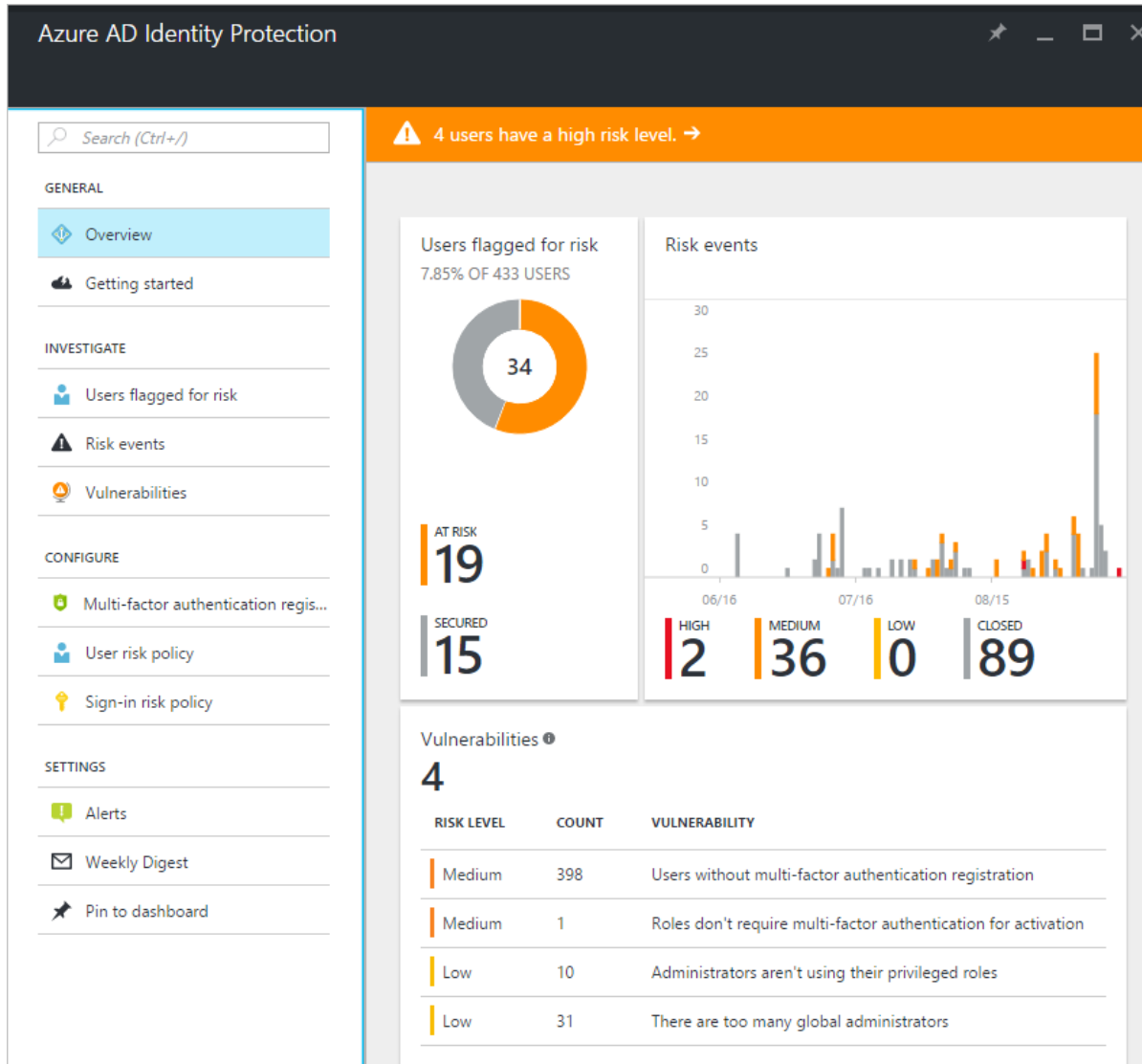
Securing Infrastructure

Securing Data

Securing Applications

Monitoring & Ops

# Azure AD Identity Protection



Azure AD Identity Protection - Users flagged for risk  
Test\_Test\_aad171

Search (Ctrl+/)

Download Refresh

Apply a user risk policy for automatic mitigation. →

Search users

USER	MFA	RISK LEVEL	RISK EVENTS	STATUS	LAST UPDATED (UTC)
John Nash		High	215 risk events	At risk	12/7/2016 10:51 AM
Jon Doe	✓	Medium	1 risk event	At risk	11/15/2016 7:18 PM
Junpu Chen	✓	Medium	0 risk events	At risk	9/12/2016 10:57 AM
Security Admin	✓	Medium	0 risk events	At risk	8/23/2016 2:40 PM
Security Reader	✓	Medium	0 risk events	At risk	8/23/2016 2:40 PM
Ben Hecht		Secured	0 risk events	Remediated	1/31/2016 3:21 PM
On-Premises Directory Synchroniz...		Secured	0 risk events	Remediated	12/14/2015 7:21 PM
secReader2		Secured	0 risk events	Remediated	9/7/2016 5:18 AM

Azure AD Identity Protection - Risk events  
AZURE AD IDENTITY PROTECTION

Last 90 days Download

Search (Ctrl+/)

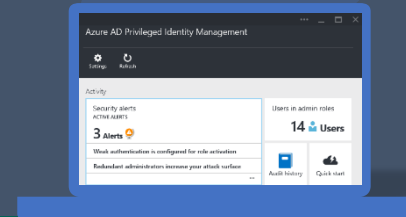
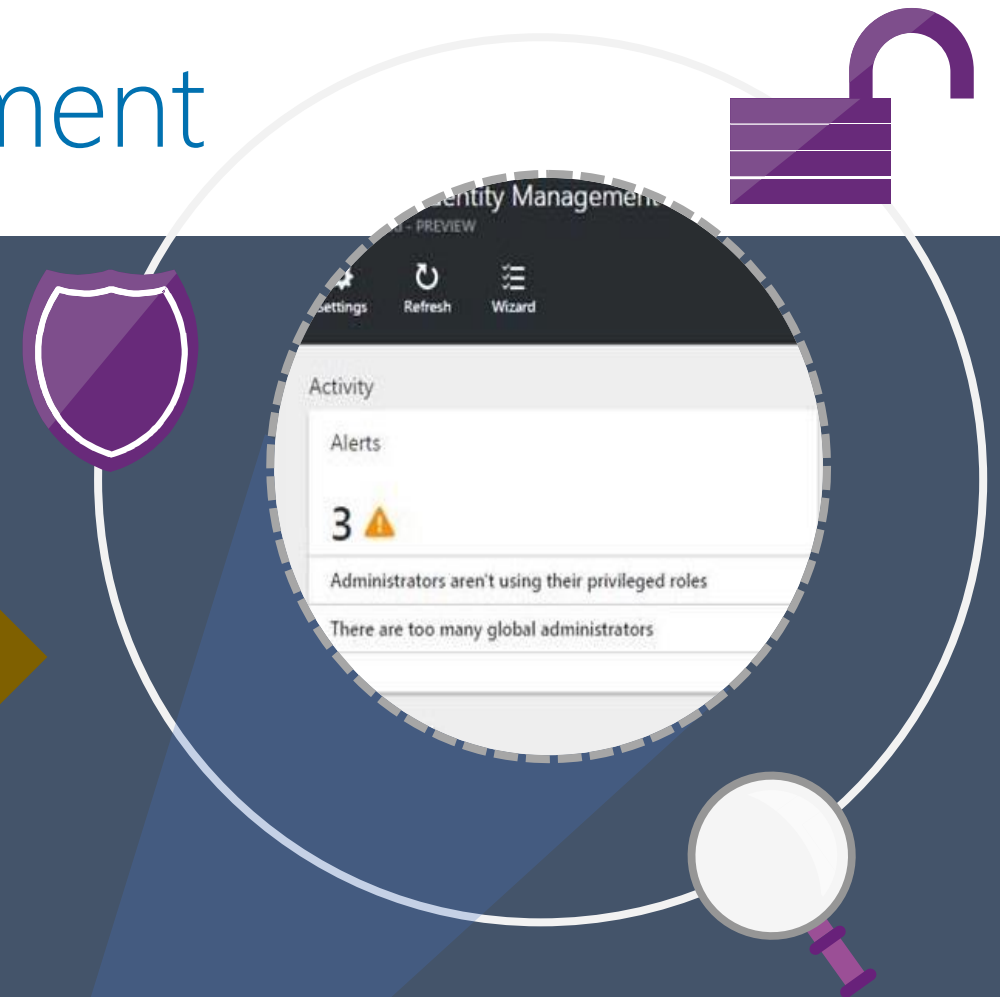
RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials ⓘ	0 of 2	9/12/2016, 11:36 PM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	37 of 50	9/9/2016, 5:58 PM
Medium	Offline	Impossible travels to atypical locations ⓘ	5 of 12	9/7/2016, 6:49 PM
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ	47 of 63	9/9/2016, 5:58 PM

# Privileged Identity Management

Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed

Provides more visibility through alerts, audit reports and access reviews



Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

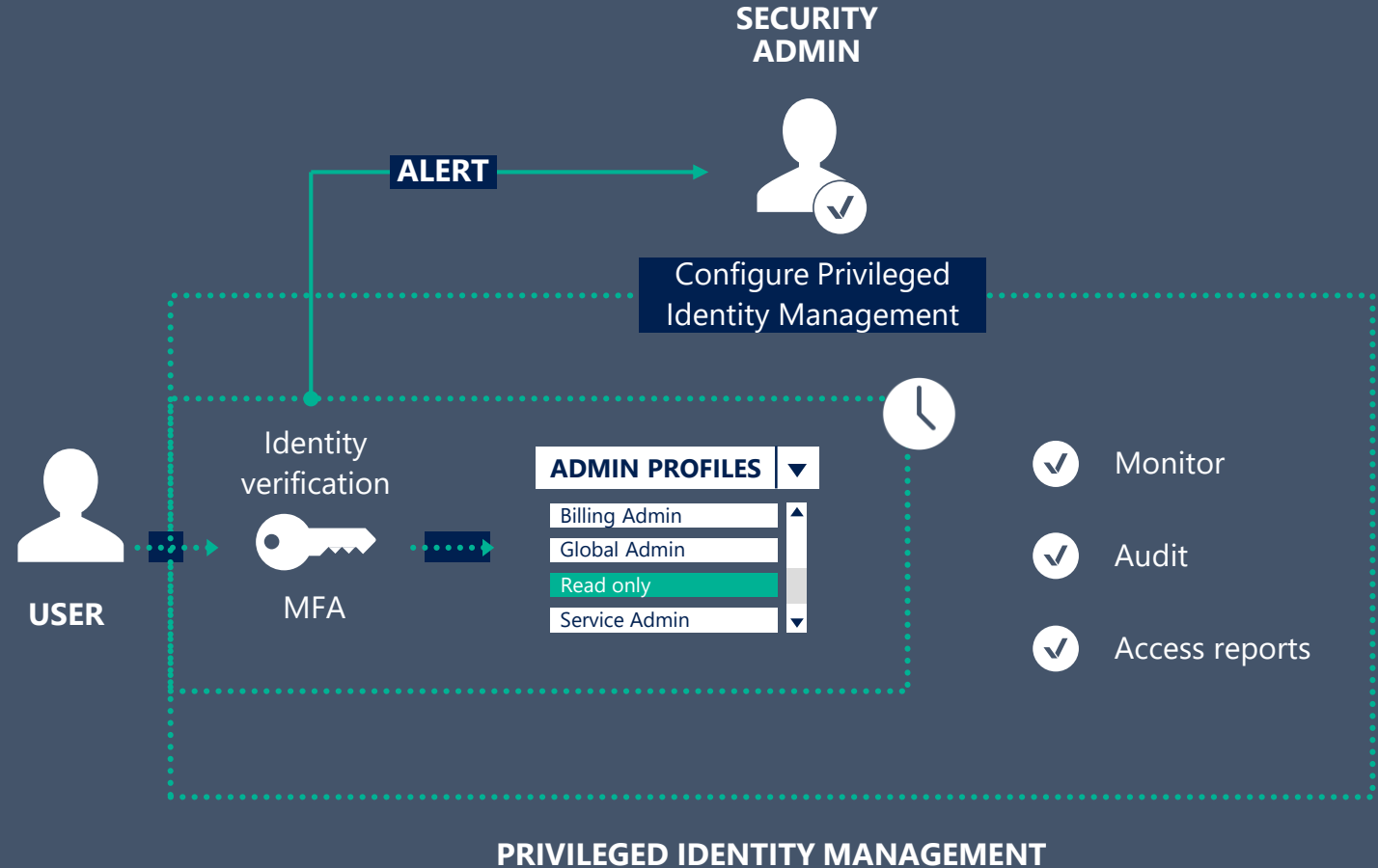
Securing Applications

Monitoring & Ops

# Privileged Identity Management

How time-limited activation of privileged roles works

- ▶ Users need to activate their privileges to perform a task
- ▶ MFA is enforced during the activation process
- ▶ Alerts inform administrators about out-of-band changes
- ▶ Users will retain their privileges for a pre-configured amount of time
- ▶ Security admins can discover all privileged identities, view audit reports and review everyone who has is eligible to activate via access reviews



# Benefits

Reduces exposure  
to attacks  
targeting admins

Removes unneeded permanent  
admin role assignments

Limits the time a user has admin  
privileges

Ensures MFA validation prior to  
admin role activation

Simplifies  
delegation

Separates role administration  
from other tasks

Adds roles for read-only views  
of reports and history

Asks users to review and justify  
continued need for admin role

Increases visibility  
and finer-grained  
control

Enables least privilege role  
assignments

Alerts on users who haven't  
used their role assignments

Simplifies reporting on admin  
activity

# Privileged Identity Management (RBAC)

Privileged Identity Management - Azure Resources (Preview)  
PREVIEW

Approvals and my audit history is now in preview →

Quick Start

TASKS

My Roles

Approve Requests (Preview)

My Requests (Preview)

Review Access

MANAGE

Azure AD Directory Roles

Azure Resources (Preview)

ACTIVITY

My Audit History (Preview)

TROUBLESHOOTING + SUPPORT

Troubleshoot

New support request

Subscription filter ⓘ  
6 selected

Search by resource name

RESOURCE	RESOURCE TYPE
Azure Internal Consumption	subscription
Azure Internal Consumption2	subscription
Azure Internal Consumption3	subscription
Azure Internal Consumption4	subscription
Subscription	subscription
Team Subscription - Ben Roscorla	subscription

# Demo

## Identity Protection and PIM





# Managed Service Identity

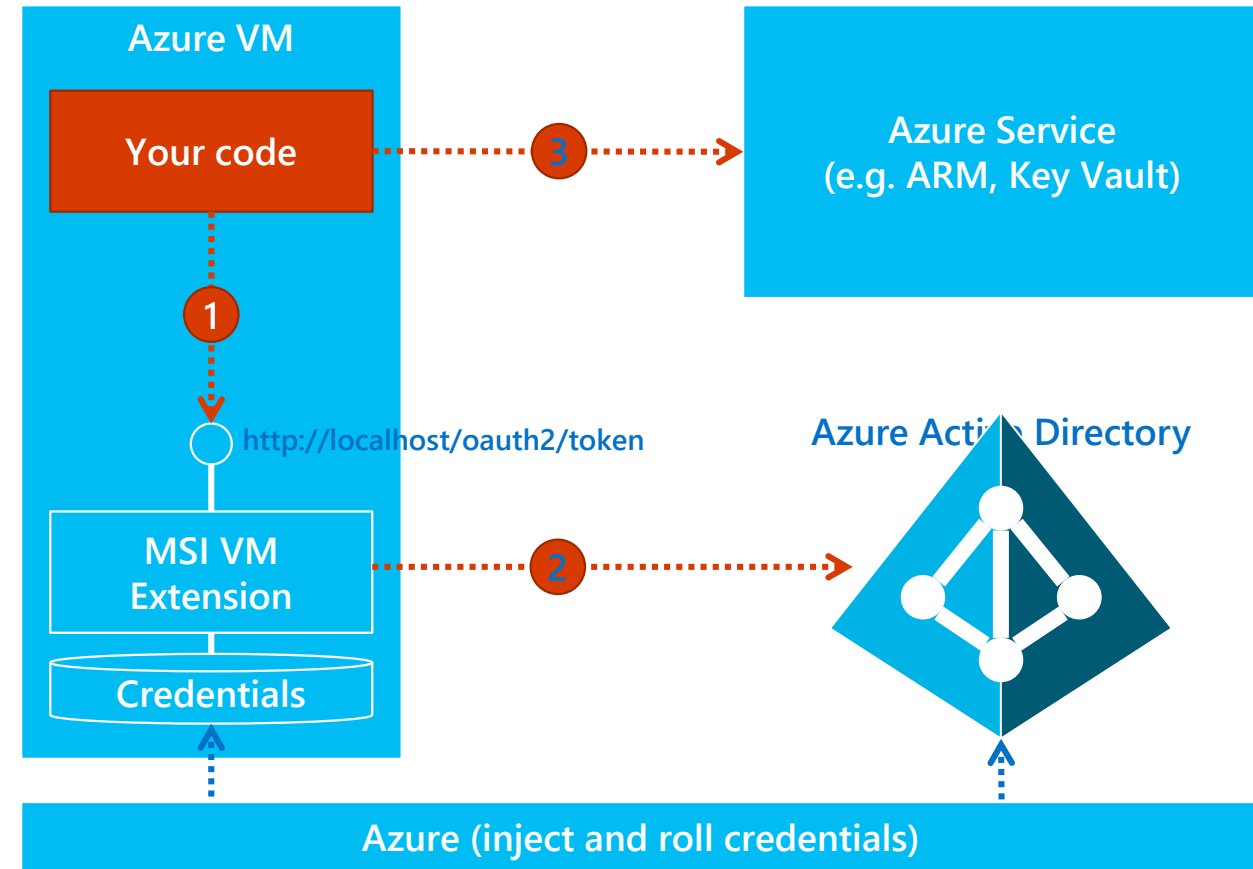
Auto-managed identity in  
Azure AD for Azure resource

Use local MSI endpoint to get  
access tokens from Azure AD

Direct authentication with  
services, or retrieve creds  
from Azure Key Vault

No additional charge for MSI

Now in preview



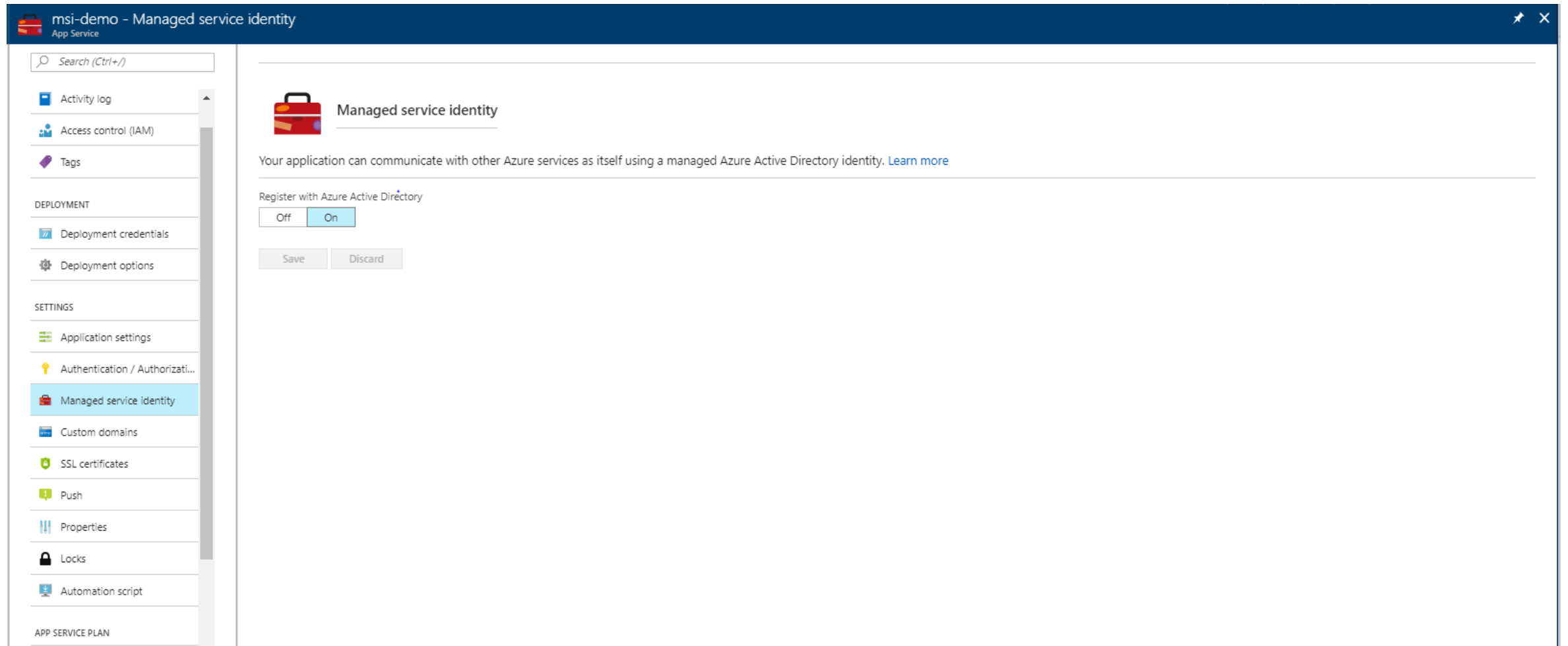
<https://docs.microsoft.com/en-us/azure/active-directory/msi-overview>

# Demo

## Set-up Managed Service Identity
















# Managed Service Identity – App Service/Functions



<https://docs.microsoft.com/en-gb/azure/app-service/app-service-managed-service-identity>

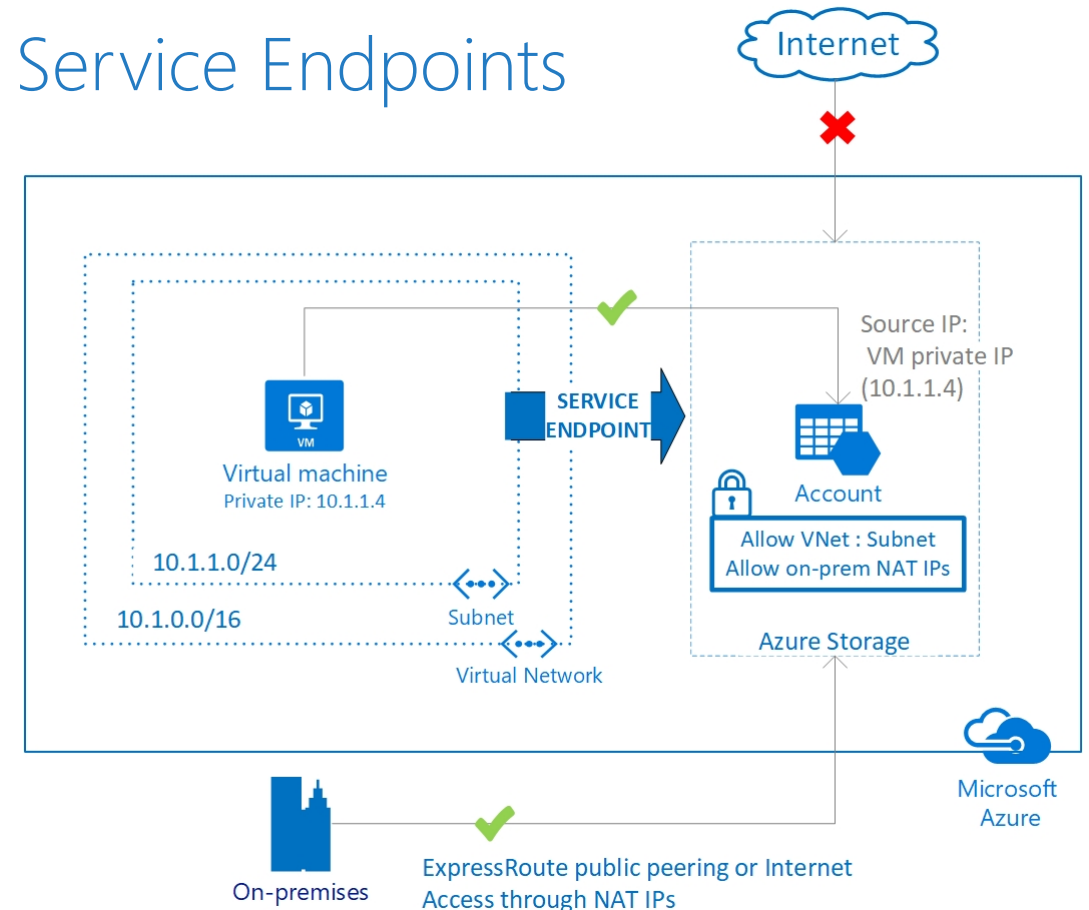
# Extra Network Features

## DDoS Standard

 Basic	Feature	 Standard
	Always on monitoring	
	Automatic mitigation for L3/L4 attacks	
	L7 Protection with Application Gateway Web application firewall	
	Globally deployed	
	Protection policies tuned to your VNet	
	Logging, alerting, and telemetry	
	Resource cost scale protection	

<https://azure.microsoft.com/en-gb/blog/azure-ddos-protection-service-preview/>

## Service Endpoints

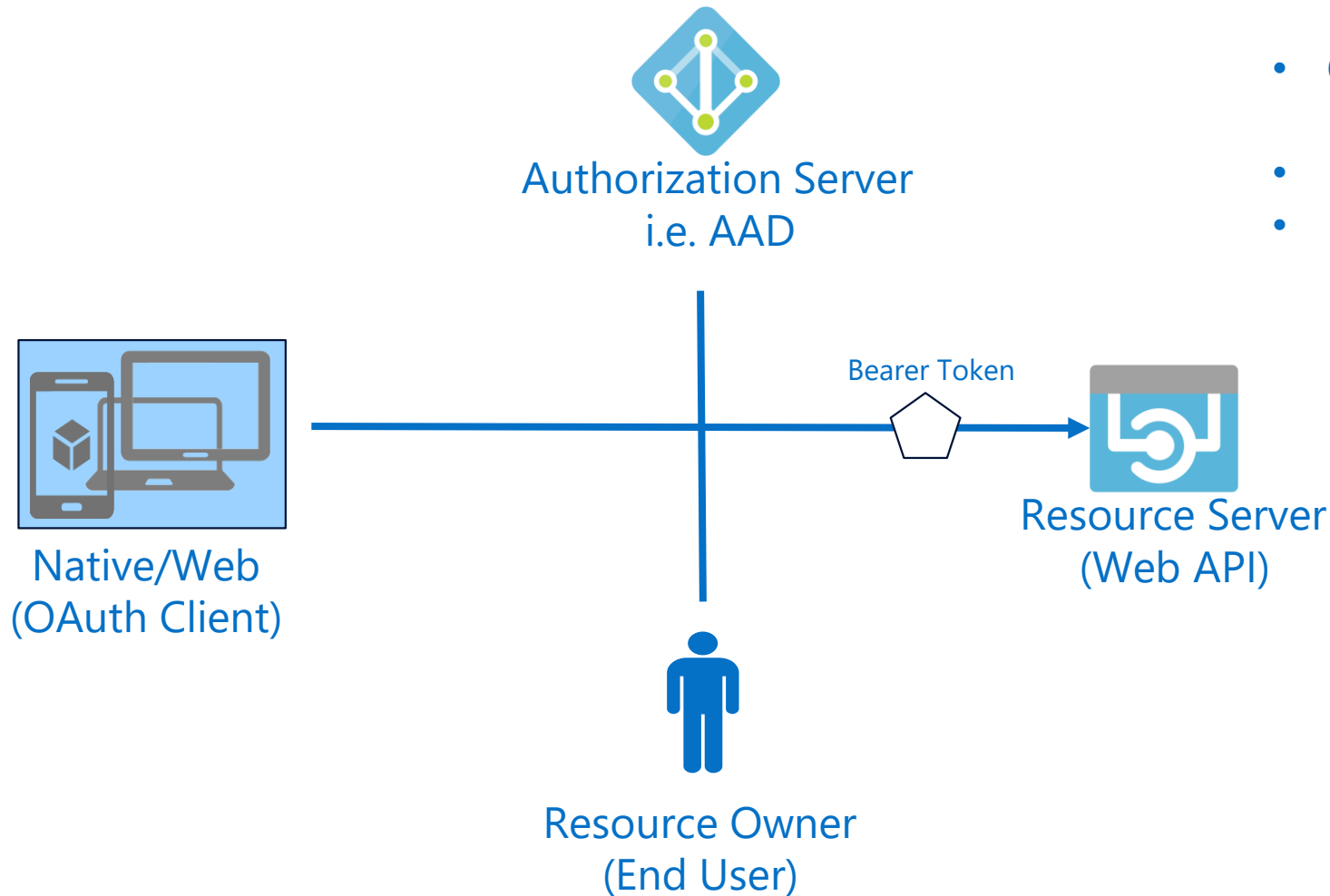


<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

# Coming Soon

Sign-In to Azure VMs using Azure AD  
“Standalone” Managed Service Identity  
RBAC “Constrained Delegation”

# App Authentication - OAuth



- Client – Means Client Device – Not User
  - OAuth has Public and Confidential clients
- Resource Owner = User
- Resource Server is where the data resides

# OAuth Flows

Authorization Code

The quintessential OAuth grant

Implicit

The bad boy of OAuth - Recommend for SPA - Browser-based (JavaScript)

Client Credentials

Run as a Service - Client (not user!)

Resource Owner  
Password Credentials

A bit like a service account - username and password

Refresh Token

Get Token without re-authentication

JWT Bearer

‘on behalf of’ – multiple hops between services

# 4 Steps for Implementing Solution Azure AD



**Design**



**Register  
in AAD**



**Implement  
Code**



**Consent**

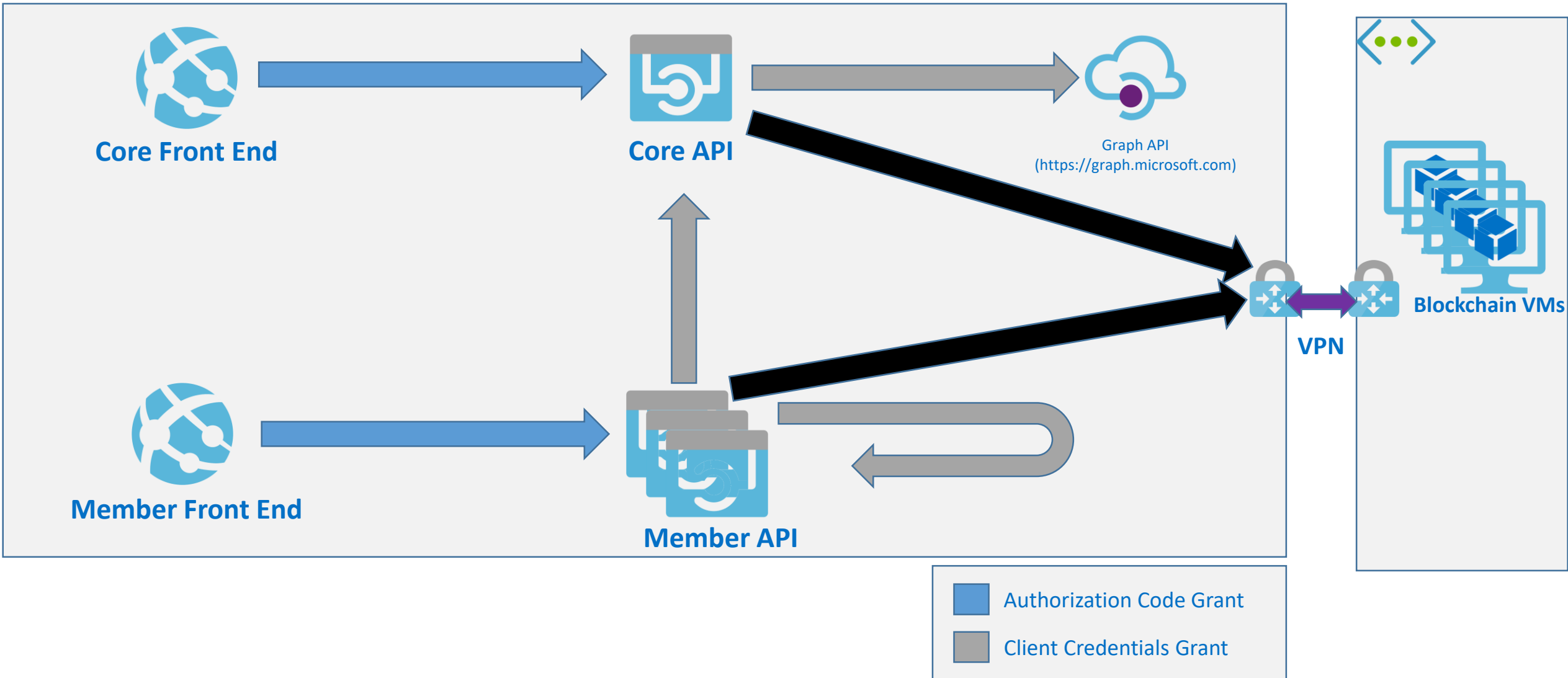


# Initial Setup

Design



Azure AD



Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

Securing Applications

Monitoring & Ops

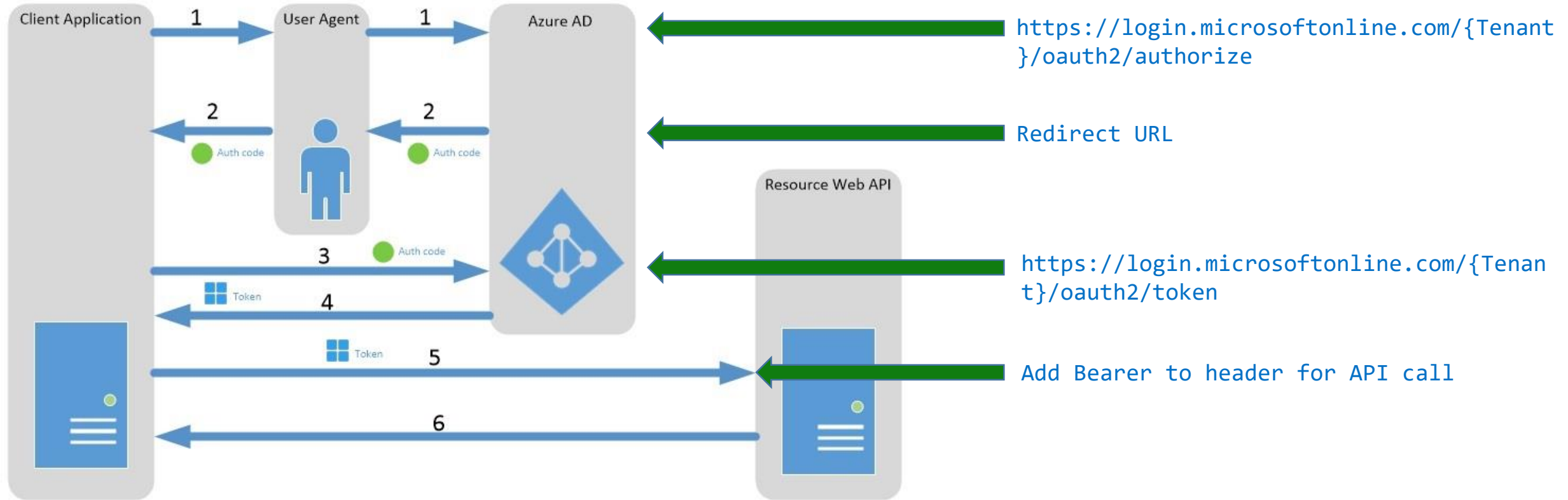
- Specify the App Type – Web or Native
- Sign on URL – Reply URL and Home Page URL
- Retrieve the Client ID
- If an API – note APP ID
- Set up Keys/Secrets for Confidential clients
- Set up Permissions

<input type="checkbox"/> APPLICATION PERMISSIONS	REQUIRES ADMIN
<input type="checkbox"/> Read files in all site collections (preview)	✓ Yes
Read and write files in all site collections (preview)	✓ Yes
Read all usage reports	✓ Yes
Read all hidden memberships	✓ Yes

<input type="checkbox"/> DELEGATED PERMISSIONS	REQUIRES ADMIN
Read files that the user selects (preview)	✗ No
Read and write files that the user selects (preview)	✗ No
Have full access to the application's folder (preview)	✗ No
Read all usage reports	✓ Yes

# You could hand roll....

## Implement Code



<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-protocols-openid-connect-code>

...or use our APIs....

Implement Code



## Web Site

### OWIN

UseOpenIdConnectAuthentication  
Function/Class Decorators

[AllowAnonymous]

[Authorize]

ClaimsPrincipal

### ADAL

AcquireTokenByAuthorizationCodeAsync

AcquireTokenSilentAsync



## Web API

### OWIN

UseWindowsAzureActiveDirectoryBearerAuth  
entication  
Function/Class Decorators

[AllowAnonymous]

[Authorize]

ClaimsPrincipal

### ADAL

AcquireTokenAsync

Client Credentials

User Assertion



## Native

### ADAL

AcquireTokenAsync

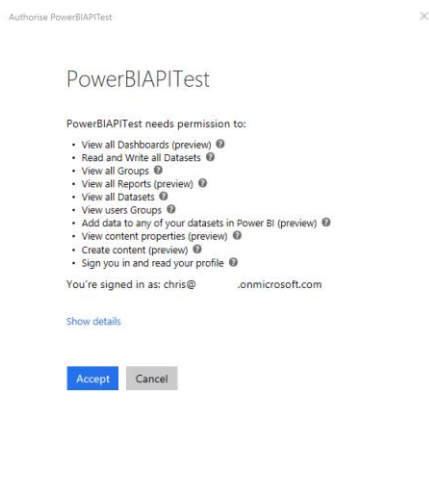
<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-developers-guide>

# Consent



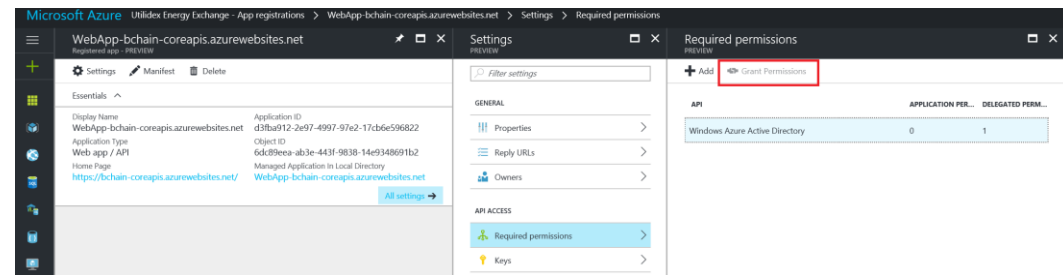
## User

<input type="checkbox"/> DELEGATED PERMISSIONS	REQUIRES ADMIN
Read files that the user selects (preview)	No
Read and write files that the user selects (preview)	No
Have full access to the application's folder (preview)	No
Read all usage reports	Yes



## Admin

<input type="checkbox"/> APPLICATION PERMISSIONS	REQUIRES ADMIN
Read files in all site collections (preview)	Yes
Read and write files in all site collections (preview)	Yes
Read all usage reports	Yes
Read all hidden memberships	Yes

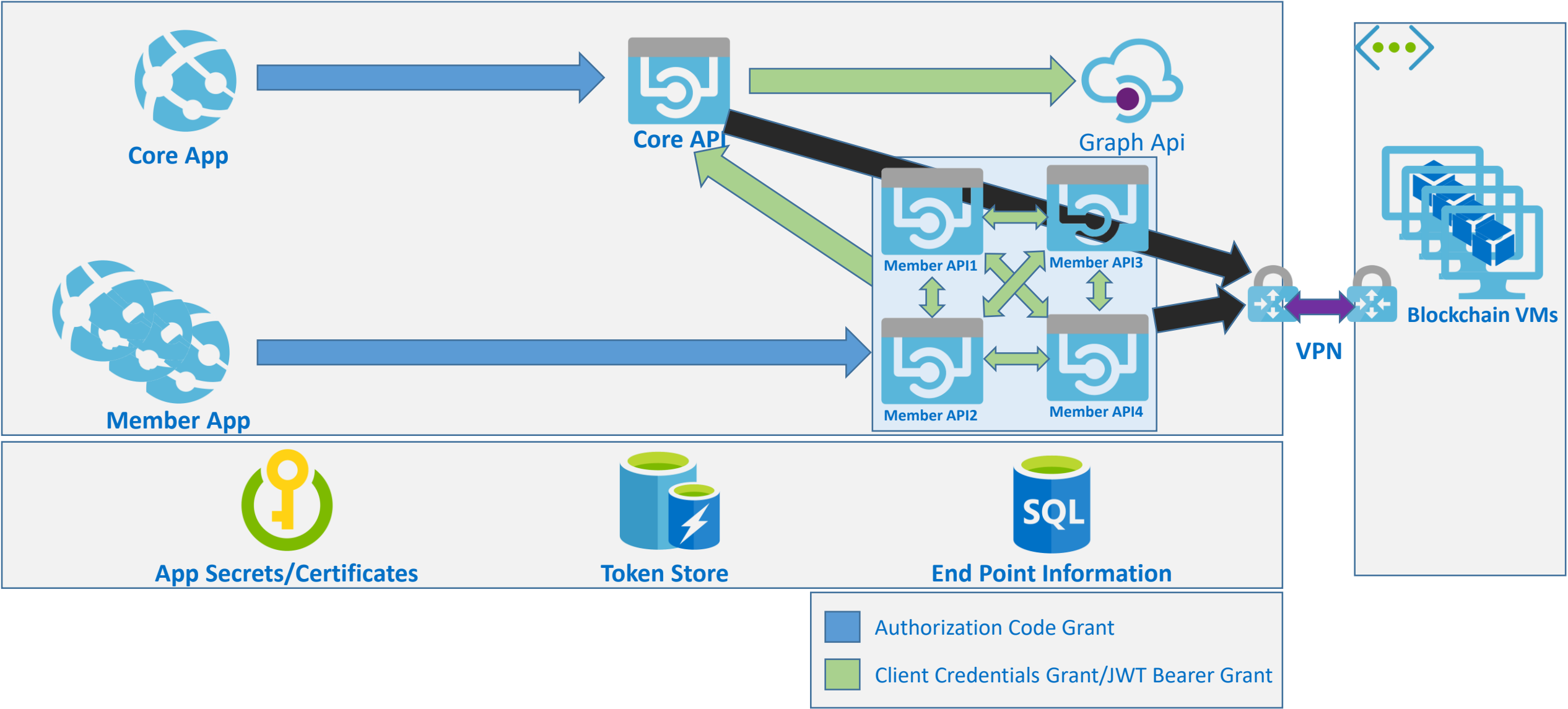


### Remove: Azure AD Access Panel

You can remove this consent by deleting the Application itself or the Service Principal which contains the consent information using a PowerShell command - Remove-MsolServicePrincipal

# Final Design

Design



# Tips

- Easier to test locally
  - But remember to register your publish ReplyToUrls
- Always work with SSL turned on
- Double check the Reply URLs and other Registration properties
- Remember Azure AD supports multi-resource refresh tokens (MRRT)
- Consent and re-consent
- There is more than one endpoint (and helper URLs)
- Use the Multi-Tenant App pattern to support more than one AAD

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-devhowto-multi-tenant-overview>