Microsoft

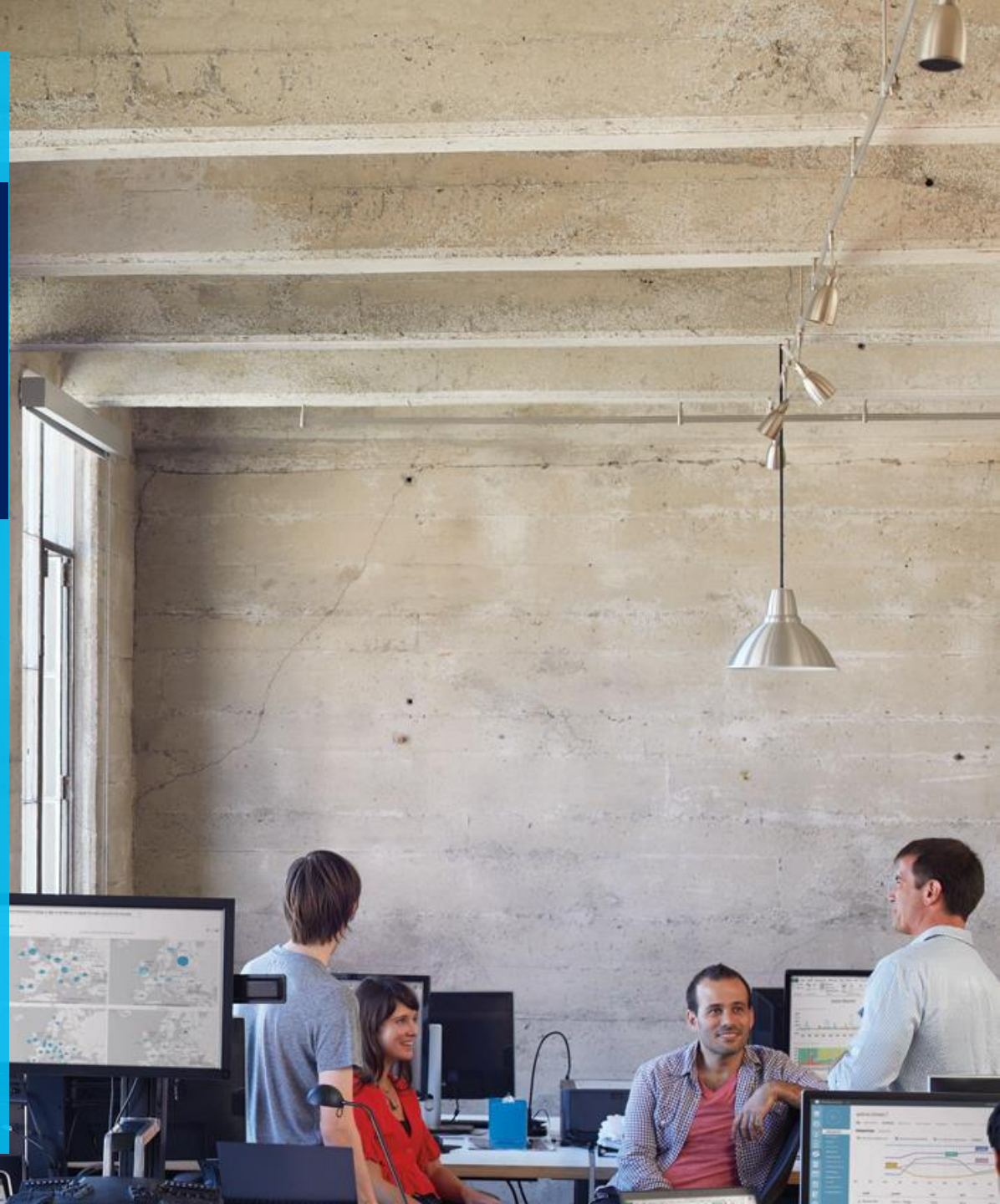
Date: 26th May 2023

Microsoft Azure Power Lunch

Today's Topic:
Protect APIs in API Management using Azure Active Directory

Series website: http://azurepowerlunch.com/

On-Demand Session Information (Recordings) are available here:
Azure Power Lunch YouTube Channel



Naveed Zaheer – Cloud Solution Architect

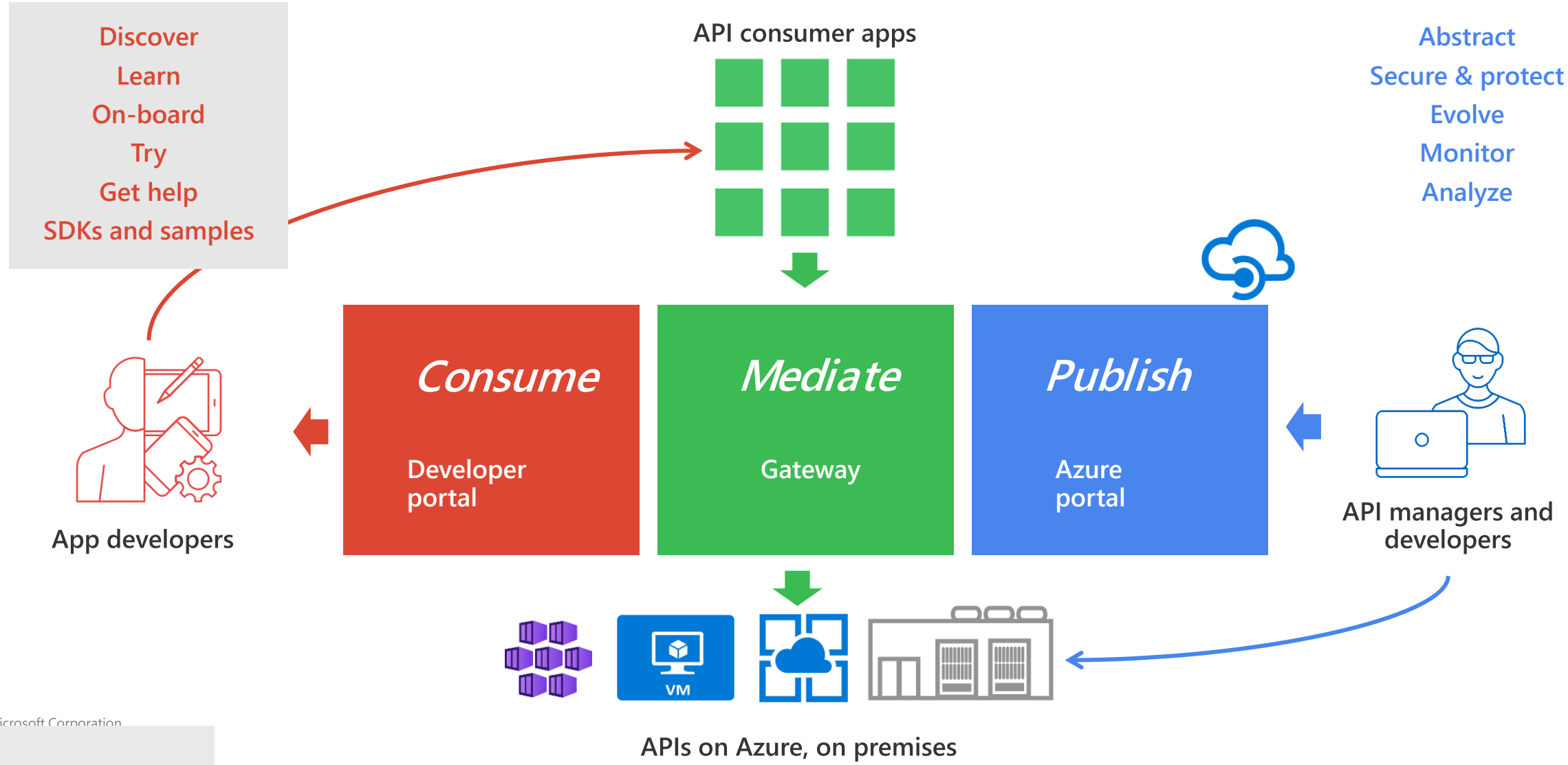


- Been with Microsoft for more than 19 years and in software industry for more than 28 years
- Spent 10+ years with Microsoft Consulting Services in areas such as AppDev, Distributed Applications, SOA and Cloud Applications
- Working with Azure since its inception
- Currently in a Cloud Solution Architect role

Agenda

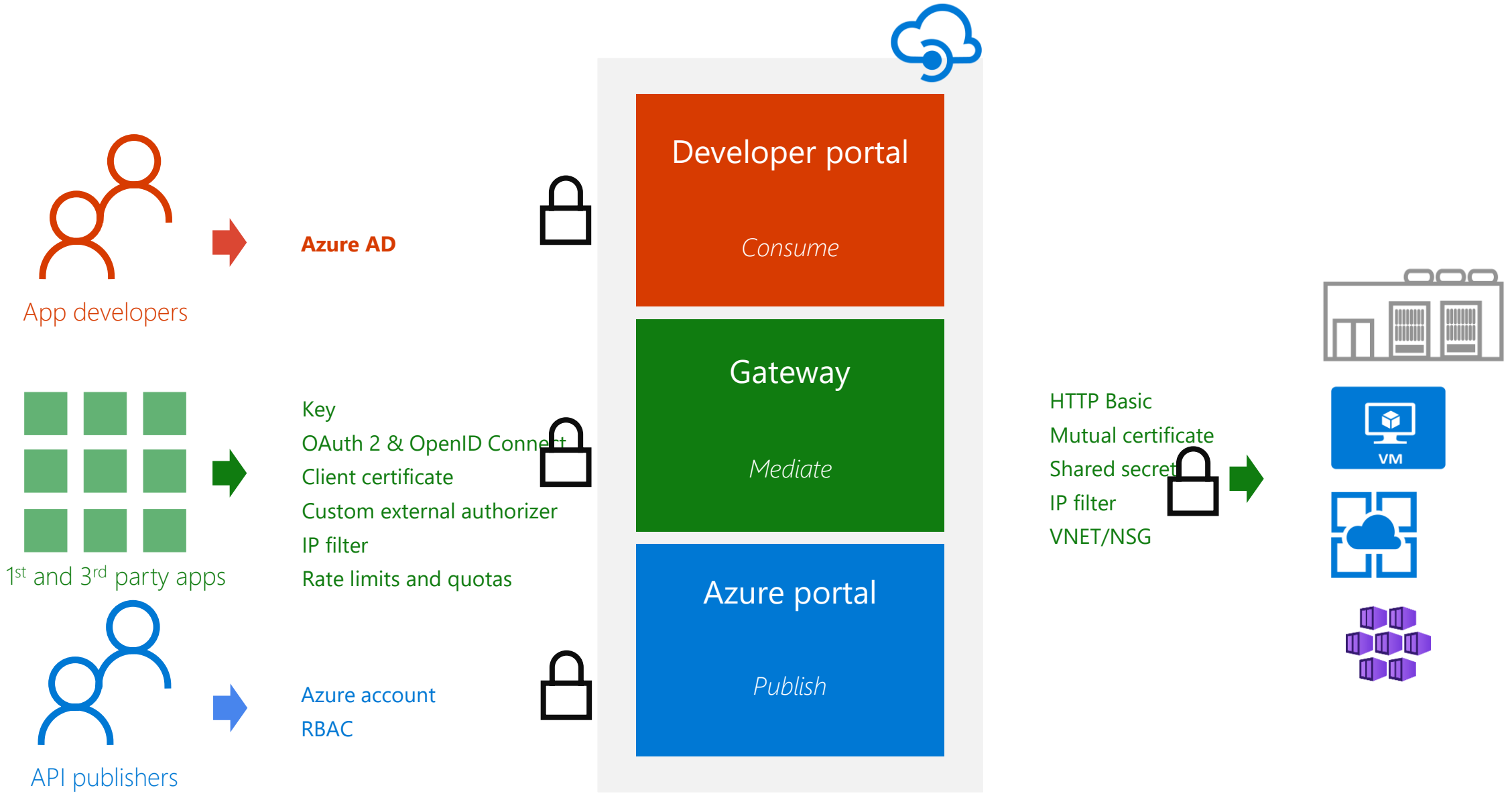
- Quick Overview of Azure API Management
- How to protect your APIs in Azure API Management using Azure AD and Oauth2 in a few easy steps?
- Frequently asked questions
- Q&A

Azure API Management
Logical Architecture

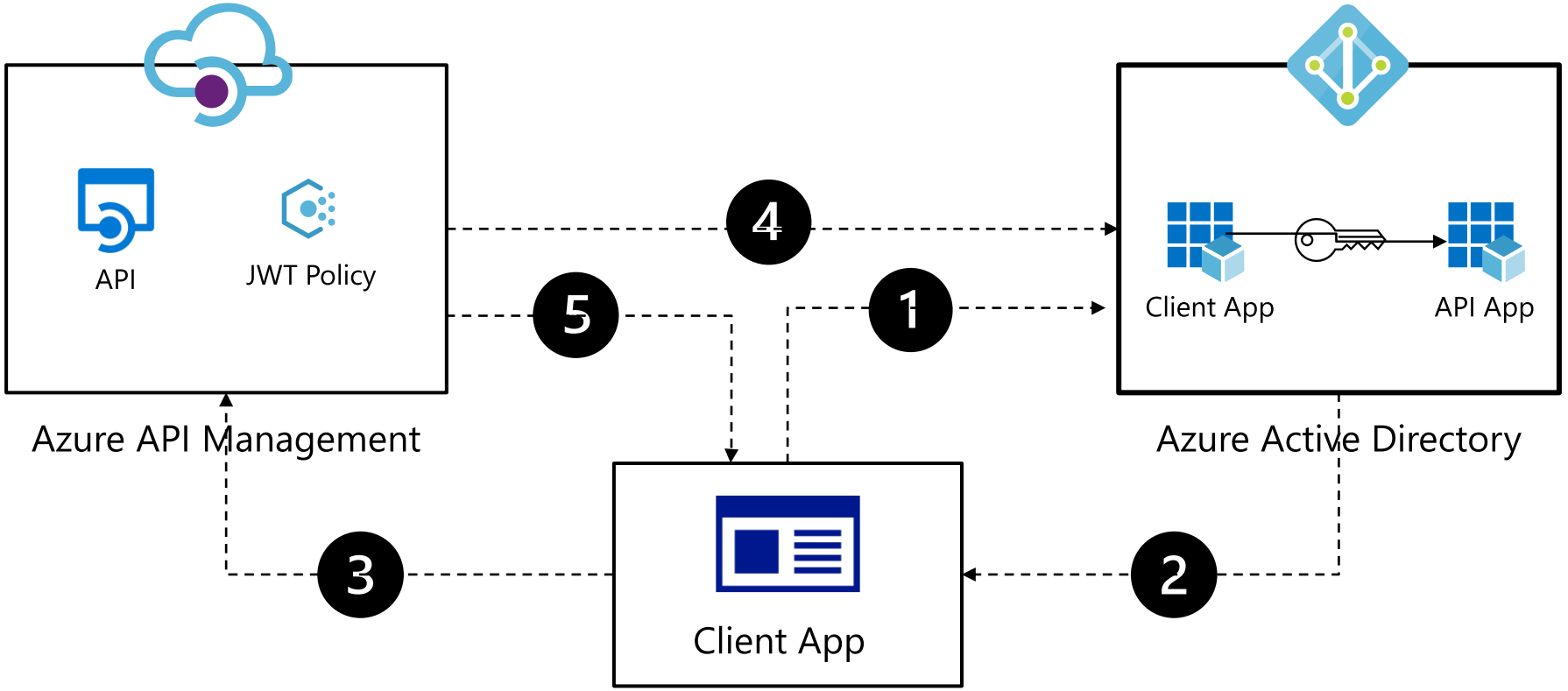


© Microsoft Corporation

Azure API Management
Security Architecture



Protecting API in APIM using Azure AD and OAuth2



1. Client App requests a token from Azure AD using the client-app credentials.
2. After successful validation, Azure AD issues the access/refresh token.
3. A developer (user of the Client App) makes an API call with the authorization header.
4. The token gets validated by using the validate-jwt policy in API Management by Azure AD.
5. Based on the validation result, the developer will receive the response in the Client App.

© Microsoft Corporation

Protecting API in APIM using Azure AD and OAuth2 – Key Steps

1. Create an App Registration to represent the API in Azure API Management
   - Resource Link: https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
2. Add App Roles to your App Registration
   - https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-add-app-roles-in-azure-ad-apps#app-roles-ui
3. Add Users and Groups to App Roles
   - https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivots=portal
4. Expose the API and Add a Scope
   - https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-expose-web-apis#add-a-scope
5. Create an App Registration to represent the Client App in Azure API Management
   - Resource Link: https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
6. Give the Client App access to the API
   - Resource Link: https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-expose-web-apis#add-a-scope
7. Add the Validate-JWT Policy to your API in API Management
   - Resource Link: https://learn.microsoft.com/en-us/azure/api-management/validate-jwt-policy

© Microsoft Corporation

Demo

Resources

- Protect an API in Azure API Management using OAuth 2.0 authorization with Azure Active Directory
- Restricting API Management access to users through AAD
- Azure API Management Validate-JWT Policy

Microsoft

© Copyright Microsoft Corporation. All rights reserved.