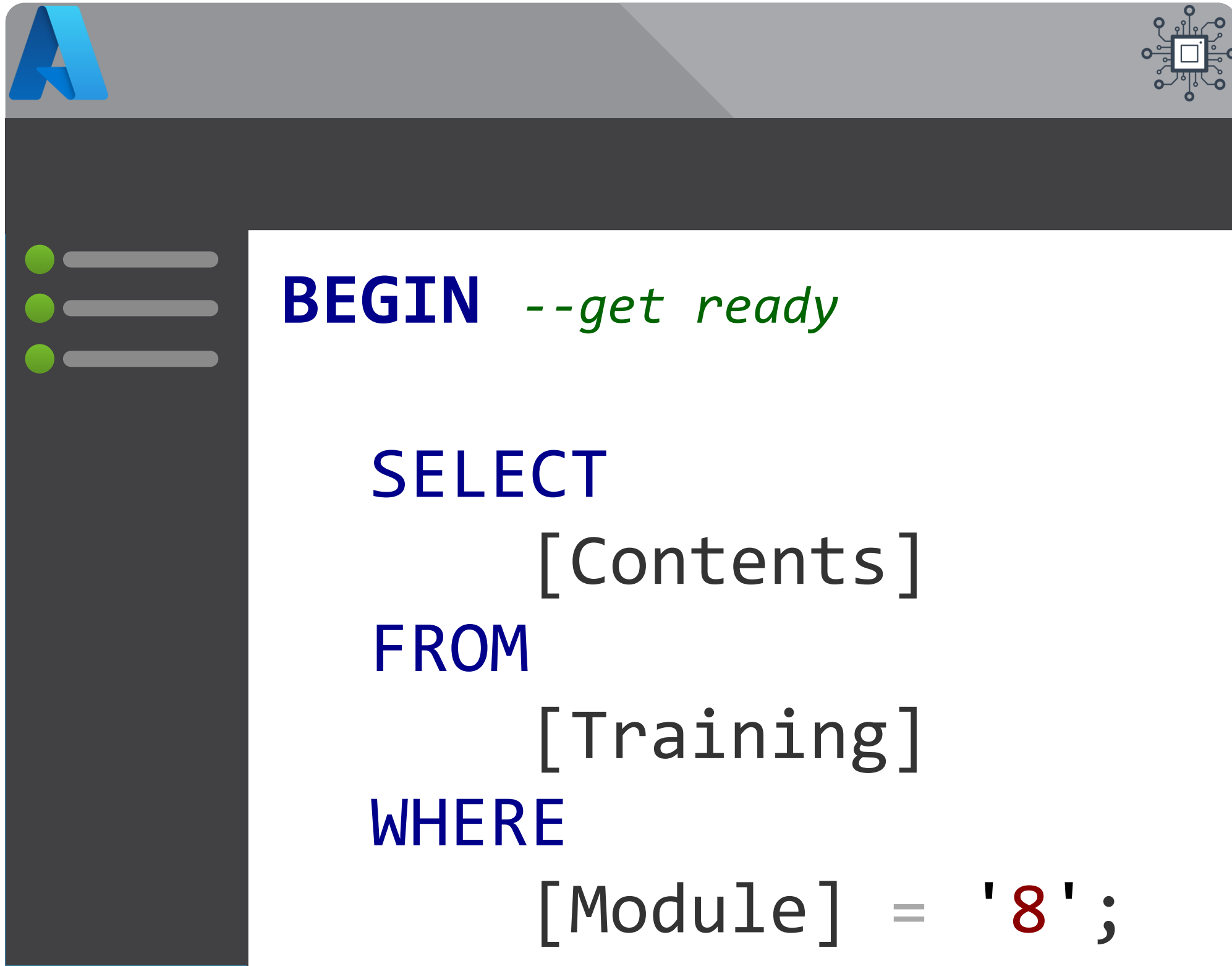


# Module 8

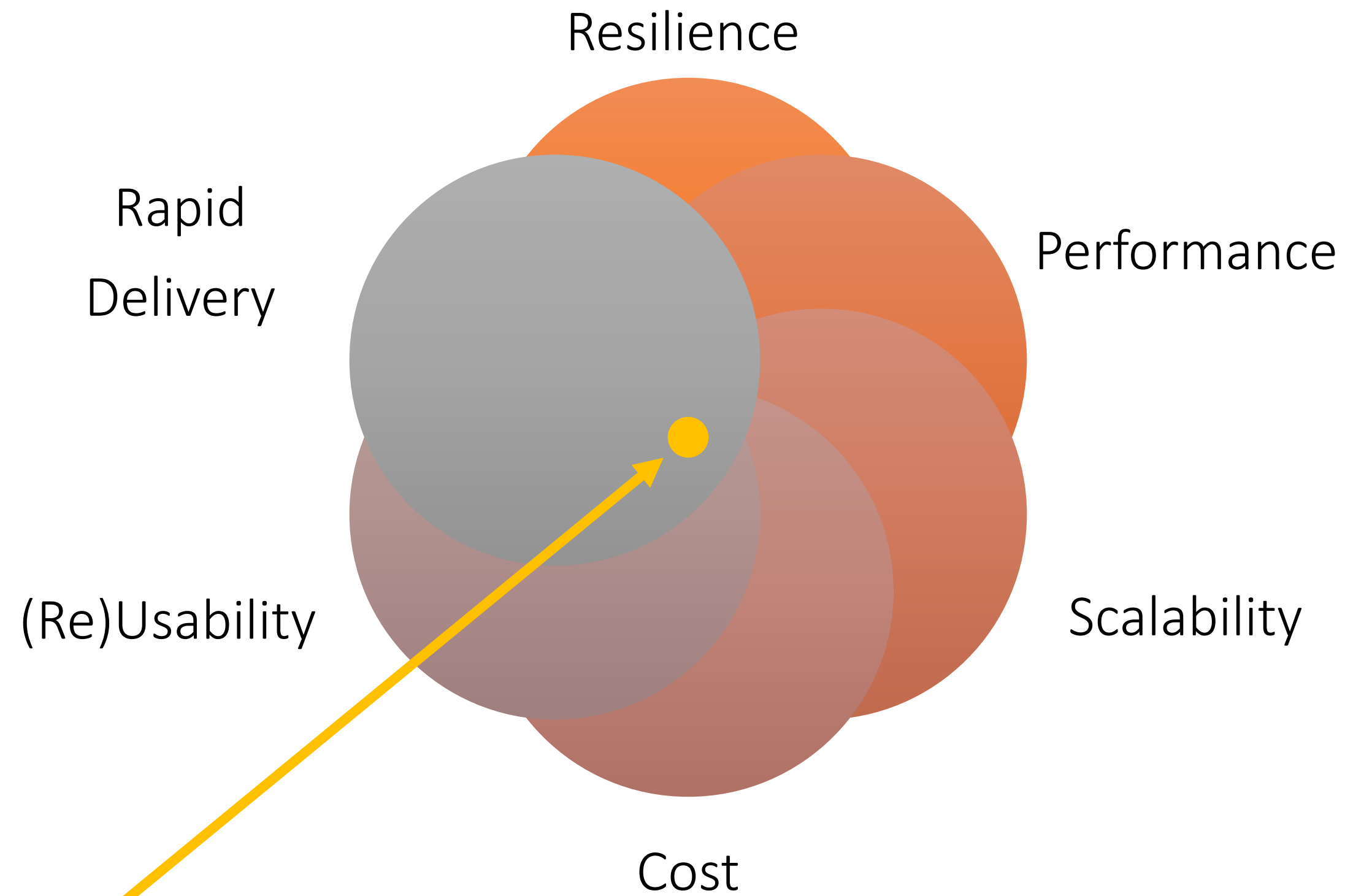
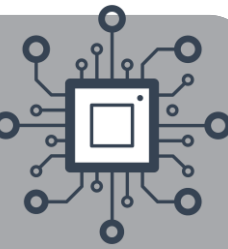
## Security



- Service Principals
- Managed Identities
- Azure Key Vault Integration
- Customer Managed Keys
- Pipeline Access & Permissions



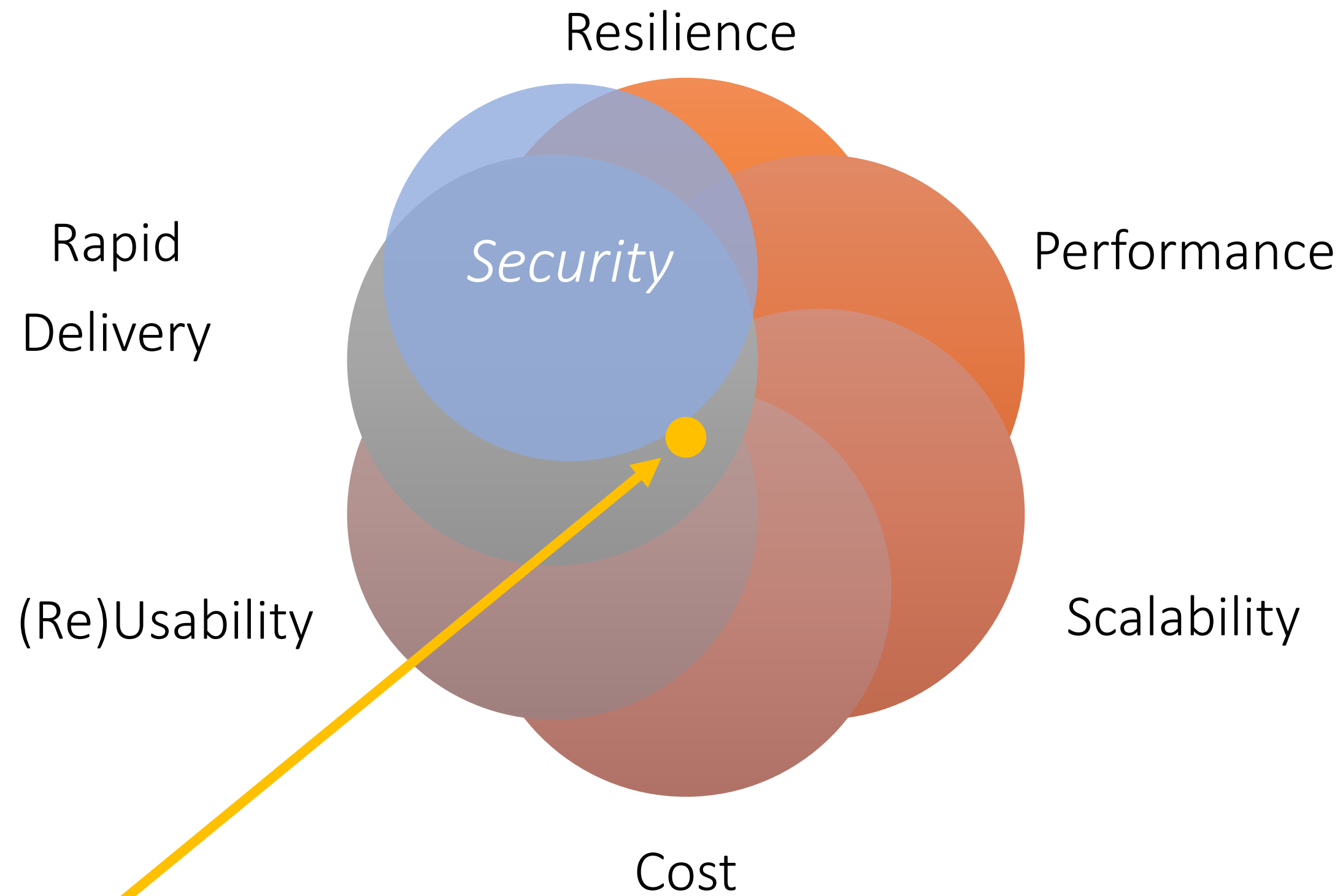
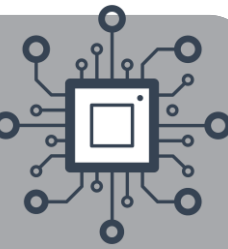
# Design Priorities



The Perfect Solution



# Design Priorities

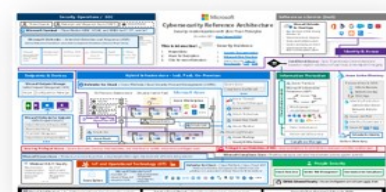


The Perfect Solution



## Capabilities

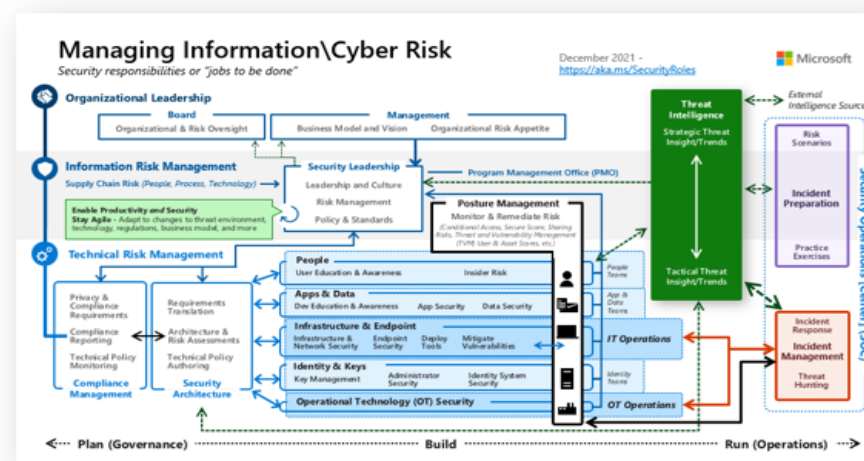
What cybersecurity capabilities does Microsoft have?



## People

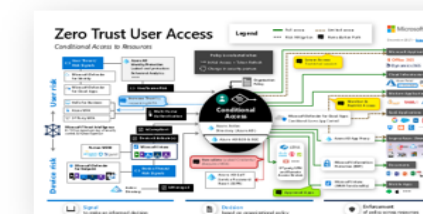
How are roles & responsibilities evolving with cloud and zero trust?

## Build Slide



## Zero Trust User Access

How to validate trust of user/devices for all resources?



## Azure Native Controls

What native security is available?



## Security Operations

## How to enable rapid incident response?



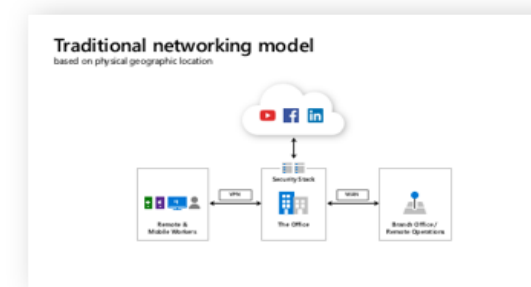
## Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?



## Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?



## Attack Chain Coverage

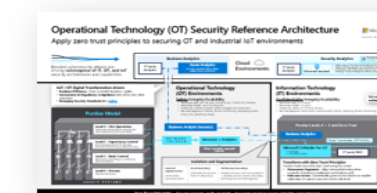
How does this map to insider and external attacks?



## Operational Technology

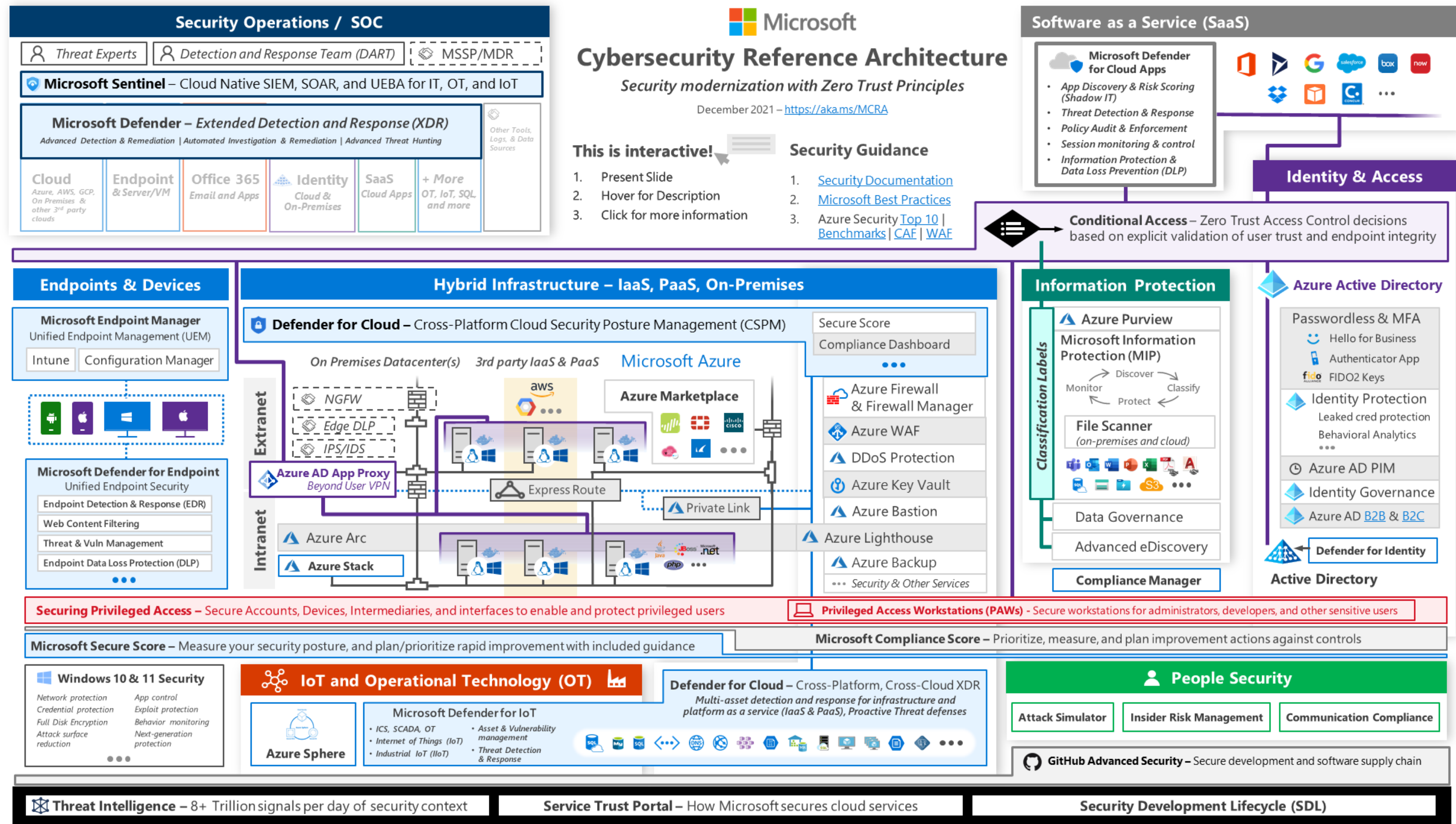
## How to enable Zero Trust Security for OT?

## Build Slide

[aka.ms/MCRA](https://aka.ms/MCRA) | December 2021 |

<https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra>

## Capabilities





# Module 8

## Security



- Service Principals
- Managed Identities
- Azure Key Vault Integration
- Customer Managed Keys
- Pipeline Access & Permissions

## Terminology Clarification & Properties

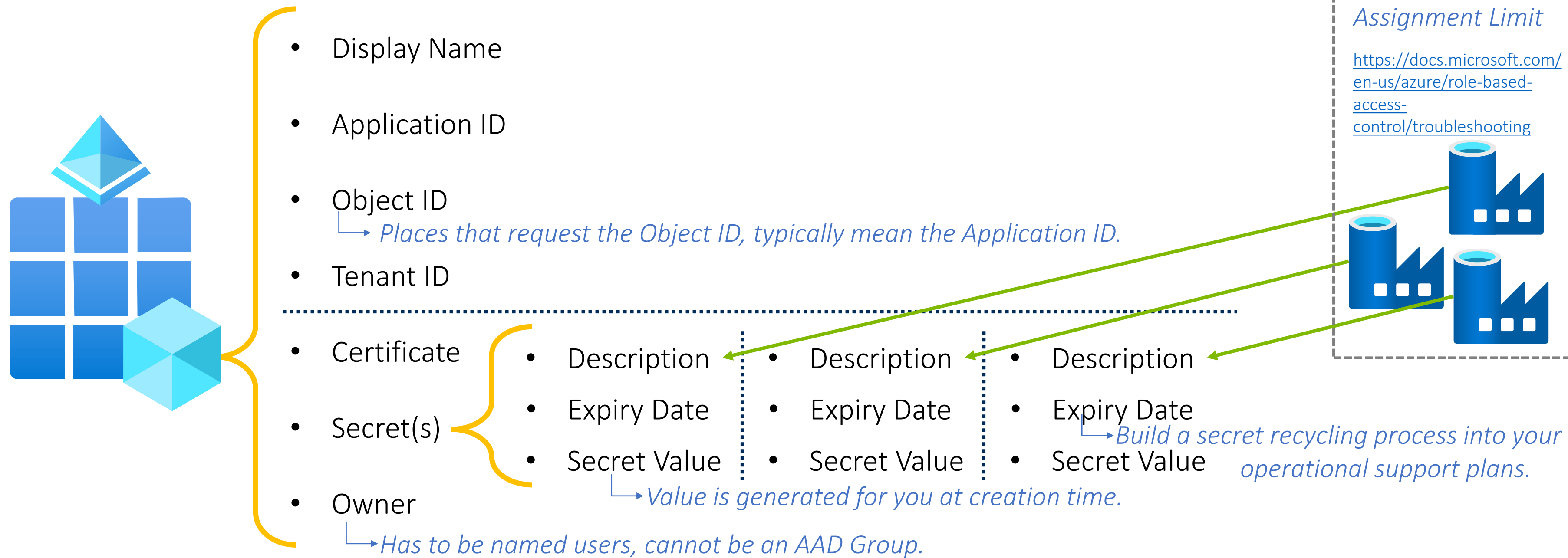
Service Account

Service Principal Name

SPN

System User

Application Registration



~~Service Account~~

Service Principal Name

SPN

~~System User~~

Application Registration



- Display Name
- Application ID
- Object ID
  - ↳ Places that request the Object ID, typically mean the Application ID.
- Tenant ID

- Certificate
- Secret(s)
- Owner
  - ↳ Has to be named users, cannot be an AAD Group.

- Description
- Expiry Date
- Secret Value
  - ↳ Value is generated for you at creation time.

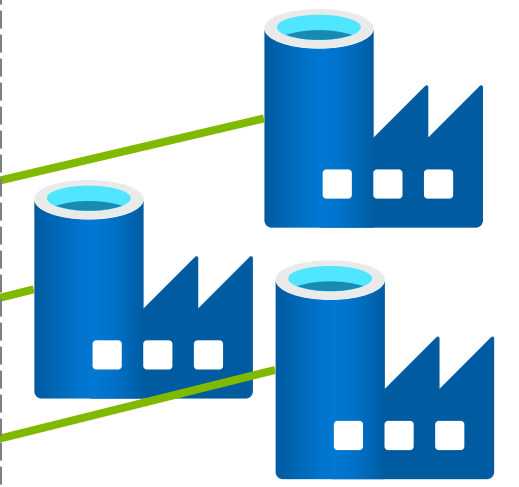
- Description
- Expiry Date
- Secret Value

- Description
- Expiry Date
- Secret Value

Build a secret recycling process into your operational support plans.

Subscription Role Assignment Limit

<https://docs.microsoft.com/en-us/azure/role-based-access-control/troubleshooting>



```
$sp = New-AzADServicePrincipal -DisplayName ServicePrincipalName
```



# Module 8

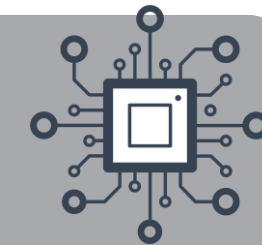
## Security



- Service Principals
- **Managed Identities**
- Azure Key Vault Integration
- Customer Managed Keys
- Pipeline Access & Permissions



# Managed Identities



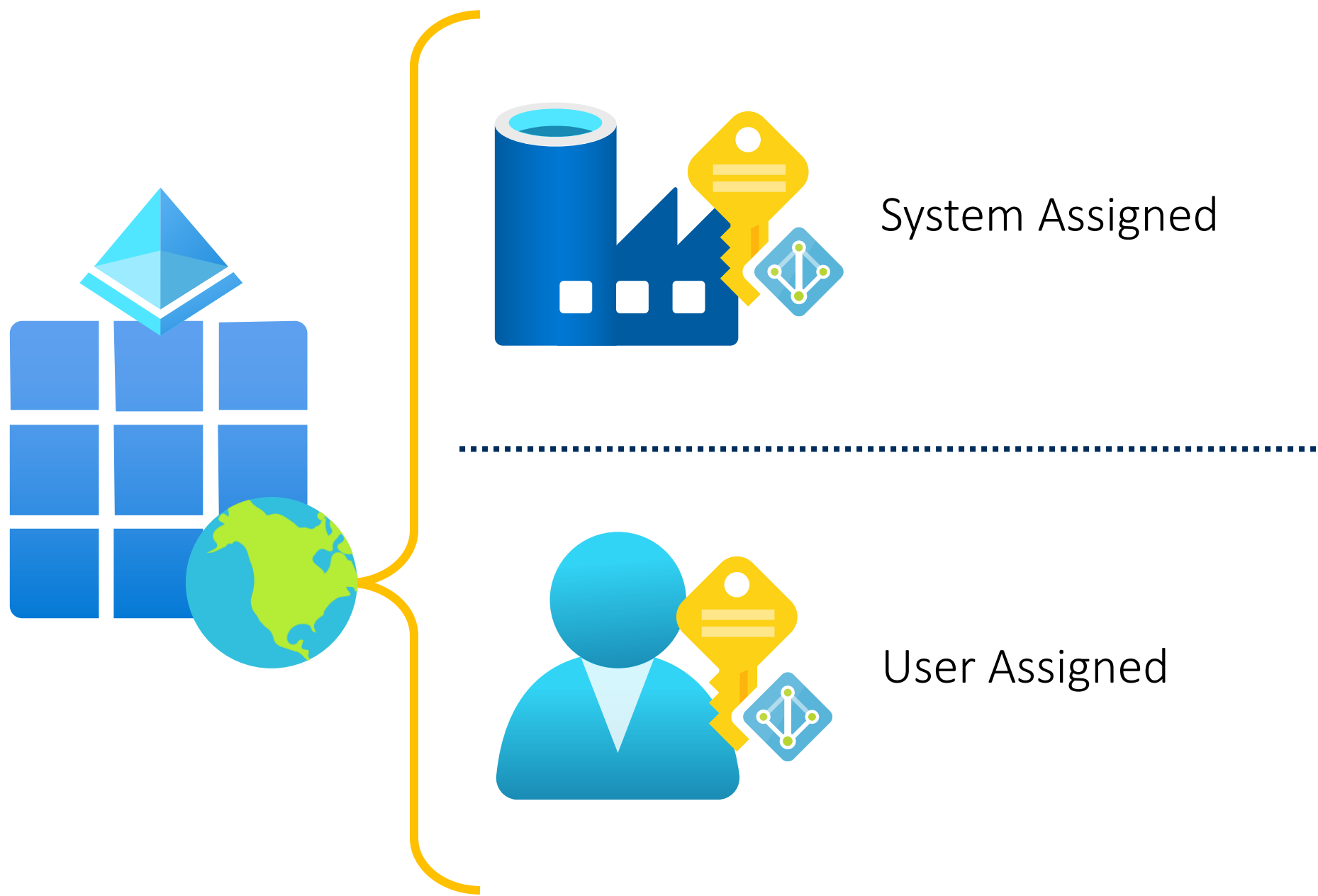
~~Service Account~~

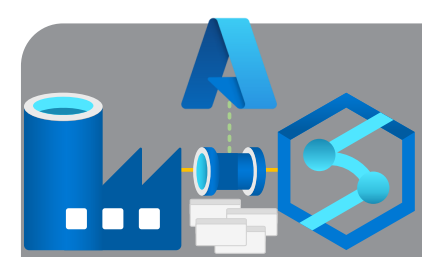
Managed Service Identity

MSI

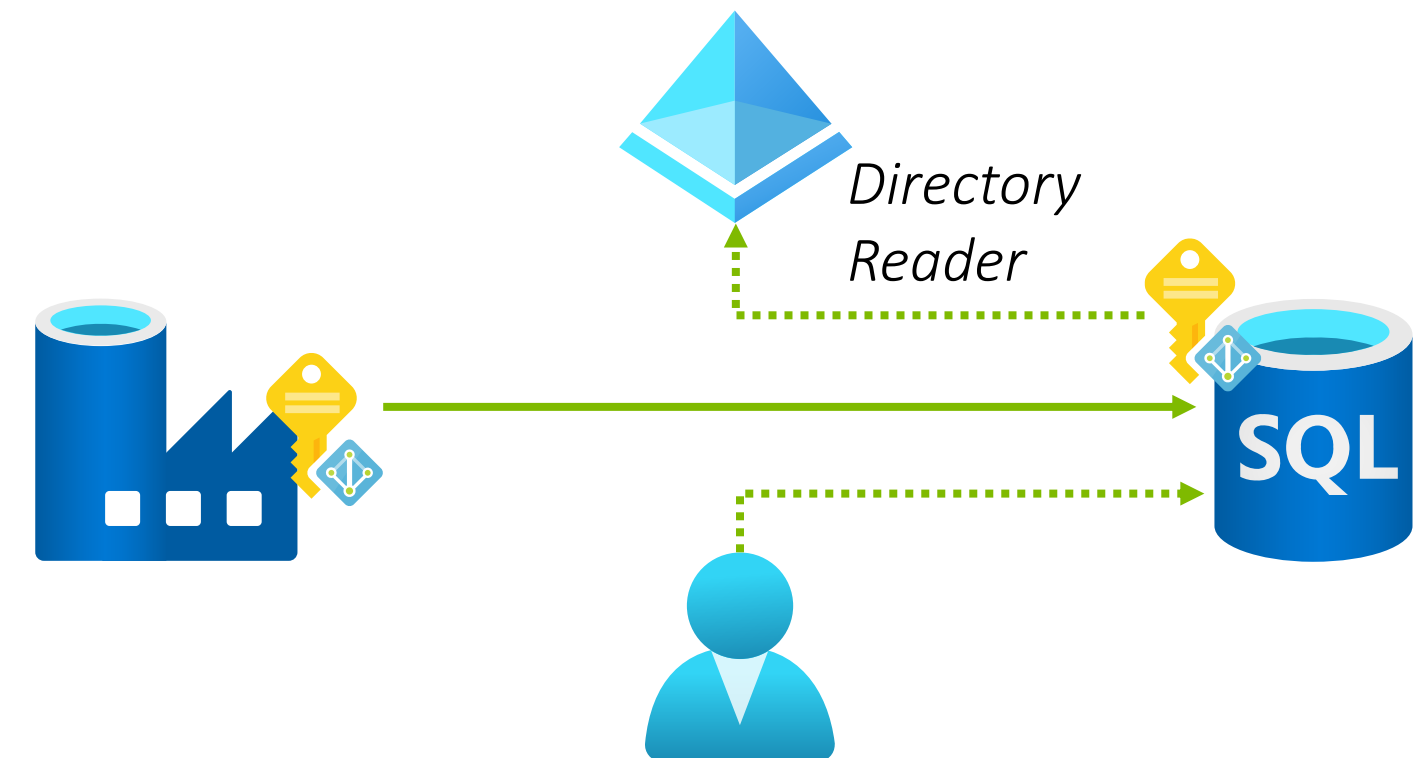
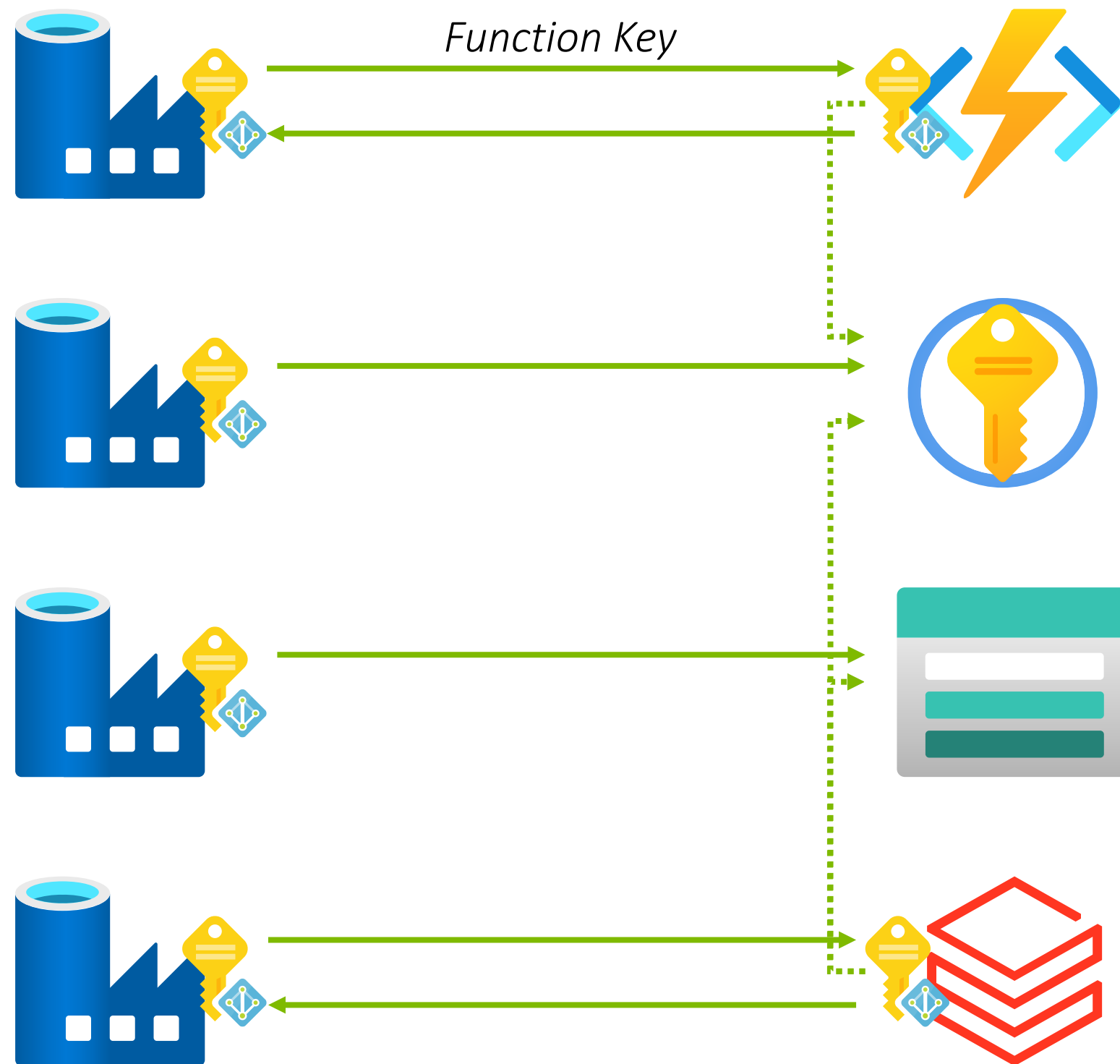
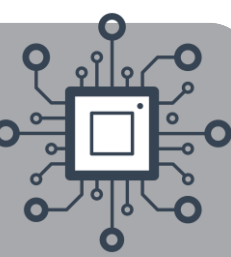
~~System User~~

Enterprise Application



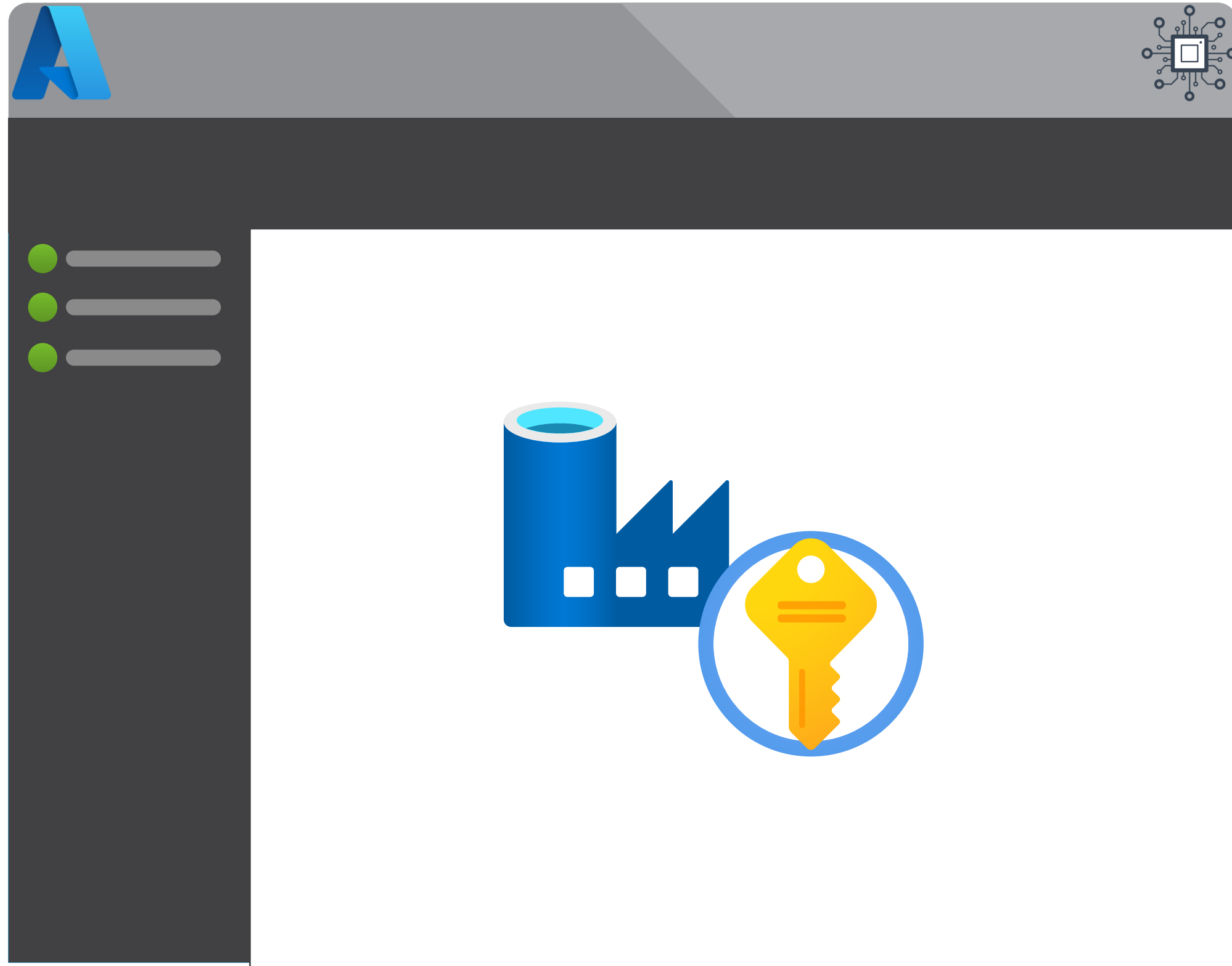


# Using Managed Identities



# Module 8

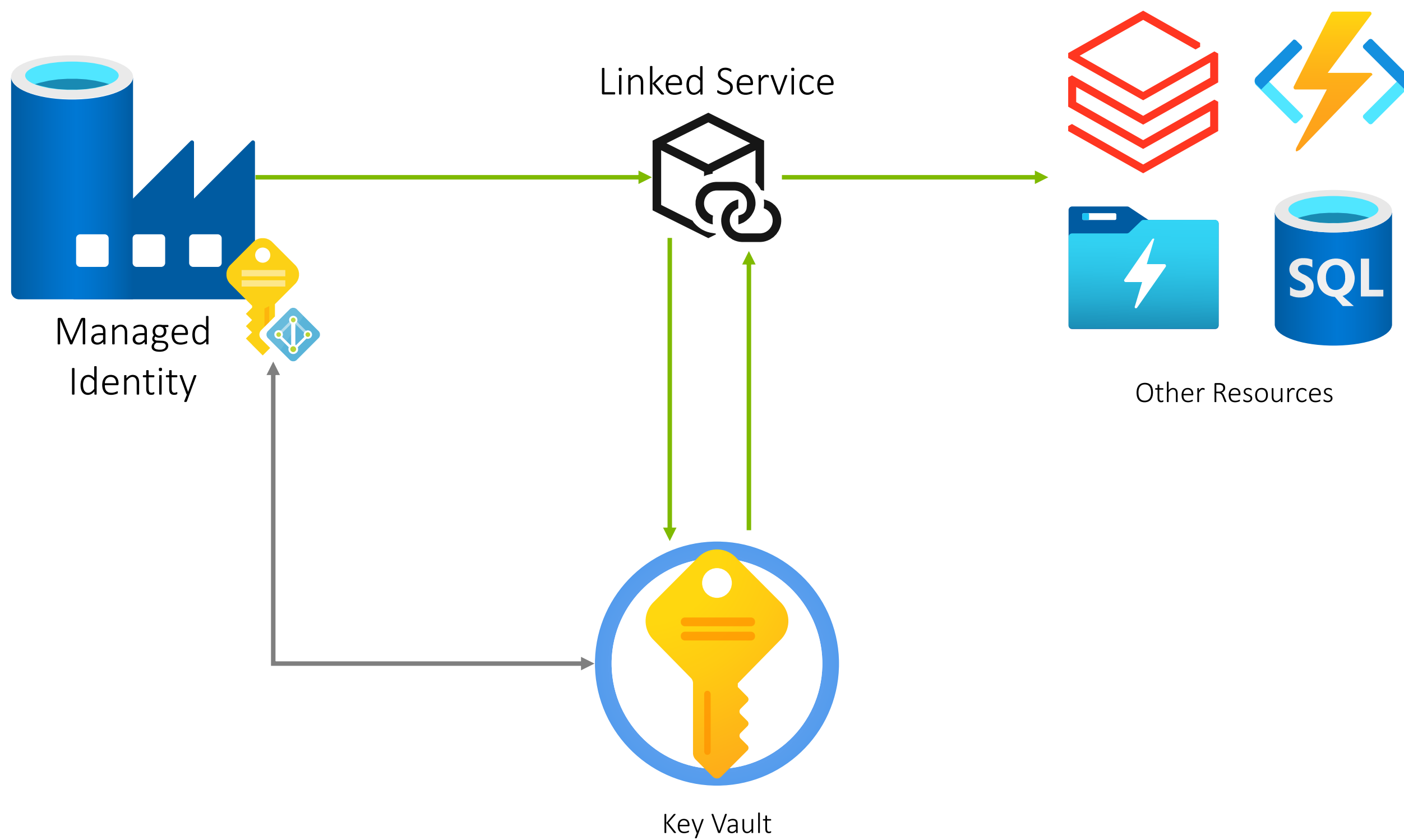
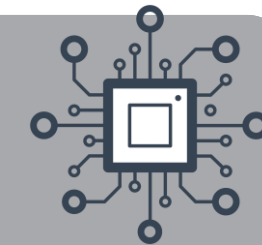
## Security



- Service Principals
- Managed Identities
- Azure Key Vault Integration
- Customer Managed Keys
- Pipeline Access & Permissions

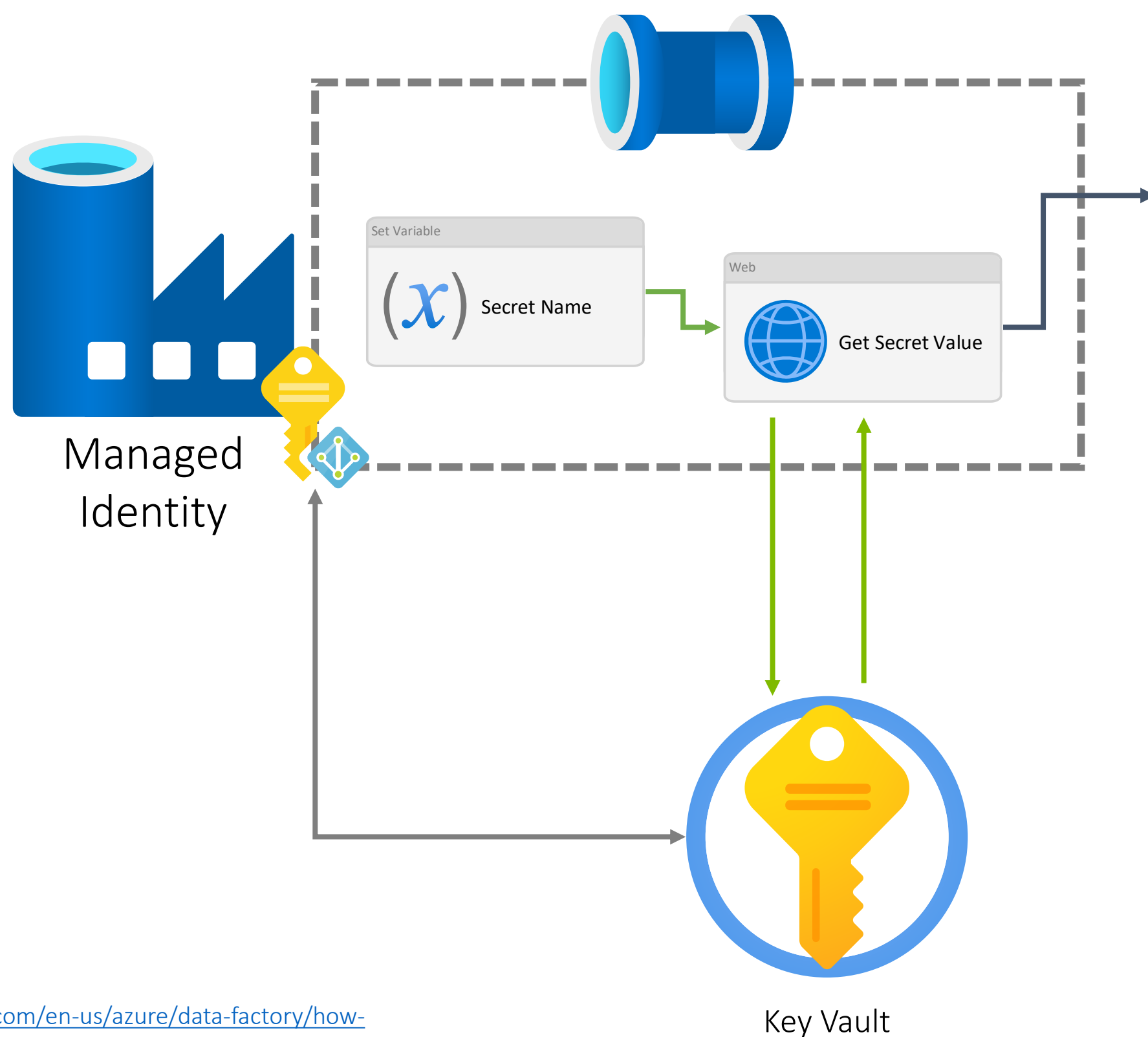
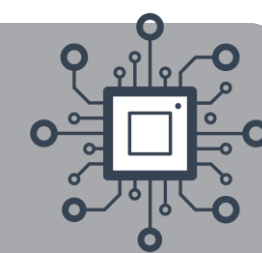


# Key Vault Integration – Option 1





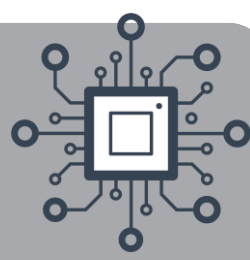
# Key Vault Integration – Option 2



## Output

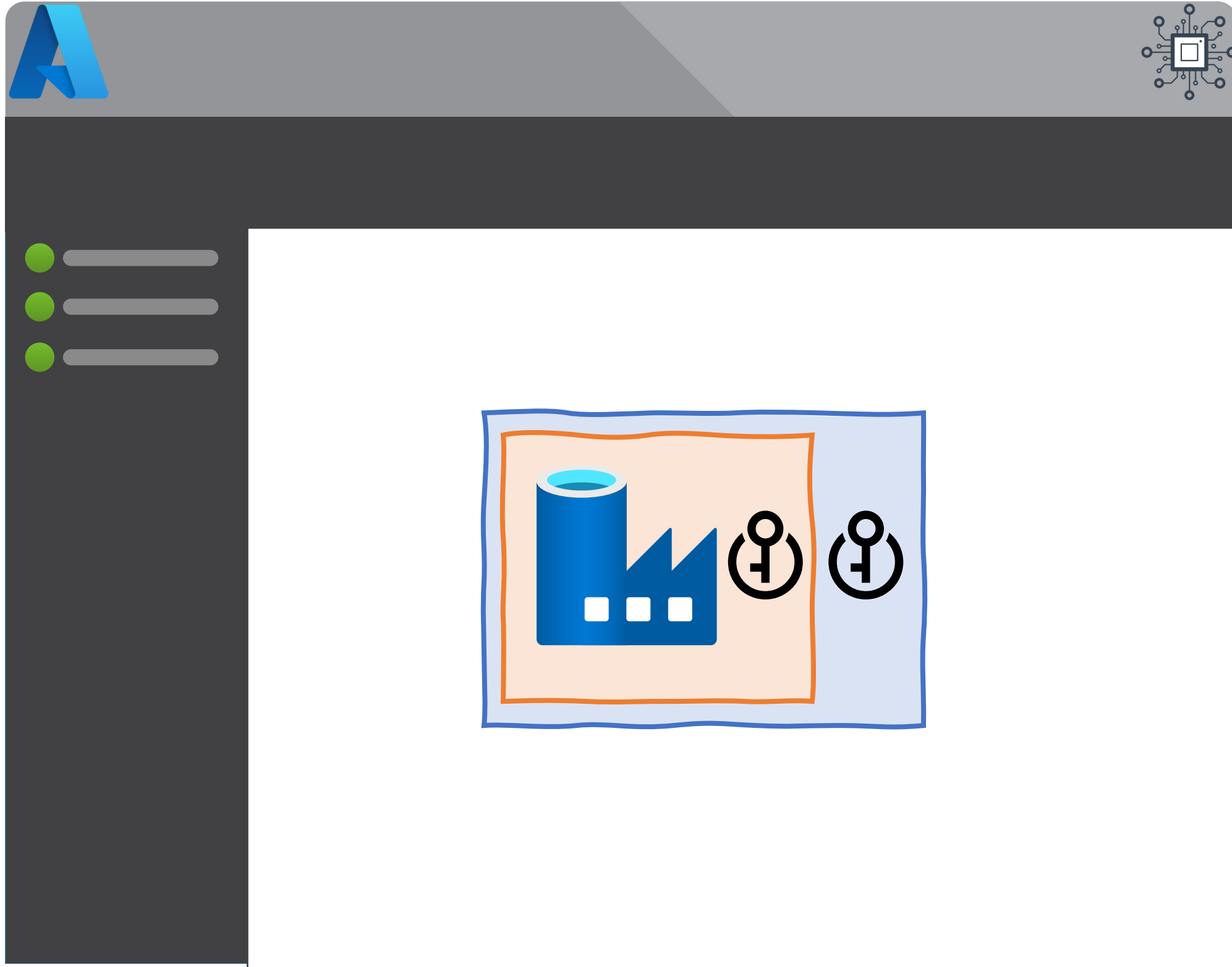
```
{
  "value": "HelloWorld!",
  "id": "https://trainingkeys01.vault.azure.net/secrets/DemoKeyGetWithWebActivity/0b8ccf8e52b241eaac58ba33c7a4d8c6",
  "attributes": {
    "enabled": true,
    "created": 1645623501,
    "updated": 1645623501,
    "recoveryLevel": "Recoverable+Purgeable"
  },
  "tags": {},
  "ADFWebActivityResponseHeaders": {
    "Pragma": "no-cache",
    "x-ms-keyvault-region": "uksouth",
    "x-ms-request-id": "a17107f2-89e3-45b4-81d1-637d92d575d0",
    "x-ms-keyvault-service-version": "1.9.291.1",
    "x-ms-keyvault-network-info": "conn_type=ipv4;addr=51.104.25.10;act_addr_fam=InterNetwork;",
    "Strict-Transport-Security": "max-age=31536000;includeSubDomains",
    "X-Content-Type-Options": "nosniff",
    "Cache-Control": "no-cache",
    "Date": "Wed, 23 Feb 2022 13:42:03 GMT",
    "X-Powered-By": "ASP.NET",
    "Content-Length": "258",
    "Content-Type": "application/json; charset=utf-8",
    "Expires": "-1"
  },
  "effectiveIntegrationRuntime": "AutoResolveIntegrationRuntime (UK South)",
  "executionDuration": 0,
  "durationInQueue": {
    "integrationRuntimeQueue": 1
  },
  "billingReference": {
    "activityType": "ExternalActivity",
    "billableDuration": [
      {
        "meterType": "AzureIR",
        "duration": 0.016666666666666666,
        "unit": "Hours"
      }
    ]
  }
}
```





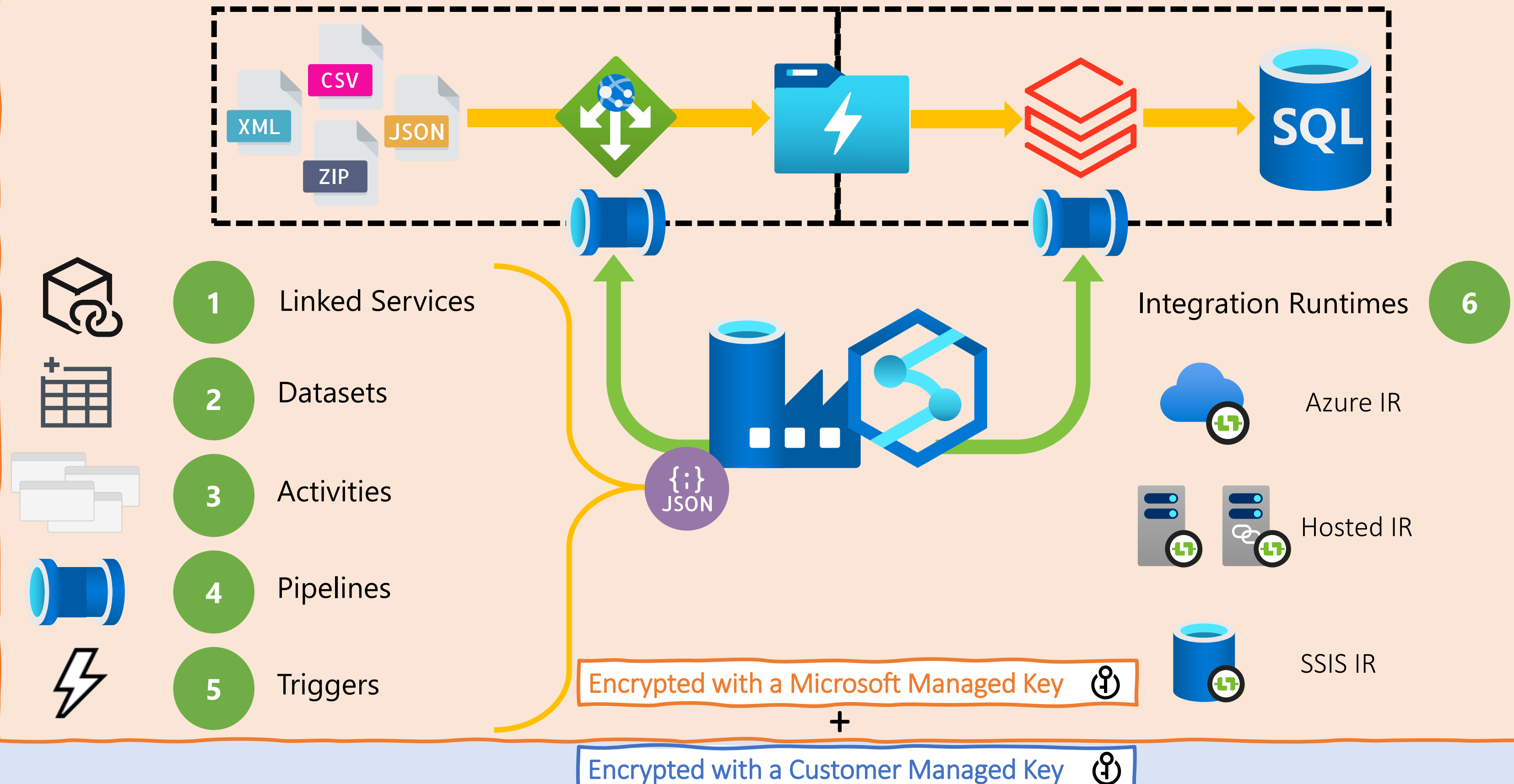
# Module 8

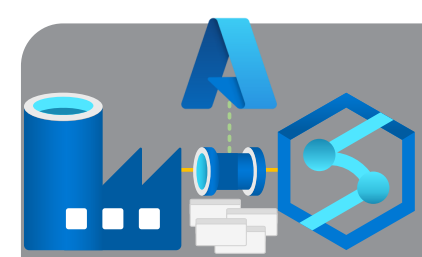
## Security



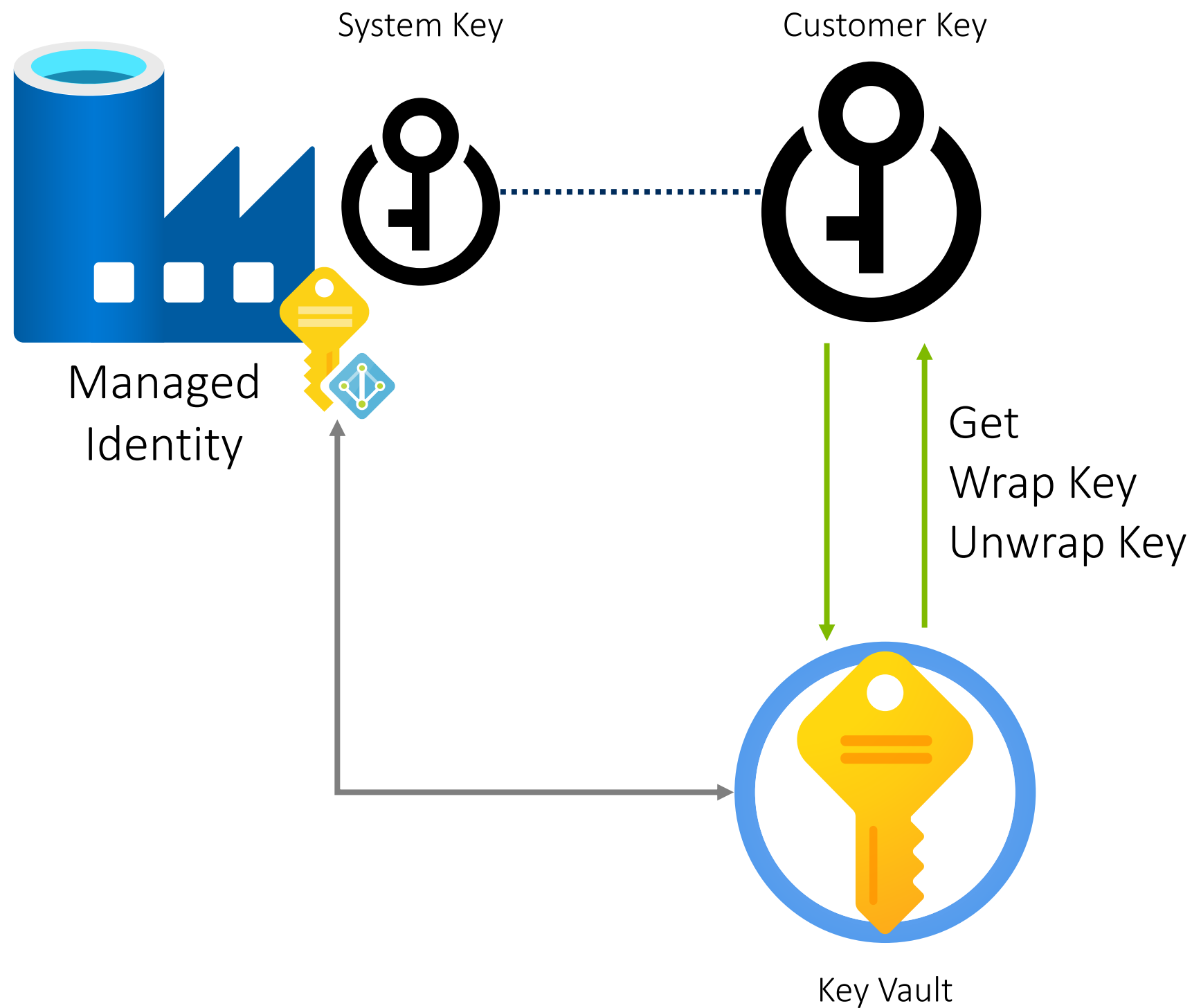
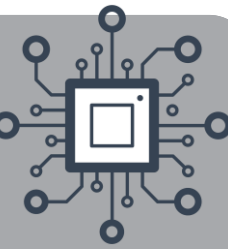
- Service Principals
- Managed Identities
- Azure Key Vault Integration
- **Customer Managed Keys**
- Pipeline Access & Permissions

# Customer Managed Keys





# Customer Managed Key

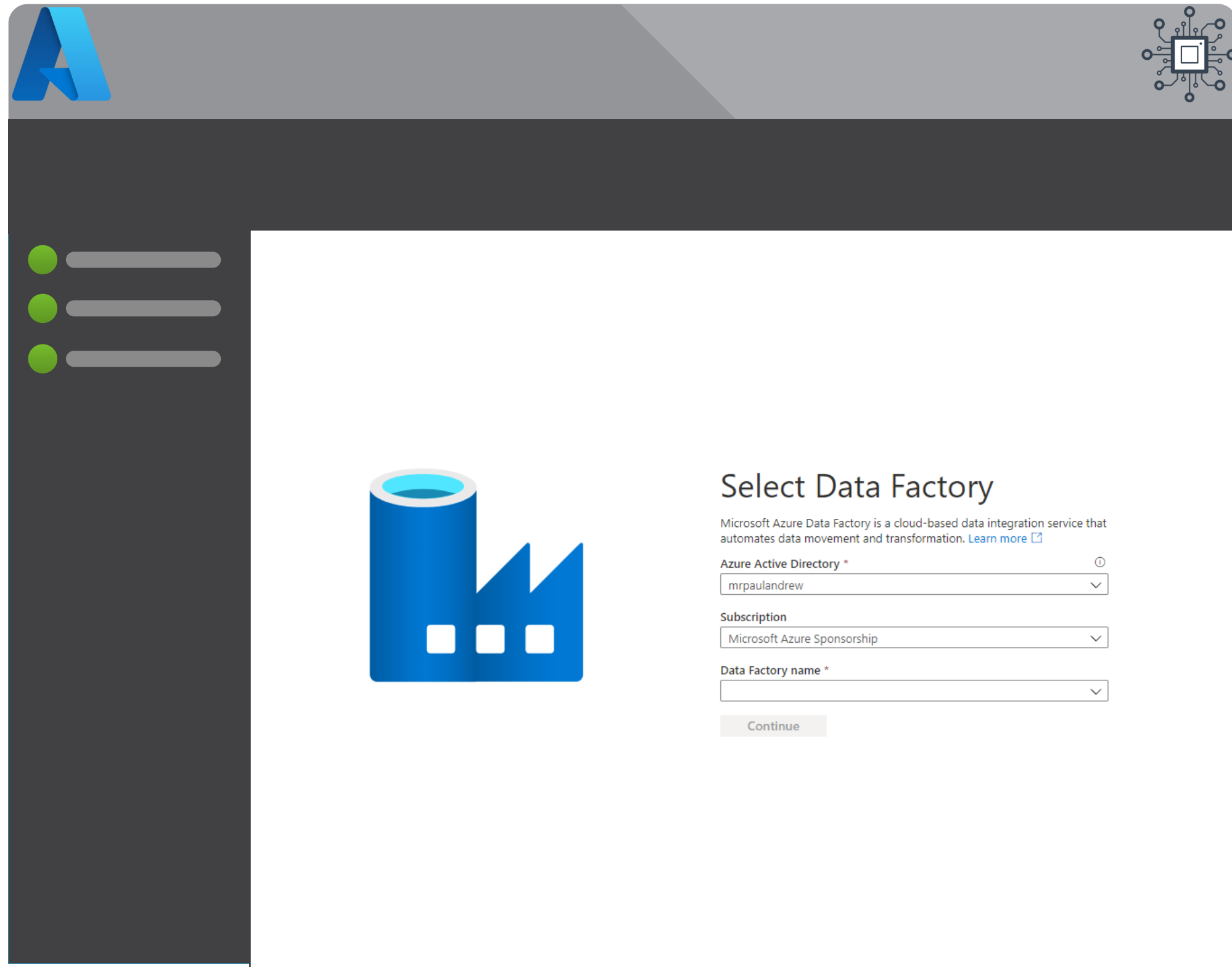


## Limitations and Issues

- Customer keys can only be stored in Key Vault.
- Can't be applied to existing Data Factory instances.
- Doesn't work with Managed Virtual Networks.
- Can't be included in ARM templates definitions.
- Must be manually version controlled.

# Module 8

## Security



The screenshot shows the Azure Data Factory 'Select Data Factory' configuration page. On the left is a dark sidebar with the Azure logo and three green circular icons. The main content area has a blue Data Factory icon (a stylized factory with a smokestack) on the left. To the right of the icon, the title 'Select Data Factory' is followed by a description: 'Microsoft Azure Data Factory is a cloud-based data integration service that automates data movement and transformation. [Learn more](#)'. Below this are three dropdown menus: 'Azure Active Directory \*' with the value 'mrpaulandrew', 'Subscription' with the value 'Microsoft Azure Sponsorship', and 'Data Factory name \*' which is currently empty. A 'Continue' button is at the bottom.

**Select Data Factory**

Microsoft Azure Data Factory is a cloud-based data integration service that automates data movement and transformation. [Learn more](#)

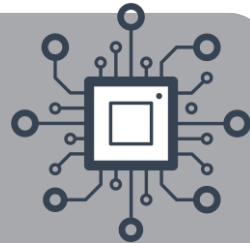
Azure Active Directory \*  
mrpaulandrew

Subscription  
Microsoft Azure Sponsorship

Data Factory name \*

Continue

- Service Principals
- Managed Identities
- Azure Key Vault Integration
- Customer Managed Keys
- Pipeline Access & Permissions



**Open Azure Data Factory Studio**  
Start authoring and monitoring your data pipelines and data flows.

[Open](#)



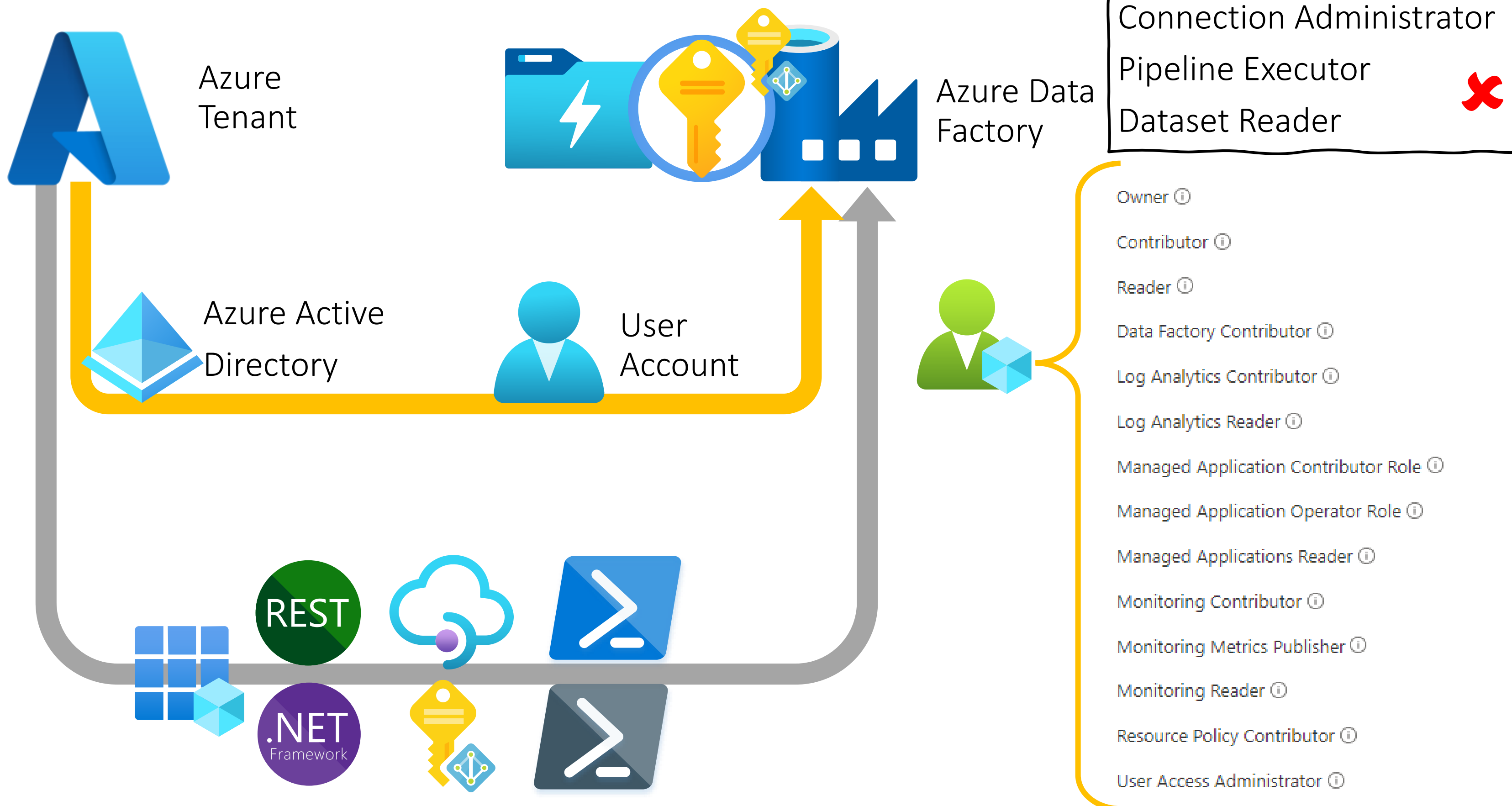
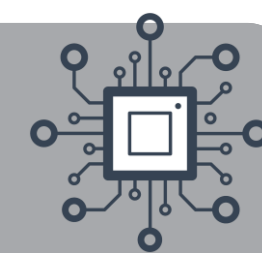
**Read documentation**  
Learn how to be productive quickly.  
Explore concepts, tutorials, and samples.

[Learn more](#)





# Accessing Everything via Data Factory





# Accessing Data Factory – Custom Roles



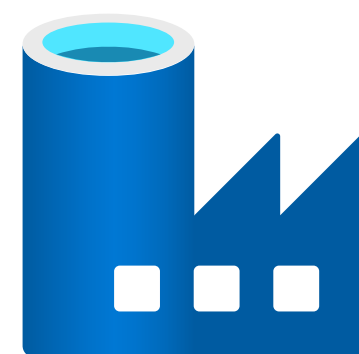
Azure  
Tenant



Azure Active  
Directory



User  
Account



Azure Data  
Factory



- Owner ⓘ
- Contributor ⓘ
- Reader ⓘ
- Data Factory Contributor ⓘ
- Log Analytics Contributor ⓘ
- Log Analytics Reader ⓘ
- Managed Application Contributor Role ⓘ
- Managed Application Operator Role ⓘ
- Managed Applications Reader ⓘ
- Monitoring Contributor ⓘ
- Monitoring Metrics Publisher ⓘ
- Monitoring Reader ⓘ
- Resource Policy Contributor ⓘ
- User Access Administrator ⓘ

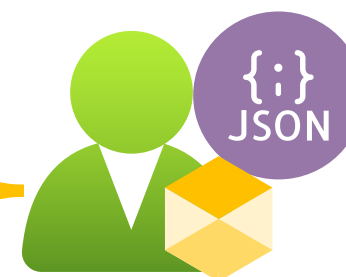
```
"Actions": [  
  "Microsoft.DataFactory/operations/read",  
  "Microsoft.DataFactory/factories/pipelines/read",  
  "Microsoft.DataFactory/factories/linkedServices/read",  
  "Microsoft.DataFactory/factories/datasets/read",  
  "Microsoft.DataFactory/factories/dataflows/read",  
  "Microsoft.DataFactory/datafactories/read"  
],
```



ADF Pipeline Executor

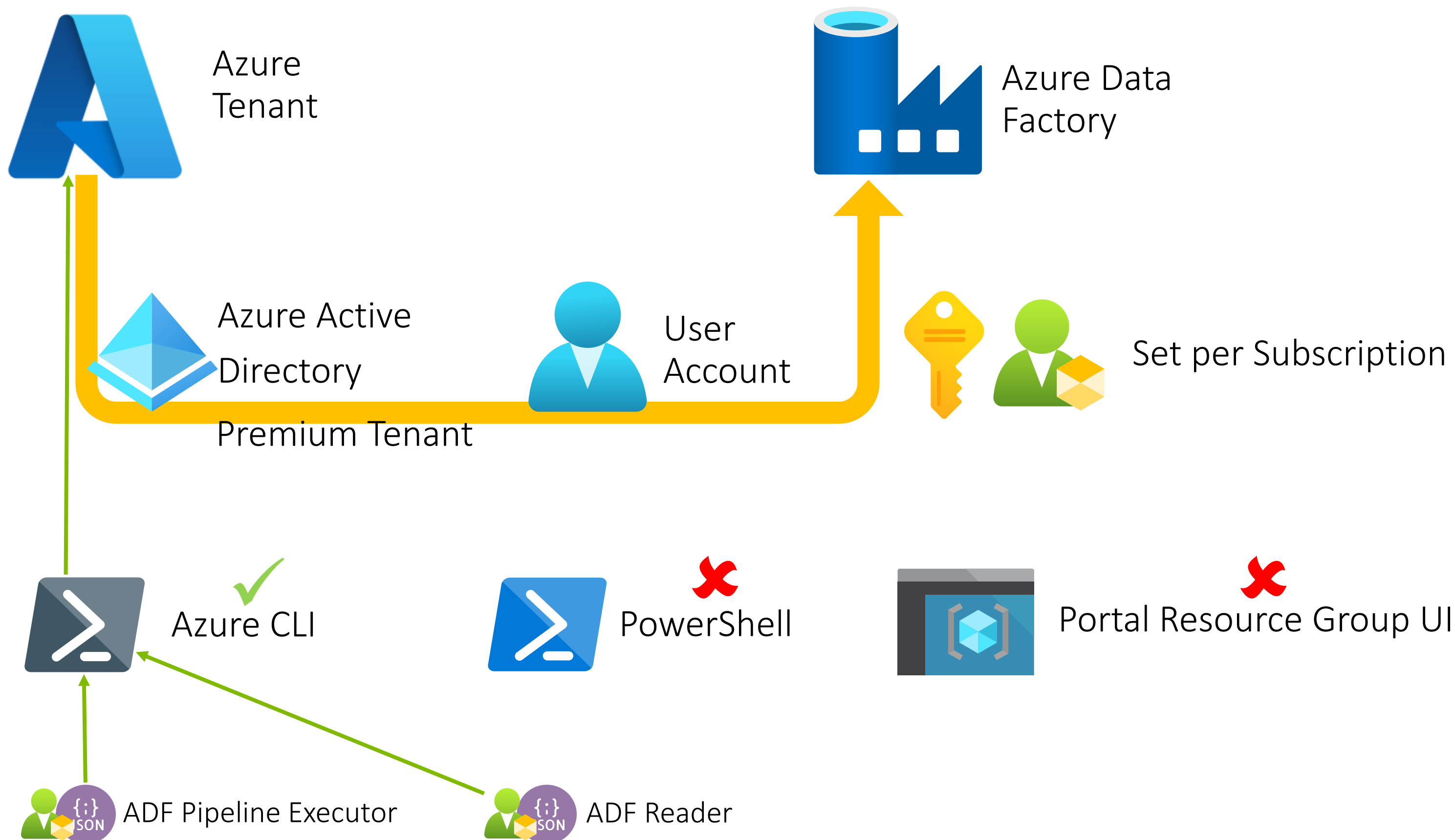


ADF Reader



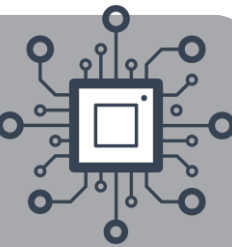


# Accessing Data Factory – Custom Roles





# Data Integration Pipeline – Security Layers



Auto (Default) Integration Runtimes



Dedicated Integration Runtimes



Private Endpoint Connections



Customer Managed Keys



System Managed Identities

User Managed Identities



Service Principals



Integrated Credentials *(Preview)*



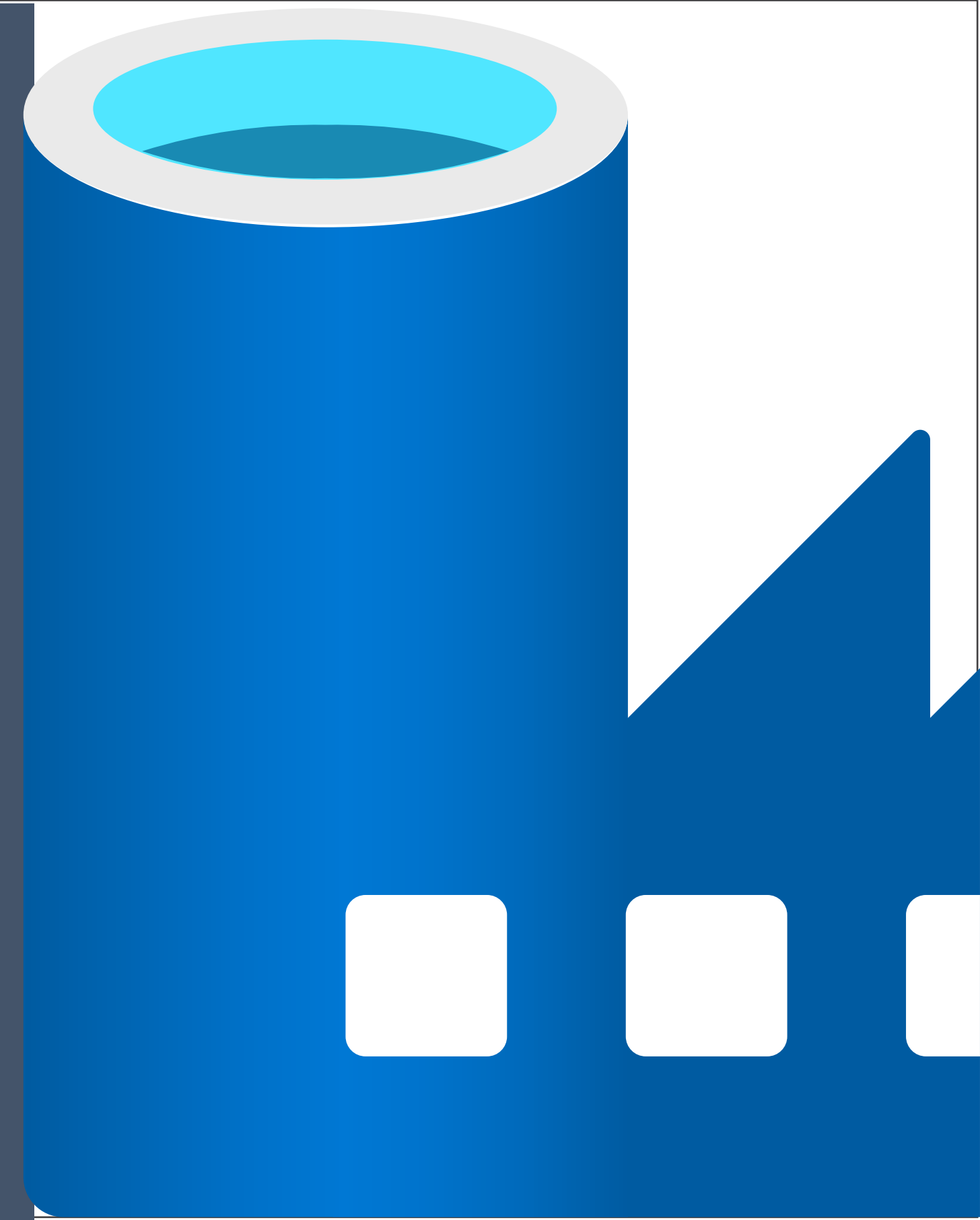
Key Store Integration



Custom User Access Roles



Default User Access Roles





# Data Integration Pipeline – Security Layers



Auto (Default) Integration Runtimes



System Managed Identities



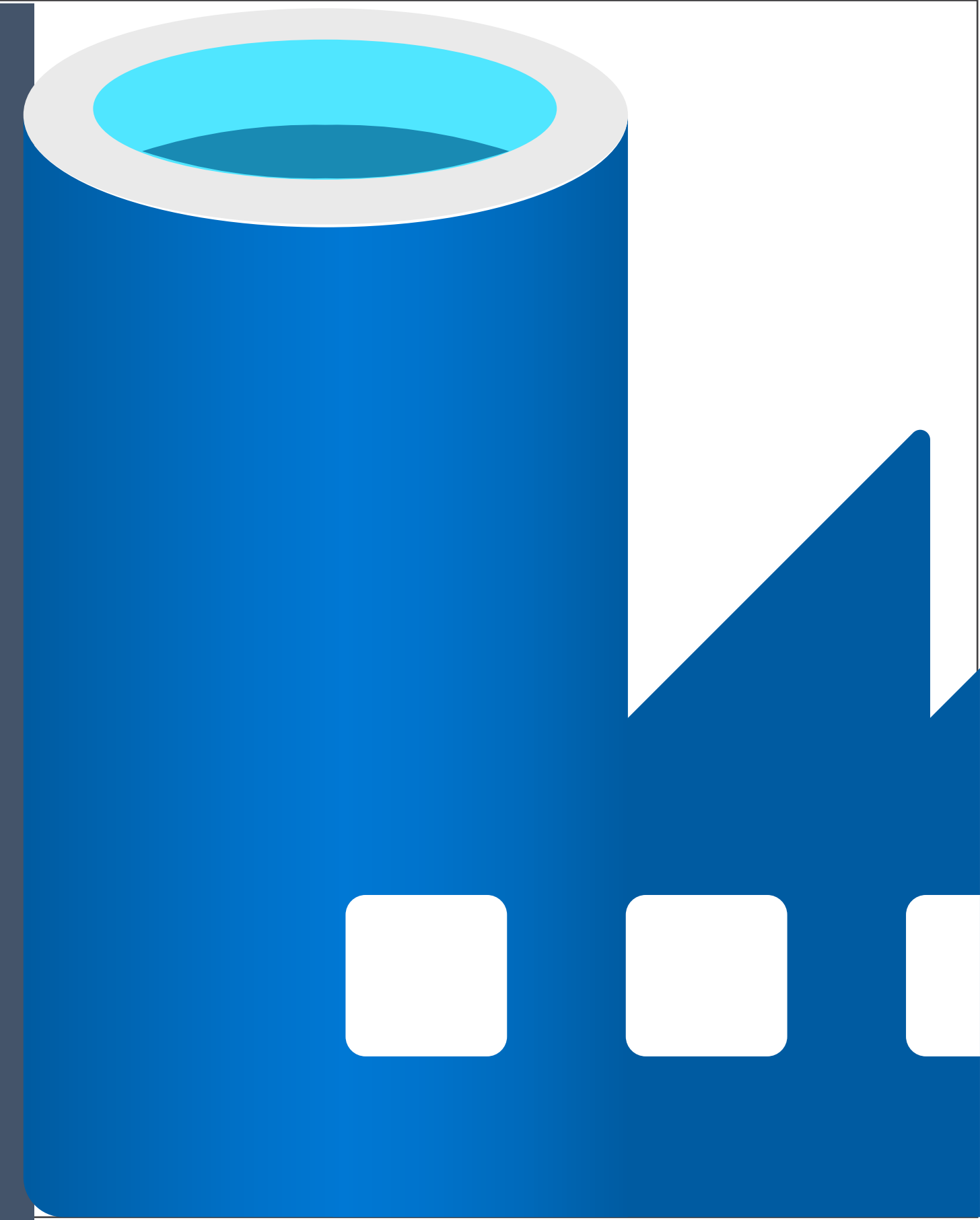
Service Principals



Key Store Integration



Default User Access Roles



# Module 8

## Security



```
SELECT
    [Contents]
FROM
    [Training]
WHERE
    [Module] = '8';
```

```
END; --module, fetch next
```

- Managed Identities
- Service Principals
- Azure Key Vault Integration
- Customer Managed Keys
- Pipeline Access & Permissions