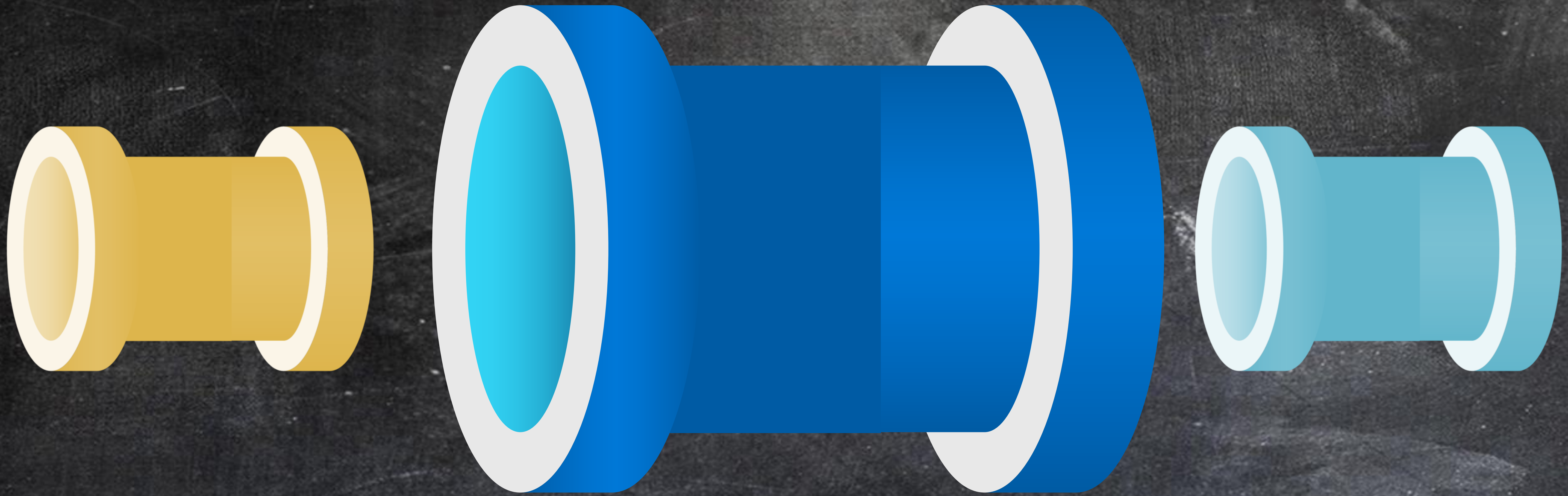
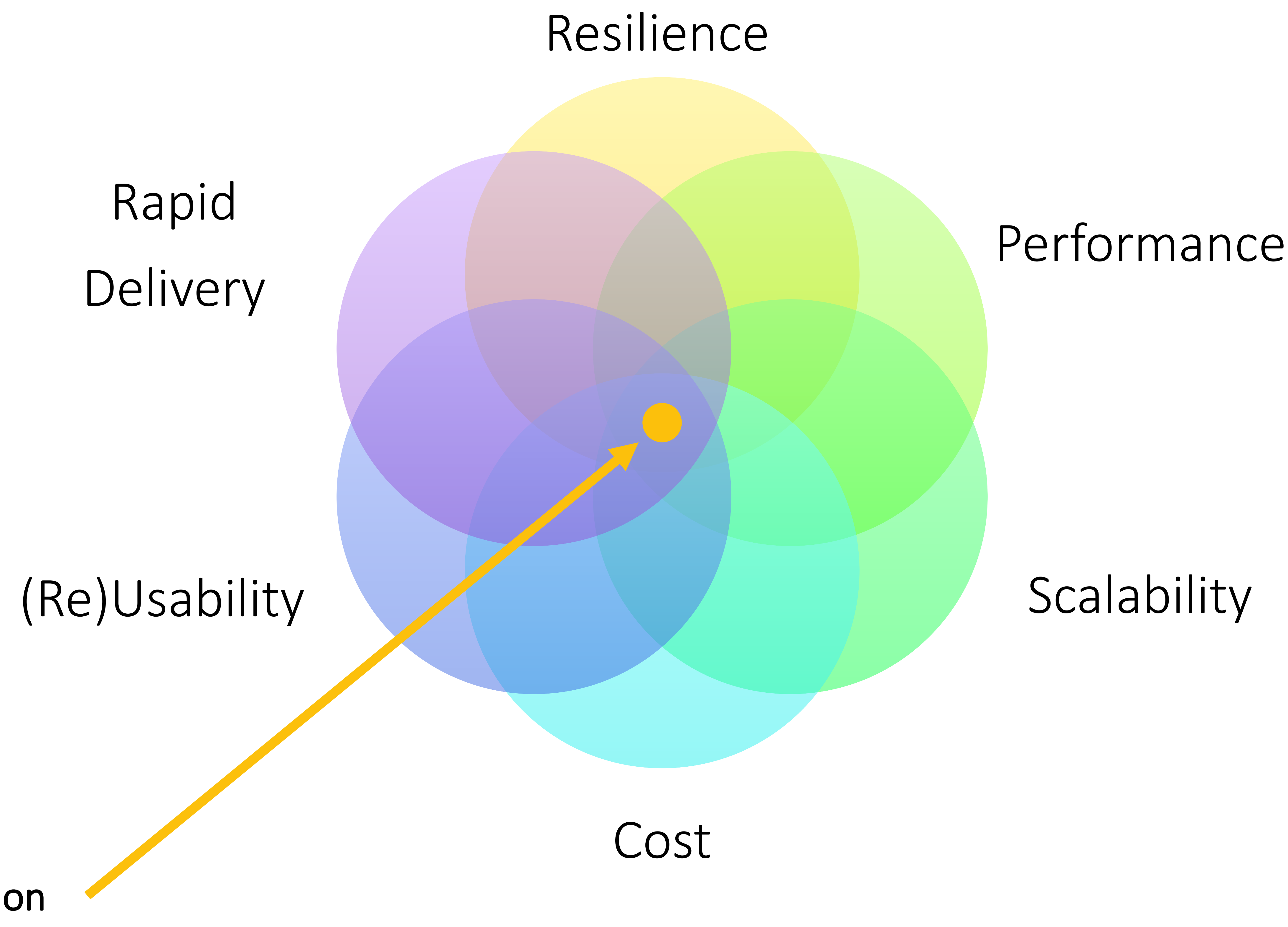
Cloud Formations

Proudly presents…

Integration Pipelines

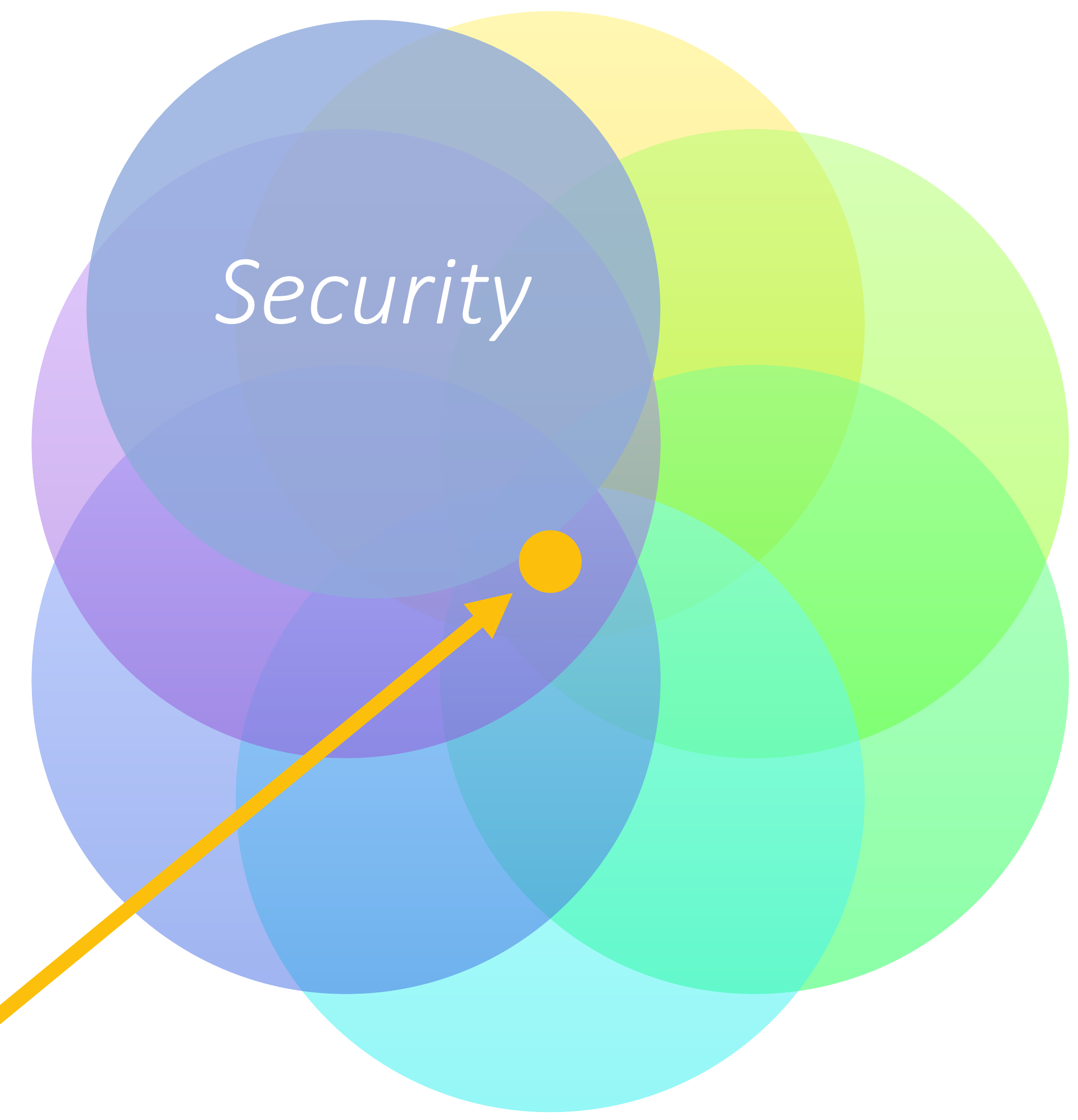


Design Priorities



The Perfect Solution

Design Priorities



Resilience

Rapid

Delivery

Performance

(Re)Usability

Scalability

Cost

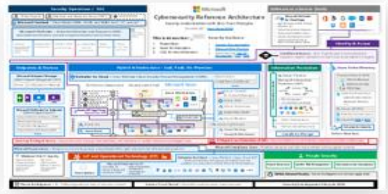
The Perfect Solution

Microsoft Cybersecurity Reference Architectures

MCRA

Capabilities

What cybersecurity capabilities does Microsoft have?



Build Slide

Azure Native Controls

What native security is available?

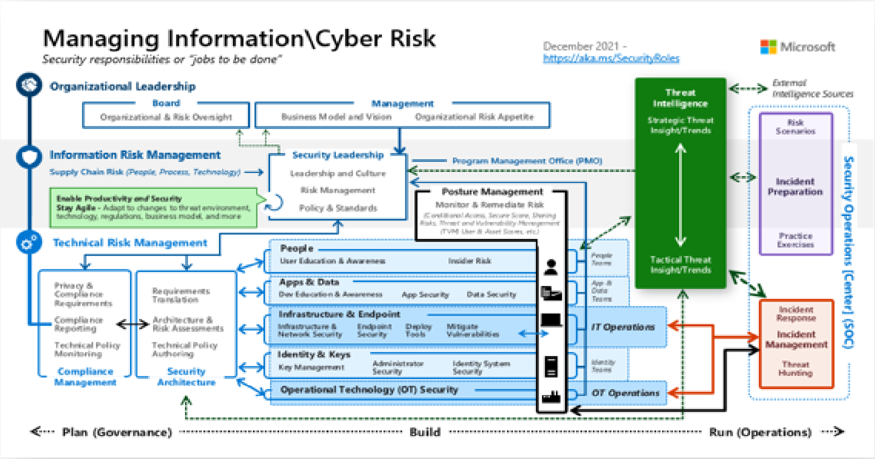
Attack Chain Coverage

How does this map to insider and external attacks?

Build Slide

People

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


Managing Information\Cyber Risk
Security responsibilities or "jobs to be done"
December 2021 - https://aka.ms/SecurityRoles
Microsoft
Organizational Leadership
Board
Organizational & Risk Oversight
Management
Business Model and Vision
Organizational Risk Appetite
Information Risk Management
Supply Chain Risk (People, Process, Technology)
Enable Productivity and Security
Stay Agile - Adapt to changes to threat environment, technology, regulations, business model, and more
Security Leadership
Leadership and Culture
Risk Management
Policy & Standards
Program Management Office (PMO)
Posture Management
Monitor & Remediate Risk
(Conditional Access, Secure Score, Sharing Risks, Threat and Vulnerability Management (TVM) User & Asset Scores, etc.)
Technical Risk Management
Privacy & Compliance Requirements
Compliance Reporting
Technical Policy Monitoring
Compliance Management
Requirements Translation
Architecture & Risk Assessments
Technical Policy Authoring
Security Architecture
People
User Education & Awareness
Insider Risk
People Teams
Apps & Data
Dev Education & Awareness
App Security
Data Security
App & Data Teams
Infrastructure & Endpoint
Infrastructure & Network Security
Endpoint Security
Deploy Tools
Mitigate Vulnerabilities
IT Operations
Identity & Keys
Key Management
Administrator Security
Identity System Security
Identity Teams
Operational Technology (OT) Security
OT Operations
Threat Intelligence
Strategic Threat Insight/Trends
Tactical Threat Insight/Trends
External Intelligence Sources
Risk Scenarios
Incident Preparation
Practice Exercises
Incident Response
Incident Management
Threat Hunting
Security Operations [Center] (SOC)
Plan (Governance)
Build
Run (Operations)

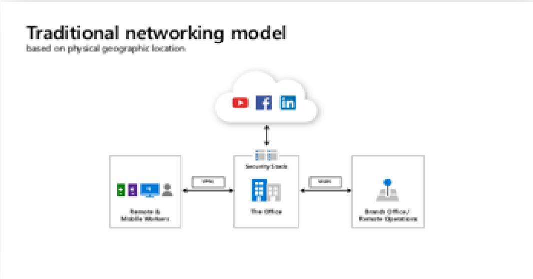
Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?

Cross-cloud and cross-platform
Comprehensive Security, Compliance and Identity capabilities that integrate with your existing solutions
Microsoft Security, Compliance, and Identity Capabilities

Secure Access Service Edge (SASE)

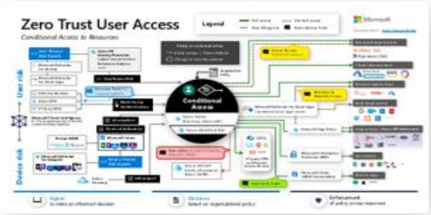
What is it? How does it compare to Zero Trust?


Traditional networking model
based on physical geographic location
The Office
Remote & Mobile Workers
Branch Office/ Remote Operations

aka.ms/MCRA | December 2021 | Microsoft

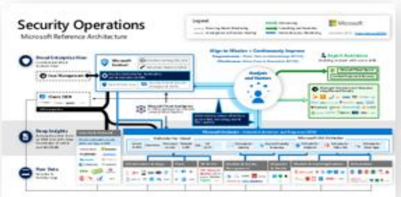
Zero Trust User Access

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



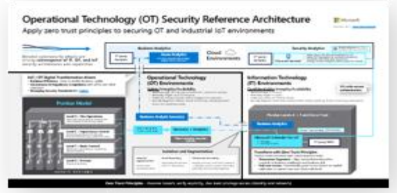
Security Operations

How to enable rapid incident response?



Operational Technology

How to enable Zero Trust Security for OT?

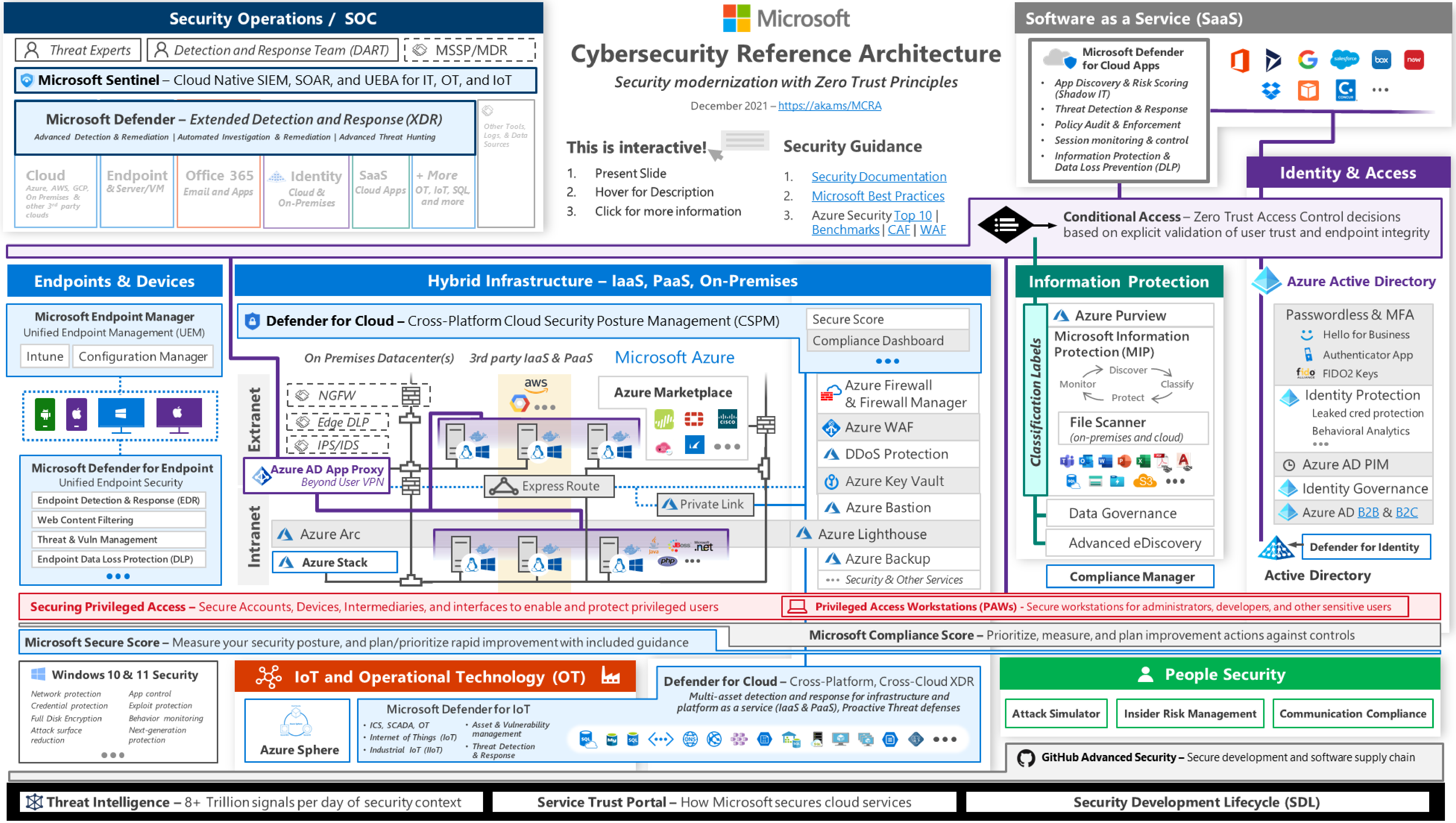


Cloud Formations - Knowledge Transfer & Training

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

Microsoft Cybersecurity Reference Architecture

Capabilities



Security Operations / SOC
Threat Experts
Detection and Response Team (DART)
MSSP/MDR
Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT
Microsoft Defender – Extended Detection and Response (XDR)
Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting
Other Tools, Logs, & Data Sources
Cloud
Azure, AWS, GCP, On Premises & other 3rd party clouds
Endpoint & Server/VM
Office 365 Email and Apps
Identity Cloud & On-Premises
SaaS Cloud Apps
+ More OT, IoT, SQL, and more
Microsoft
Cybersecurity Reference Architecture
Security modernization with Zero Trust Principles
December 2021 – https://aka.ms/MCRA
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Security Guidance
1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF
Software as a Service (SaaS)
Microsoft Defender for Cloud Apps
• App Discovery & Risk Scoring (Shadow IT)
• Threat Detection & Response
• Policy Audit & Enforcement
• Session monitoring & control
• Information Protection & Data Loss Prevention (DLP)
Identity & Access
Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity
Endpoints & Devices
Microsoft Endpoint Manager
Unified Endpoint Management (UEM)
Intune
Configuration Manager
Microsoft Defender for Endpoint
Unified Endpoint Security
Endpoint Detection & Response (EDR)
Web Content Filtering
Threat & Vuln Management
Endpoint Data Loss Protection (DLP)
Hybrid Infrastructure – IaaS, PaaS, On-Premises
Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)
Secure Score
Compliance Dashboard
On Premises Datacenter(s)
3rd party IaaS & PaaS
Microsoft Azure
aws
Extranet
NGFW
Edge DLP
IPS/IDS
Azure AD App Proxy
Beyond User VPN
Azure Marketplace
Express Route
Private Link
Intranet
Azure Arc
Azure Stack
Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services
Information Protection
Classification Labels
Azure Purview
Microsoft Information Protection (MIP)
Discover
Classify
Protect
Monitor
File Scanner
(on-premises and cloud)
Data Governance
Advanced eDiscovery
Compliance Manager
Azure Active Directory
Passwordless & MFA
Hello for Business
Authenticator App
FIDO2 Keys
Identity Protection
Leaked cred protection
Behavioral Analytics
Azure AD PIM
Identity Governance
Azure AD B2B & B2C
Defender for Identity
Active Directory
Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users
Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users
Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance
Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls
Windows 10 & 11 Security
Network protection
Credential protection
Full Disk Encryption
Attack surface reduction
App control
Exploit protection
Behavior monitoring
Next-generation protection
IoT and Operational Technology (OT)
Azure Sphere
Microsoft Defender for IoT
• ICS, SCADA, OT
• Internet of Things (IoT)
• Industrial IoT (IIoT)
• Asset & Vulnerability management
• Threat Detection & Response
Defender for Cloud – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses
People Security
Attack Simulator
Insider Risk Management
Communication Compliance
GitHub Advanced Security – Secure development and software supply chain
Threat Intelligence – 8+ Trillion signals per day of security context
Service Trust Portal – How Microsoft secures cloud services
Security Development Lifecycle (SDL)

Cloud Formations - Knowledge Transfer & Training

Module 8 – Security

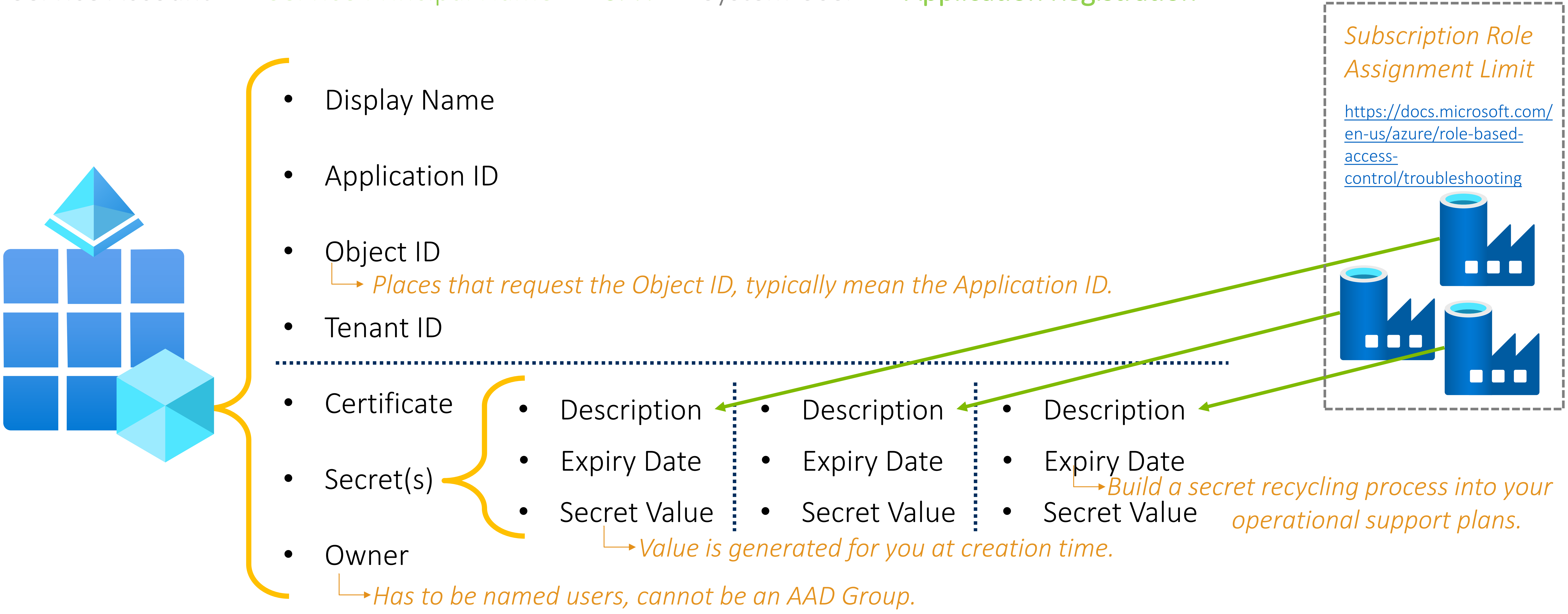
Service Principals

Cloud Formations

Service Principals

Terminology Clarification & Properties

~~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)
  - Description
  - Expiry Date
  - Secret Value
    - Value is generated for you at creation time.
  - Description
  - Expiry Date
  - Secret Value
  - Description
  - Expiry Date
    - Build a secret recycling process into your operational support plans.
  - Secret Value
- Owner
  - Has to be named users, cannot be an AAD Group.

Subscription Role Assignment Limit

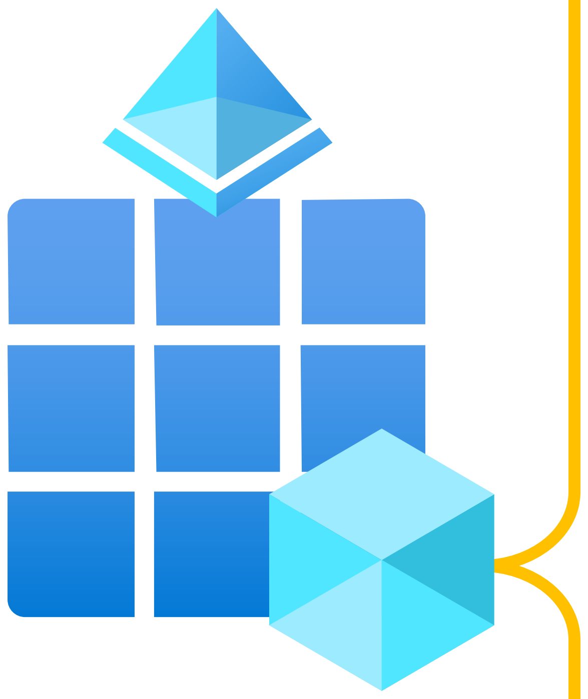
https://docs.microsoft.com/en-us/azure/role-based-access-control/troubleshooting

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

Service Principals

Terminology Clarification & Properties

~~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

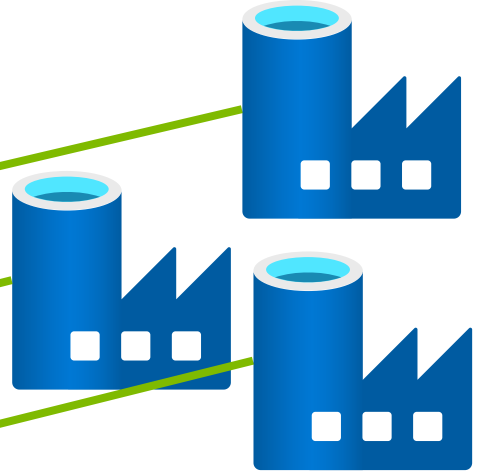
- Certificate
- Secret(s)
  - Description
  - Expiry Date
  - Secret Value
    - Value is generated for you at creation time.

  - Description
  - Expiry Date
  - Secret Value

  - Description
  - Expiry Date
    - Build a secret recycling process into your operational support plans.
  - Secret Value
- Owner
  - Has to be named users, cannot be an AAD Group.

Subscription Role Assignment Limit

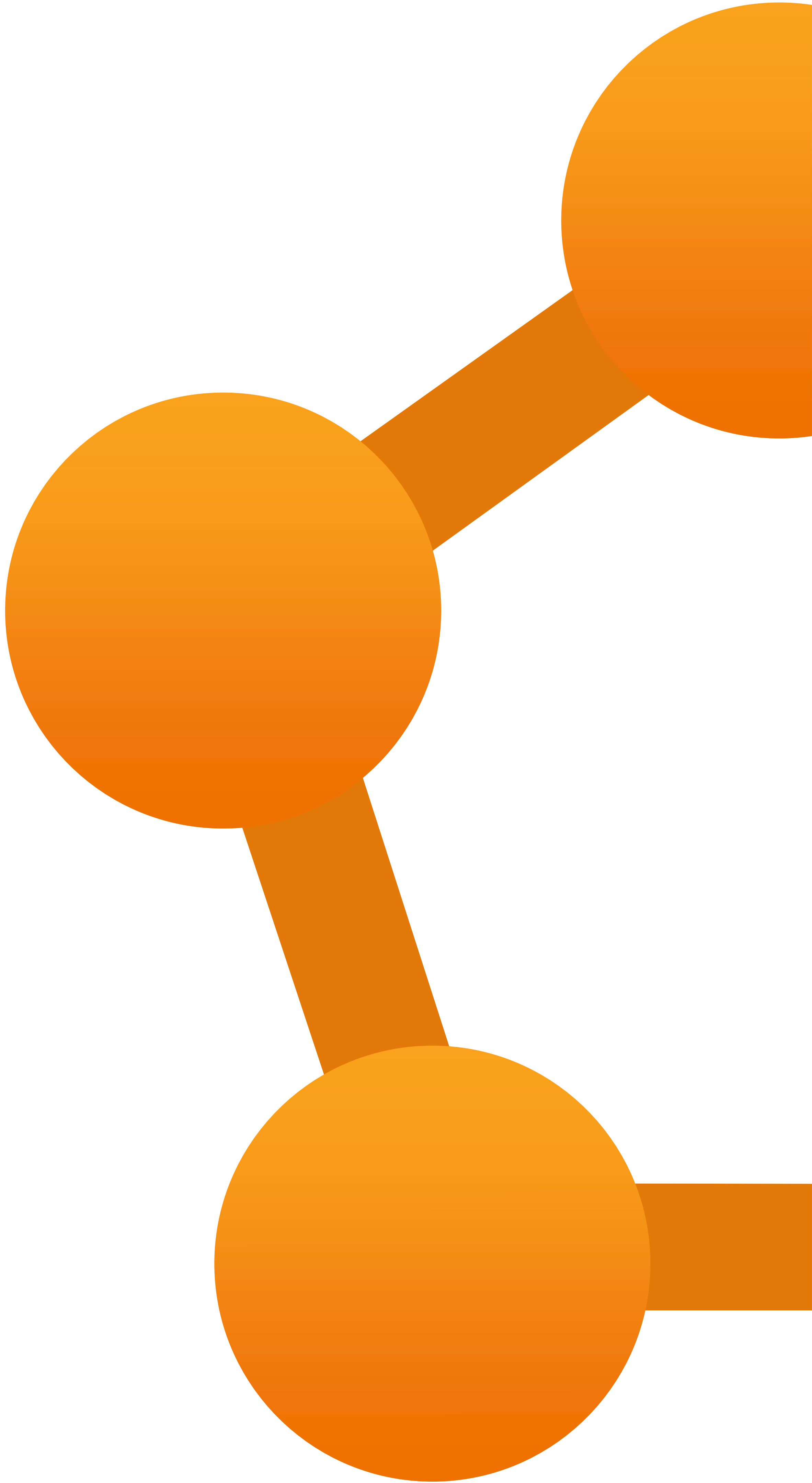
https://docs.microsoft.com/en-us/azure/role-based-access-control/troubleshooting



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

Module 8 – Security

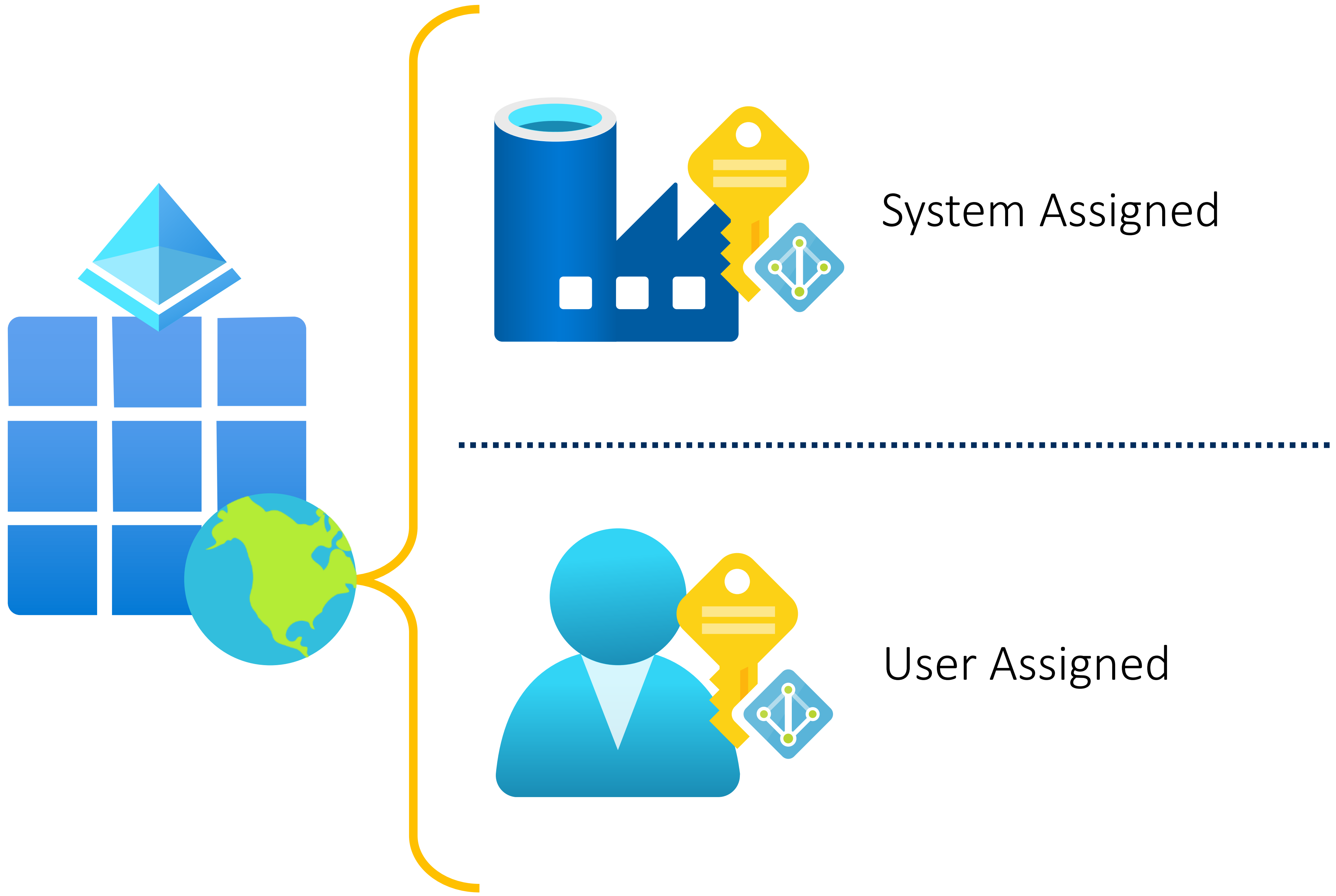
Managed Identities



Cloud Formations

Managed Identities

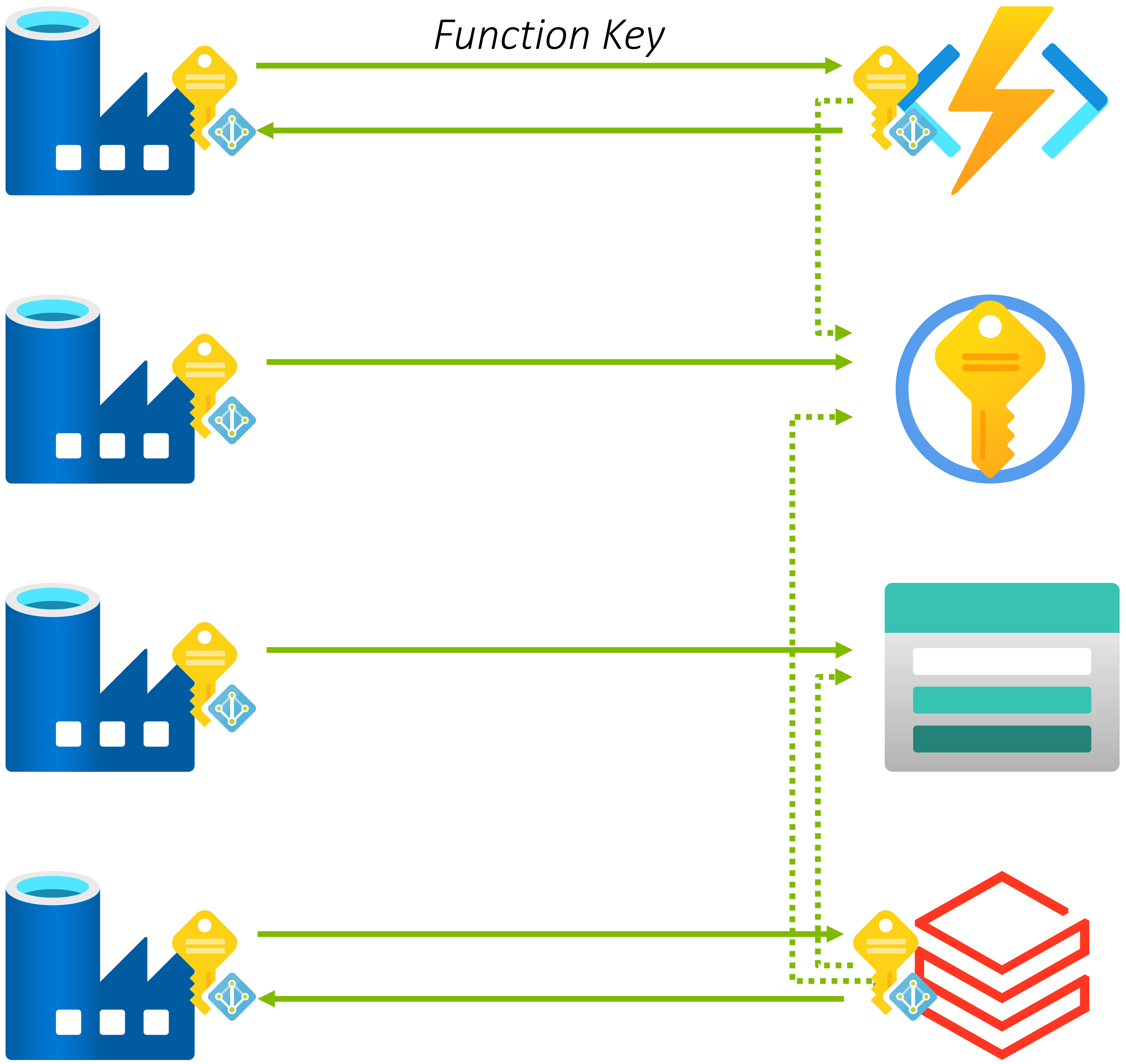
~~Service Account~~ Managed ~~Service~~ Identity M~~S~~I ~~System User~~ **Enterprise Application**

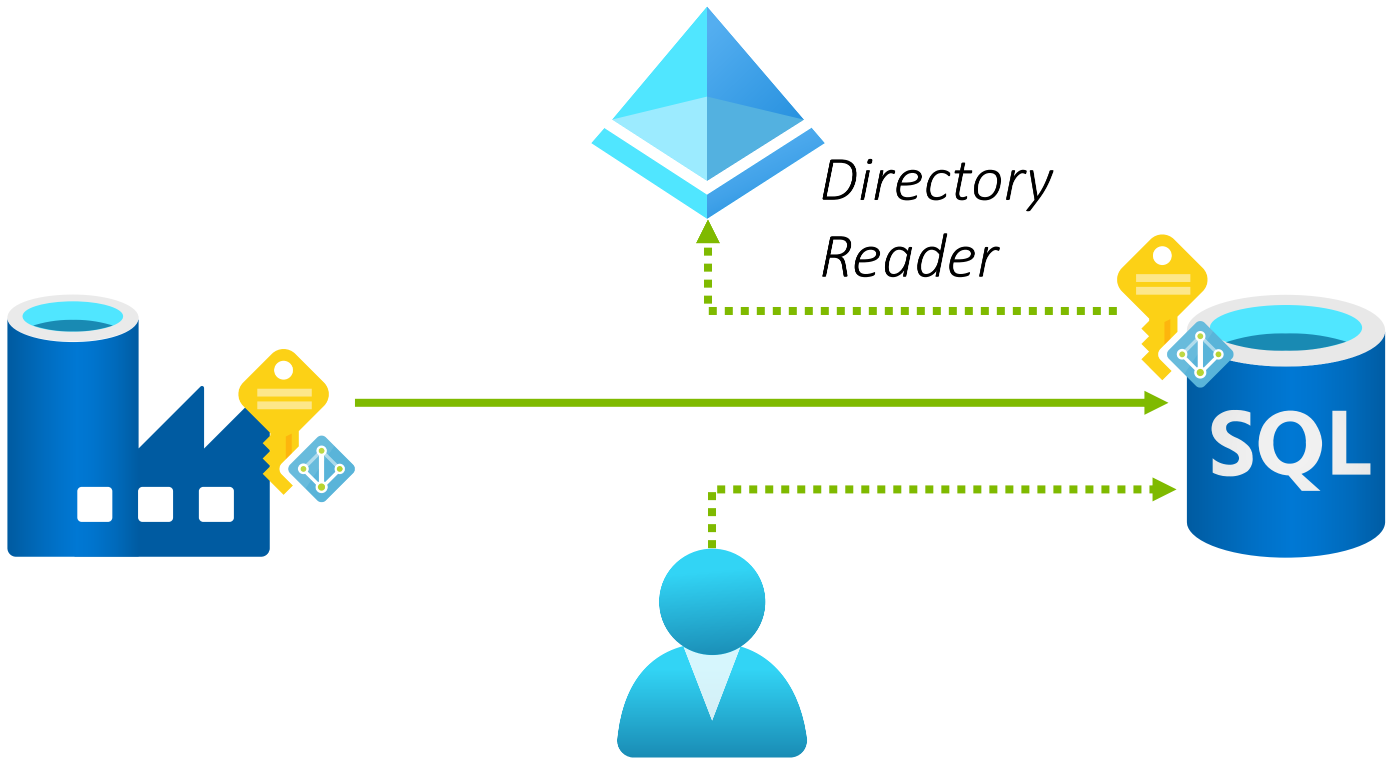


System Assigned

User Assigned

Using Managed Identities

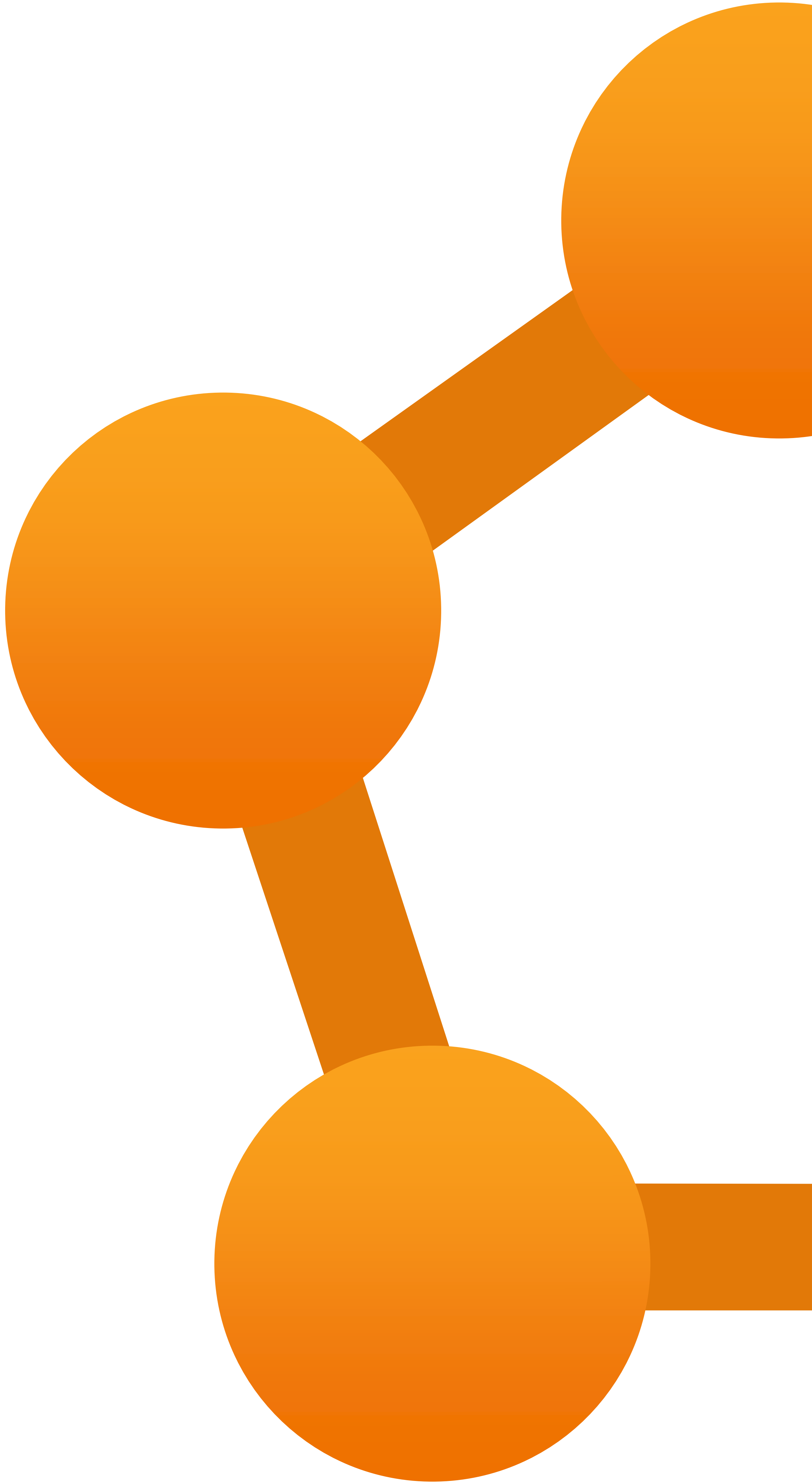




https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-directory-readers-role

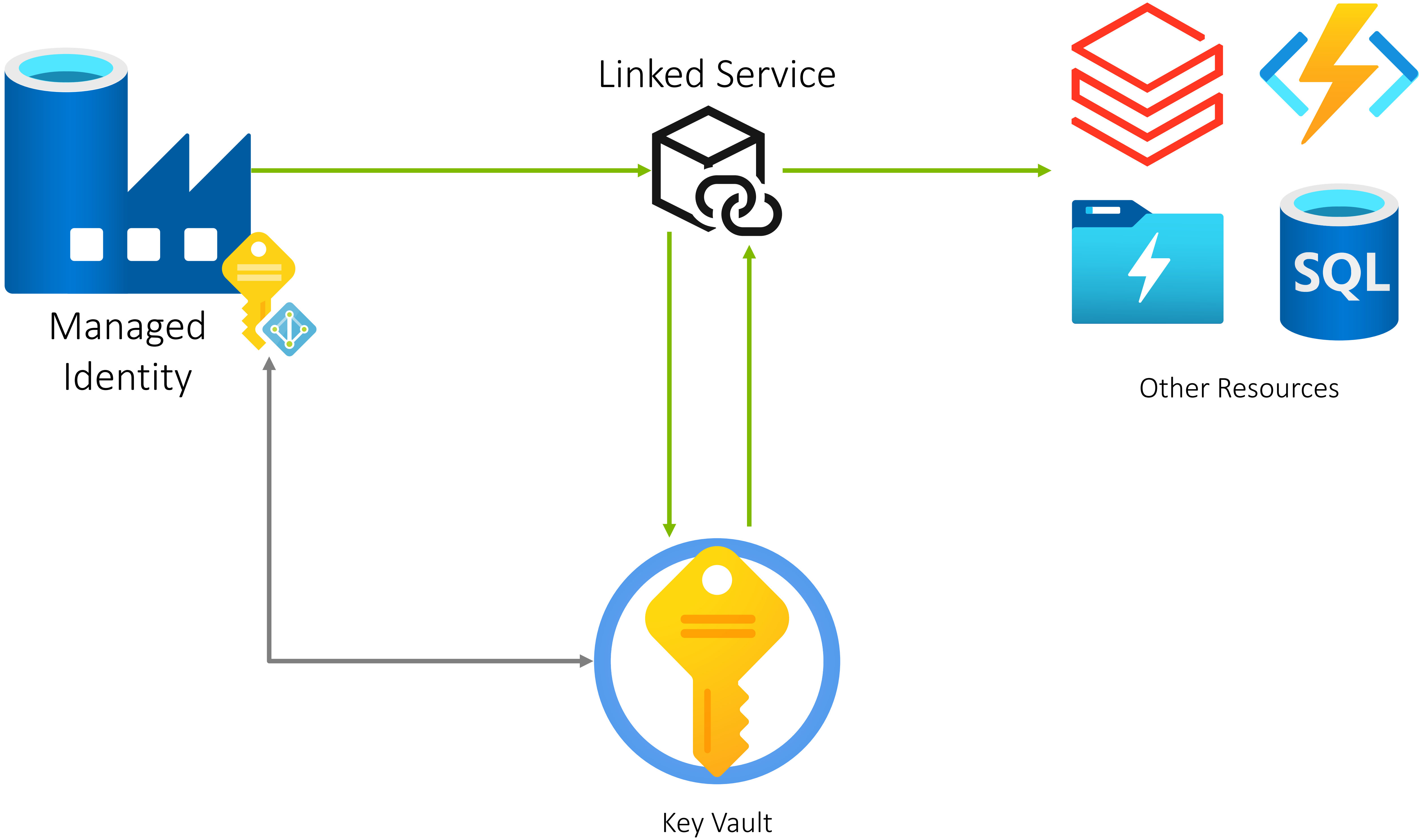
Module 8 – Security

Key Vault Integration & Return Values

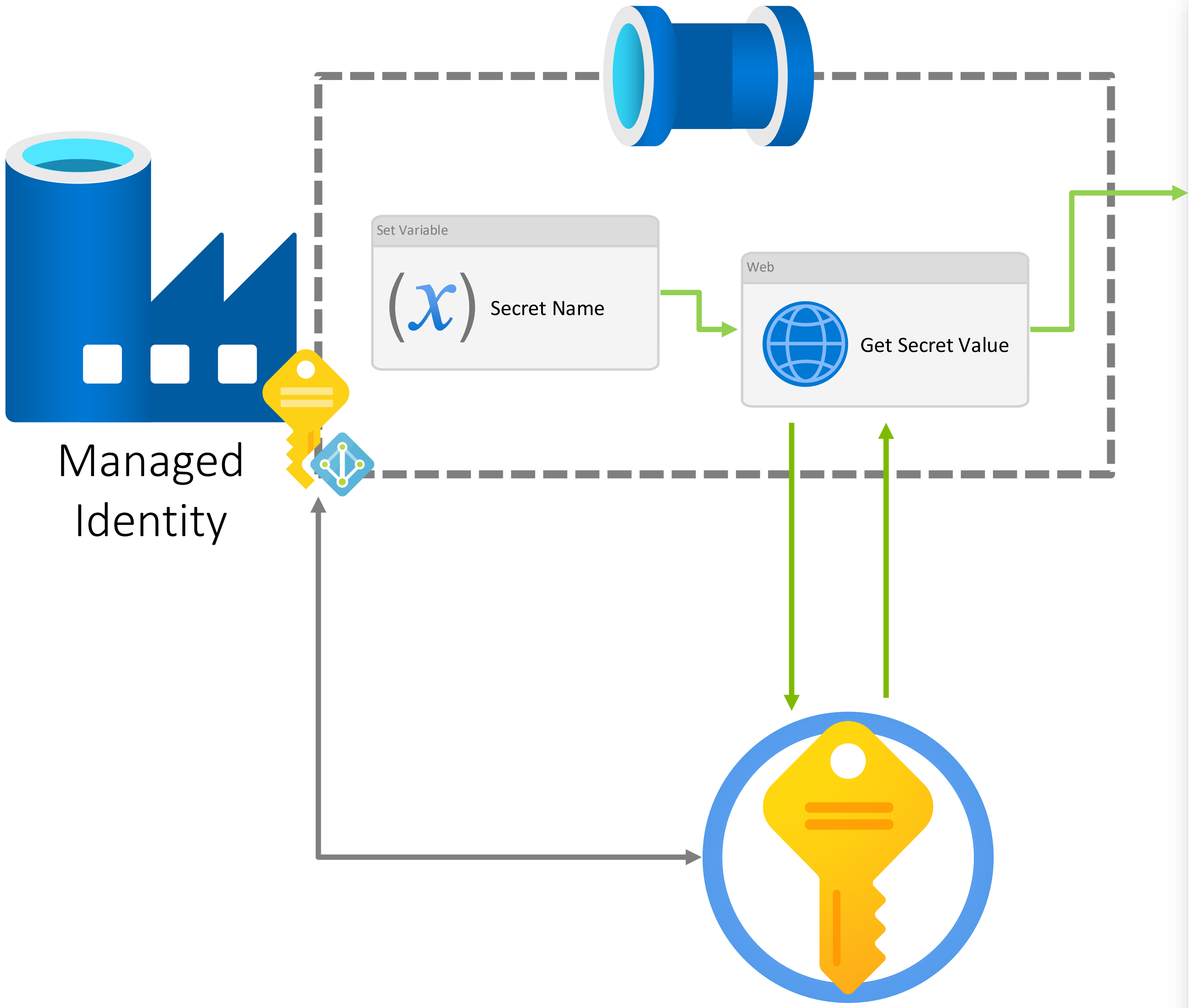


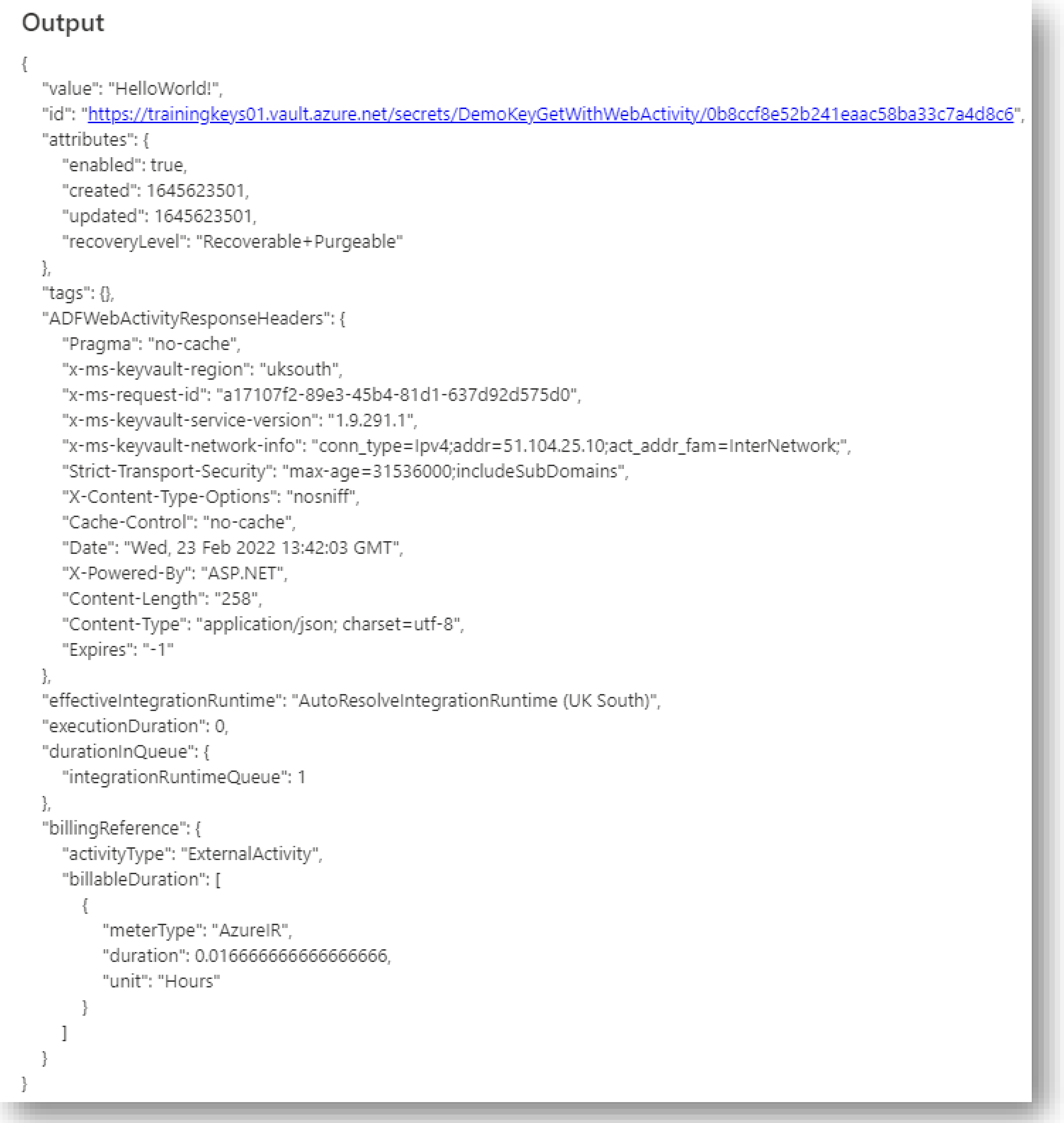
Cloud Formations

Key Vault Integration – Option 1



Key Vault Integration – Option 2



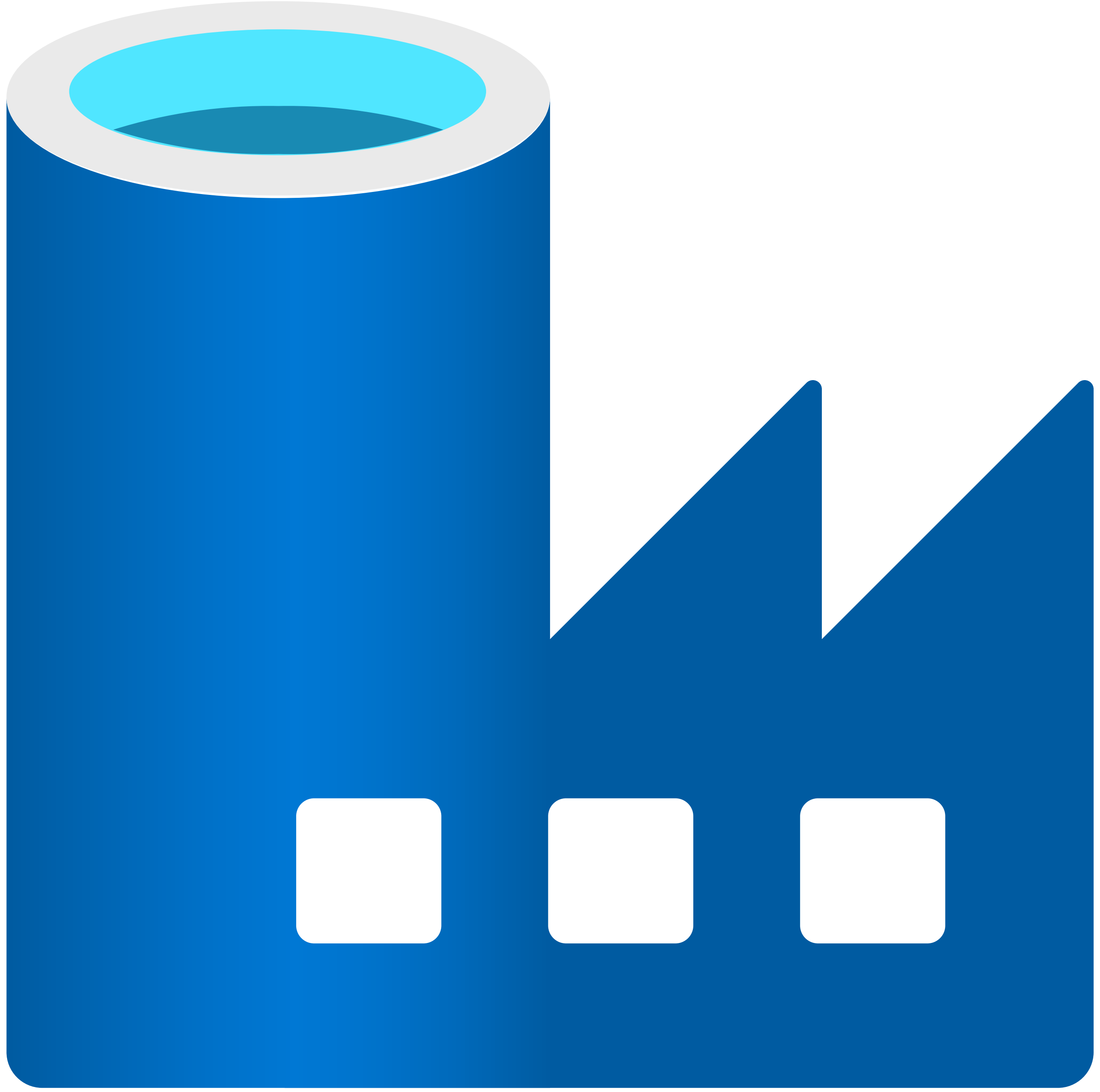


Output

```
{
   "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"
         }
      ]
   }
}
```

https://docs.microsoft.com/en-us/azure/data-factory/how-to-use-azure-key-vault-secrets-pipeline-activities

Azure Portal



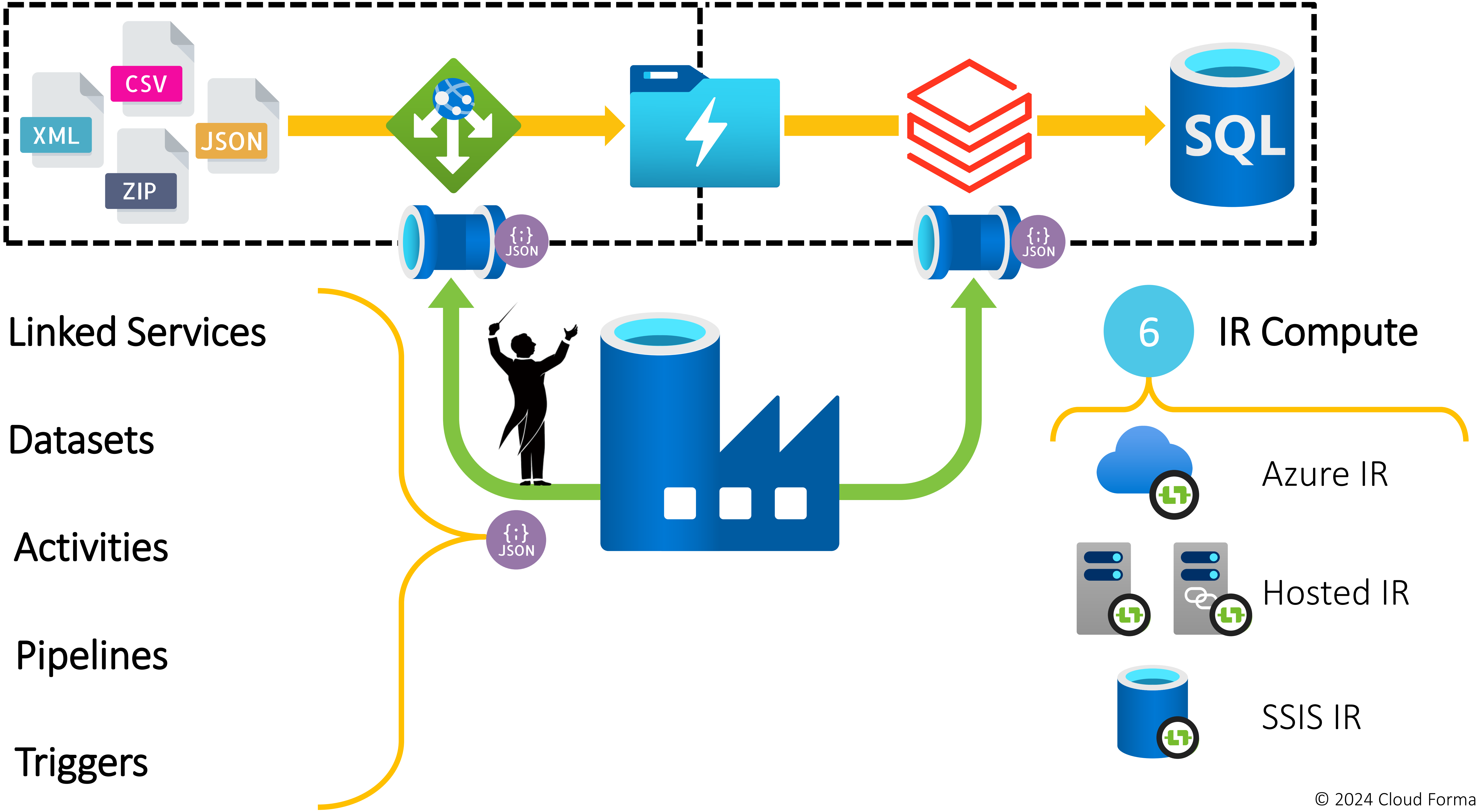
Module 8 – Security

Customer Managed Keys

Cloud Formations

Data Factory Core Components

Cloud Formations - Knowledge Transfer & Training



1 Linked Services

2 Datasets

3 Activities

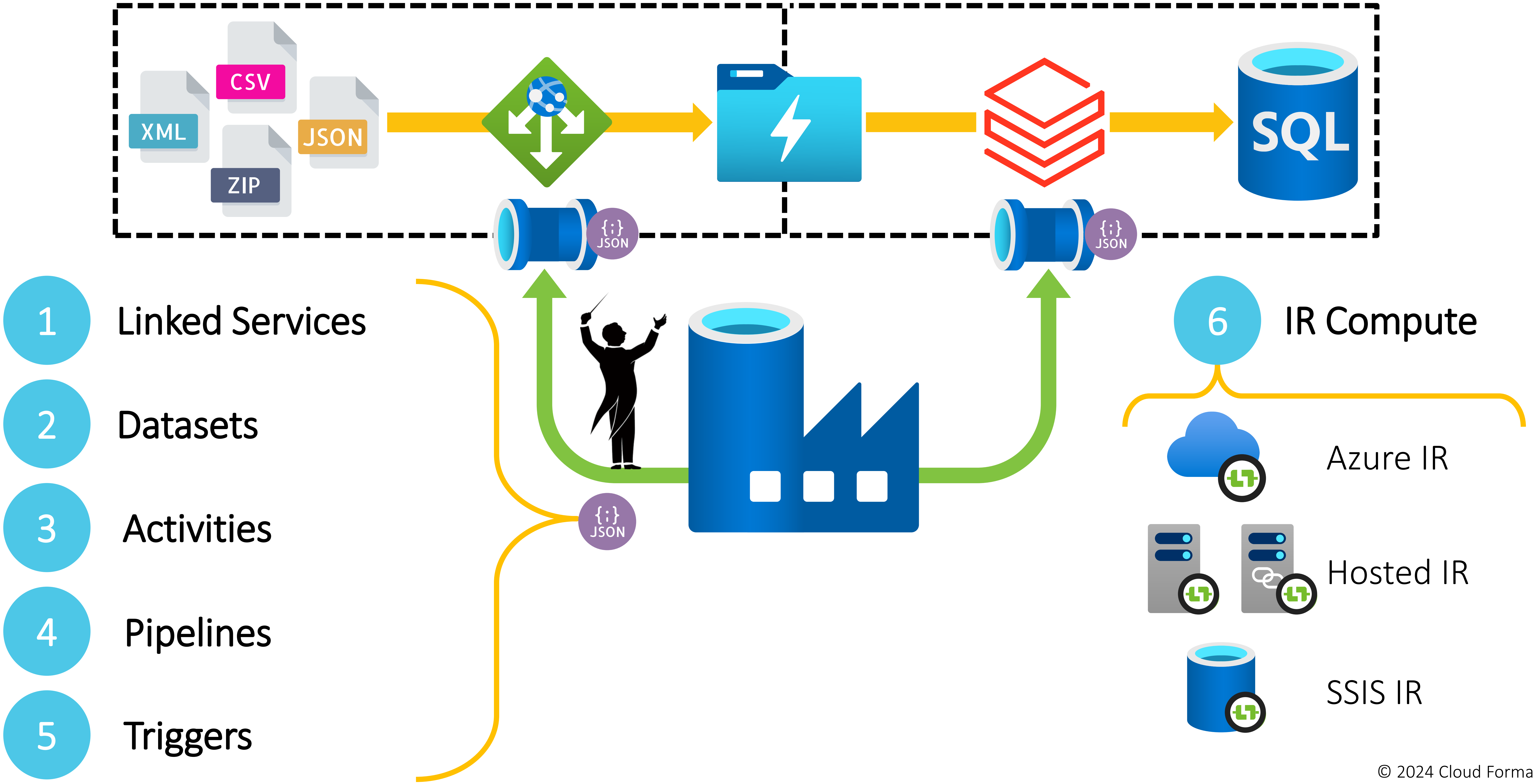
4 Pipelines

5 Triggers

6 IR Compute

- Azure IR
- Hosted IR
- SSIS IR

Data Factory Core Components



1 Linked Services

2 Datasets

3 Activities

4 Pipelines

5 Triggers

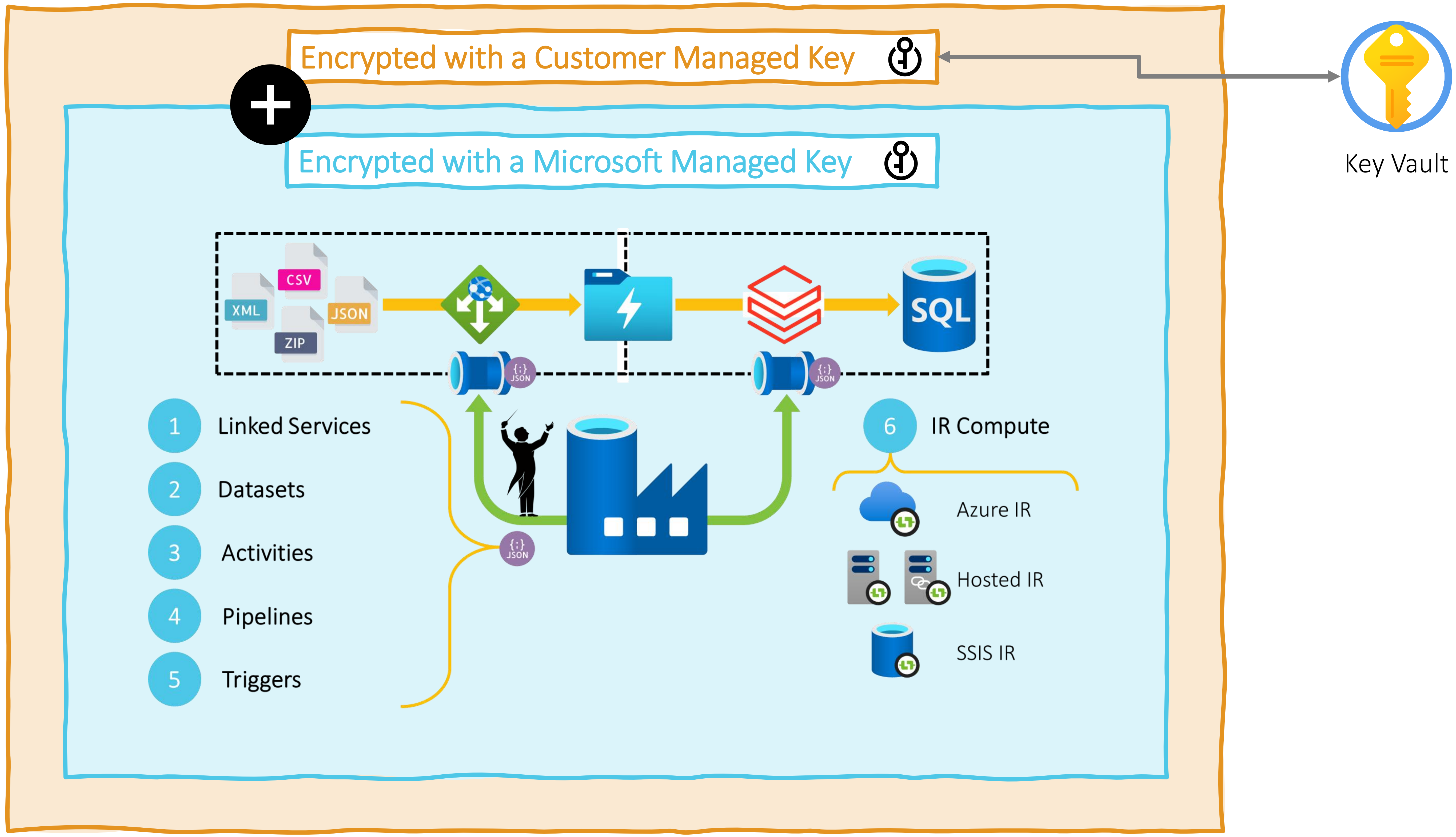
6 IR Compute

Azure IR

Hosted IR

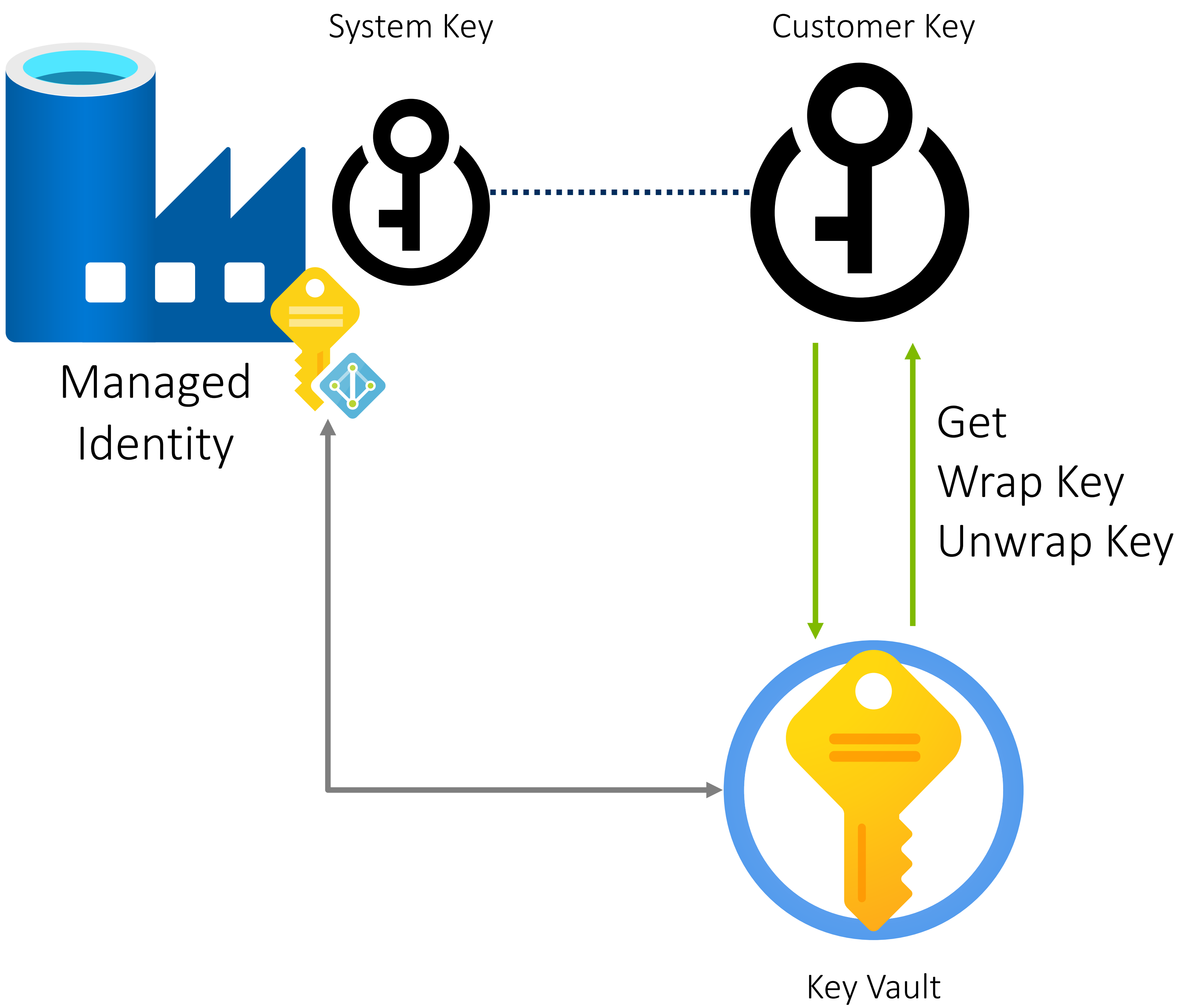
SSIS IR

Customer Managed Keys



https://learn.microsoft.com/en-us/azure/data-factory/enable-customer-managed-key

Customer Managed Key

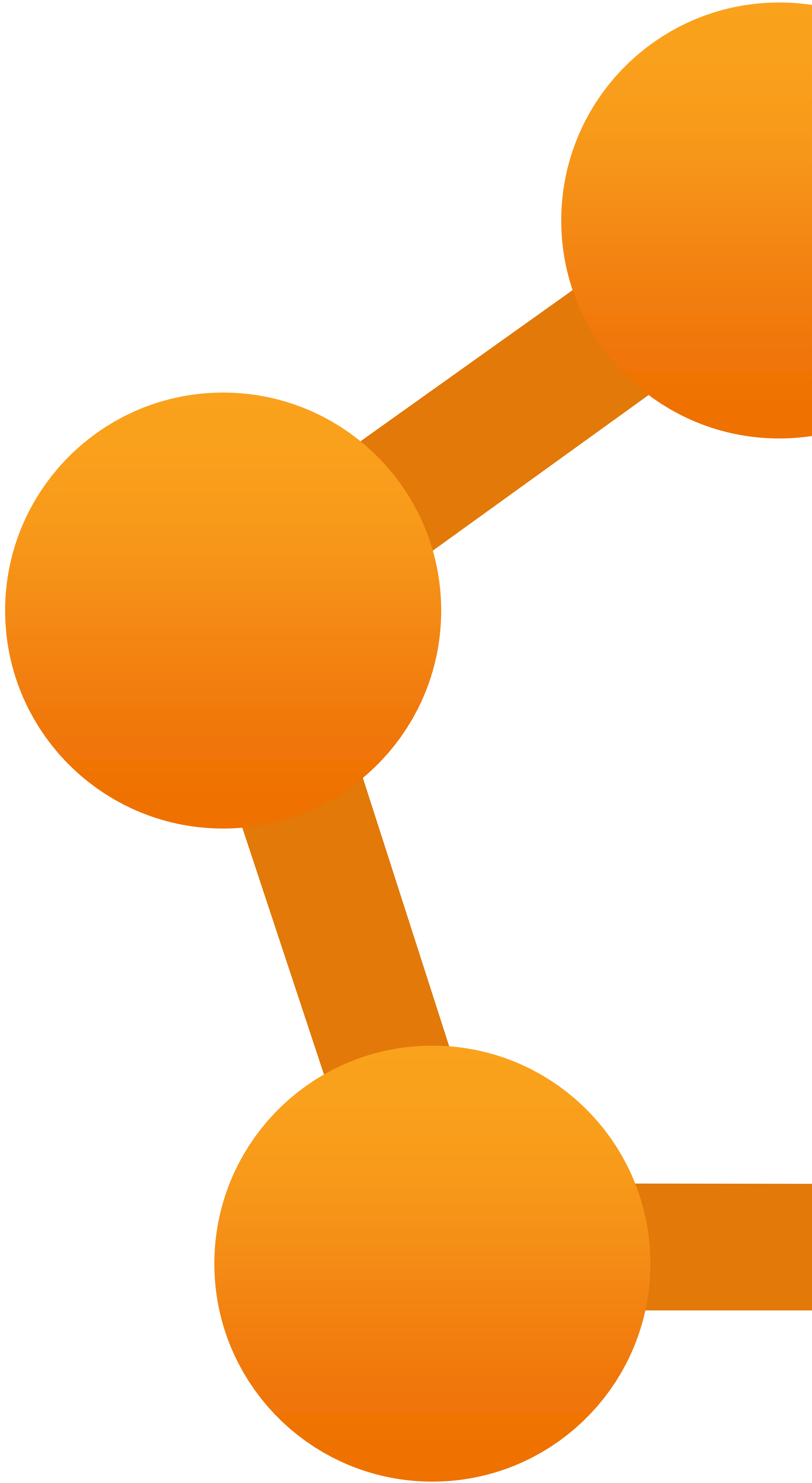


Limitations and Issues

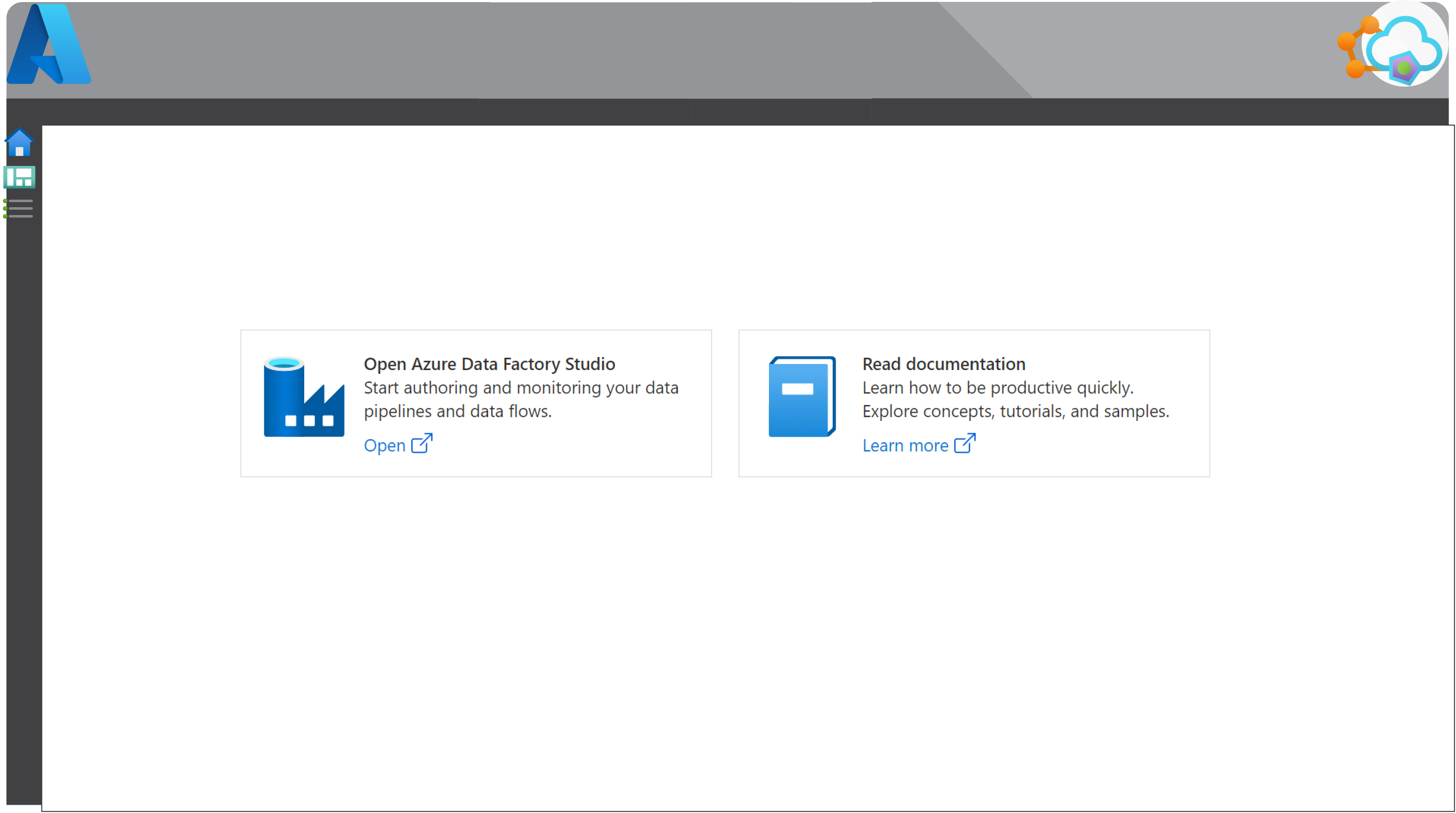
- Customer keys can only be stored in Key Vault.
- Can’t be applied to existing Data Factory instances.
- Doesn’t work with Managed Virtual Networks.
- Can’t be included in ARM templates definitions.
- Must be manually version controlled
- Not supported in Synapse Analytics
- Not supported in Microsoft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

Module 8 – Security

Pipeline Access & Permissions



Cloud Formations



Open Azure Data Factory Studio

Start authoring and monitoring your data pipelines and data flows.

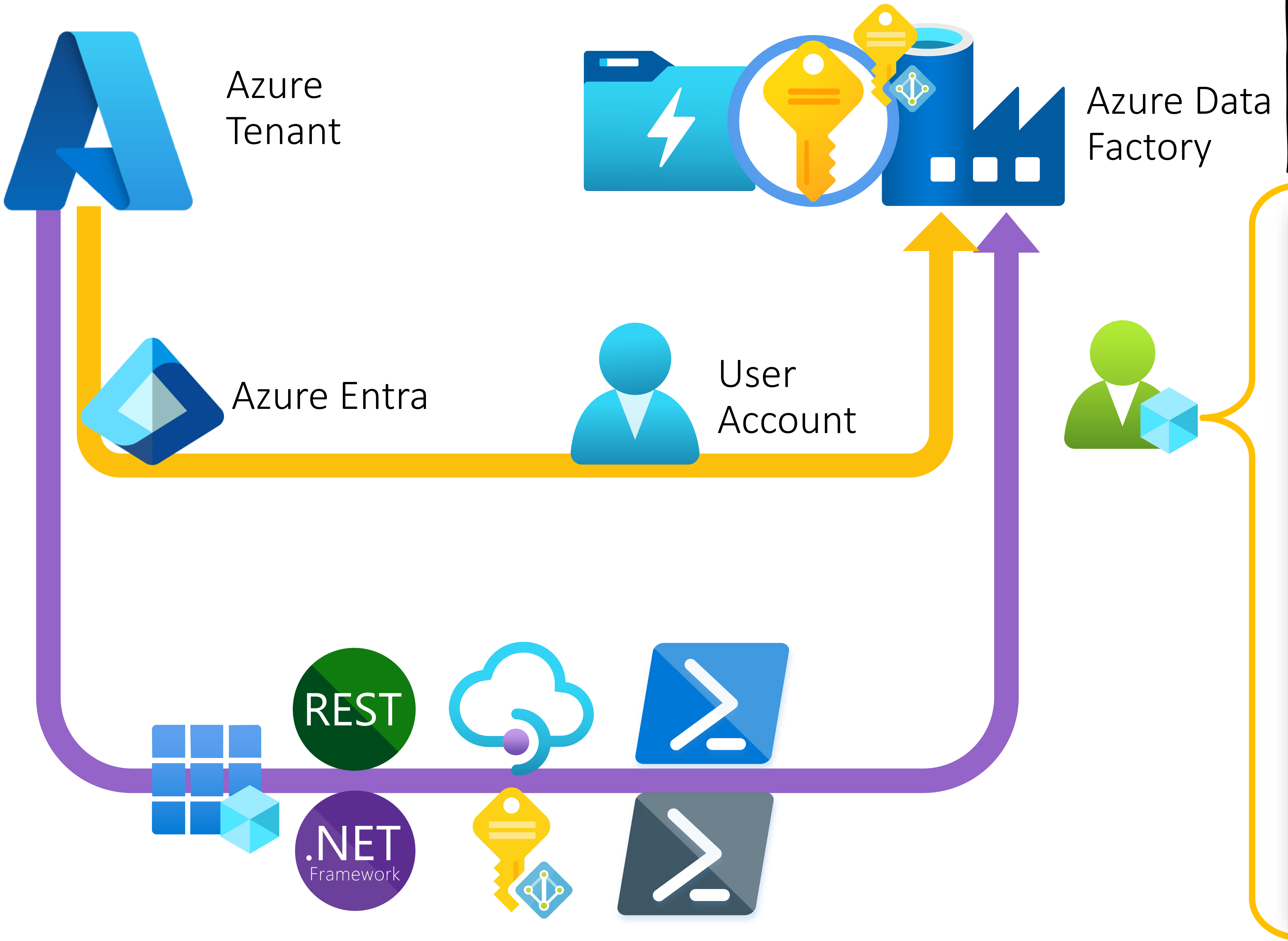
Open

Read documentation

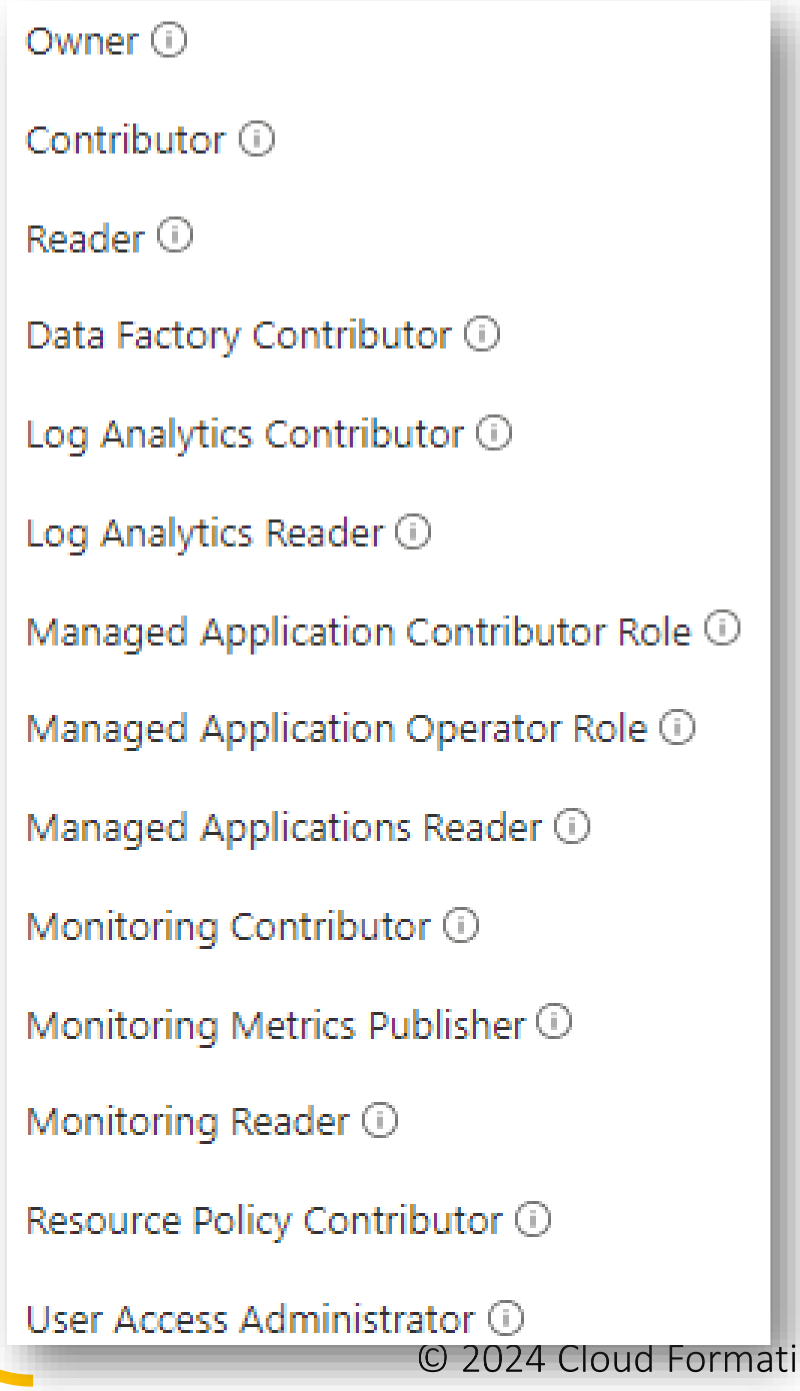
Learn how to be productive quickly. Explore concepts, tutorials, and samples.

Learn more

Accessing Everything via Data Factory

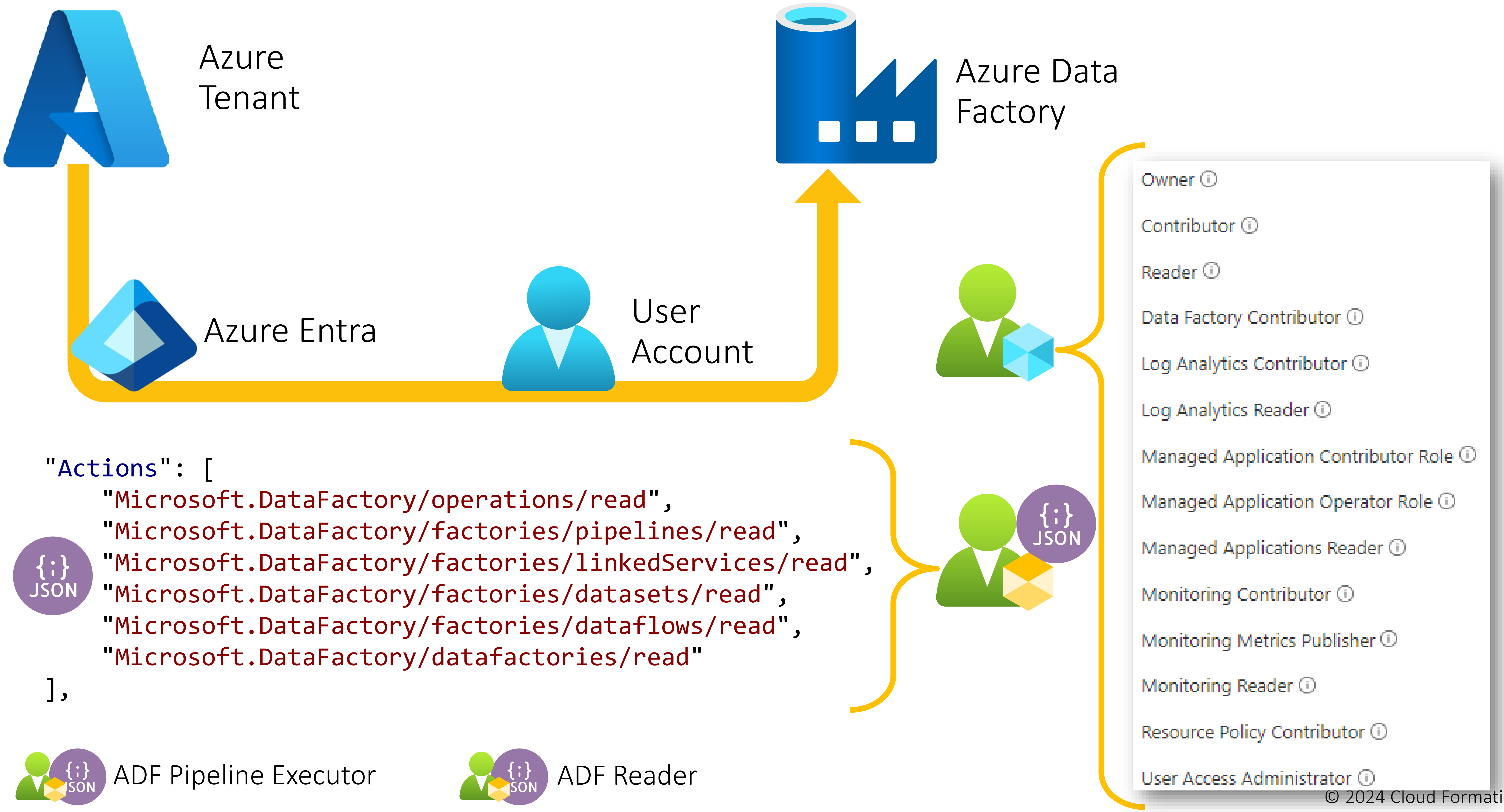


Connection Administrator
Pipeline Executor ✗
Dataset Reader


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 ⓘ

Cloud Formations - Knowledge Transfer & Training

Accessing Data Factory – Custom Roles



```
"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"
],
```

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 ⓘ

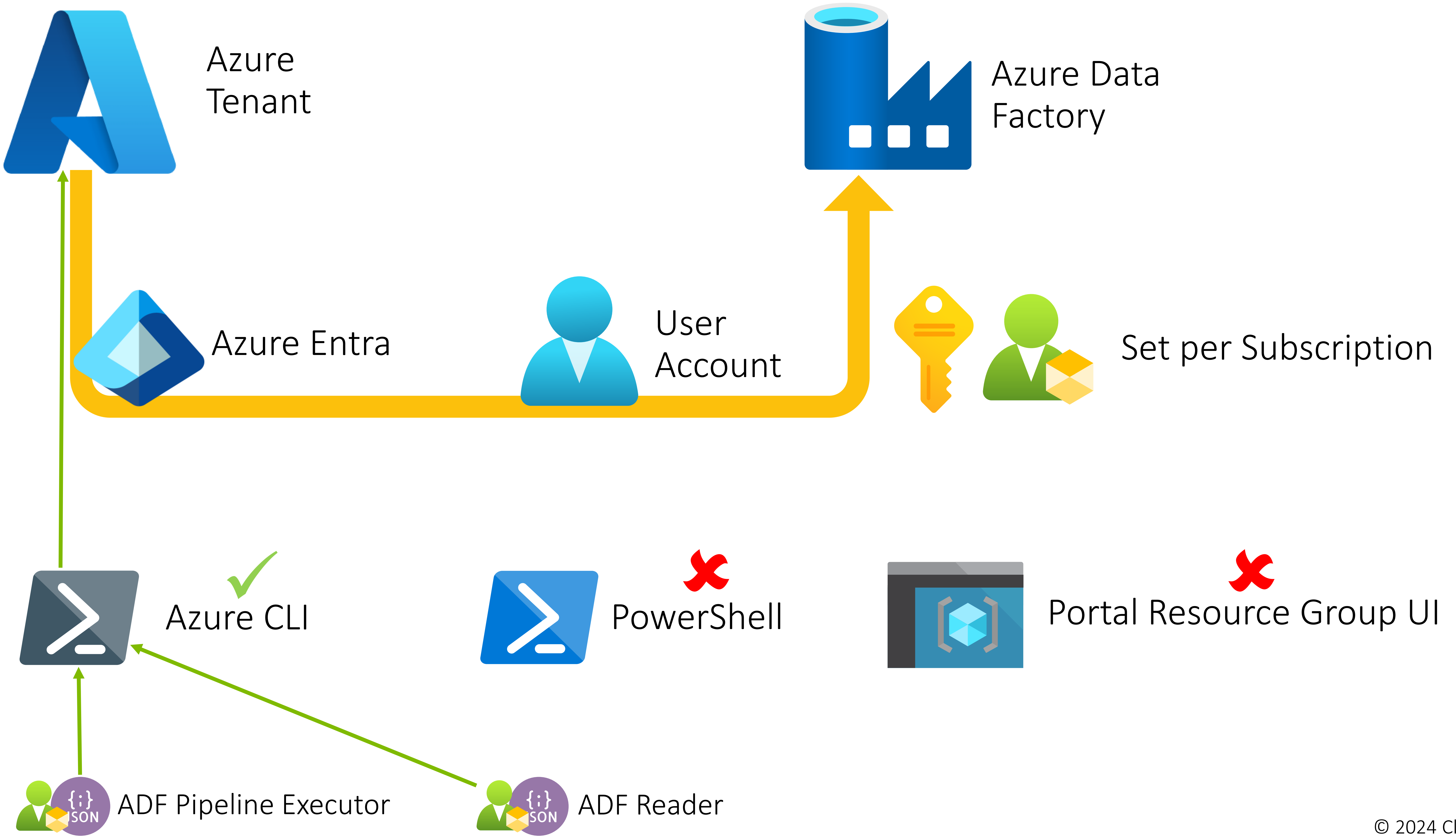
Monitoring Metrics Publisher ⓘ

Monitoring Reader ⓘ

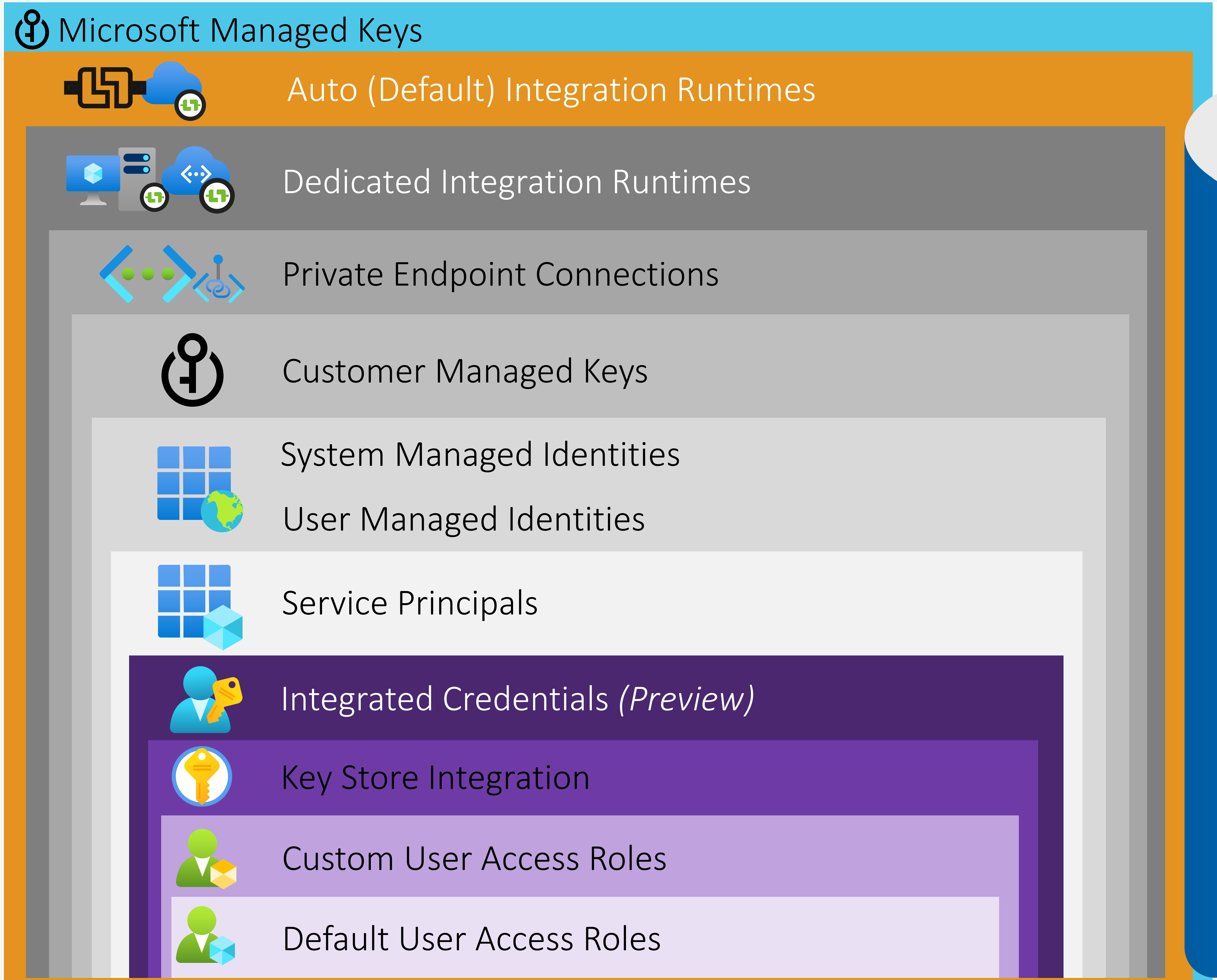
Resource Policy Contributor ⓘ

User Access Administrator ⓘ

Accessing Data Factory – Custom Roles



Data Integration Pipeline – Security Layers



Microsoft Managed Keys

Auto (Default) Integration Runtimes

Dedicated Integration Runtimes

Private Endpoint Connections

Customer Managed Keys

System Managed Identities

User Managed Identities

Service Principals

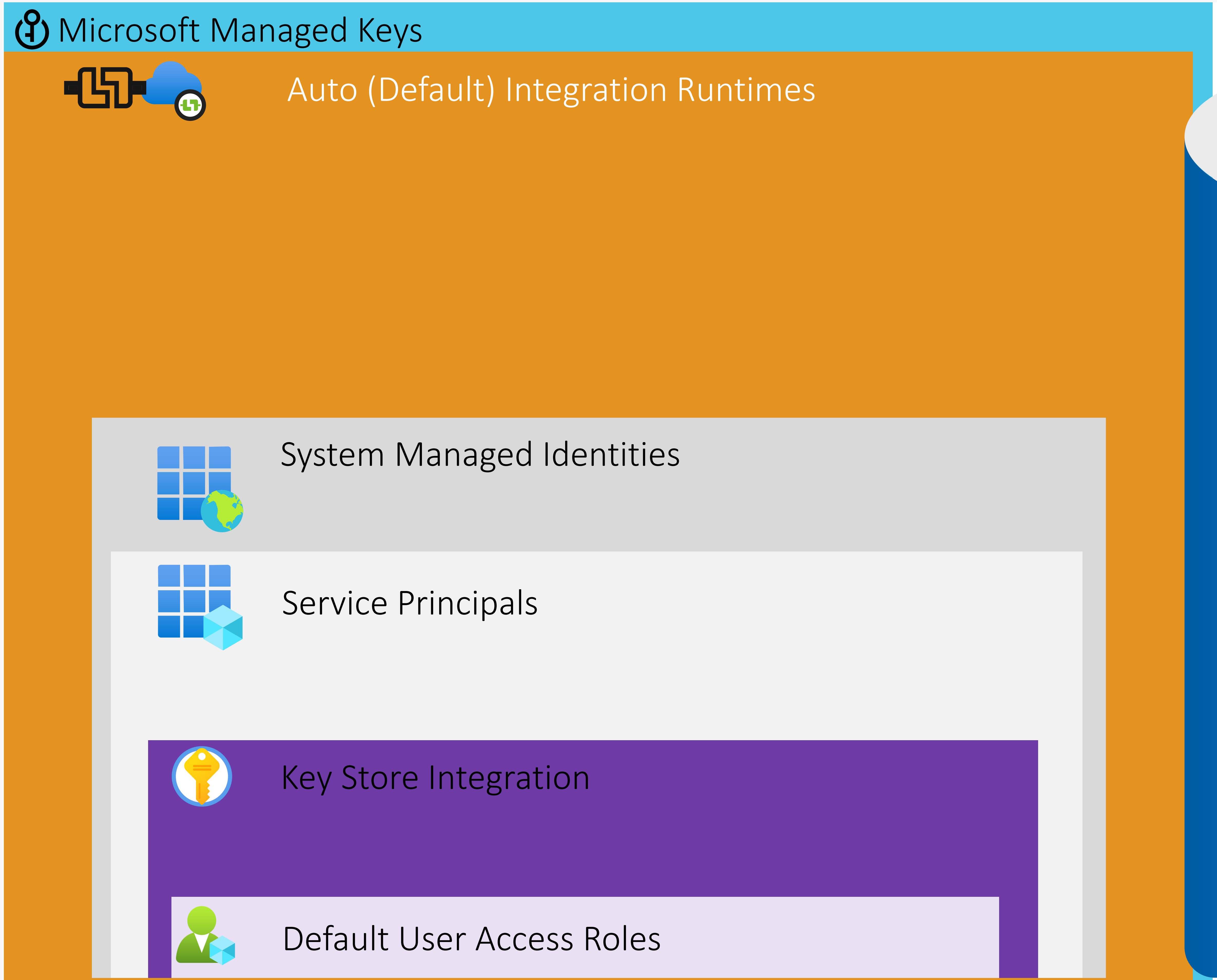
Integrated Credentials *(Preview)*

Key Store Integration

Custom User Access Roles

Default User Access Roles

Data Integration Pipeline – Security Layers



Microsoft Managed Keys

Auto (Default) Integration Runtimes

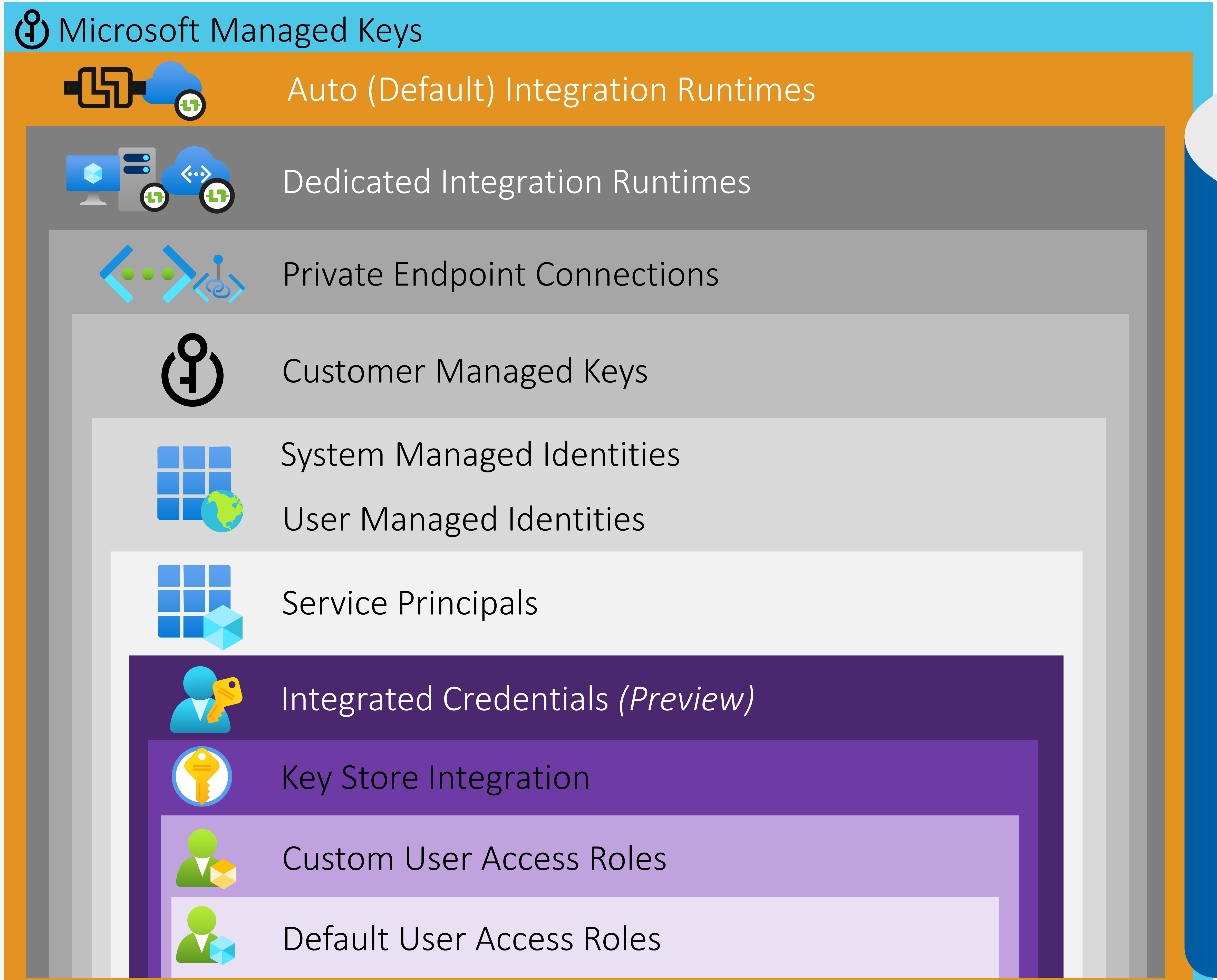
System Managed Identities

Service Principals

Key Store Integration

Default User Access Roles

Data Integration Pipeline – Security Layers



Microsoft Managed Keys

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

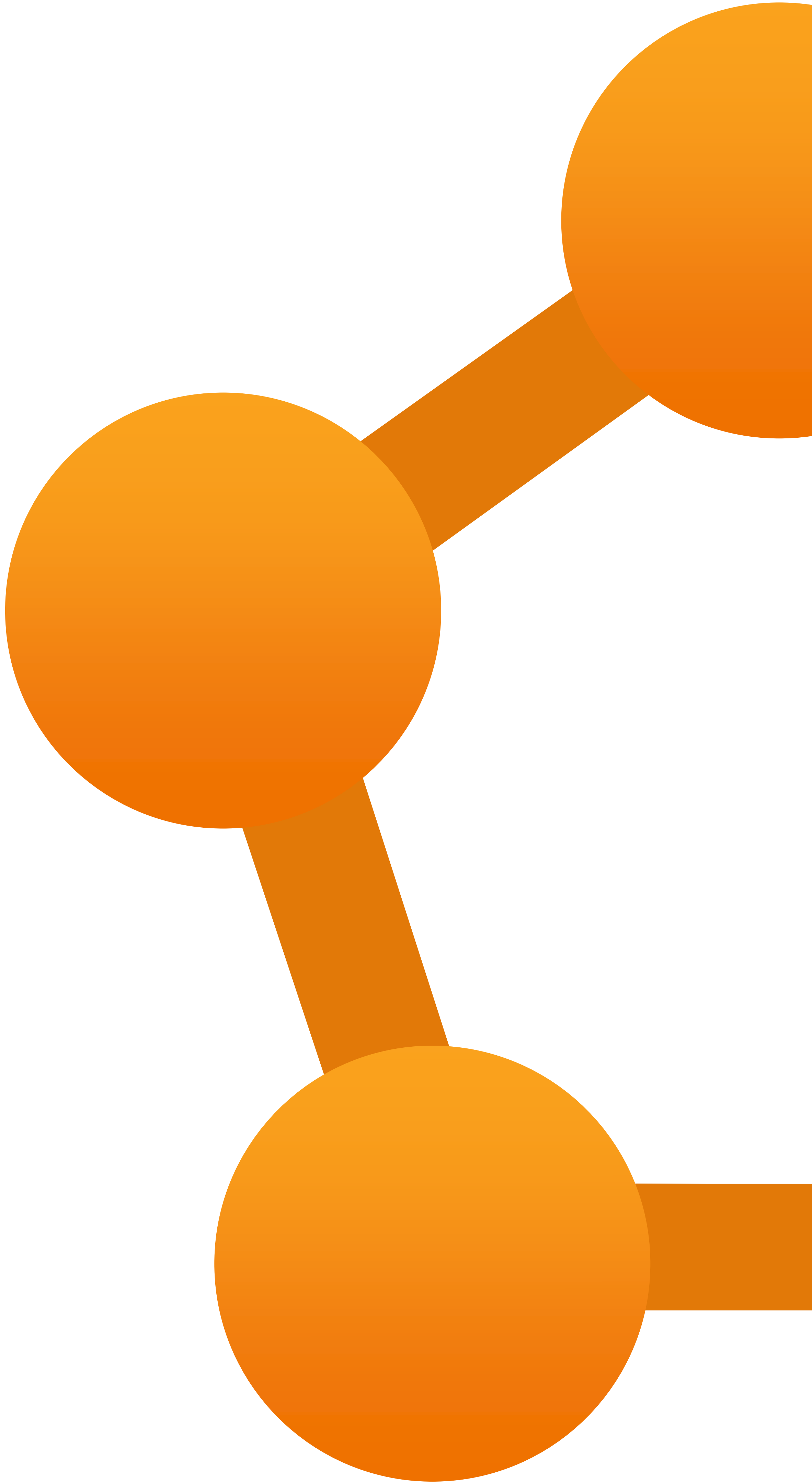
Default User Access Roles

Cloud Formations - Knowledge Transfer & Training

Module 8

Security ✓

Any questions?



Cloud Formations