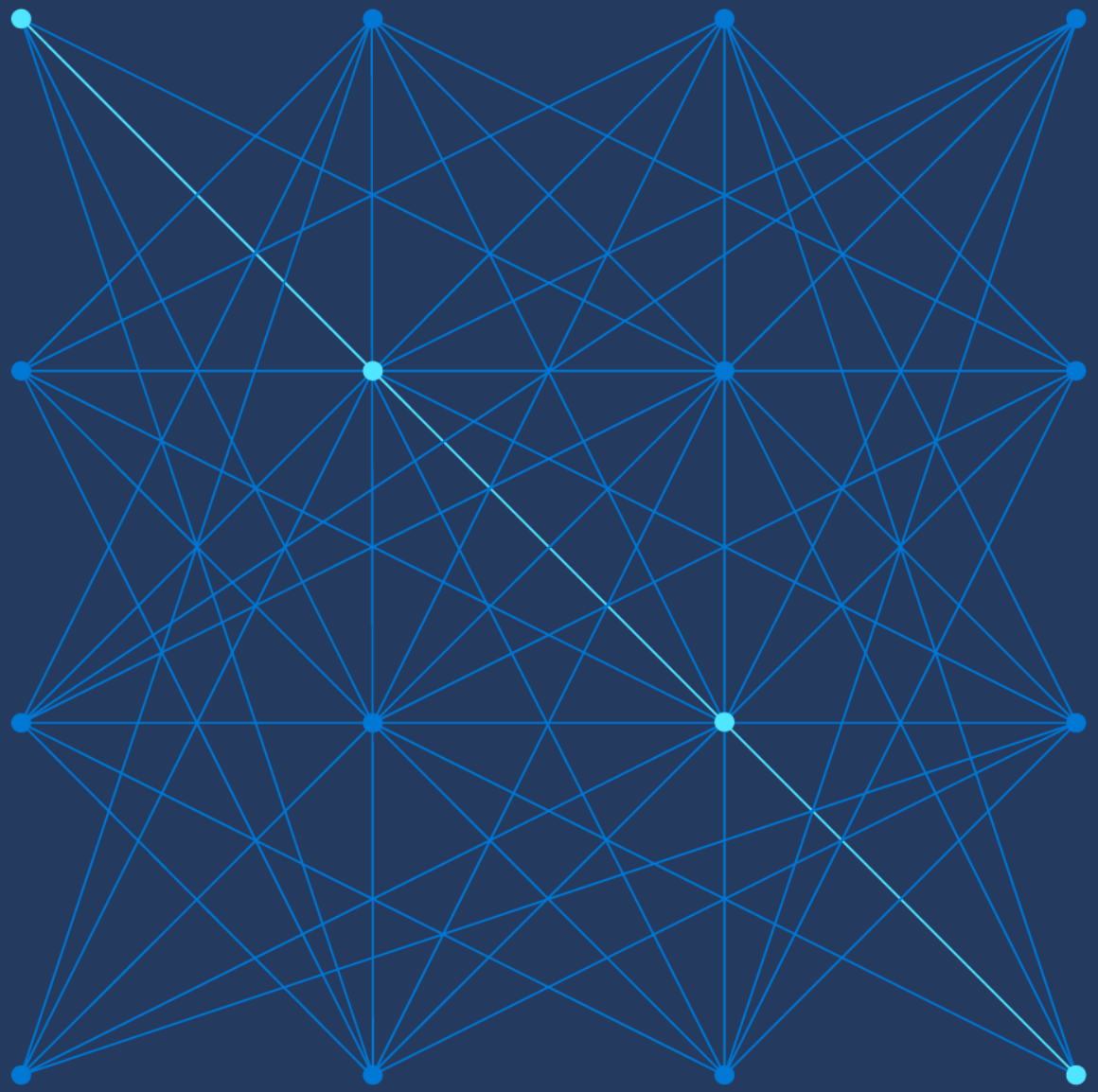
Microsoft

Azure Machine Learning Security

06/10/2022

Narjes Majdoub
Cloud Solutions Architect, Data & AI

Khadidiatou Ba
Cloud Solutions Architect, Security



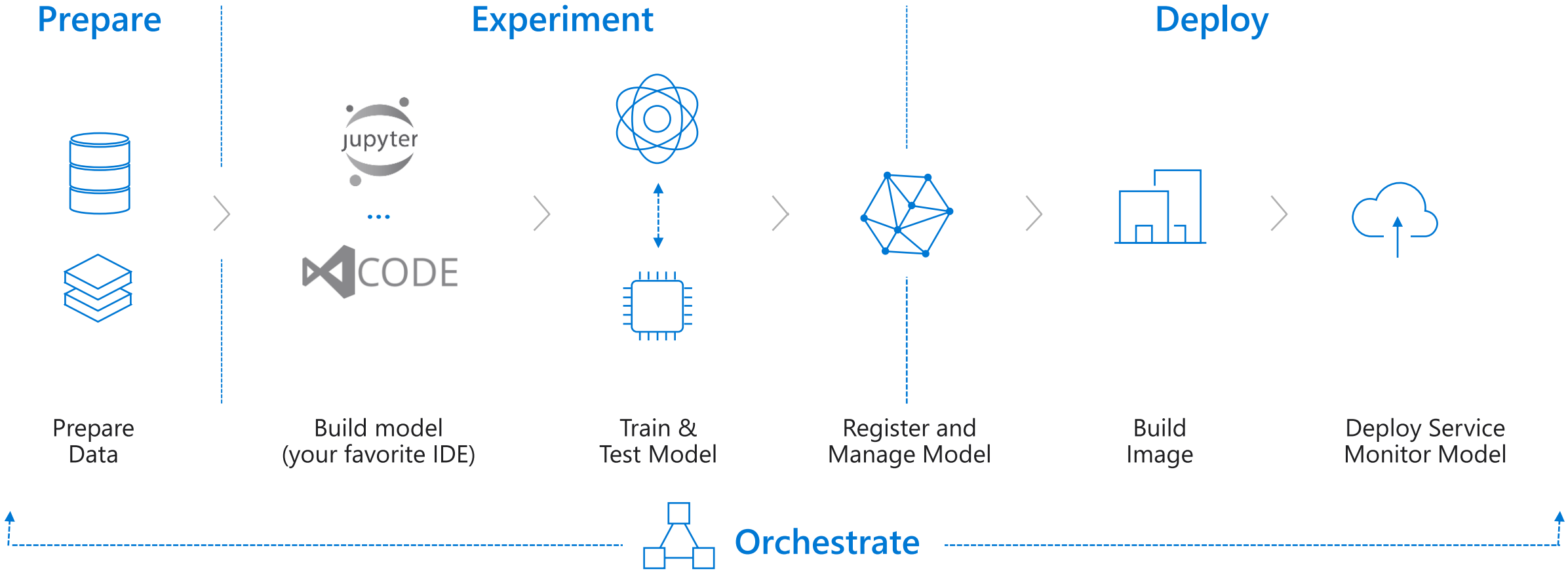
Agenda

1. Machine Learning & Security Overview
2. AML Security Best practices
   - IAM
   - Network security
   - Secure compute
   - Data protection
   - Secure MLOps
3. Governance and Monitoring
4. Demo

Introduction: ML & Security Overview

What is Machine Learning ?

Typical end to end process

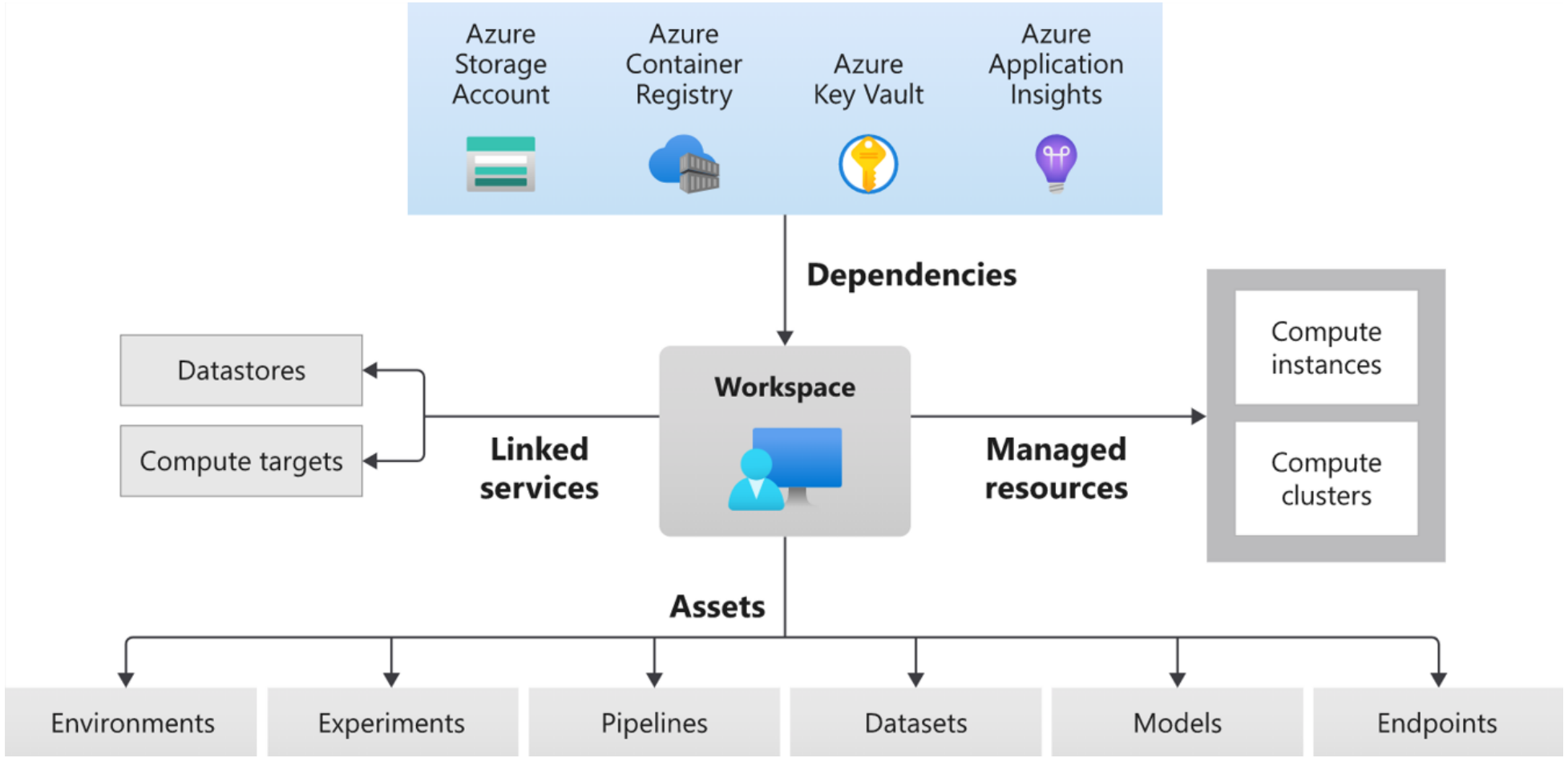


What is Azure Machine Learning ?

Customer Promise

ML for all skill levels	Full lifecycle management with MLOPs	State-of-the-art Responsible ML	Open & Interoperable
Automated ML + drag & drop + code first	Integrated with Azure DevOps/Github Event-driven ML workflows: Event grid Github actions	Responsible, trustworthy and explainable solutions	Any tool + any framework

Azure Machine Learning overview

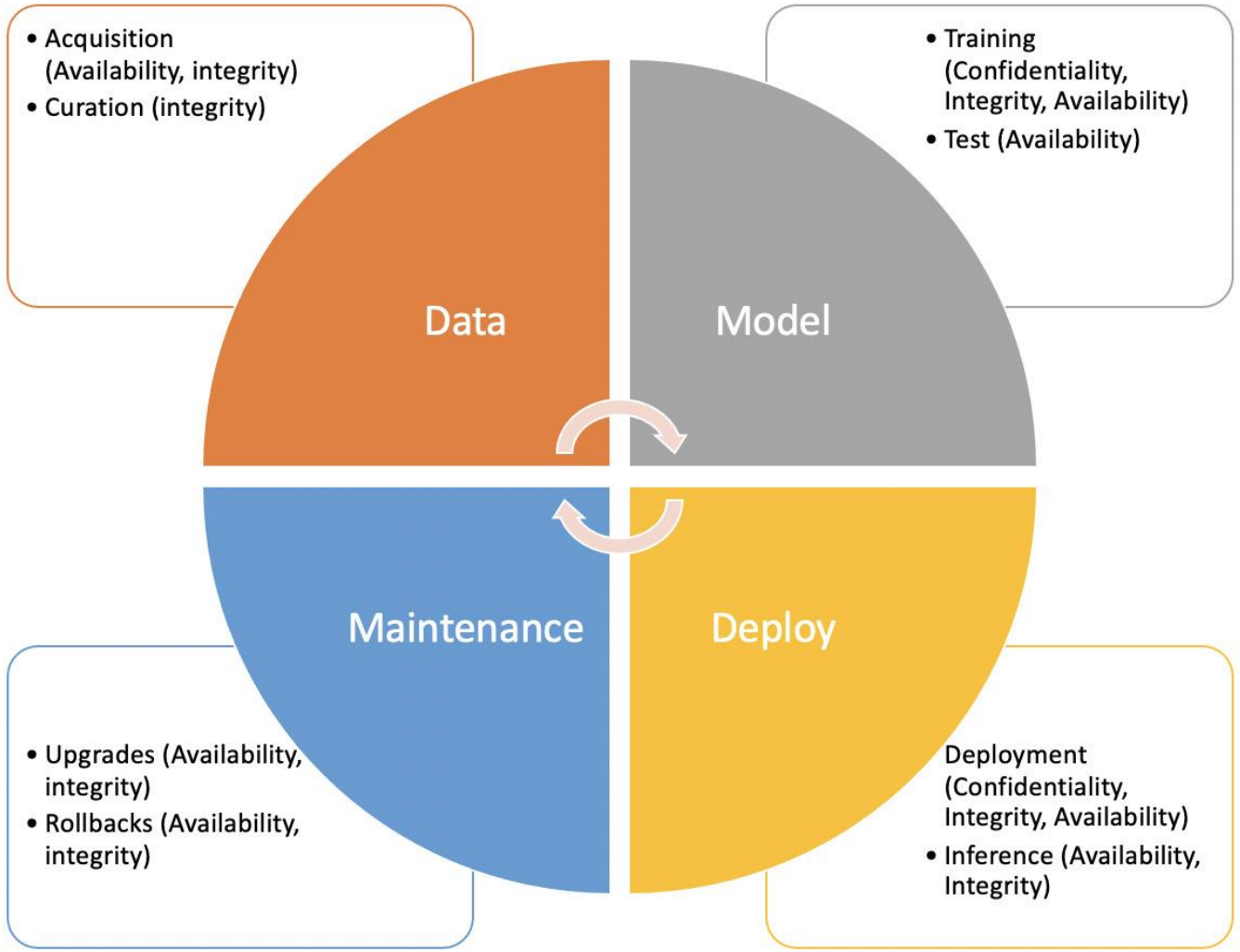


Security Overview : Confidentiality, Integrity, Availability (CIA)

Confidentiality, Integrity, Availability, or CIA, is a common way to think about security trade-offs.

- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data.
- **Integrity** refers to keeping data or messages correct.
- **Availability** refers to making data available to those who need it.
- **Traceability** refers to the ability to identify the origin and reconstruct the journey (of a product), from production to distribution.
- **Non-repudiation** refers to the undeniable character of an action

Reflecting CIA on ML lifecycle



Engineering MLOps | Microsoft Azure

Security Overview : Common threats

There are different types of security threats. Some aim to steal data, some aim to extort money, and others to disrupt normal operations, such as a denial of service attack. This unit looks at some of the common threats.

Data breach

Include:

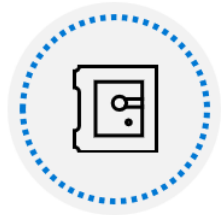
- Phishing
- Spear phishing
- Tech support scams
- SQL injection
- Malware designed to steal passwords or bank details.

Dictionary attack

It is a type of identity attack.

A hacker attempts to steal an identity by trying a large number of known passwords.

Dictionary attacks are also known as brute force attacks.



Ransomware

It is a type of malware that encrypts files and folders.

It attempts to extort money from victims.

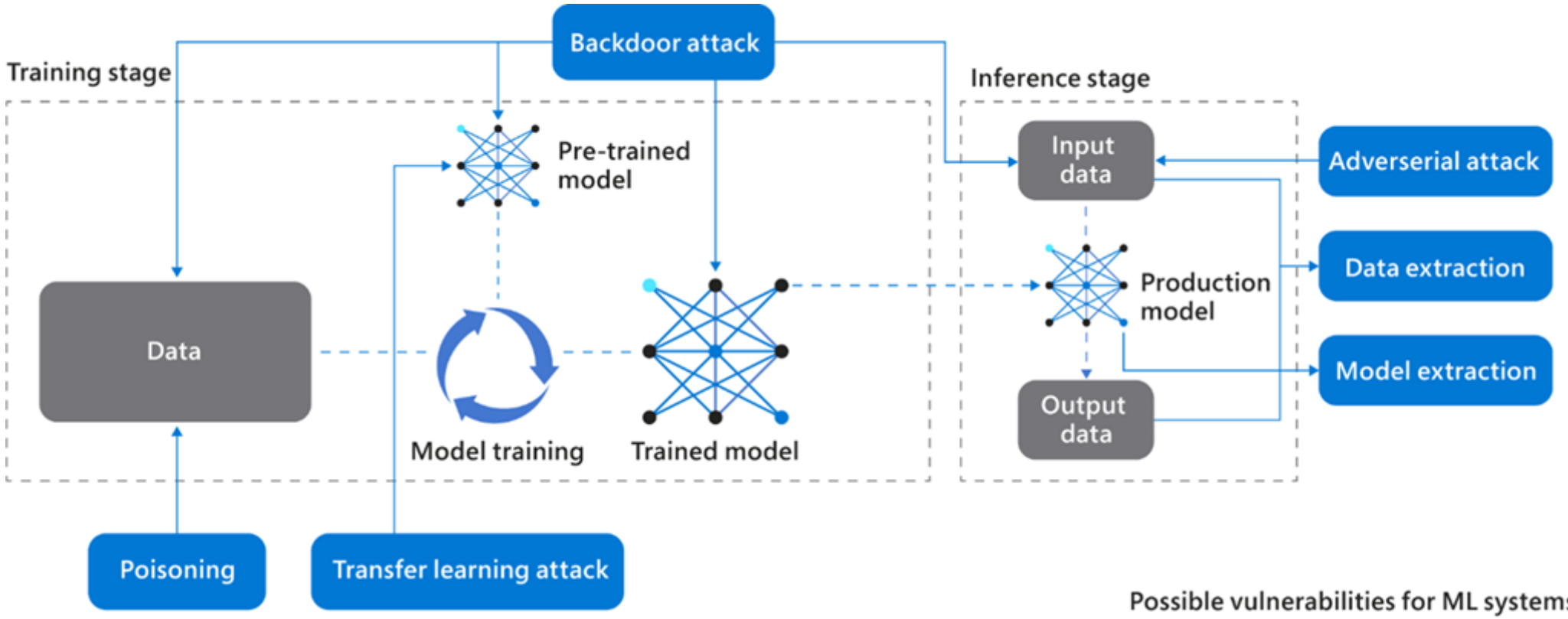
Disruptive attacks

A Distributed Denial of Service (DDoS) attack attempts to exhaust an application's resources.

DDoS attacks can be targeted at any endpoint.

Other common threats include coin miners, rootkits, trojans, worms, and exploits and exploit kits.

Security Overview : Possible threats on ML systems



Possible vulnerabilities for ML systems

Source

Security Overview : What is Zero Trust ?

Verify Explicitely

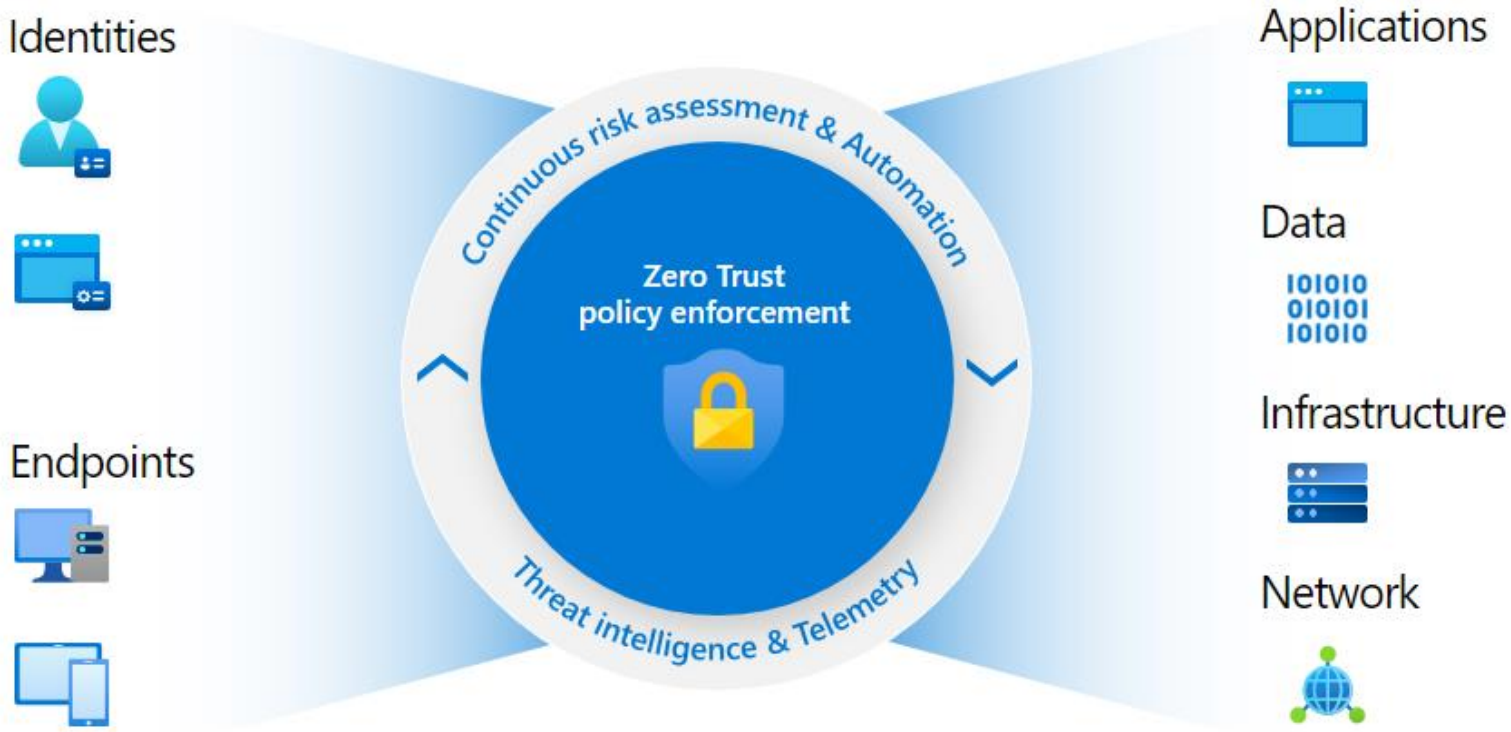
Always authenticate and authorize based on all available data points

Use least privileged access

Limit user access with Just-in-Time and Just-Enough-Access (JIT/JEA), risk based adaptative policies and data protection

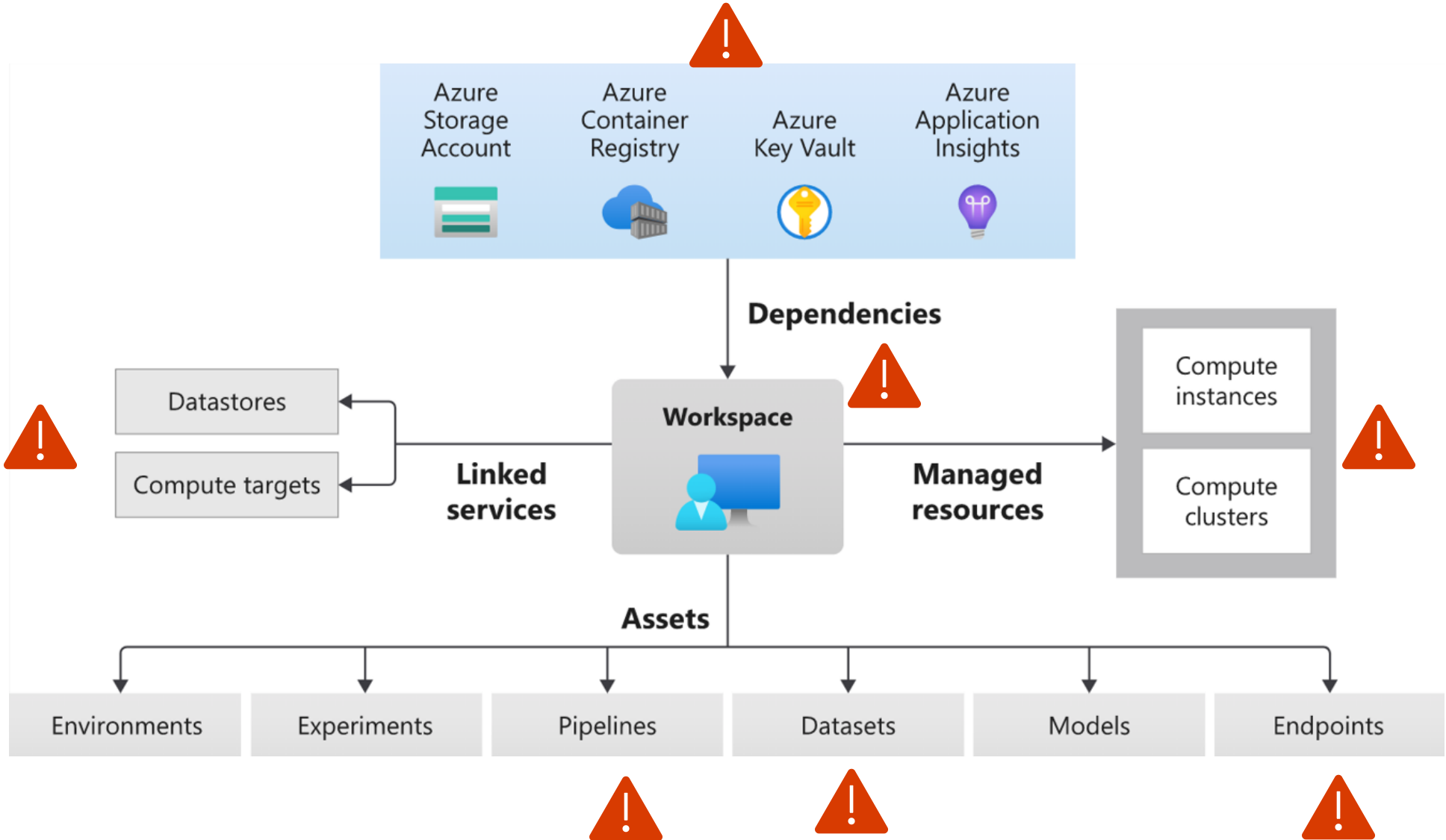
Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection and improve defenses.



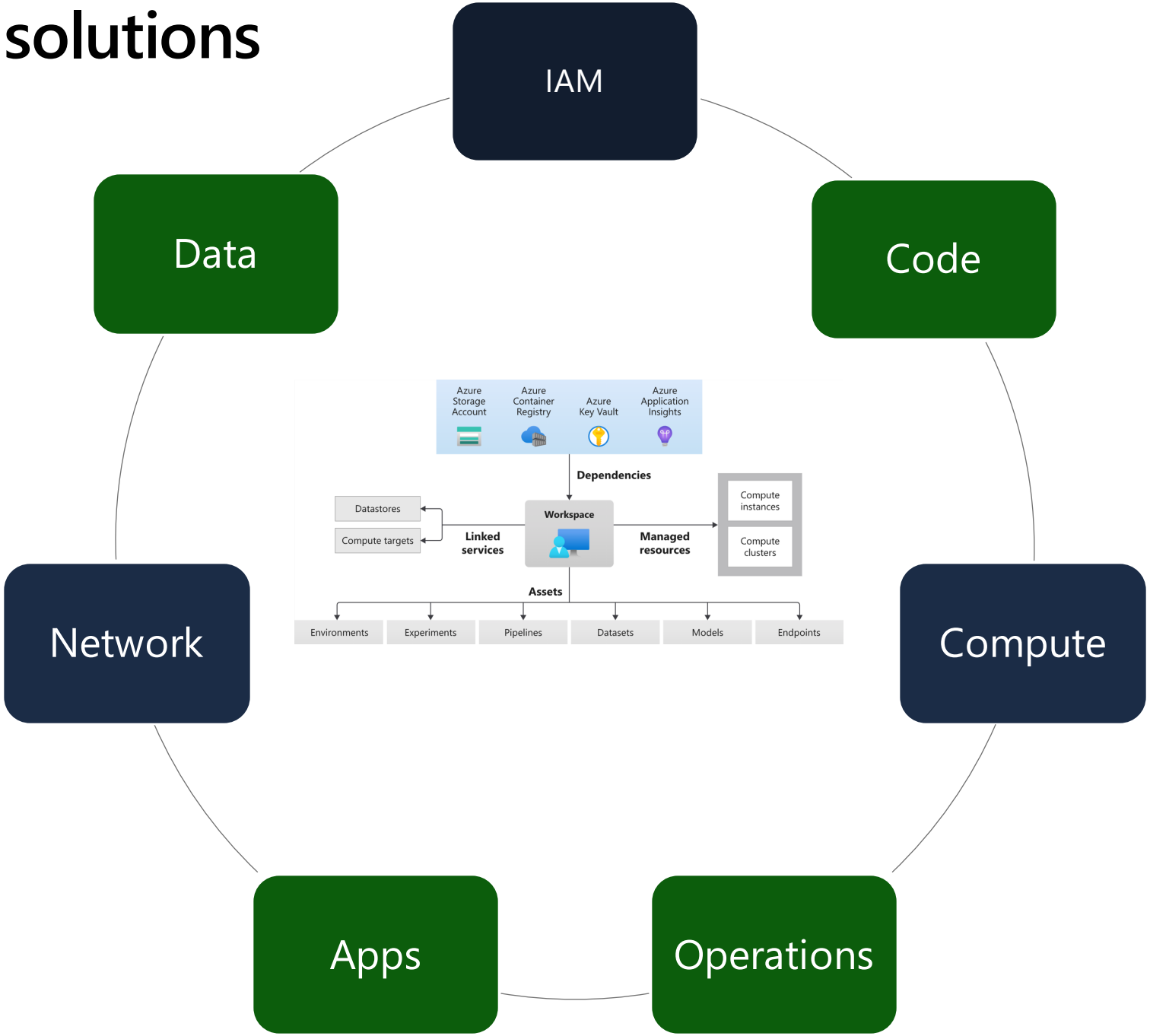
Azure ML Security challenges

What can possibly go wrong ?



But there are solutions

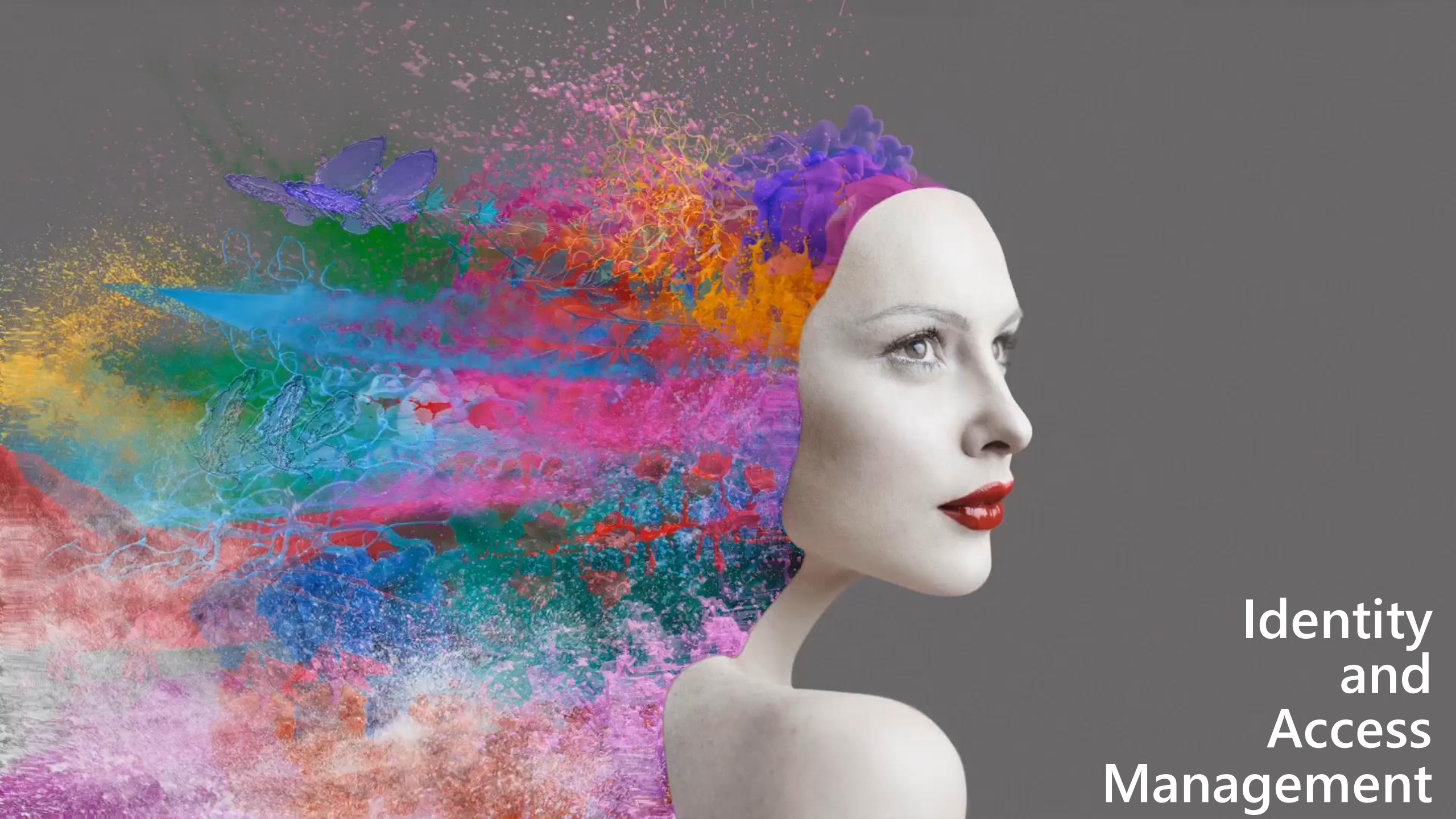
Security pillars



Microsoft

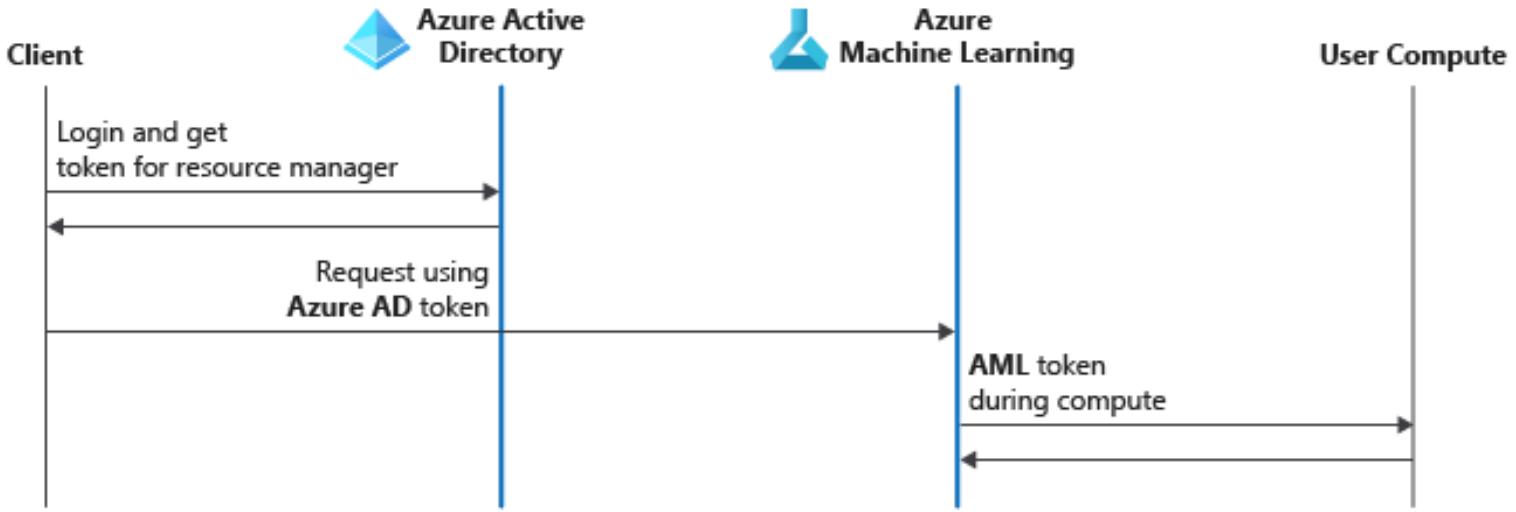
Azure ML Security Best Practices

1- IAM
2- Network security
3- Secure compute
4- Data protection
5- Secure MLOps



Identity and Access Management

Restrict access to resource and operations



Workspace assigned managed identity

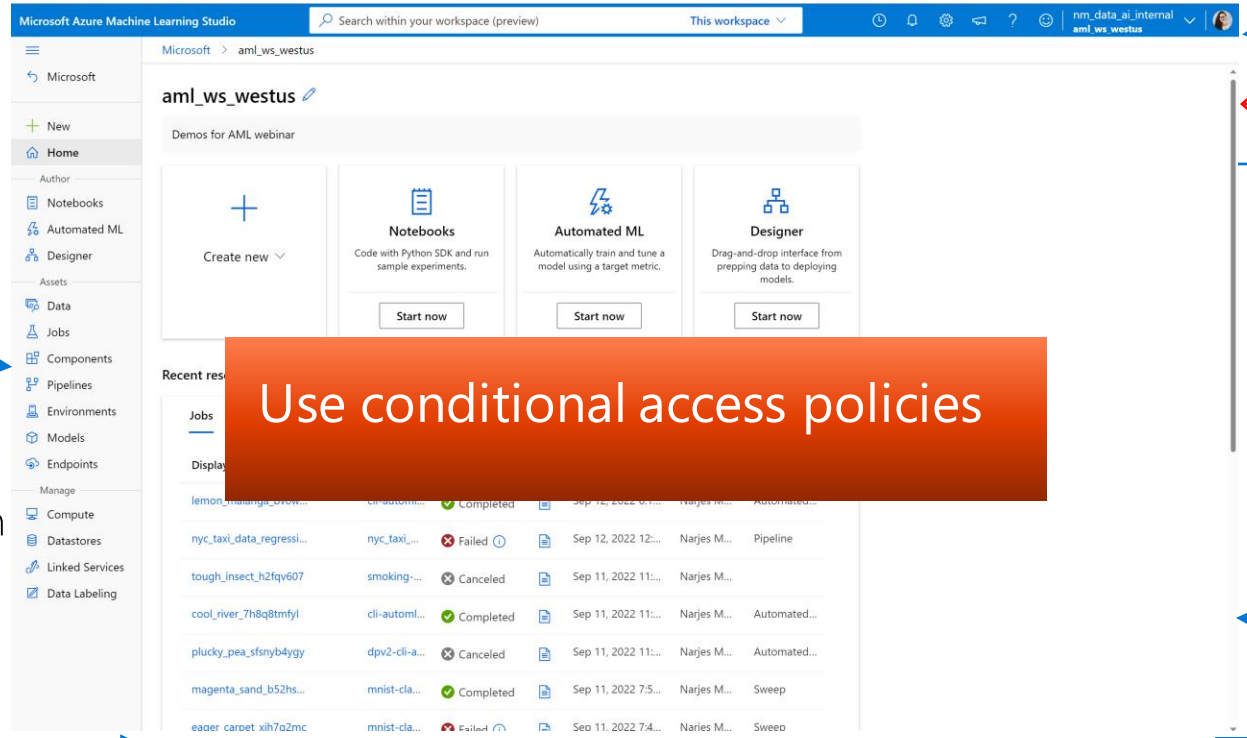
Resource	Permissions
Workspace	Contributor
Storage account	Storage Blob Data Contributor
Key vault	Access to all keys, secrets, certificates
Azure Container Registry	Contributor
Resource group that contains the workspace	Contributor

Authentication for AML workspace

Managed identity

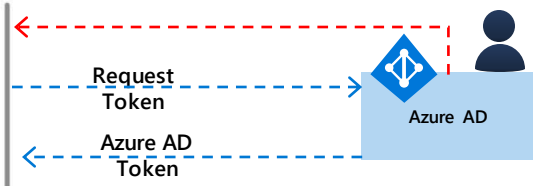
Aml Compute
Azure VM

- Python SDK without storing credentials in code/ user interaction
- Cluster to access workspace



Use conditional access policies

Interactive



- Experimentation + iterative dev
- Access per-user

Service principal

- Automated process + no user interaction
- CI/CD workflows

Azure CLI session

- Already using cli to manage resources
- Sign in once

Authorization

Role Based Access Control – Default roles

Role	Access level
AzureML Data Scientist	Can perform all actions within an Azure Machine Learning workspace, except for creating or deleting compute resources and modifying the workspace itself.
Reader	Read-only actions in the workspace. Readers can list and view assets, including datastore credentials, in a workspace. Readers can't create or update these assets.
Contributor	View, create, edit, or delete (where applicable) assets in a workspace. For example, contributors can create an experiment, create or attach a compute cluster, submit a run, and deploy a web service.
Owner	Full access to the workspace, including the ability to view, create, edit, or delete (where applicable) assets in a workspace. Additionally, you can change role assignments.

Authorization

Define custom roles for granular access

- Specify the definition for the custom role.
- Use the it to create the new custom role.
- Use ARM templates for repeatability for complex assignments

`data_scientist_custom_role.json` :

JSON Copy

```
{
    "Name": "Data Scientist Custom",
    "IsCustom": true,
    "Description": "Can run experiment but can't create or delete compute.",
    "Actions": ["*"],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/*/delete",
        "Microsoft.MachineLearningServices/workspaces/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/delete",
        "Microsoft.Authorization/*/write"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>/resourceGroups/<resource_group_name>/providers/
    Microsoft.MachineLearningServices/workspaces/<workspace_name>"
    ]
}
```

Azure CLI

```
az role definition create --role-definition data_scientist_role.json
```

- Can be made available at:
  - ML workspace
  - Resource group
  - Subscription

JSON

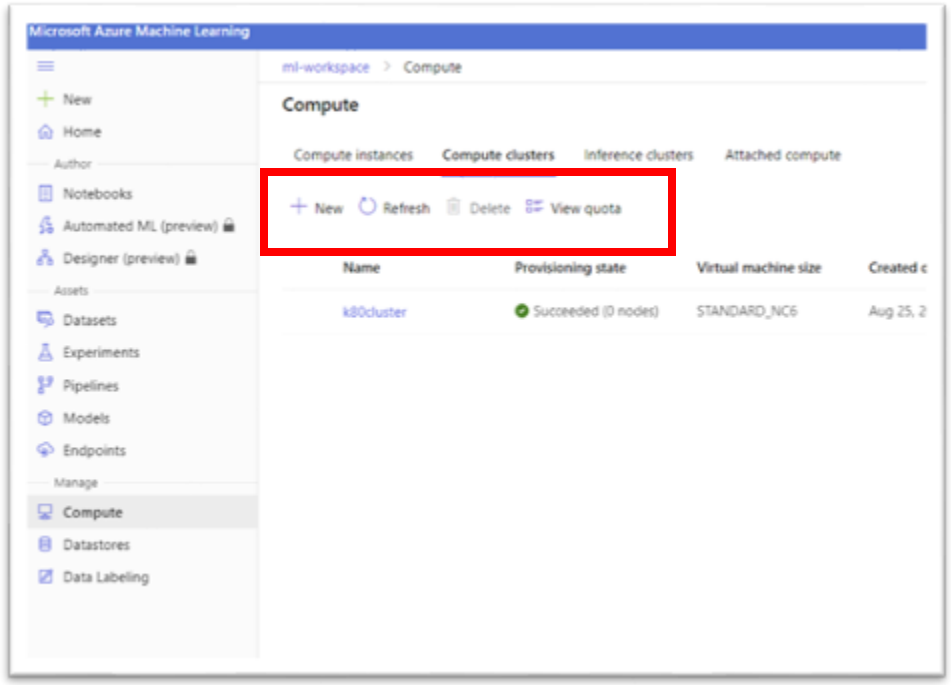
Copy

```
{
    "Name": "MLOps Custom",
    "IsCustom": true,
    "Description": "Can run pipelines against a published pipeline endpoint",
    "Actions": [
        "Microsoft.MachineLearningServices/workspaces/read",
        "Microsoft.MachineLearningServices/workspaces/endpoints/pipelines/read",
        "Microsoft.MachineLearningServices/workspaces/metadata/artifacts/read",
        "Microsoft.MachineLearningServices/workspaces/metadata/snapshots/read",
        "Microsoft.MachineLearningServices/workspaces/environments/read",
        "Microsoft.MachineLearningServices/workspaces/metadata/secrets/read",
        "Microsoft.MachineLearningServices/workspaces/modules/read",
        "Microsoft.MachineLearningServices/workspaces/components/read",
        "Microsoft.MachineLearningServices/workspaces/datasets/*/read",
        "Microsoft.MachineLearningServices/workspaces/datastores/read",
        "Microsoft.MachineLearningServices/workspaces/environments/write",
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/read",
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/write",
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/submit/action",
        "Microsoft.MachineLearningServices/workspaces/experiments/jobs/read",
        "Microsoft.MachineLearningServices/workspaces/experiments/jobs/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/artifacts/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/snapshots/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/codes/*/write",
        "Microsoft.MachineLearningServices/workspaces/environments/build/action",
    ],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/computes/write",
        "Microsoft.MachineLearningServices/workspaces/write",
        "Microsoft.MachineLearningServices/workspaces/computes/delete",
        "Microsoft.MachineLearningServices/workspaces/delete",
        "Microsoft.MachineLearningServices/workspaces/computes/listKeys/action",
        "Microsoft.MachineLearningServices/workspaces/listKeys/action",
        "Microsoft.Authorization/*"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>"
    ]
}
```

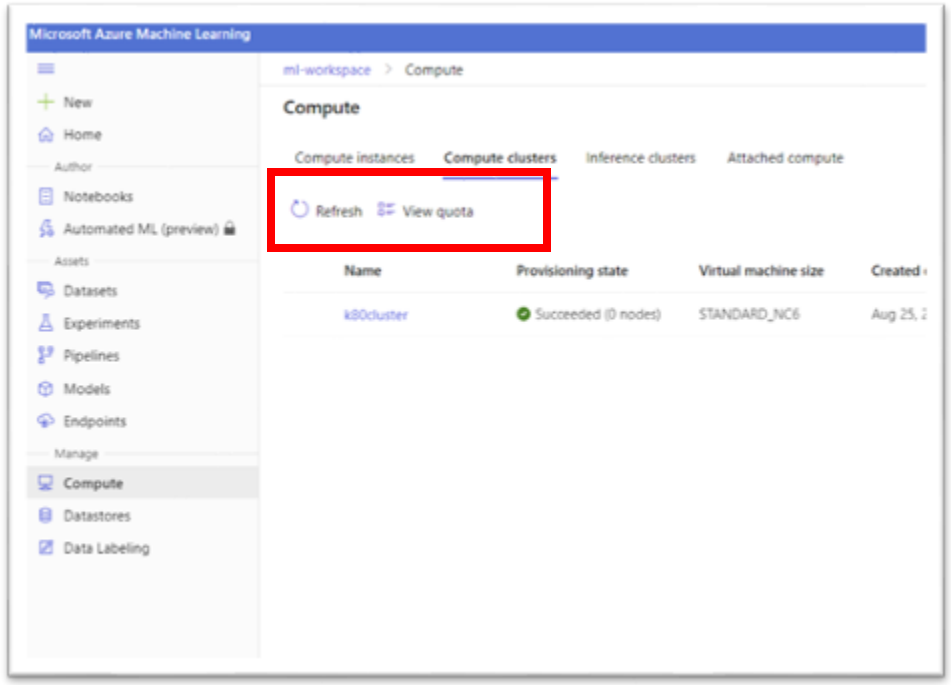
Authorization

RBAC user experience

Project Manager Experience



Data Scientist Experience



Workspace access management

IAM patterns

Self-service pattern

Data-centric pattern

Project-centric pattern

[Machine learning enterprise security - Cloud Adoption Framework | Microsoft Learn]

IAM Recap

Secure access to deployed resources :

- Storage Account
- Key Vault
- ACR
- AML & Studio
- Training & inference ressources

MI

Managed Identities everywhere

AuthN

Authenticate requests

RBAC

Least Privilege

Centralize identities

- Use system managed identities whenever possible (compute)
- Assign only required roles/permissions to MIs
- Review and reconcile user access regularly
- Avoid using admin account to deploy services

Authenticate with Azure AD

- Configure Identity based access to Key Vault, SA and ACR (instead of credential based)
- Use Azure AD authentication for access to Web Services
- No secrets in code : avoid handling access keys or Service Principals in entry script or elsewhere


Secure Network

Secure network overview

Use cases and main services

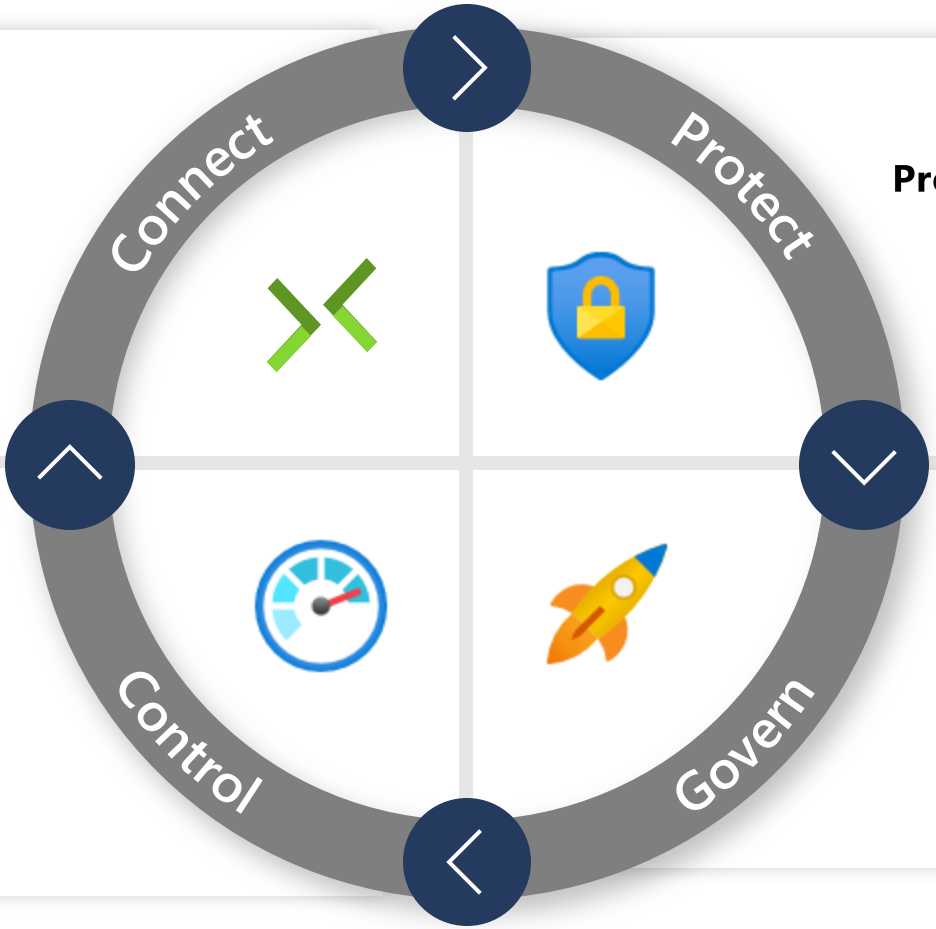
Restrict access to resources:

Virtual Network, subnets

Private Endpoints/Private Link

Service endpoints

ExpressRoute, VPN



Protect endpoints & apps from attacks:

DDoS Protection

Azure WAF

Control traffic flows:

Network Security Groups

Network Watcher

Azure Monitor

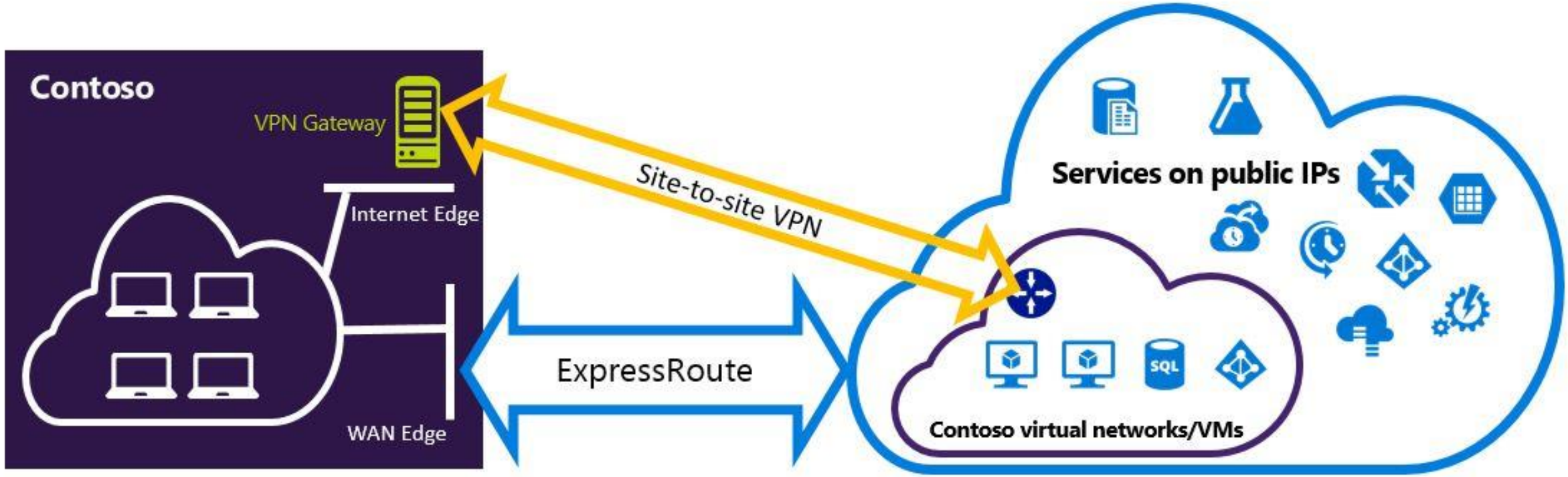
Prevent & stop data exfiltration:

Azure Firewall

Azure Bastion

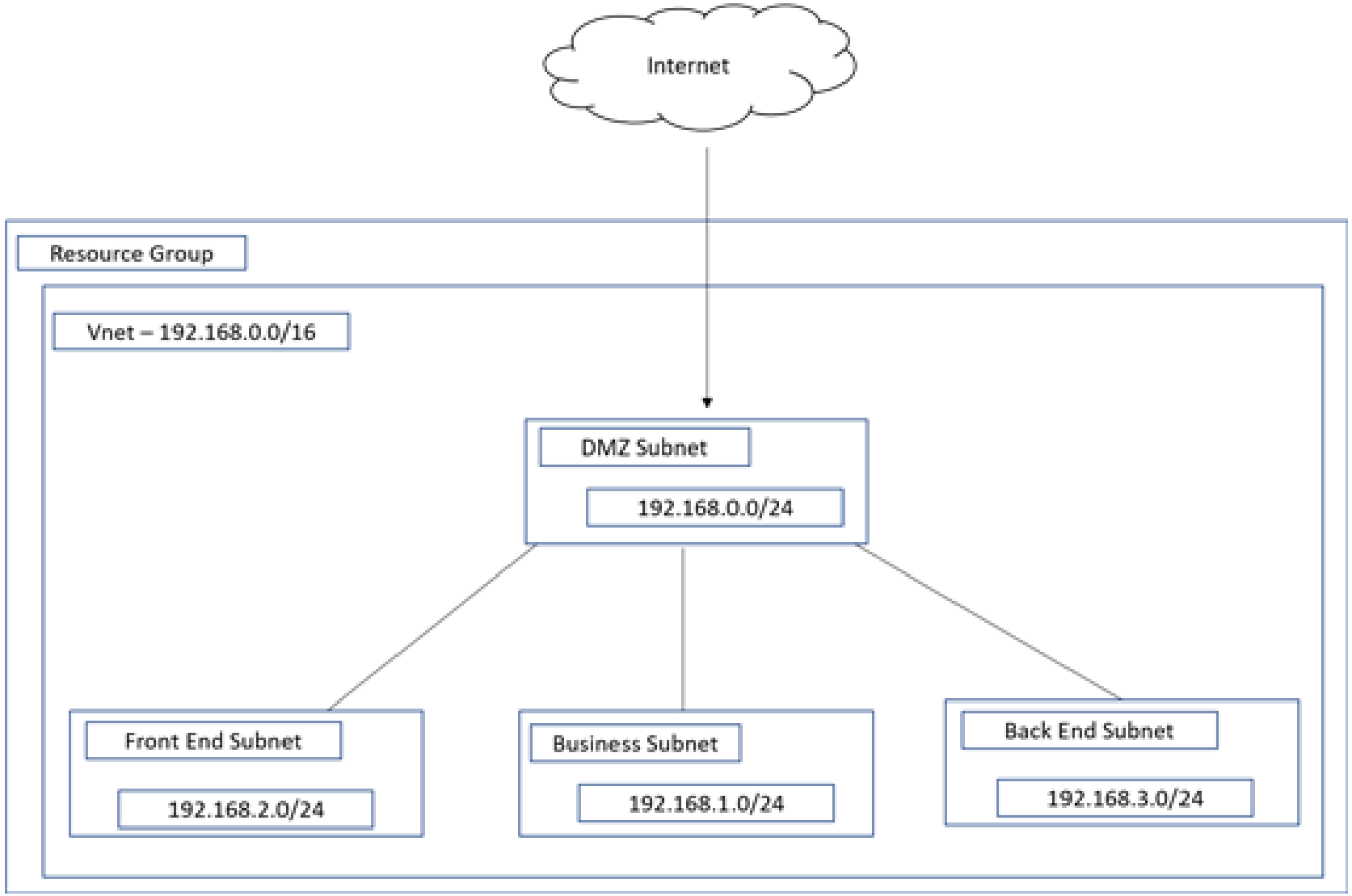
Azure networking concepts

ExpressRoute & VPN



Azure networking concepts

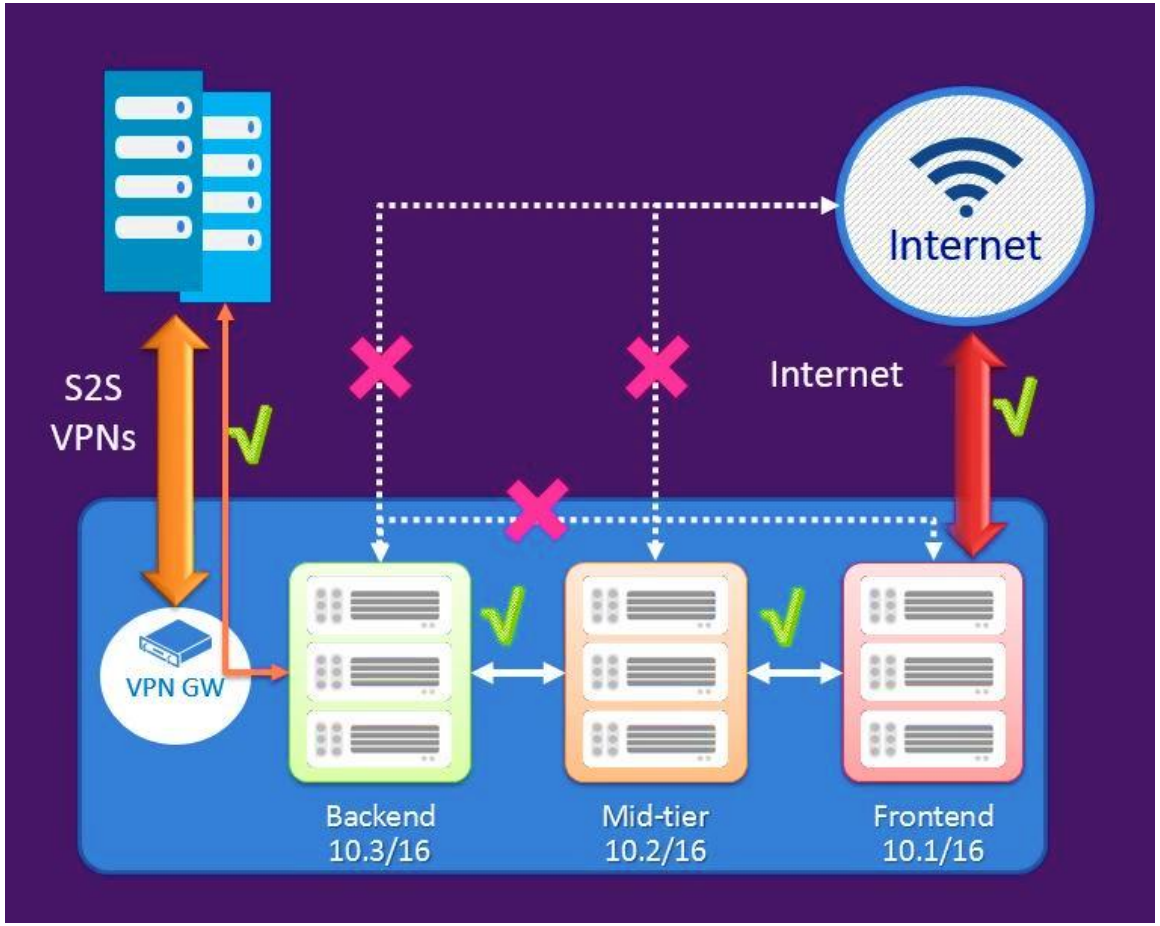
Vnet & Subnet



Azure networking concepts

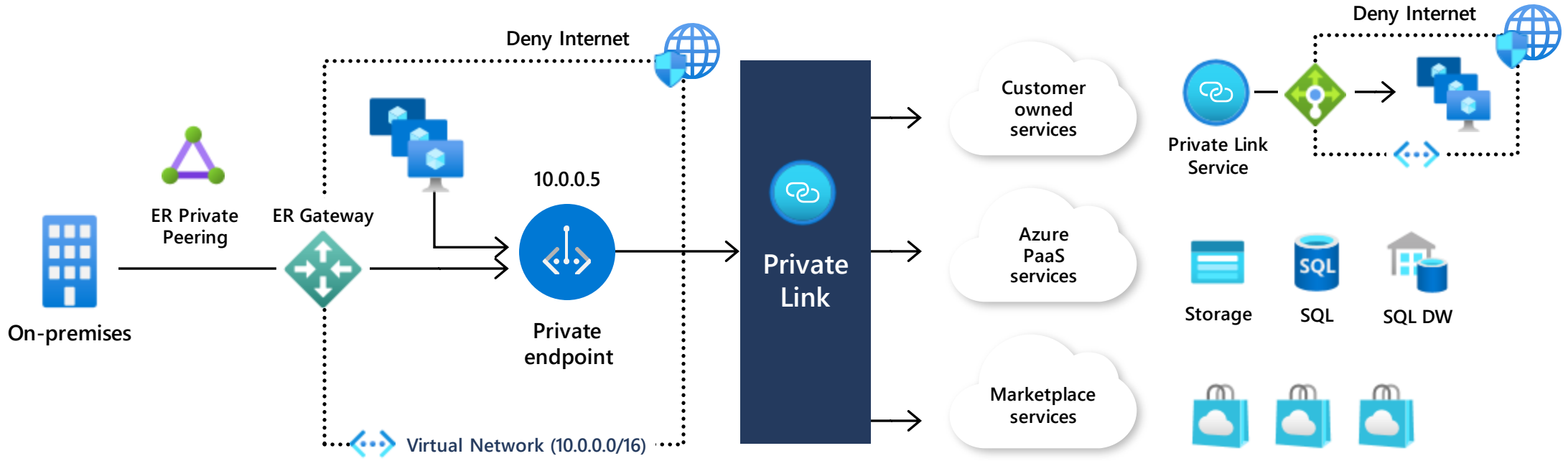
Network Security Groups

- **Group of rules to filter inbound and outbound traffic.**
  - 200+ rules per group.
- **Attached to :**
  - A Virtual Machine (Network Interface)
  - A subnet
  - Both
- **Rules based on 5-Tuples**
  - Source IP Address
  - Source Port
  - Destination IP Address
  - Destination port
  - Protocol (TCP or UDP)
- **Tags :** Internet , Load Balancer , Virtual Network
- NSG rules are **stateful**



Azure networking concepts

Private endpoint and Private Link



Private access from Virtual Network resources, peered networks and on-premise networks	In-built Data Exfiltration Protection	Predictable private IP addresses for PaaS resources	Unified experience across PaaS, Customer Owned and marketplace Services

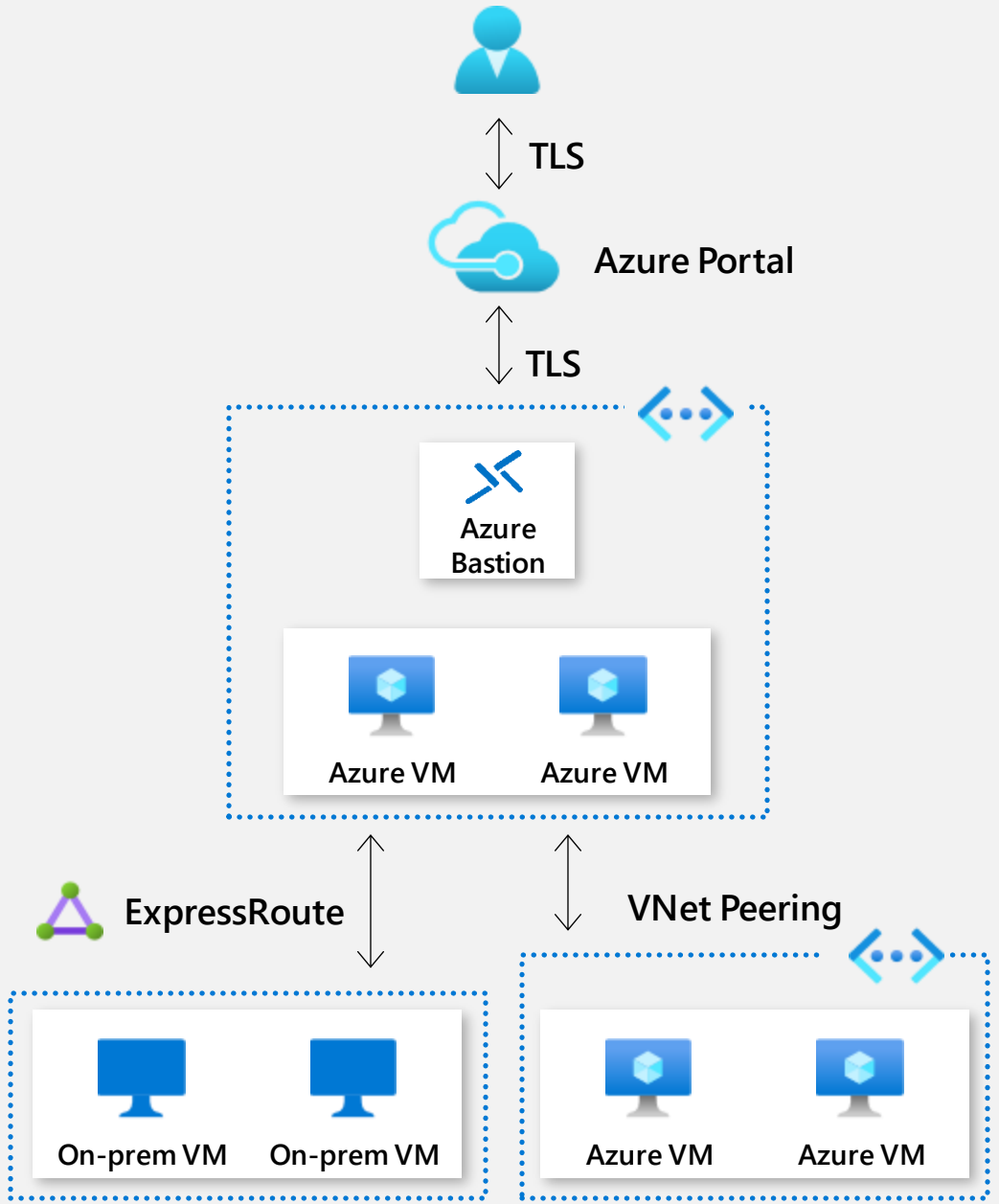
Azure networking concepts

Azure Bastion

Fully managed with autoscaling and hardened PaaS service to securely access virtual machines through a single access point

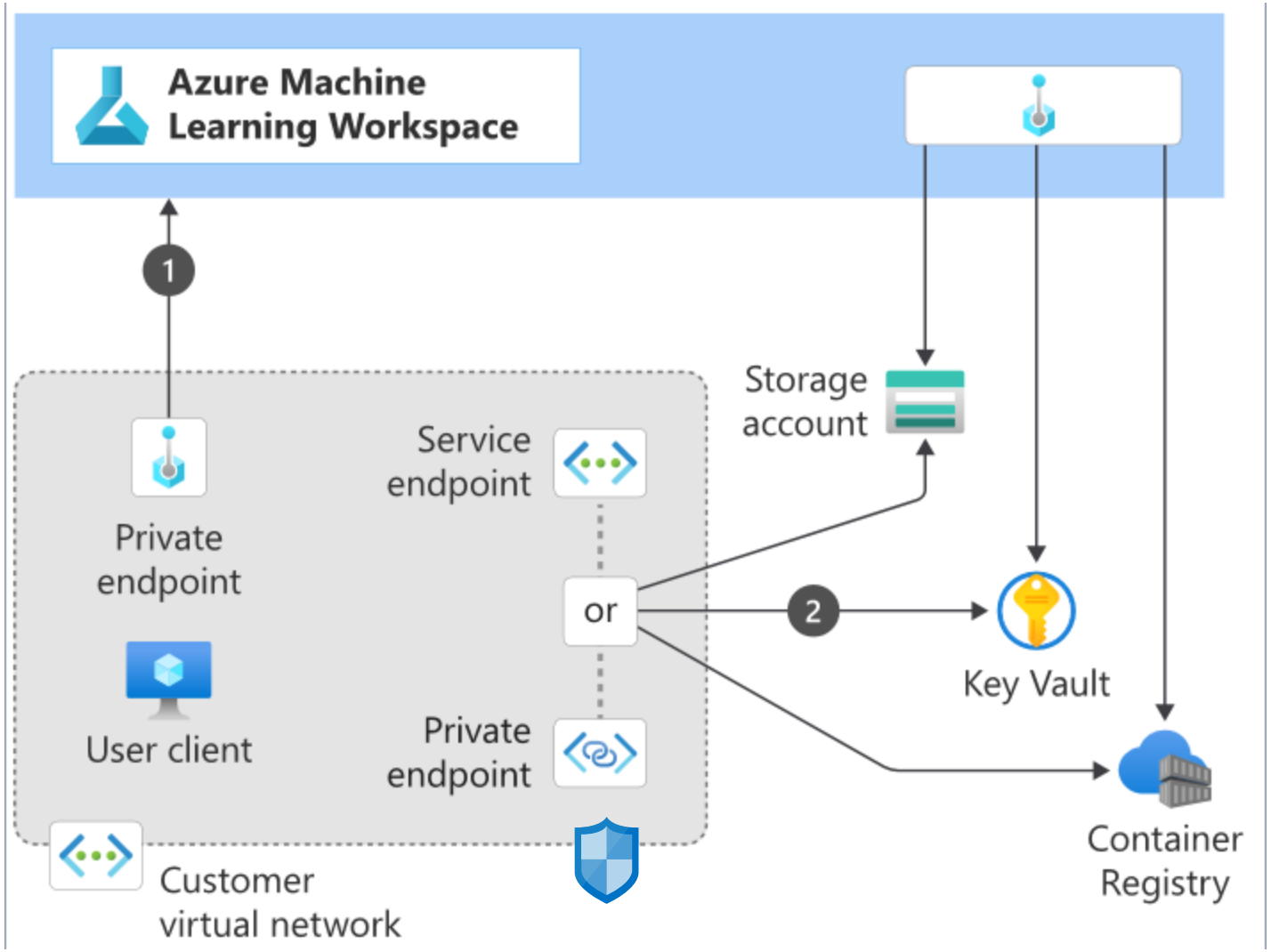
Secure RDP/SSH to Azure VMs over SSL using Private IP

Single click experience to log into your Azure virtual machines and avoid public Internet exposure



Secure network

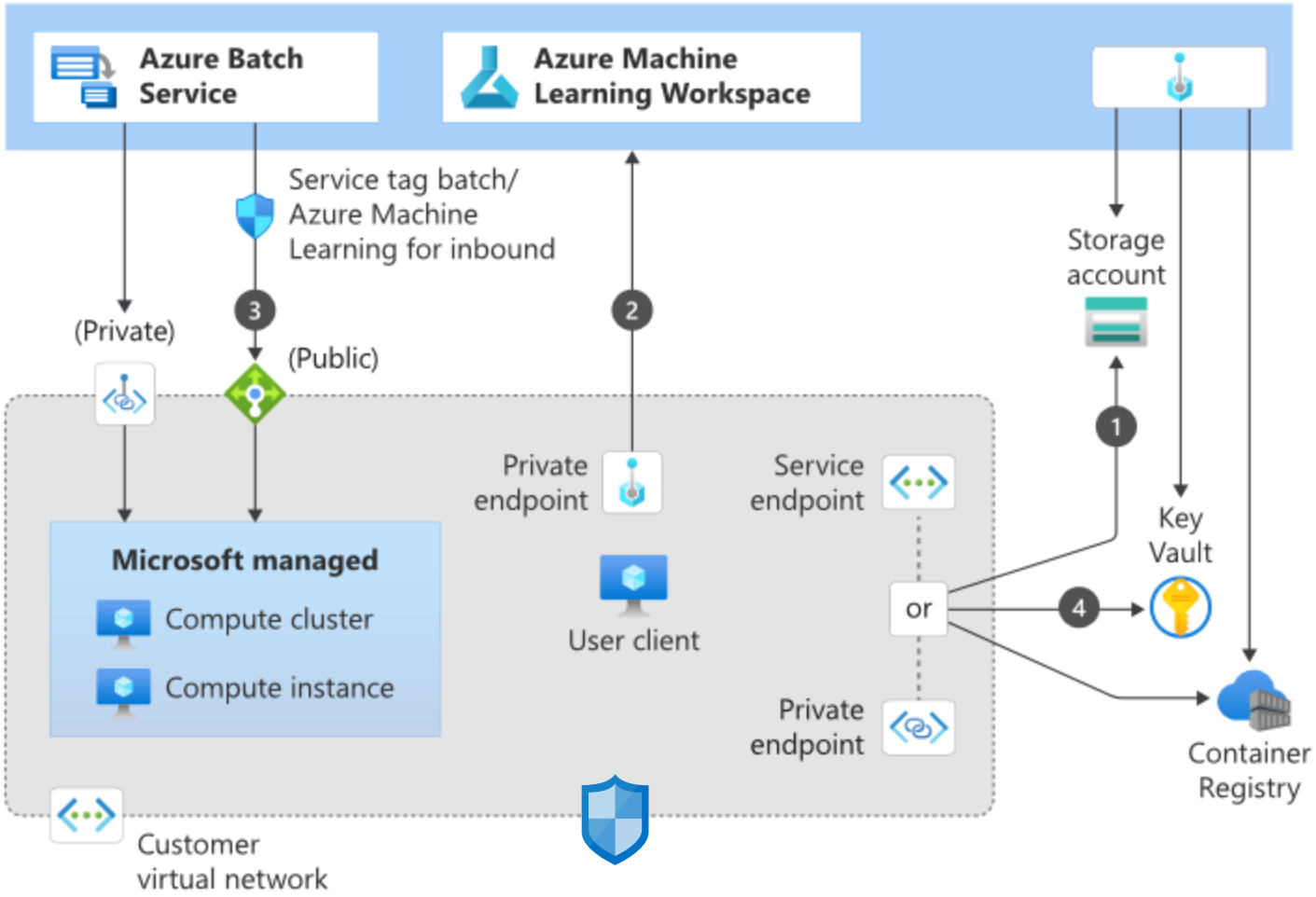
Create a private workspace



- Custom **Vnet**
- **Private endpoint** to workspace (1)
- Private endpoints for connected resources: SA, KV, ACR (2)
- **VPN** or **ExpressRoute** for Onprem connectivity
- **Bastion** for remote access
- **Subnets** for workspace, training, inference, user-VMs and bastion

Secure network

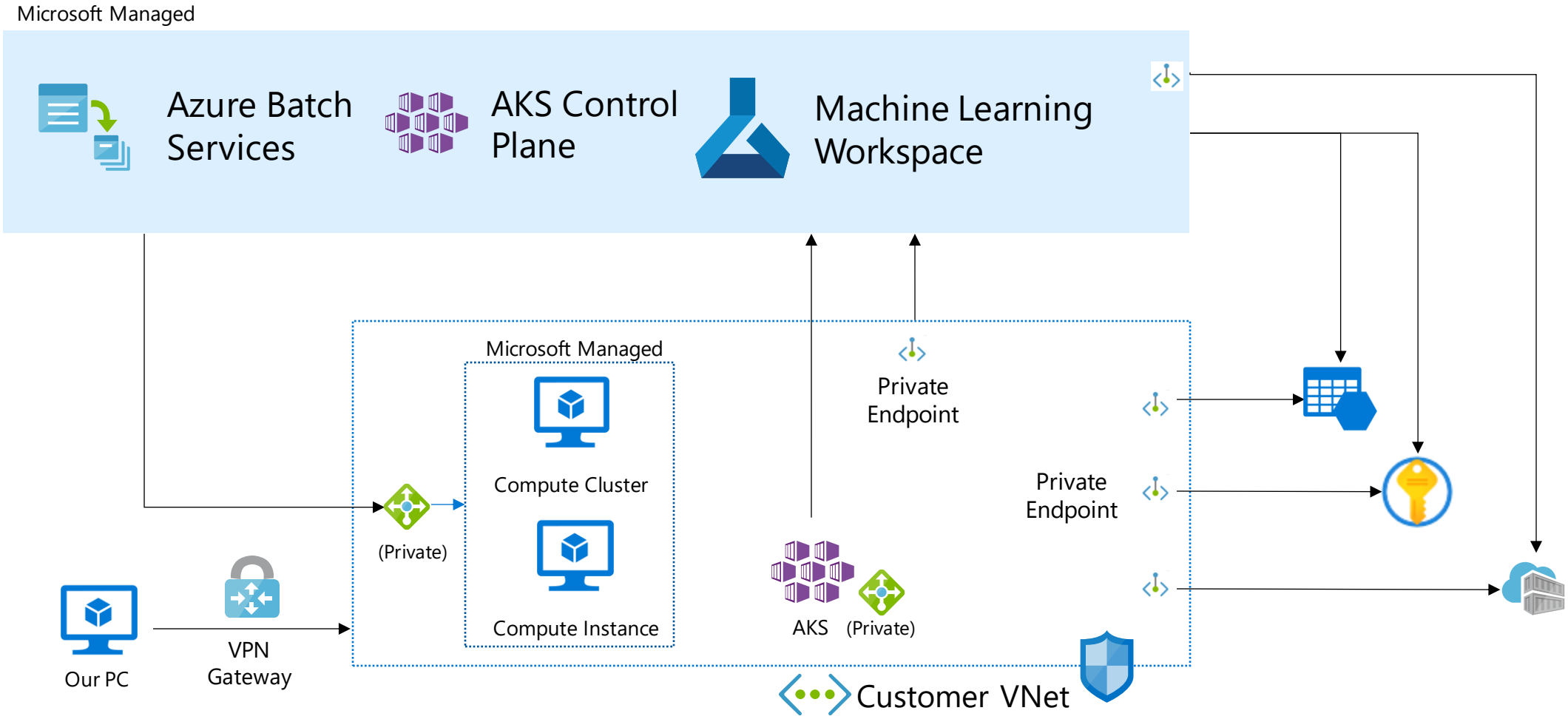
Isolate the training environment



- 0. Data-scientist connects to AML client (Studio, SDK, API)
- 1. Client uploads training scripts & data
- 2. Client submits training job to AML workspace
- 3. Azure Batch service receives training job & submits it to compute resource
- 4. Compute resource receives begins training & securely downloads required files.

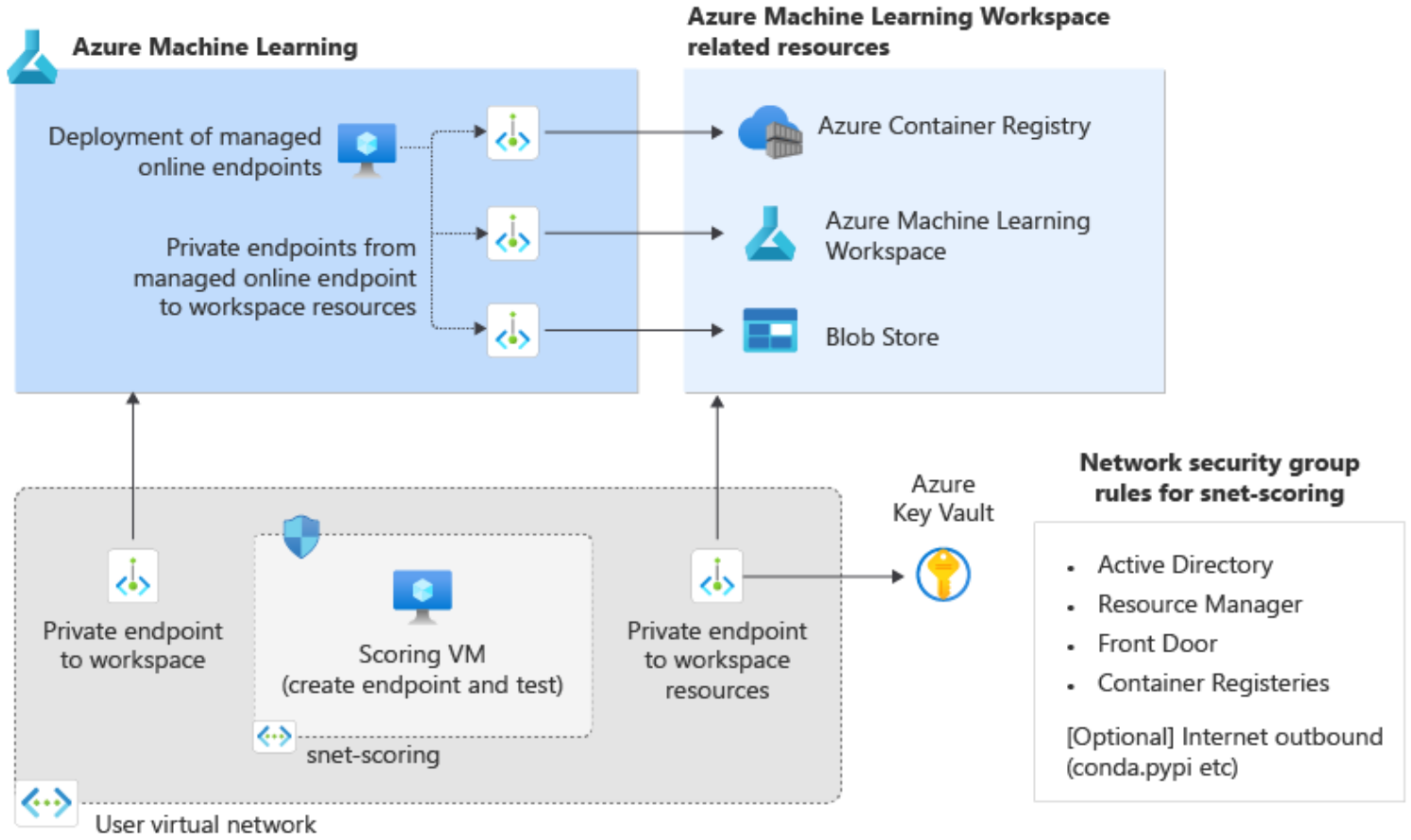
Secure network

Isolate the inferencing environment : AKS use case



Secure network

Isolate the inferencing environment : Managed Online Endpoint use-case (**public preview**)

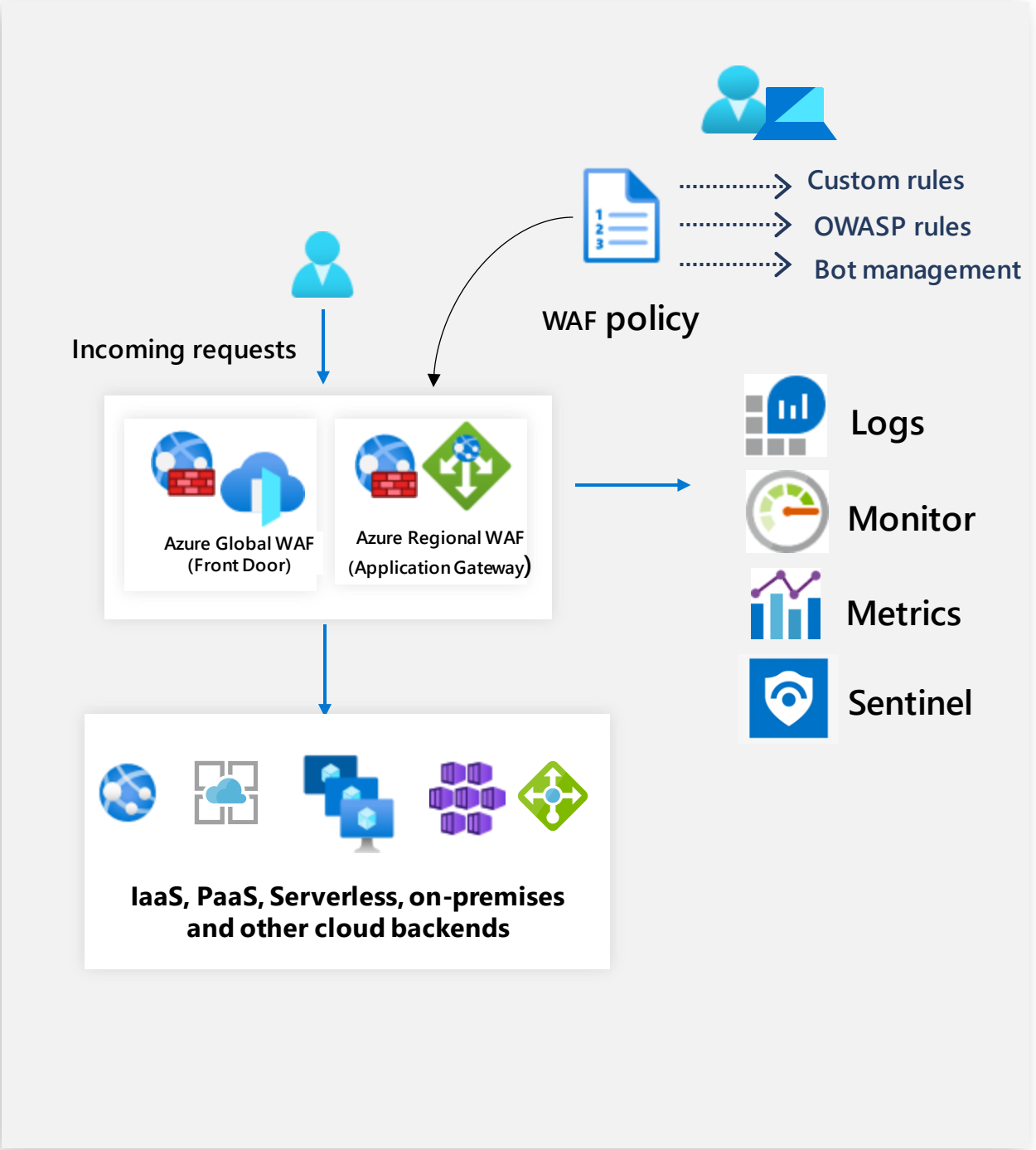


- **Inbound** requests from client to **online endpoint** go through workspace private endpoint in the customer vnet
- **Outbound** communications between **deployment** and Azure resources go through their respective private endpoints.

Secure network

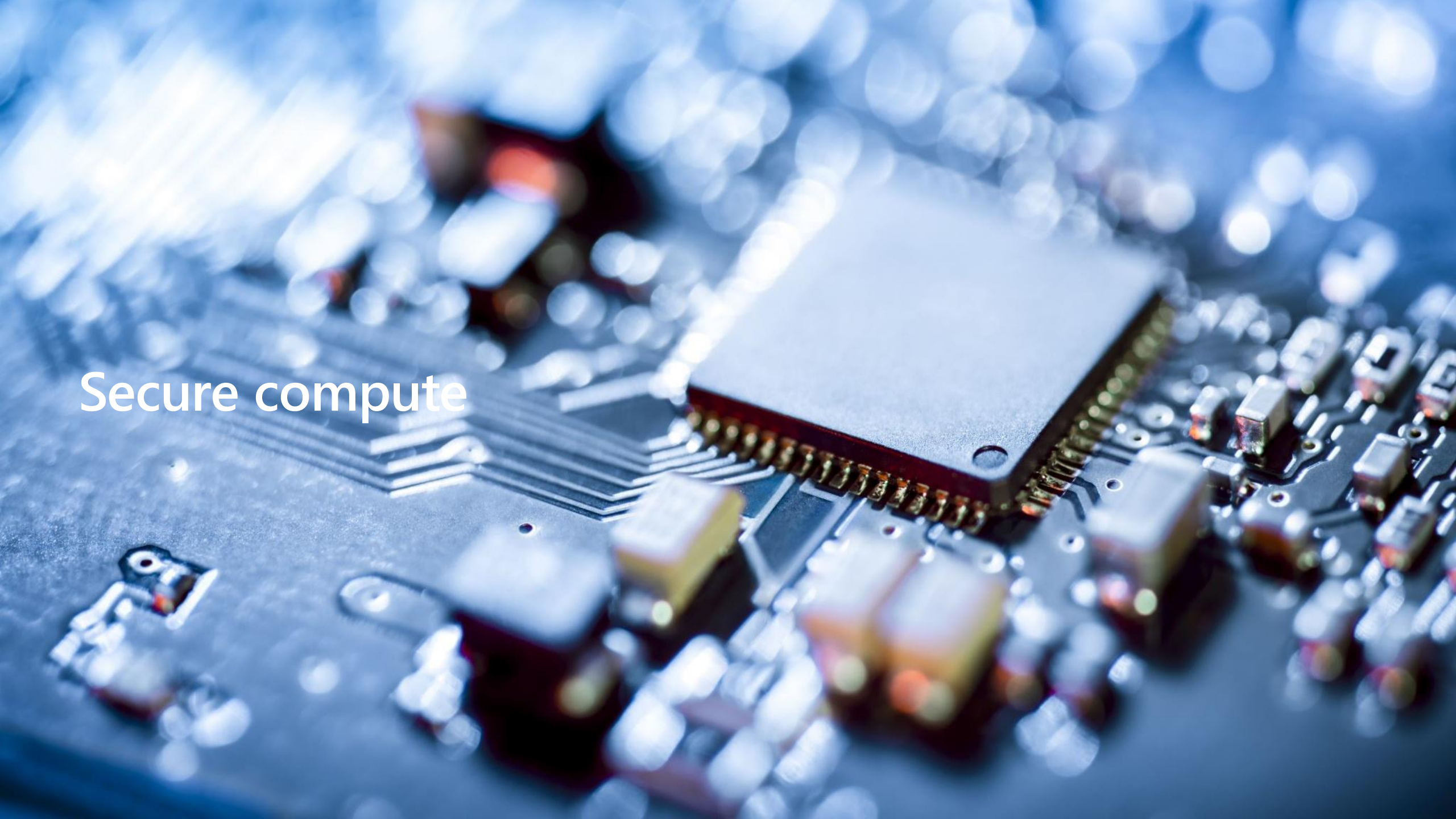
Protect public endpoints with Azure WAF

- ✓ **Powerful custom rules engine**
  - Geo-filtering
  - IP Restriction
  - HTTP Parameter Filtering
  - Size Restriction
- ✓ **Conditional rate limiting at Azure network edge**
- ✓ **Preconfigured OWASP top 10**
- ✓ **Bot protection integration with Microsoft Threat Intelligence**
- ✓ **Easy configuration: ARM, Portal, API, PS, CLI, Terraform**



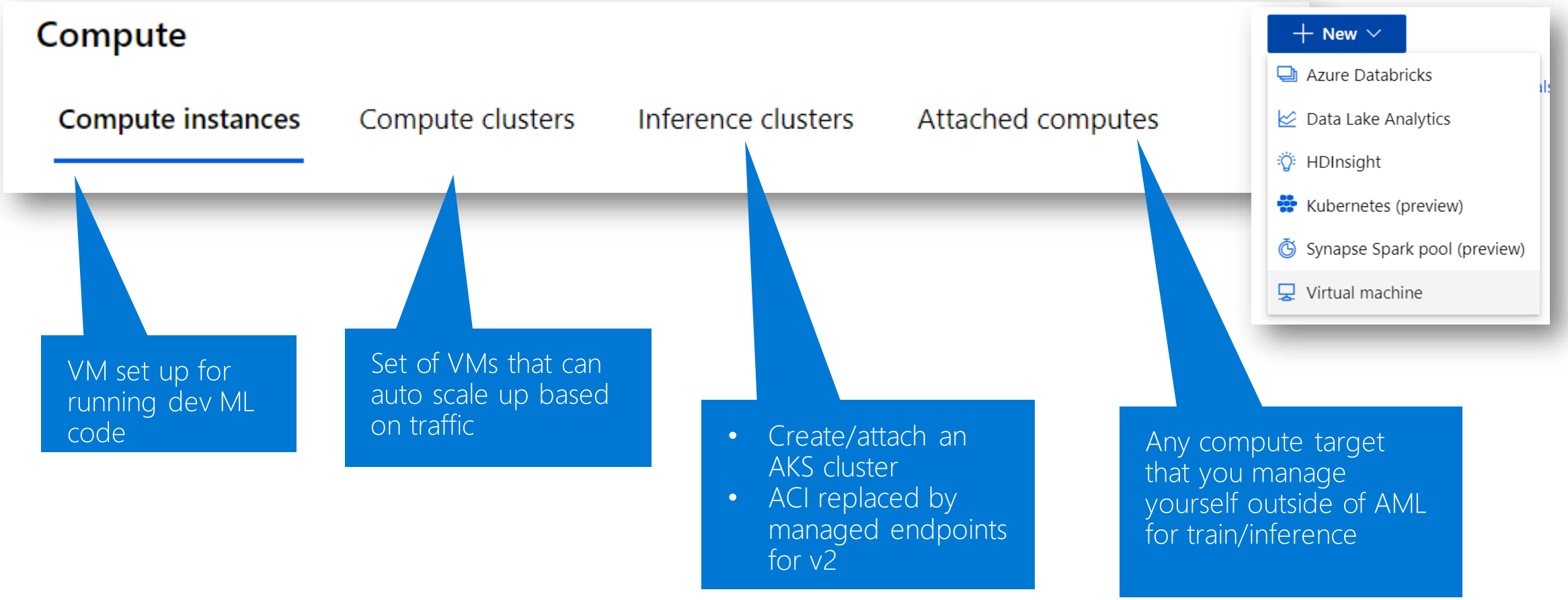
Network Recap

- Create a **private workspace**
  - Deploy **private endpoint** in vnet
  - Integrate with **private DNS zones**
  - Access Studio via **VPN** or **Express Route** from internal network on premise or private Azure VM behind a **Bastion**
- Configure **private exposition** for KeyVault, Storage Account & ACR
- Configure private exposition of Compute resources
- Configure private exposition of ML endpoints when public access is not needed
- Enforce **TLS >=1.2** to encrypt data in transit
- Add **WAF** in front of public web services


Secure compute

Secure compute

Compute options



Secure Compute

- ✓ Compute
  - ✓ Latest patches and checks for vulnerability
  - ✓ MS managed: Updated and released monthly
  - ✓ AML checks and validates any machine learning packages that may require an upgrade

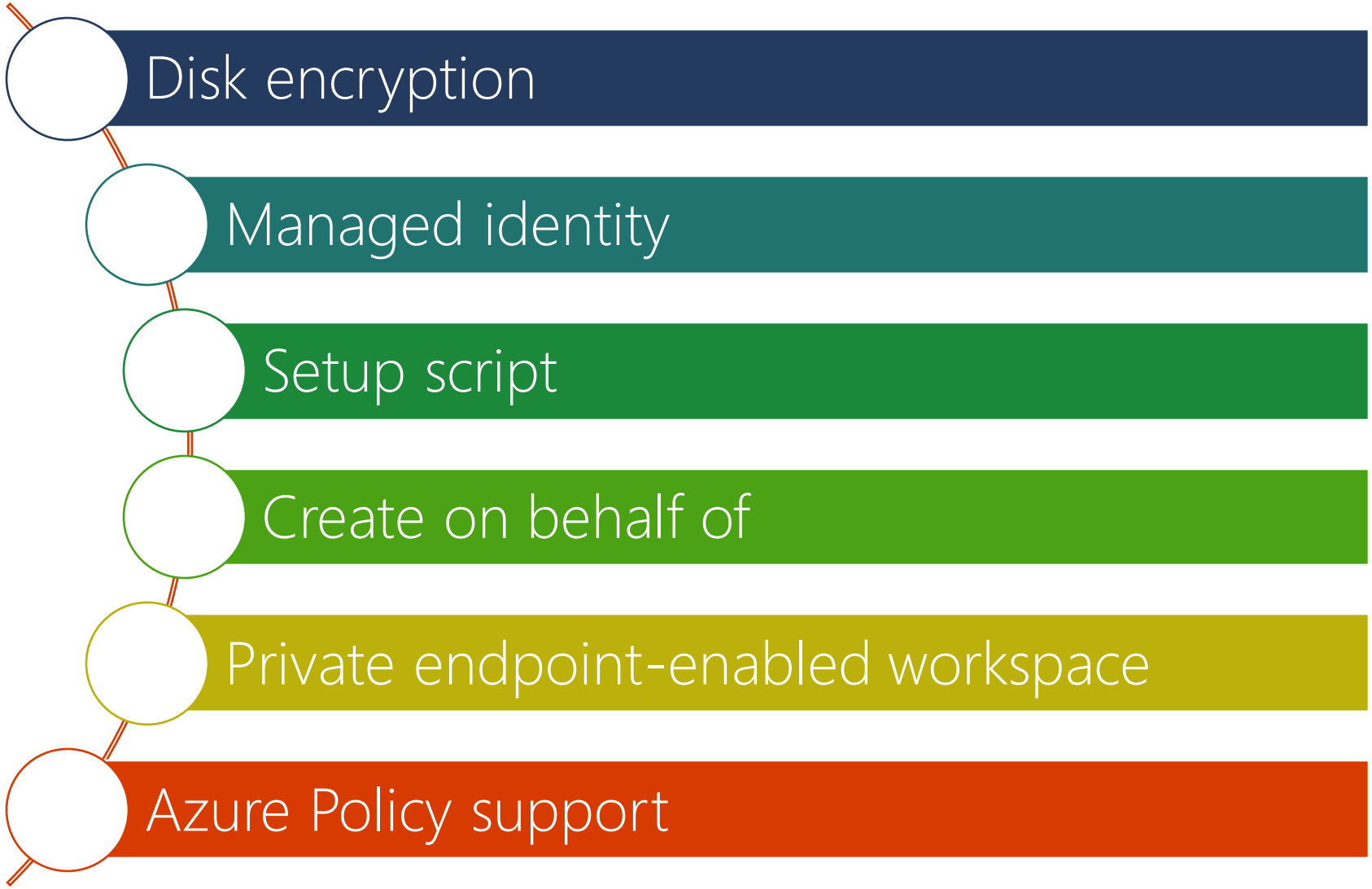
- ✓ Managing environments and container images:
  - ✓ Managed images get frequent security patches to address vulnerabilities
  - ✓ You are responsible for vulnerability once you customize images
  - ✓ Manage deletion of images over time

- ✓ You can deploy a compute cluster or compute instance in your virtual network and configure NSGs or use user defined routing

- ✓ Preview – Deploy no public IP compute

Secure AML compute

Considerations/Recommendations



Secure compute

Set up managed identity

- For compute clusters/ Instances [Preview]
- 1 system assigned or multiple user-assigned

System-assigned	User-assigned
Enabled directly on the compute cluster	Created as a stand-alone Azure resource.
Shared life cycle with the compute cluster.	Independent life cycle.
Can't be shared. Associated to a single resource	Can be shared across many Azure resources.

Create compute cluster

Virtual Machine

Advanced Settings

Configure Settings

Configure compute cluster settings for your selected virtual machine size.

Name	Category	Cores	Available quota	RAM	Storage	Cost/Node
Standard_DS3_v2	General purpose	4	66 cores	14 GB	28 GB	$0.29/hr

Compute name *

cpu-cluster-eastus

Minimum number of nodes *

0

Maximum number of nodes *

4

Idle seconds before scale down *

120

Enable SSH access

Authentication type

SSH public key Admin password

Admin username *

azureuser

SSH public key source *

Generate new key pair

Key pair name *

Advanced settings

Enable virtual network

Assign a managed identity

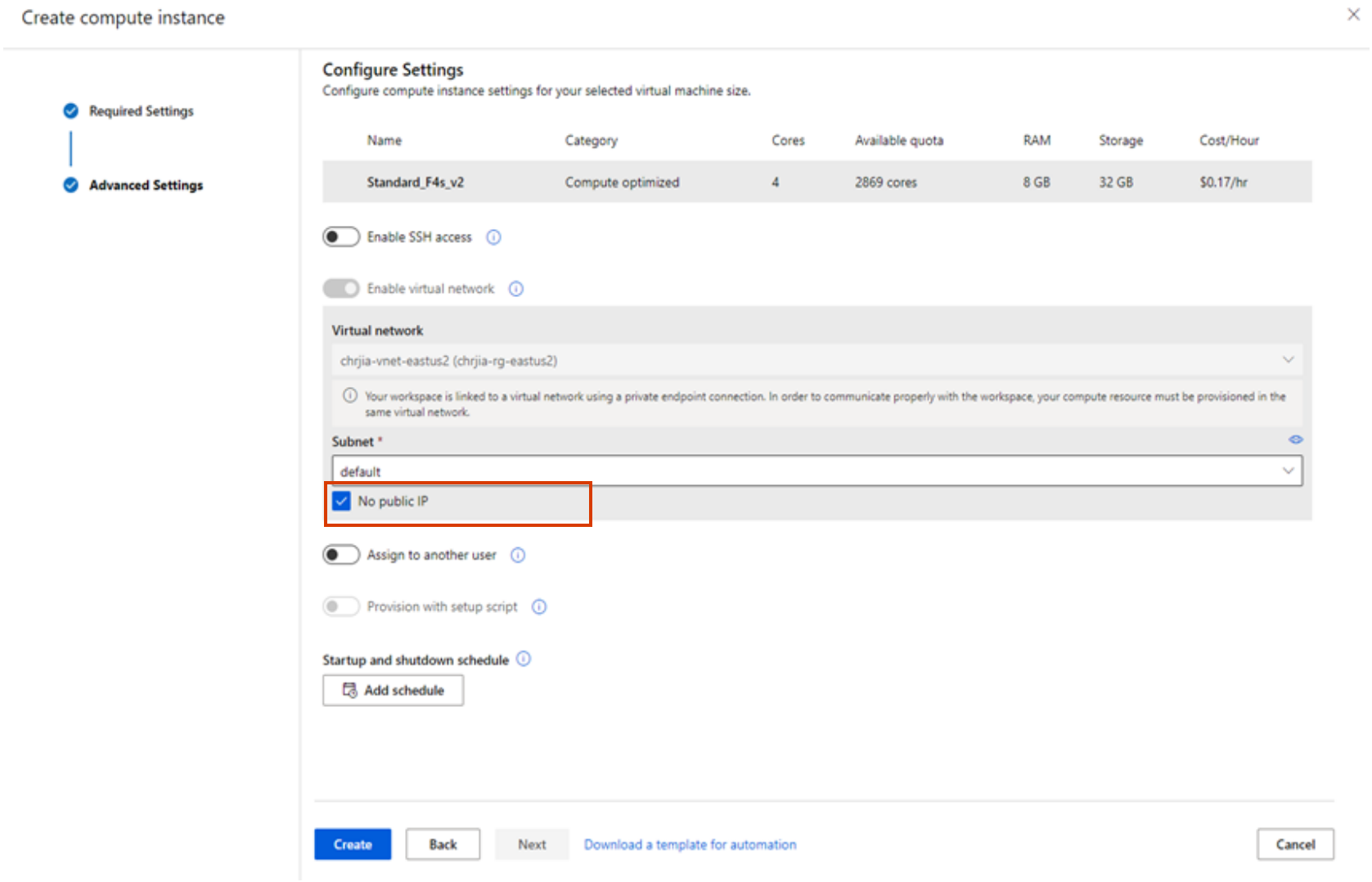
Identity type

System-assigned User-assigned

Secure compute

No Public IP Compute Clusters and Instances - Preview

[Secure training environments with virtual networks - Azure Machine Learning | Microsoft Learn]



Compute Recap

Use Managed compute ressources with automated security updates

Create a jumpbox for secure access to compute nodes & Studio

Enable **Azure Disk Encryption** on custom compute resources

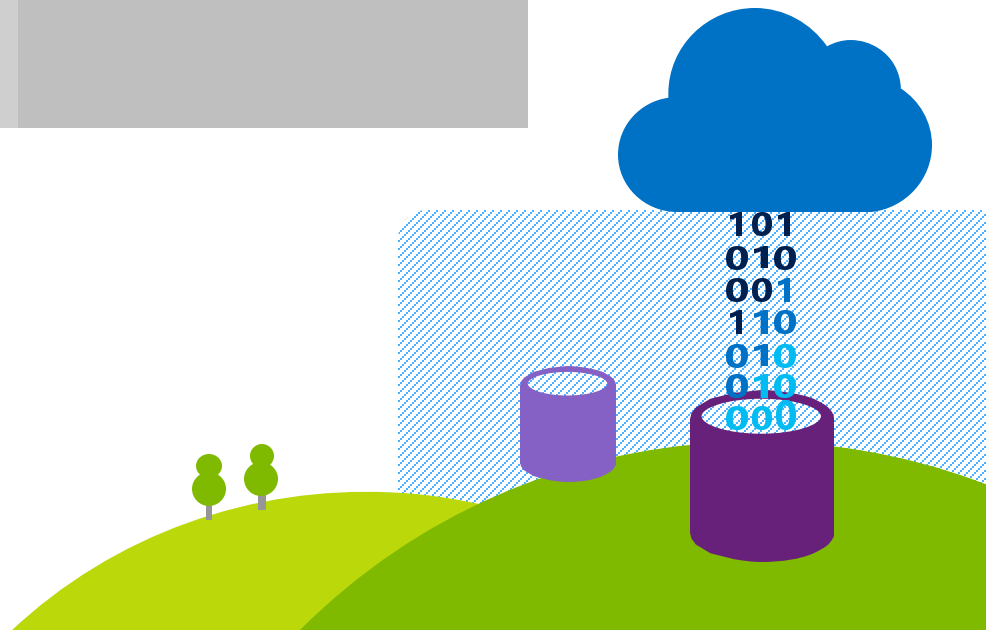
Here's a comparison of Disk Storage SSE, ADE, encryption at host, and Confidential disk encryption.

	Encryption at rest (OS and data disks)	Temp disk encryption	Encryption of caches	Data flows encrypted between Compute and Storage	Customer control of keys	Does not use your VM's CPU	Works for custom images	Enhanced Key Protection	Microsoft Defender for Cloud disk encryption status
Azure Disk Storage Server-Side Encryption at rest	✅	❌	❌	❌	✅ When configured with DES	✅	✅	❌	Unhealthy, not applicable if exempt
Azure Disk Encryption	✅	✅	✅	✅	✅	❌	❌ Does not work for custom Linux images	❌	Healthy
Encryption at Host	✅	✅	✅	✅	✅	✅	✅	❌	Unhealthy, not applicable if exempt
Confidential disk encryption	✅ For the OS disk only	❌	✅ For the OS disk only	✅ For the OS disk only	✅ For the OS disk only	❌	✅	✅	Unhealthy, not applicable if exempt


Secure data

Data protection

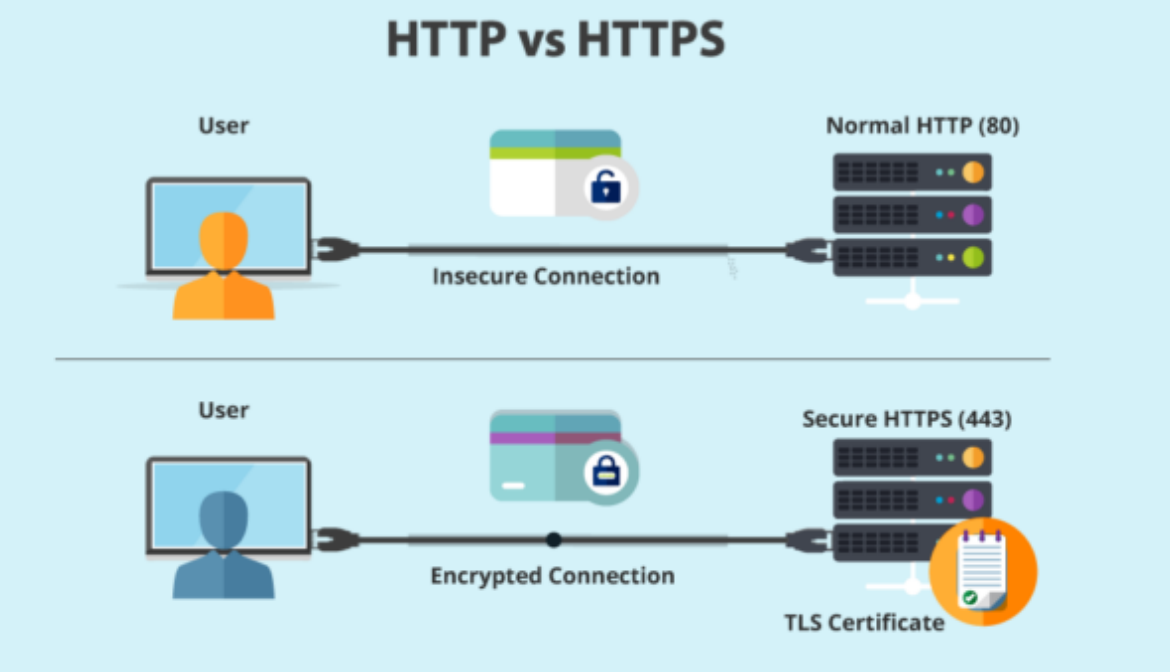
Encryption for data in transit	Encryption for data at rest	Securing data in use	Data segregation
Industry standard SSL/TLS protocols are used for encrypting data in transit	Customers can implement a range of encryption options for virtual machines and storage	Confidential computing protects data in use while in RAM and during computation	Employ logical isolation and access controls



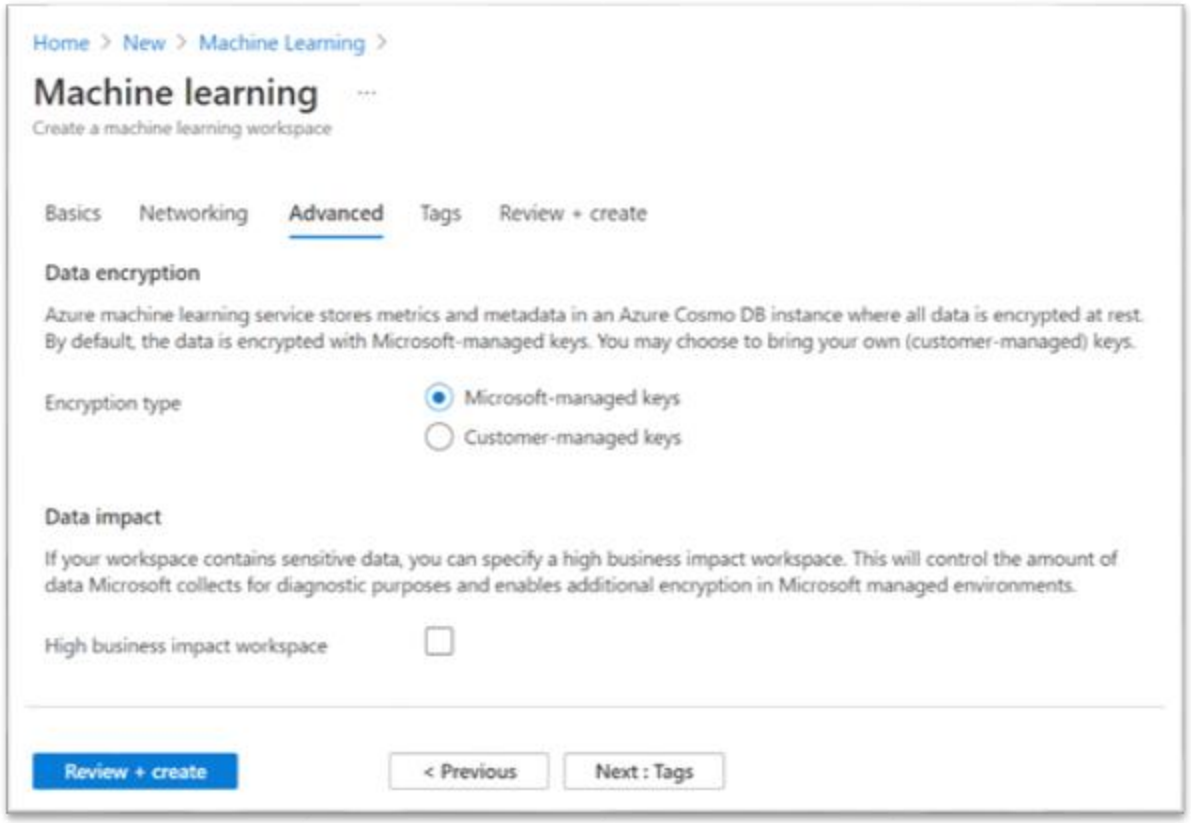
Secure data
Encryption in transit

All internal communication between Azure Machine Learning services are secured using TLS

To secure external calls made to the **inferencing endpoint**, use TLS 1.2+



Secure data
Azure Cosmos DB



- Stores metadata and is encrypted at rest with Microsoft-managed keys
- Can be encrypted using customer key
- Can use dedicated Cosmos DB to store run information
- Cosmos DB can be provisioned using customer key through SDK, CLI or REST APIs

Secure data

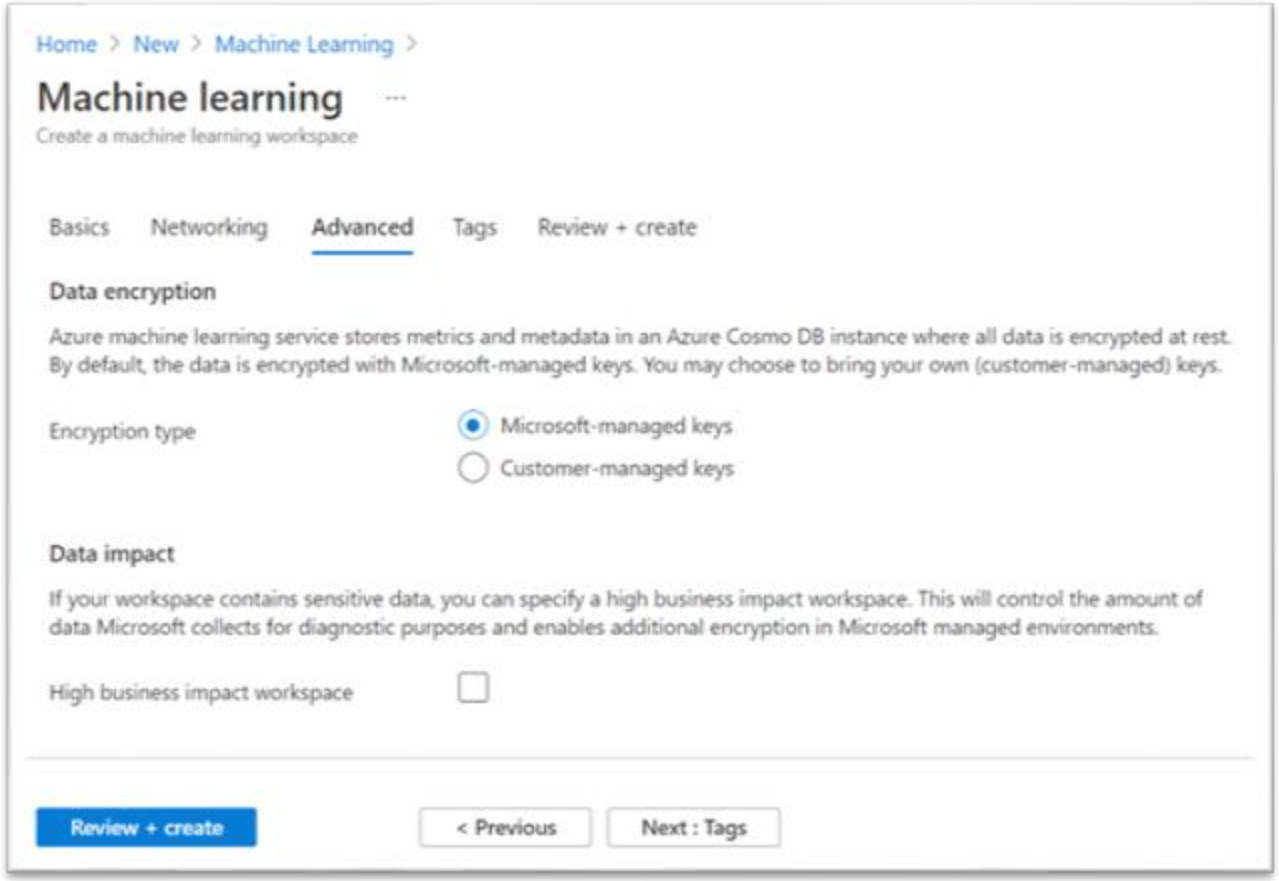
Data Collection and Handling

Non-user information like dataset name, experiment name, environment variables may be collected for diagnostic purposes

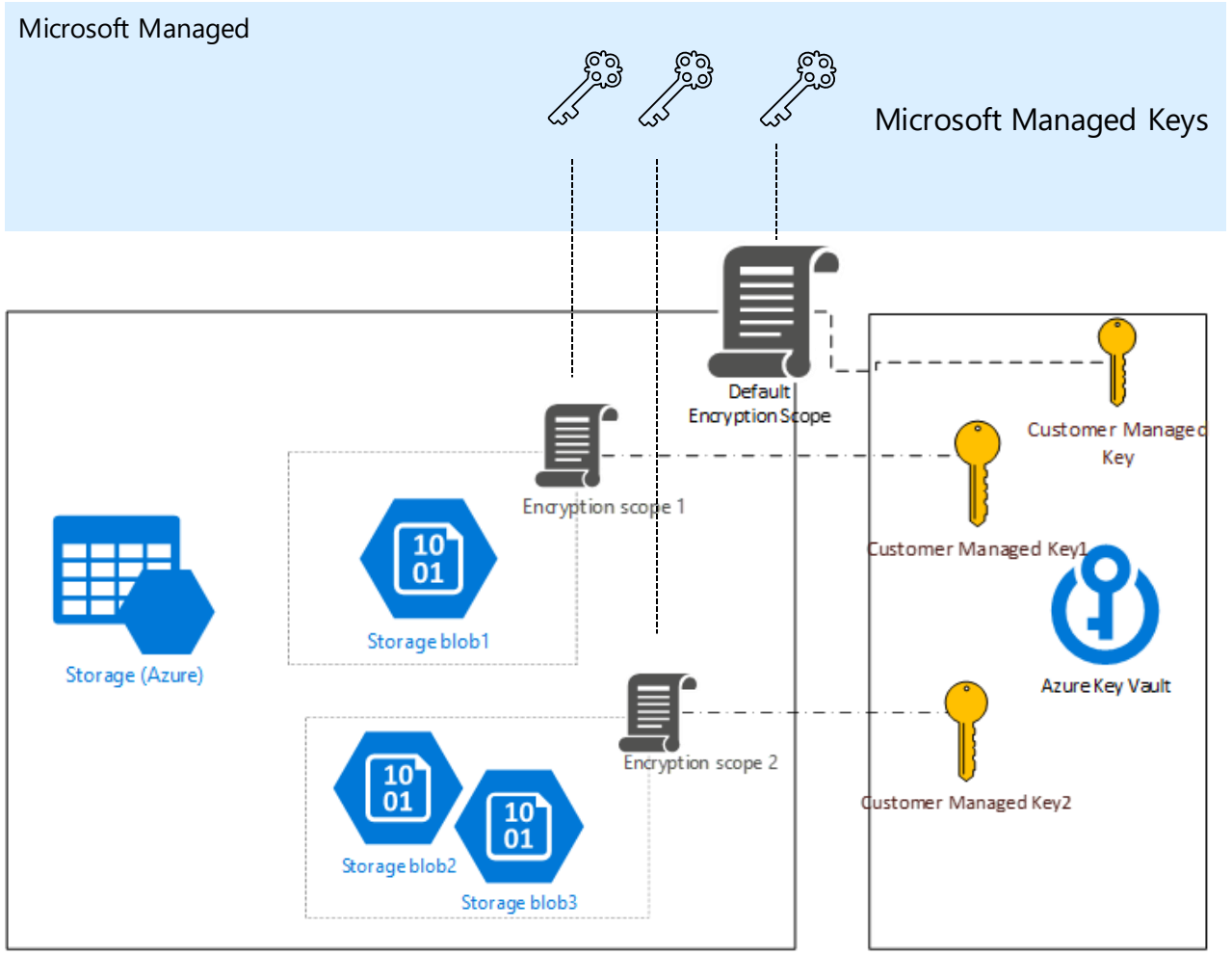
Collected data is stored using Microsoft-managed keys in Microsoft owned storage within same region as your workspace

Avoid storing sensitive information in environment variables which could appear in telemetry logs accessible to Microsoft Support engineers

Use **hbi_workspace** to opt out diagnostic data being collected by Microsoft



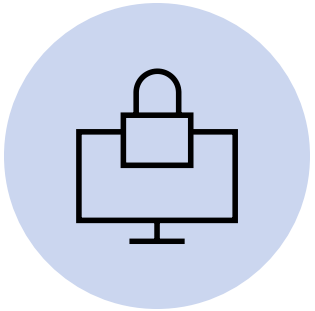
Secure data
Azure Blob Storage



- Snapshots, output and logs are stored in Azure Blob Storage
- All data is encrypted at rest with Microsoft-managed keys
- Azure Storage Blob can be encrypted using customer key
- Storage key can be rotated and revoked at any time. It usually takes an hour for the change to be effective
- Supports encryption scopes

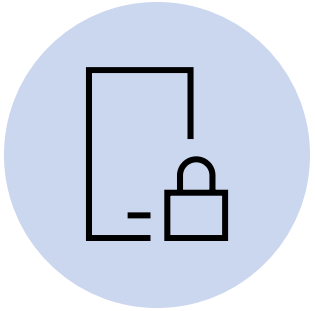
Secure data

Azure Container Registry / Azure Container Instance

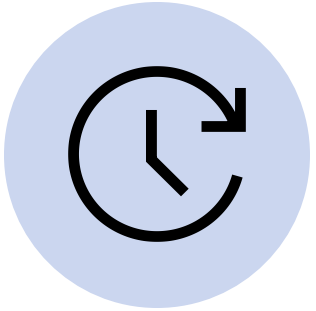


All container images are encrypted at rest

User-managed ACR can be used with customer-managed keys

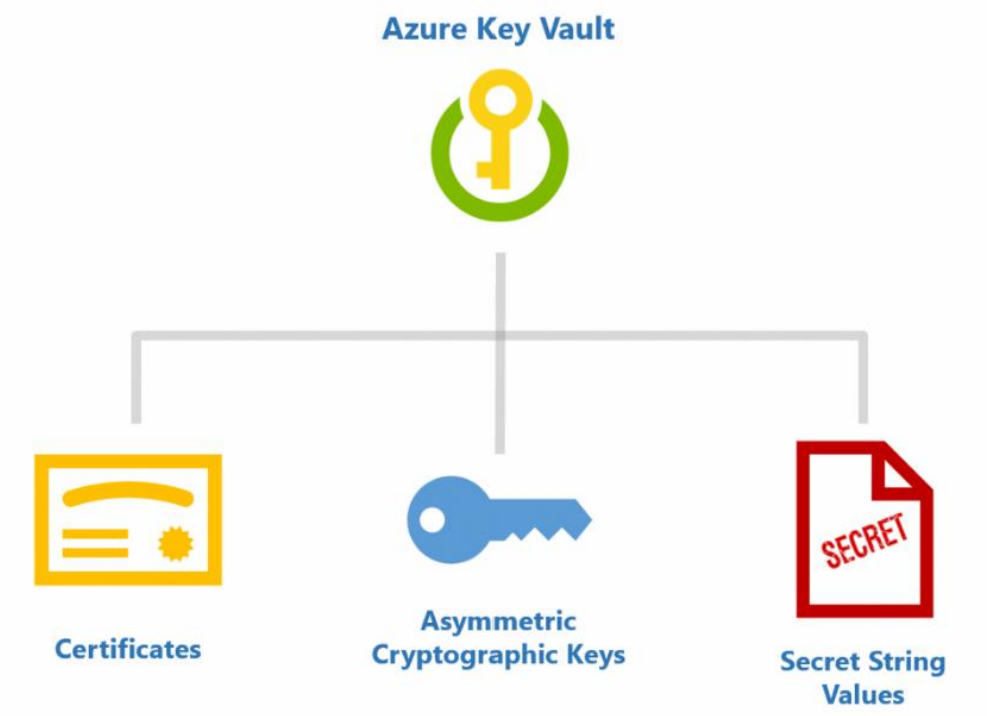


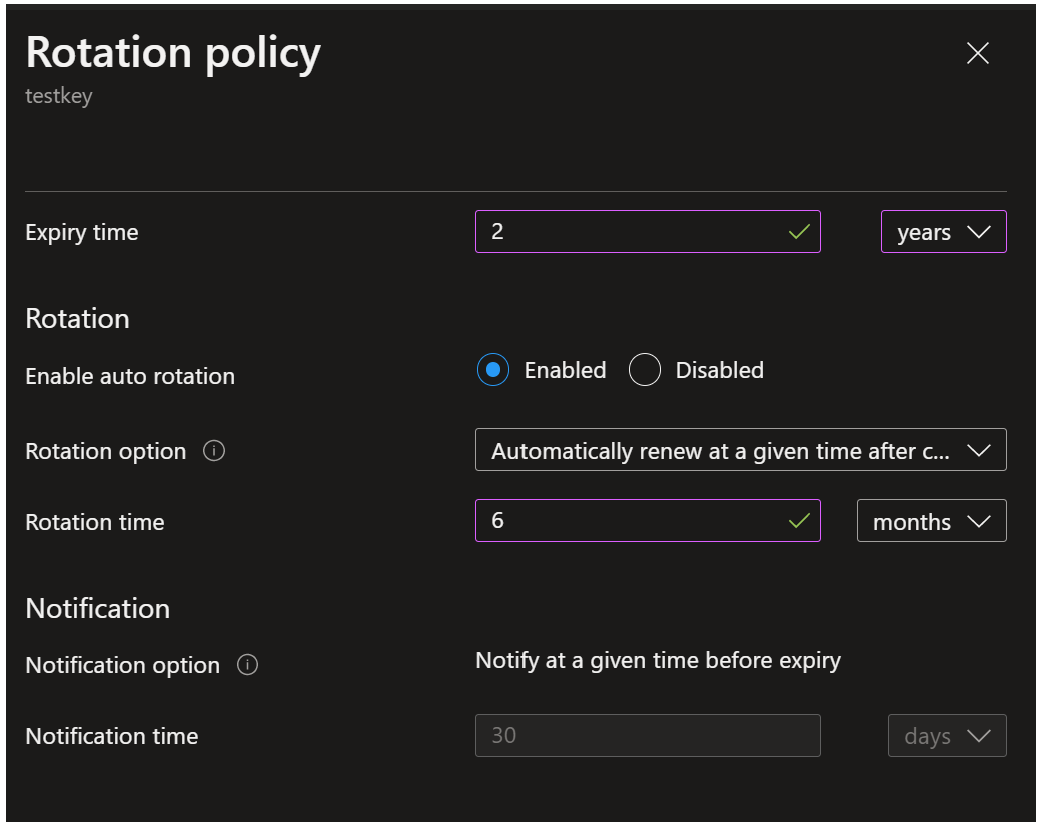
Deployed Azure Container Instance (ACI) can be encrypted using customer-managed key



Deployed Azure Kubernetes Service resource can be configured to use customer-managed keys at any time

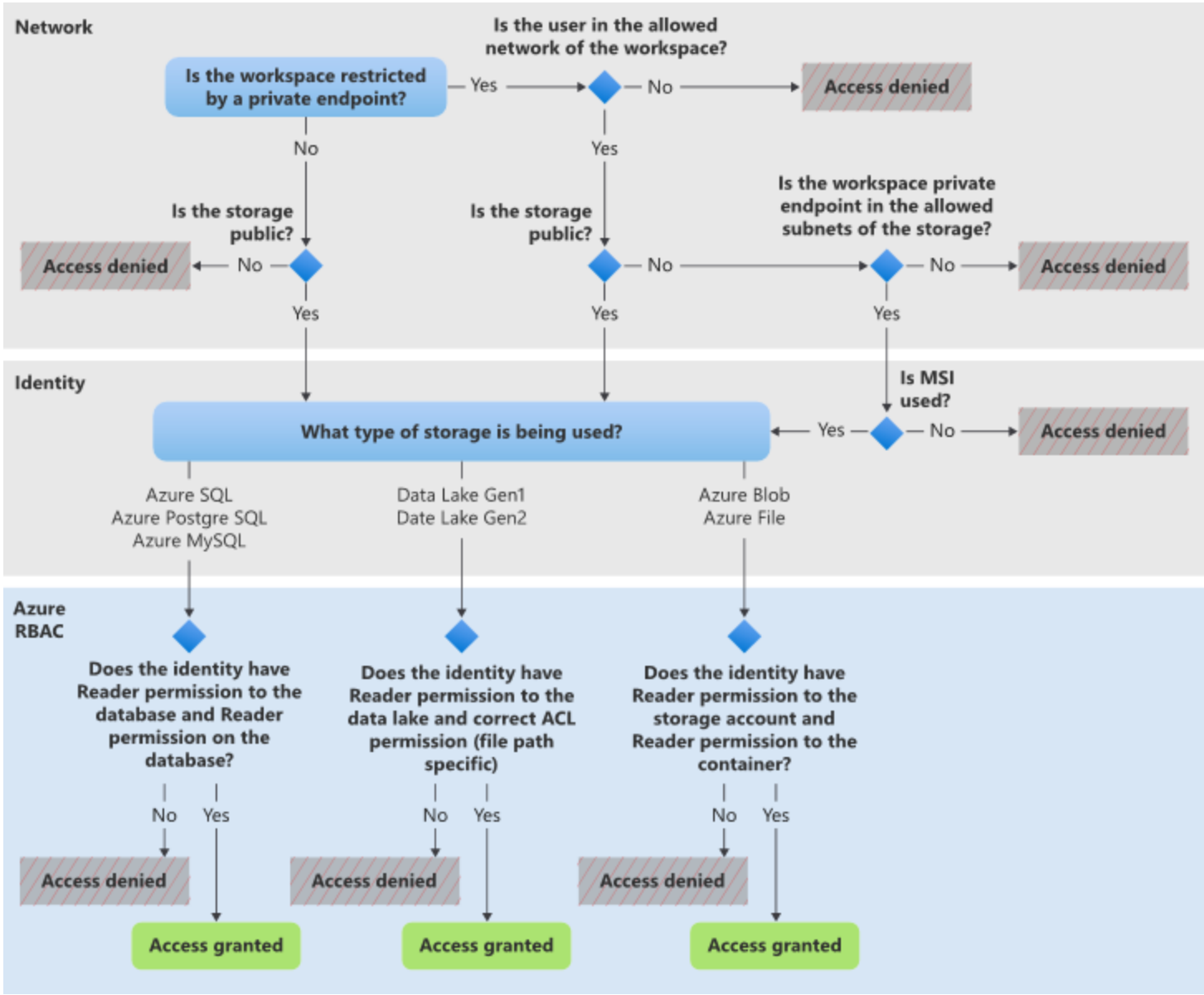
Secure data
Key vault





Secure data
Data Access Flow

- Where is access from ?
- Who is accessing?
- Do they have permission?
- What operation is being performed ?
- Where is this operation being run ?



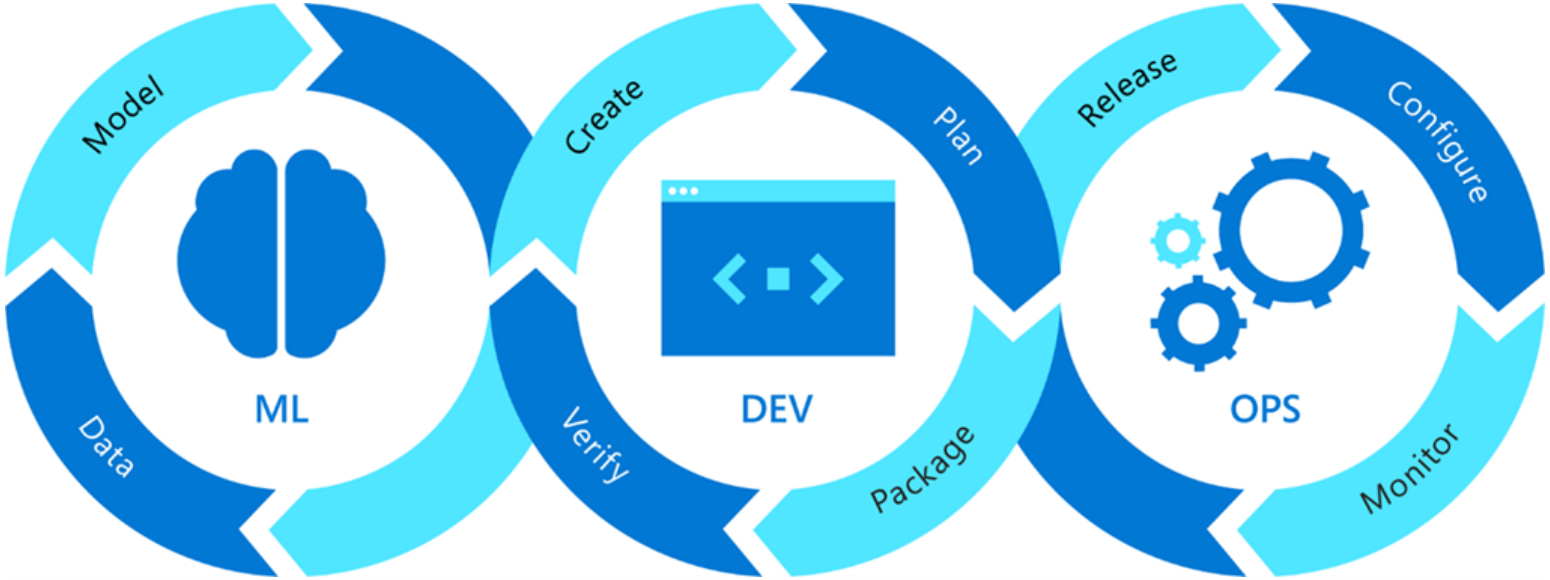
Data & Secrets Recap

- Activate HTTPS on all endpoints (training and scoring)
- Encrypt data at rest with Microsoft or Customer managed keys
- Flag production Workspace as High Business Impact

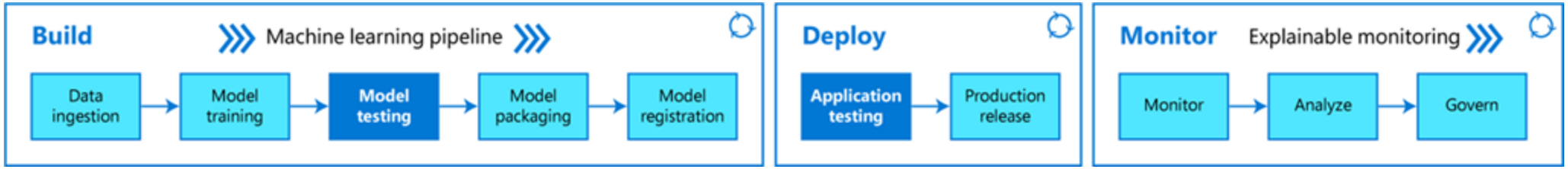
- Encrypt datastores at rest
  - Blob Storage
  - Cosmos DB
  - ACR
  - ACI
  - AKS
  - ML Compute
  - Databricks ?
  - MS generated data
- Encrypt data in transit with TLS1.2+
- Control Microsoft collected data with hbi flag
- Store secrets in Key Vault

Secure MLOps

MLOps = DevOps + Machine learning

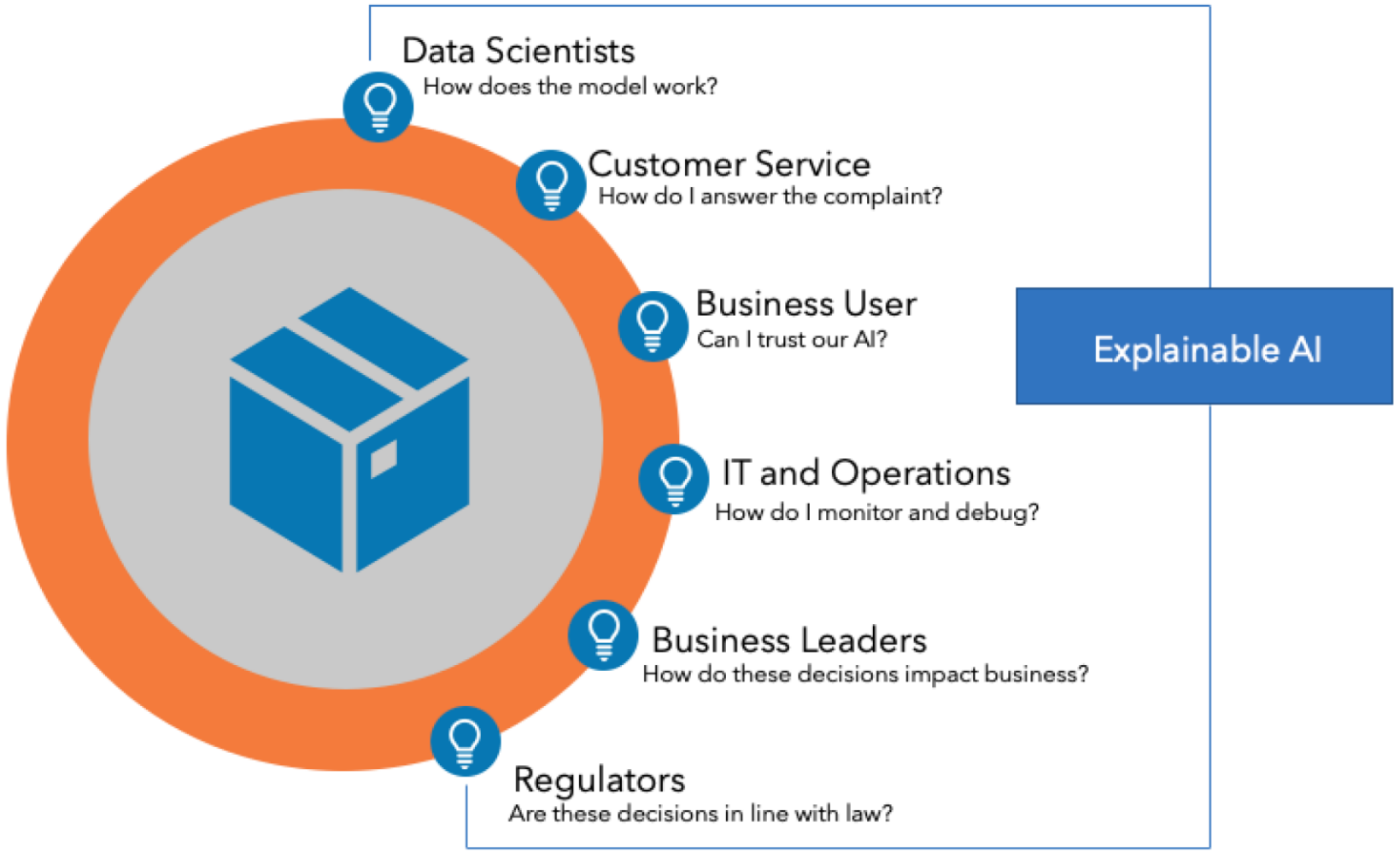


MLOps workflow

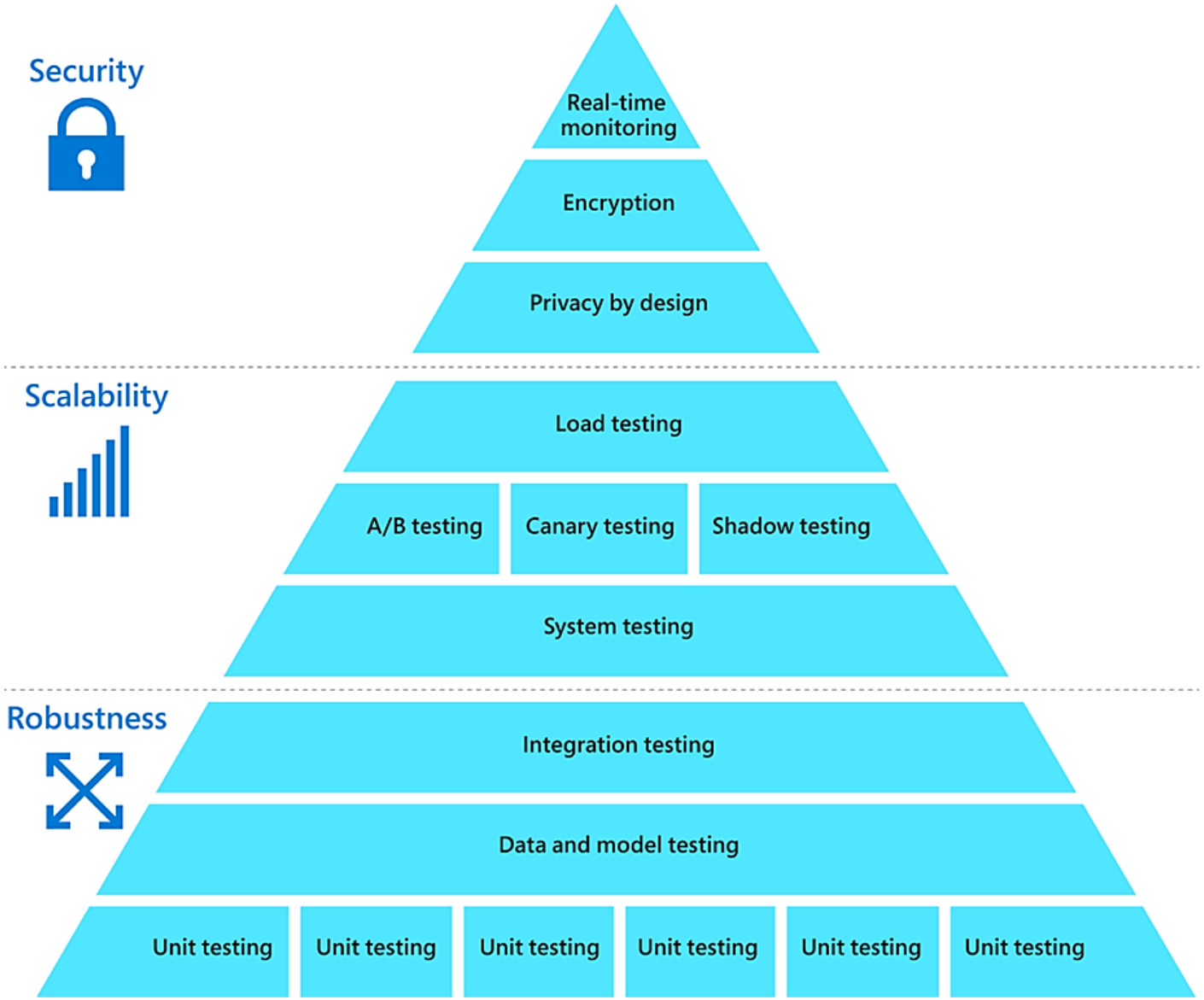


Source

Explainable Monitoring

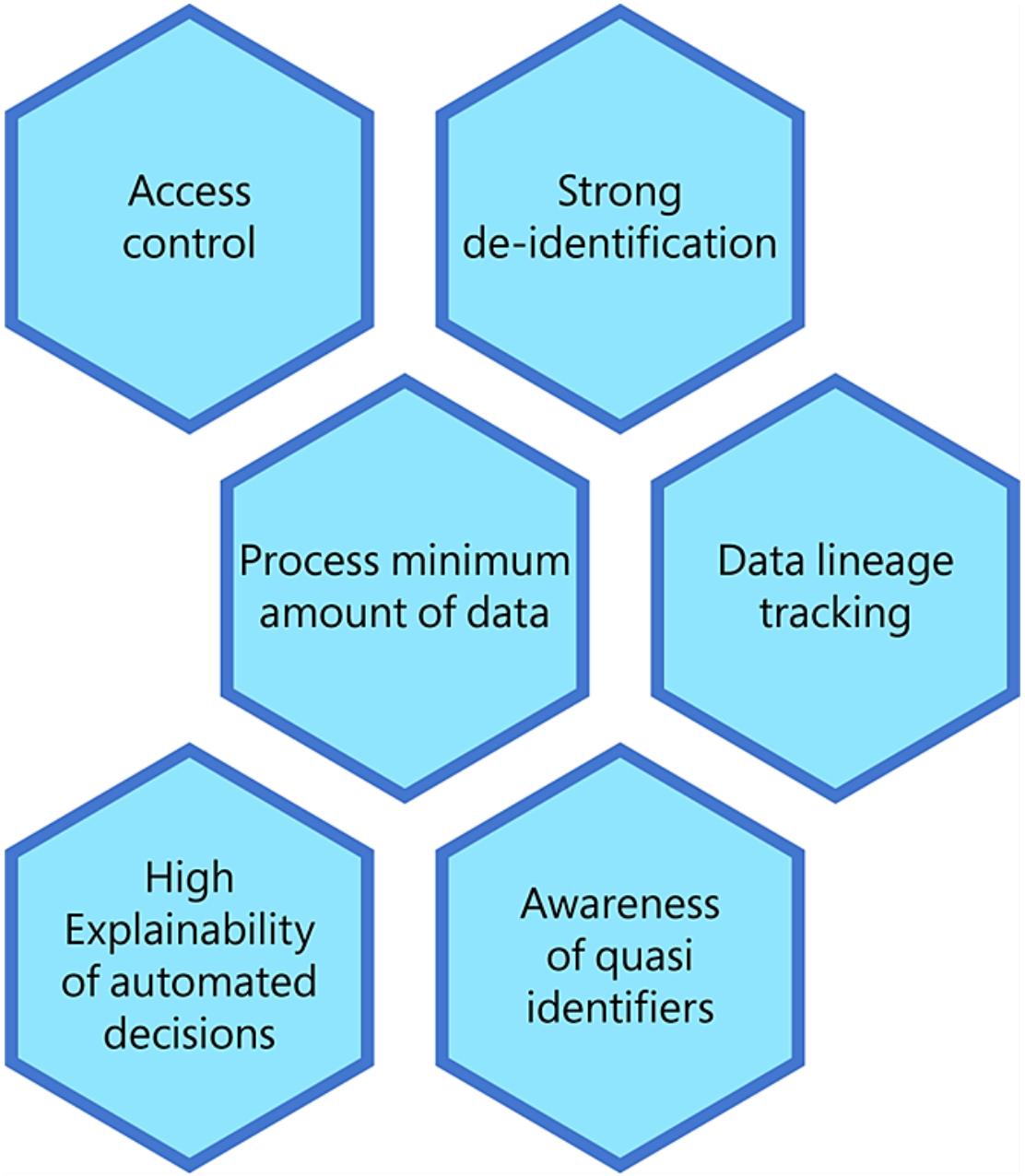


Hierarchy of needs for testing ML systems



Privacy by design

- ✓ A philosophy or approach for embedding **privacy**, **fairness**, and **transparency** in the design IT.
- ✓ This approach will enable possible **data breaches** and **attacks** to be avoided.



Secure MLOps pipelines

Build

- Use **reliable/official sources** for data, model and web service code
- Integrate security controls to pipelines: **application code scanning**, **data integrity checks**, **azure policy**
- Scan **dependencies** and **artifacts**, example with GitHub Advanced Security

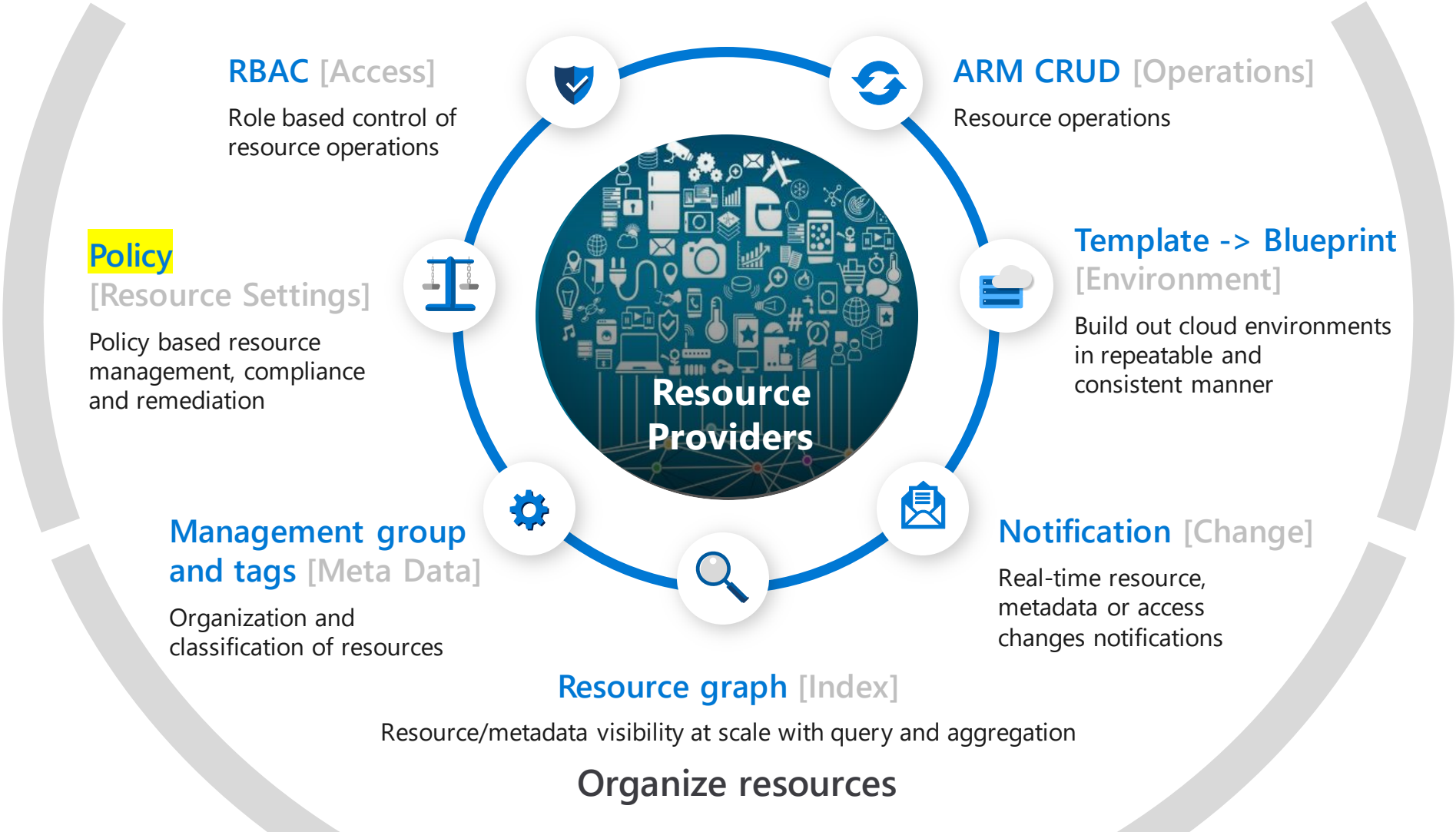
Run

- Scan built container images with **Defender for Containers** and remediate vulnerabilities
- Activate image signing on Azure Container Registry, when possible, with **Content Trust**
- Review app insights data for anomalies
- Activate security alerts on **Defender for Cloud** and **Sentinel**

Governance & Monitoring

Azure Governance

Consistent and integrated collection of resource governance capabilities natively built into ARM



Azure Policy Key Features

Enforcement and Compliance

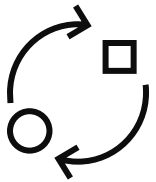
Turn on built-in policies or build custom ones for all resource types

Real-time policy evaluation and enforcement

Periodic and on-demand compliance evaluation

VM In-Guest Policy

Kubernetes Admission Controller



Apply policies at scale

Apply policies to a Management Group with control across your entire organization

Apply multiple policies and aggregate policy states with policy initiative

Exclusion Scope

Remediation

Real time remediation

Remediation on existing resources

Policies and Governance

AzureML let's you configure the following policies using Azure Policy

Customer-managed key

Audit or enforce whether workspaces must use a customer-managed key.

Private link

Audit or enforce whether workspaces use a private endpoint to communicate with a virtual network

Private endpoint

Configure the Azure Virtual Network subnet where the private endpoint should be created.

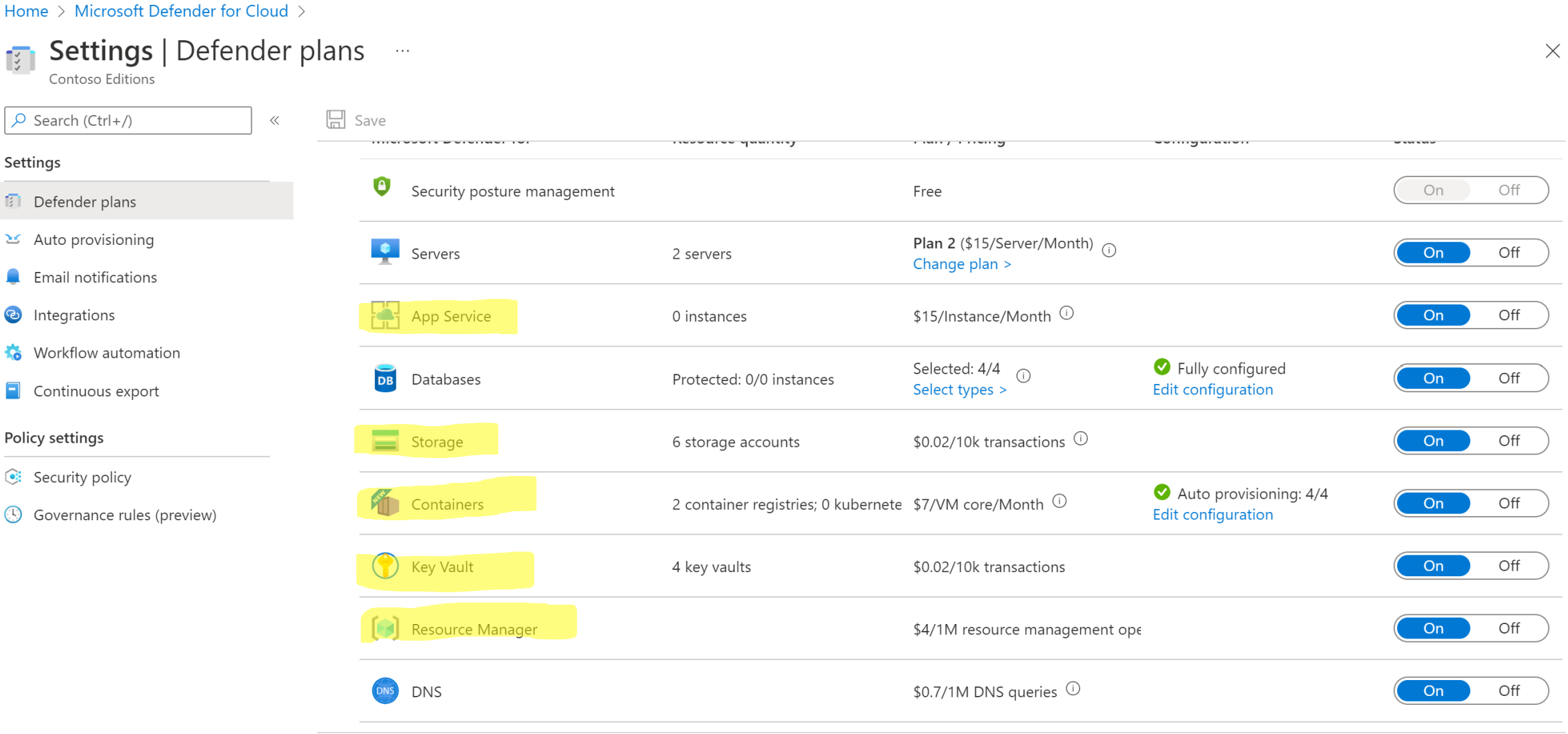
Private DNS zone

Configure the private DNS zone to use for the private link.

Disable local authentication

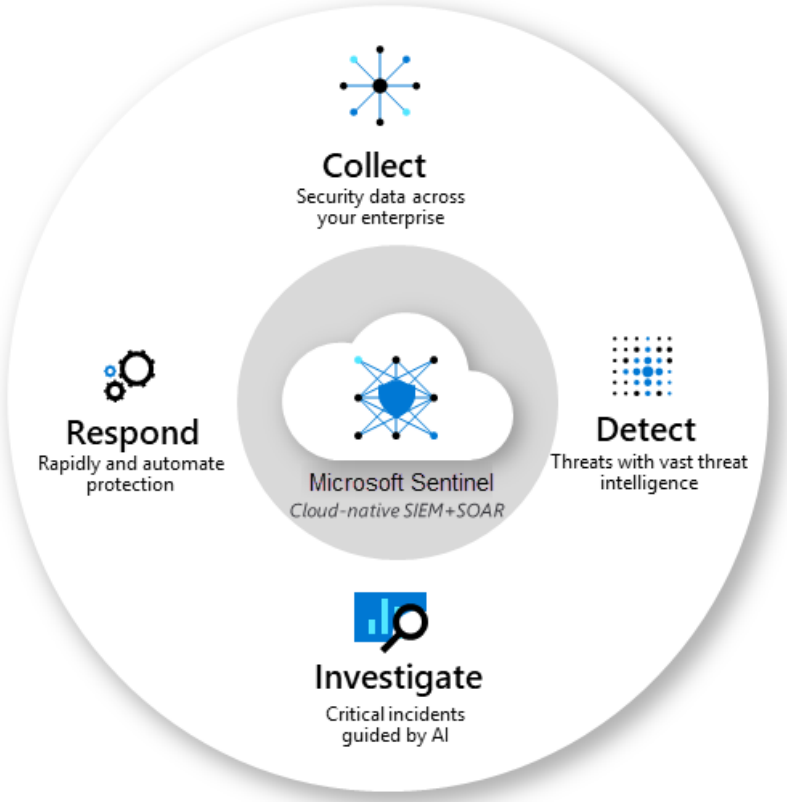
Ensure that Machine Learning require Azure Active Directory identities exclusively for authentication.

Security monitoring: Defender for Cloud

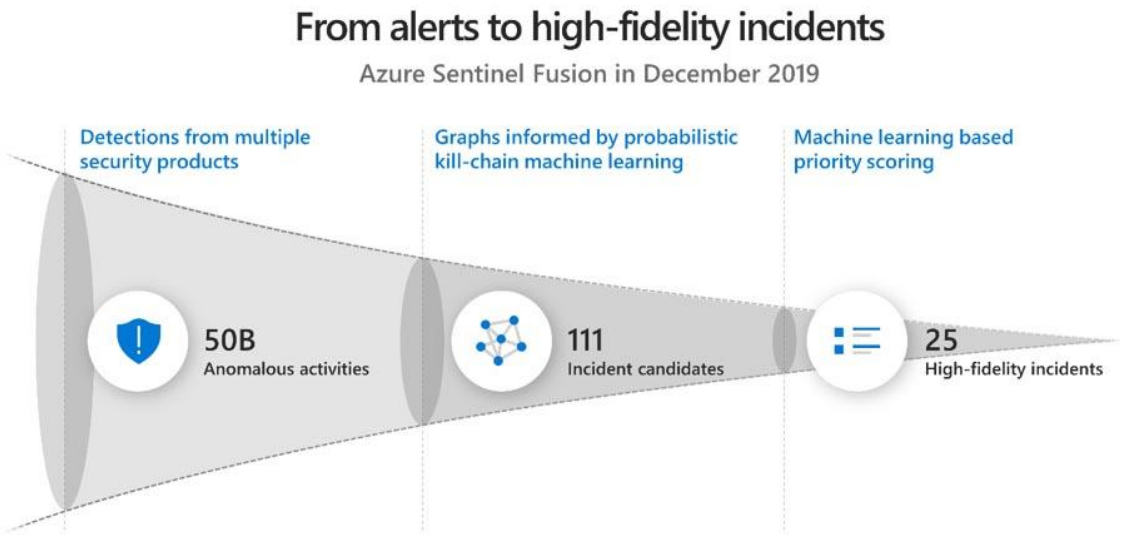


Sentinel integration

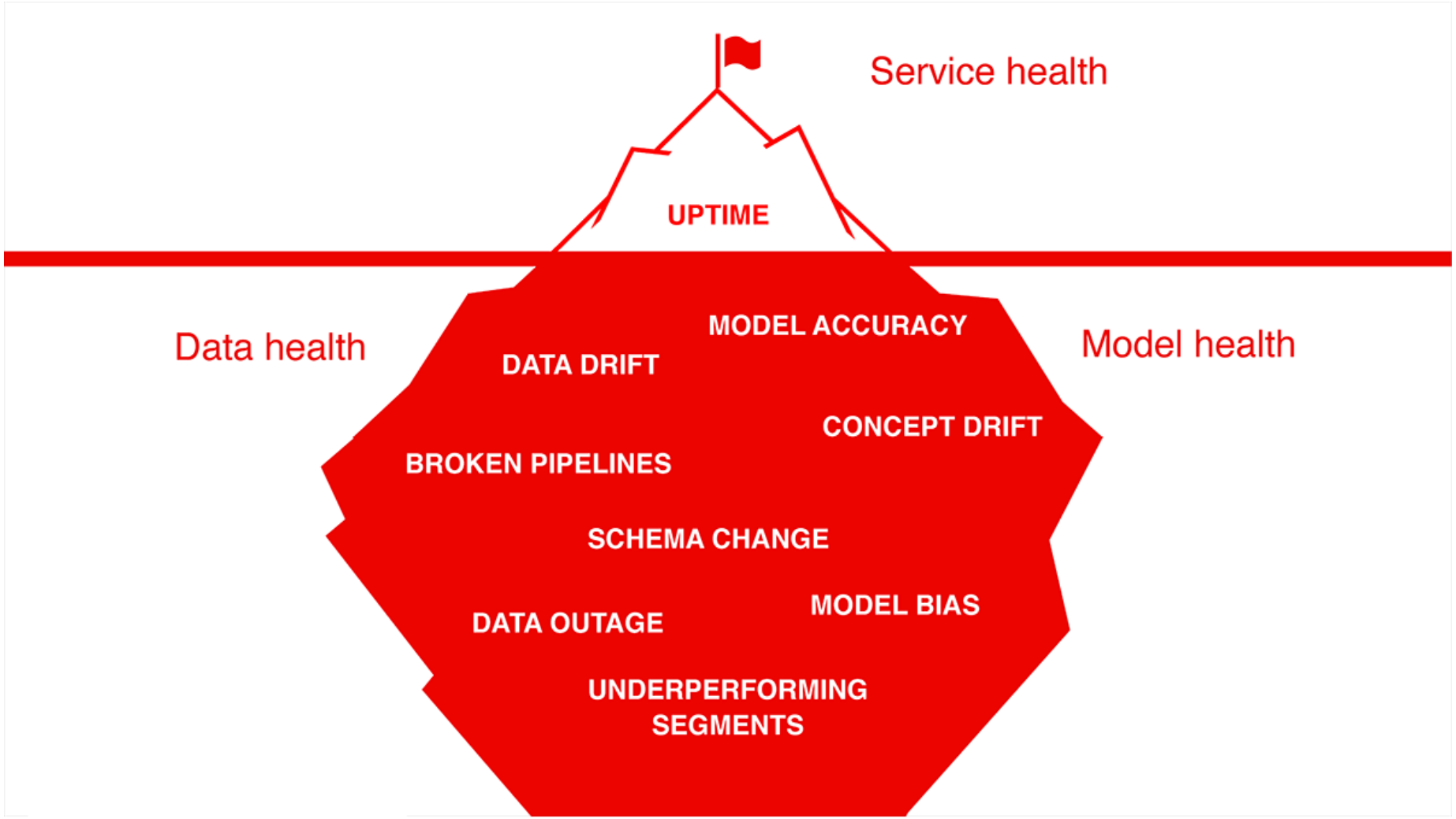
Sentinel for ML



ML for Sentinel

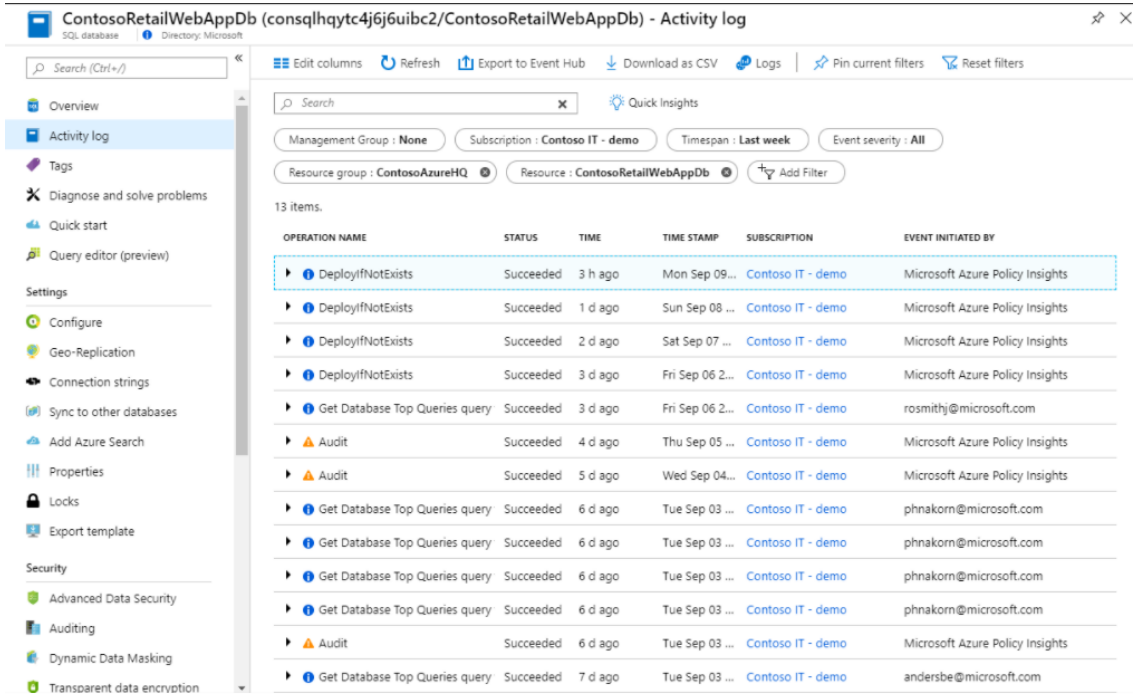


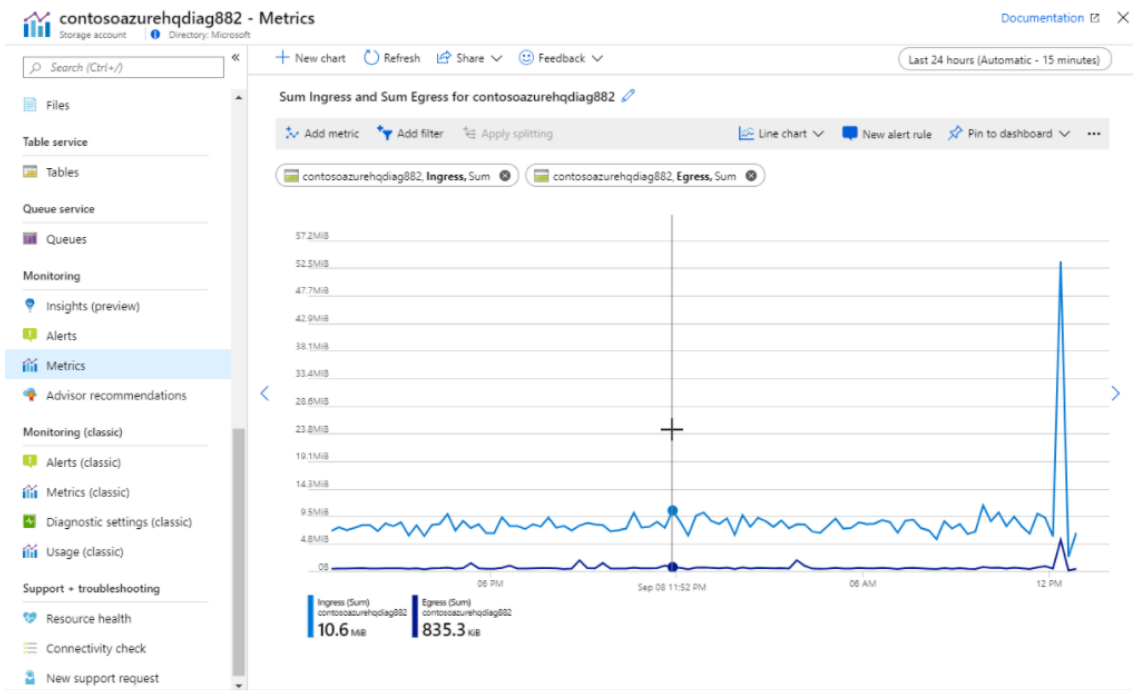
Monitoring ML systems



source

Monitor Azure Machine Learning





Activity Log & metrics

[Monitoring Azure Machine Learning - Azure Machine Learning | Microsoft Learn]

Resource Log Events

Compute

- AmlComputeClusterEvent
- AmlComputeCpuGpuUtilization
- AmlComputeJobEvent
- ComputeInstanceEvent

MLOps

- ModelsChangeEvent / ModelsReadEvent / ModelsActionEvent
- DeploymentReadEvent / DeploymentEventACI / DeploymentEventAKS
- InferencingOperationAKS / InferencingOperationACI
- EnvironmentChangeEvent / EnvironmentReadEvent
- PipelineChangeEvent / PipelineReadEvent
- AmlRunStatusChangedEvent / RunEvent / RunReadEvent

Data Management

- DataLabelChangeEvent / DataLabelReadEvent
- DataStoreChangeEvent / DataStoreReadEvent
- DataSetChangeEvent / DataSetReadEvent

Recommended alerts

Alert type	Condition	Description
Model Deploy Failed	Aggregation type: Total, Operator: Greater than, Threshold value: 0	When one or more model deployments have failed
Quota Utilization Percentage	Aggregation type: Average, Operator: Greater than, Threshold value: 90	When the quota utilization percentage is greater than 90%
Unusable Nodes	Aggregation type: Total, Operator: Greater than, Threshold value: 0	When there are one or more unusable nodes

Azure Machine Learning Metrics - Model

Metric	Unit	Description
Model Register Succeeded	Count	Number of model registrations that succeeded in this workspace
Model Register Failed	Count	Number of model registrations that failed in this workspace
Model Deploy Started	Count	Number of model deployments started in this workspace
Model Deploy Succeeded	Count	Number of model deployments that succeeded in this workspace
Model Deploy Failed	Count	Number of model deployments that failed in this workspace

Azure Machine Learning Metrics - Quota

Metric	Unit	Description
Total Nodes	Count	Number of total nodes. This total includes some of Active Nodes, Idle Nodes, Unusable Nodes, Preempted Nodes, Leaving Nodes
Active Nodes	Count	Number of Active nodes. The nodes that are actively running a job.
Idle Nodes	Count	Number of idle nodes. Idle nodes are the nodes that are not running any jobs but can accept new job if available.
Unusable Nodes	Count	Number of unusable nodes. Unusable nodes are not functional due to some unresolvable issue. Azure will recycle these nodes.
Preempted Nodes	Count	Number of preempted nodes. These nodes are the low-priority nodes that are taken away from the available node pool.
Leaving Nodes	Count	Number of leaving nodes. Leaving nodes are the nodes that just finished processing a job and will go to Idle state.
Total Cores	Count	Number of total cores
Active Cores	Count	Number of active cores
Idle Cores	Count	Number of idle cores
Unusable Cores	Count	Number of unusable cores
Preempted Cores	Count	Number of preempted cores
Leaving Cores	Count	Number of leaving cores
Quota Utilization Percentage	Count	Percent of quota utilized

Azure Machine Learning Metrics - Resource

Metric	Unit	Description
CpuUtilization	Count	Percentage of utilization on a CPU node. Utilization is reported at one-minute intervals.
GpuUtilization	Count	Percentage of utilization on a GPU node. Utilization is reported at one-minute intervals.
GpuMemoryUtilization	Count	Percentage of memory utilization on a GPU node. Utilization is reported at one-minute intervals.
GpuEnergyJoules	Count	Interval energy in Joules on a GPU node. Energy is reported at one-minute intervals.

Azure Machine Learning Metrics - Run

Metric	Unit	Description
Cancelled Runs	Count	Number of runs canceled for this workspace.
Cancel Requested Runs	Count	Number of runs where cancel was requested for this workspace.
Completed Runs	Count	Number of runs completed successfully for this workspace.
Failed Runs	Count	Number of runs failed for this workspace.
Finalizing Runs	Count	Number of runs entered finalizing state for this workspace.
Not Responding Runs	Count	Number of runs not responding for this workspace.
Not Started Runs	Count	Number of runs in Not Started state for this workspace.
Preparing Runs	Count	Number of runs that are preparing for this workspace.
Provisioning Runs	Count	Number of runs that are provisioning for this workspace.
Queued Runs	Count	Number of runs that are queued for this workspace.
Started Runs	Count	Number of runs running for this workspace.
Starting Runs	Count	Number of runs started for this workspace.
Errors	Count	Number of run errors in this workspace.
Warnings	Count	Number of run warnings in this workspace.

Governance & Monitoring Recap

- Configure Azure policy for audit and compliance
- Enable Defender for Cloud plans for:
  - Storage
  - Keyvault
  - Containers
  - Resource Manager
  - App Service
- Configure diagnostic settings logs for workspace resources
- Configure notifications for security alerts
- Integrate with Sentinel

Recap

Enable security features on all used services and resources.

IAM

Azure AD authentication

RBAC authorization

Managed Identities for resources

Network

Stay away from the internet

Private exposition and connectivity with Private Endpoints

Compute

Prefer managed compute resources with automated updates

Enable Azure Disk Encryption on custom VMs

Endpoints

Require authentication on exposed scoring endpoints

Enable TLS 1.2

Add application protection with WAF

Data

TLS1.2+ everywhere

Encryption at rest with Microsoft or Customer Managed Keys

MLOps

Use reliable sources for base images, dependencies, libraries and data

Review and remediate image vulnerabilities on Defender for Cloud

Governance

Leverage Azure Policy

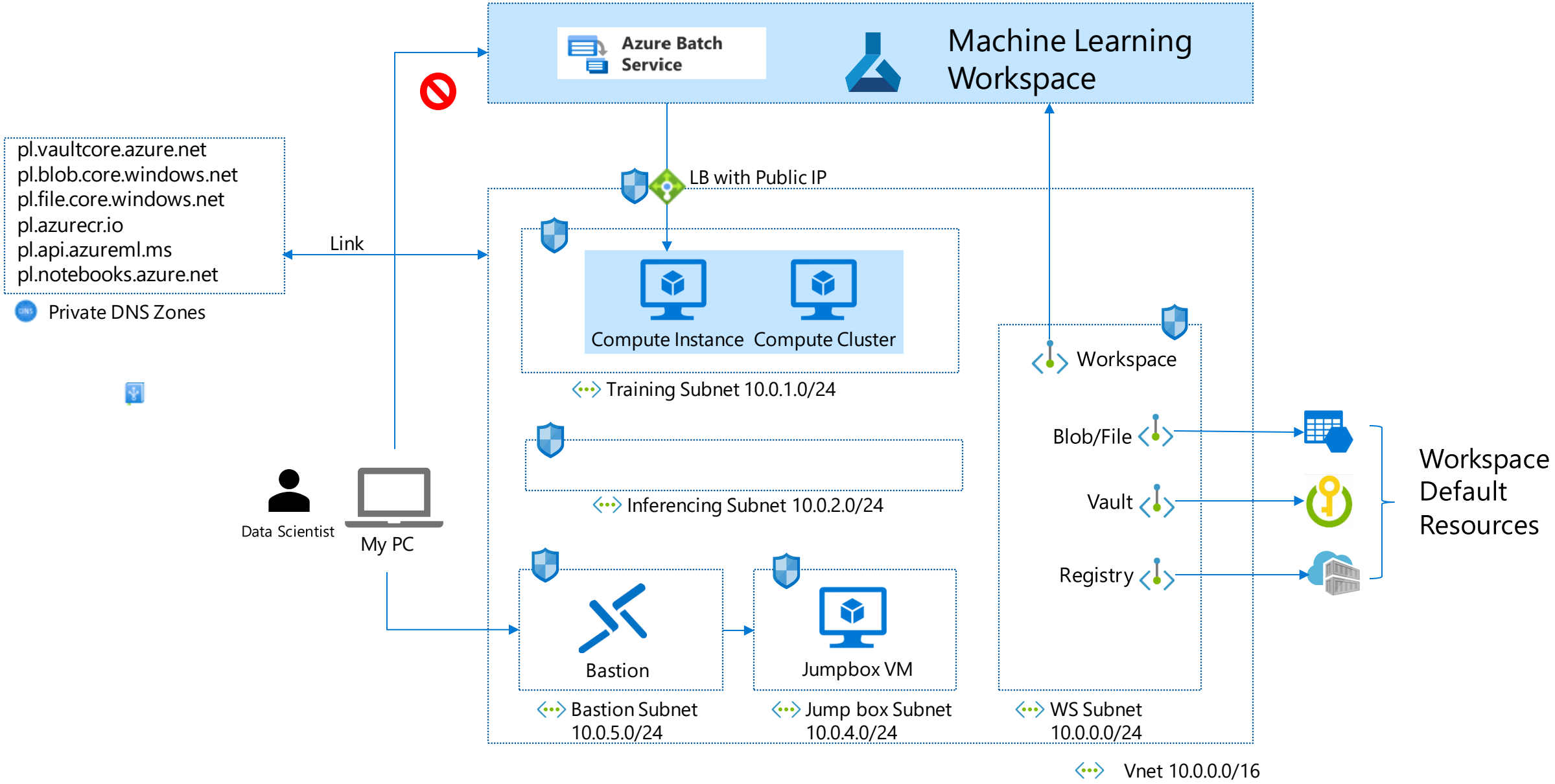
Enable Defender for Cloud workload protections

Remediate vulnerabilities

Enable notifications

Demo: Create a Secure ML Workspace

Demo Environment



https://github.com/Azure/terraform/tree/master/quickstart/201-machine-learning-moderately-secure

Demo Setup

Create a Vnet & several subnets for :

- ML Workspace
- Training
- Inferencing
- Jumpbox VM
- Bastion

Create NSGs for the subnets

Create below resources with a private endpoint in the Vnet:

- Storage Account
- Key Vault
- Azure Container Registry
- AML Workspace

Create private DNS zones linked to the Vnet

Create a jumpbox in the Vnet.

Connect to the jumpbox and use the Azure Machine Learning studio.

Create an Azure Machine Learning compute instance and compute cluster for training

Ressources created with private Endpoints

Azure Virtual Network (VNet) & Subnet(s)

Azure Storage Account and 2 Private Endpoints with DNS Zones:

- privatelink.blob.core.windows.net
- privatelink.file.core.windows.net

Azure Container Registry and Private Endpoint with DNS Zone:

- privatelink.azurecr.io

Azure Key Vault and Private Endpoint with DNS Zone:

- privatelink.vaultcore.azure.net

Azure Machine Learning workspace and Private Endpoint with 2 DNS Zones:

- privatelink.api.azureml.ms
- privatelink.notebooks.azure.net

Q&A

Enregistrez vous dès maintenant au prochain Webinars Data AI

Event Webinar (Les jeudis de la Data & AI) - L200/300	Date	Duration (min)	Link
Azure Scale Analytics - Architectures Data Mesh dans Azure avec Azure Synapse, Microsoft Purview et Azure Data Share	13/10/2022	120	https://msevents.microsoft.com/event?id=139685175
MLOps avec Azure Machine Learning	20/10/2022	120	https://msevents.microsoft.com/event?id=1245885767
SQL Server 2022 et hybridation native avec Azure SQL Managed Instance	10/11/2022	120	https://msevents.microsoft.com/event?id=145826476
Machine Learning dans Azure Synapse Analytics	17/11/2022	120	https://msevents.microsoft.com/event?id=3637723312
Azure Cosmos DB et IA	24/11/2022	120	https://msevents.microsoft.com/event?id=2646013445
Azure et les Services Cognitifs	08/12/2022	120	https://msevents.microsoft.com/event?id=3772037220
La gouvernance de données dans Azure avec Microsoft Purview	15/12/2022	120	https://msevents.microsoft.com/event?id=1499560981
MLOps avec Azure Machine Learning	12/01/2023	120	https://msevents.microsoft.com/event?id=4115194515
Data processing dans Azure ave Azure Synapse, Azure Batch, Spark, Notebook, etc.	19/01/2023	120	https://msevents.microsoft.com/event?id=1537241181
Déploiement et sécurisation des workspace Azure Synapse	26/01/2023	120	https://msevents.microsoft.com/event?id=1806467748
Azure Machine Learning pour les Citizen Data Scientists	09/02/2023	120	En cours
PowerBI - Self Service Analytics	16/02/2023	120	https://msevents.microsoft.com/event?id=1401519679
L'IA responsable avec Azure machine learning	09/03/2023	120	https://msevents.microsoft.com/event?id=2072953112
Machine Learning dans Azure Synapse Analytics	16/03/2023	120	https://msevents.microsoft.com/event?id=3413014857
Les bases de données Open Source dans le cloud Azure	23/03/2023	120	https://msevents.microsoft.com/event?id=2727487131
Hybridation des services de Machine Learning Azure	06/04/2023	120	https://msevents.microsoft.com/event?id=1624914222
La gouvernance de données dans Azure avec Microsoft Purview	13/04/2023	120	https://msevents.microsoft.com/event?id=3909342839
Les solutions SQL dans Azure (PaaS, IaaS, SaaS)	04/05/2023	120	https://msevents.microsoft.com/event?id=1162207895
Data processing dans Azure ave Azure Synapse, Azure Batch, Spark, Notebook, etc.	16/05/2023	120	https://msevents.microsoft.com/event?id=3517068442
Hybridation des services de données Azure	24/05/2023	120	https://msevents.microsoft.com/event?id=2996507398
Self Service Analytics	01/06/2023	120	En cours