Seminar Microsoft Azure Design

DZ-Bank Hamburg, 23. -26. Februar 2026

https://github.com/www42/Hamburg

Tag 1 Einführung

- Einführung Azure
- Einführung Künstliche Intelligenz

Tag 2 Architektur

- Azure Well-Architected Framework
- Cloud Adoption Framework

Tag 3 Azure Services

- Compute, Applications, Network, Migrations
- Storage,Databases, Data Integration

Tag 4 Deep Dive

- Governance, Authentication, Authorization, Monitoring
- Backup, Disaster Recovery, High Availability

Thomas Jäkel

brainymotion

Lead Trainer Cloud Infrastructure

Microsoft Certified Trainer since 1999

https://github.com/www42/Hamburg

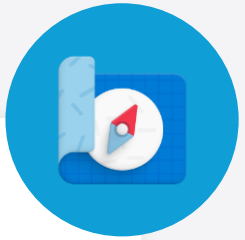
Let’s have a great time together

We all contribute to a great class

$9^{00} - 17^{00}$

$12^{00} - 12^{45}$

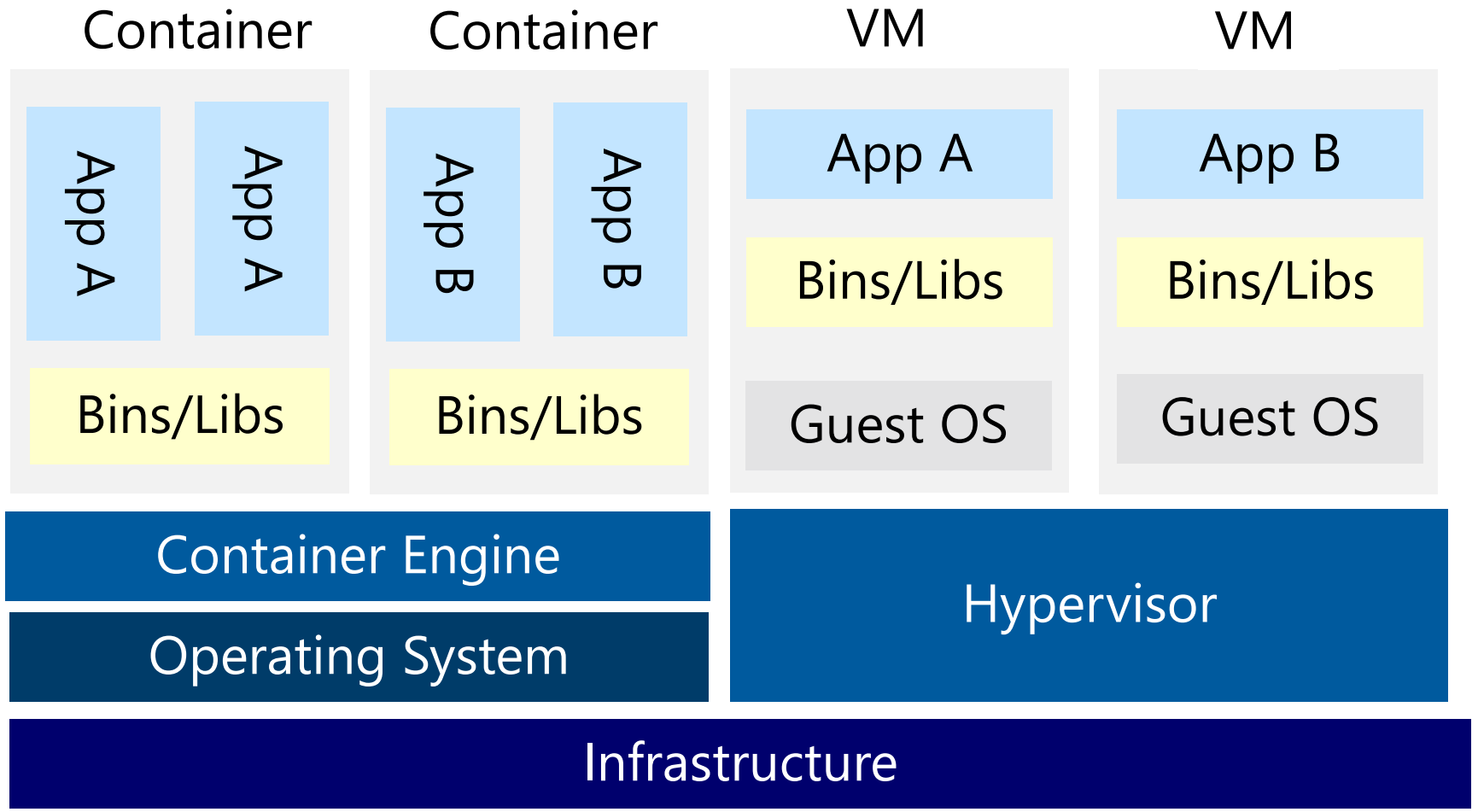
What you should know about our facilities



Plan and implement advanced security for compute

Compare Containers to Virtual Machines

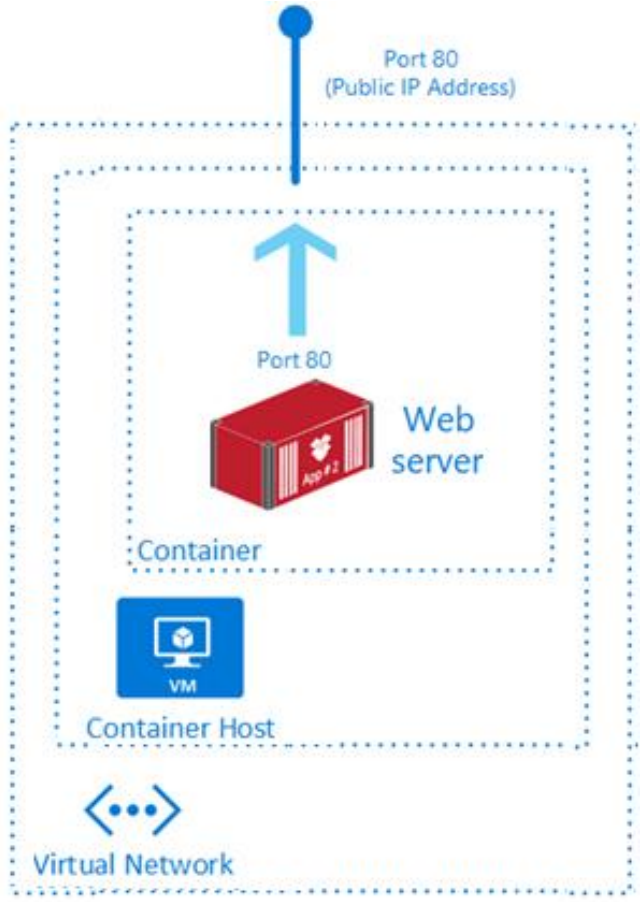
- Isolation
- Operating System
- Deployment
- Persistent storage
- Fault tolerance



Review Azure Container Instances

ACI

- PaaS Service
- Fast startup times
- Public IP connectivity and DNS name
- Isolation features
- Custom sizes
- Persistent storage
- Linux and Windows Containers
- Co-scheduled Groups
- Virtual network Deployment

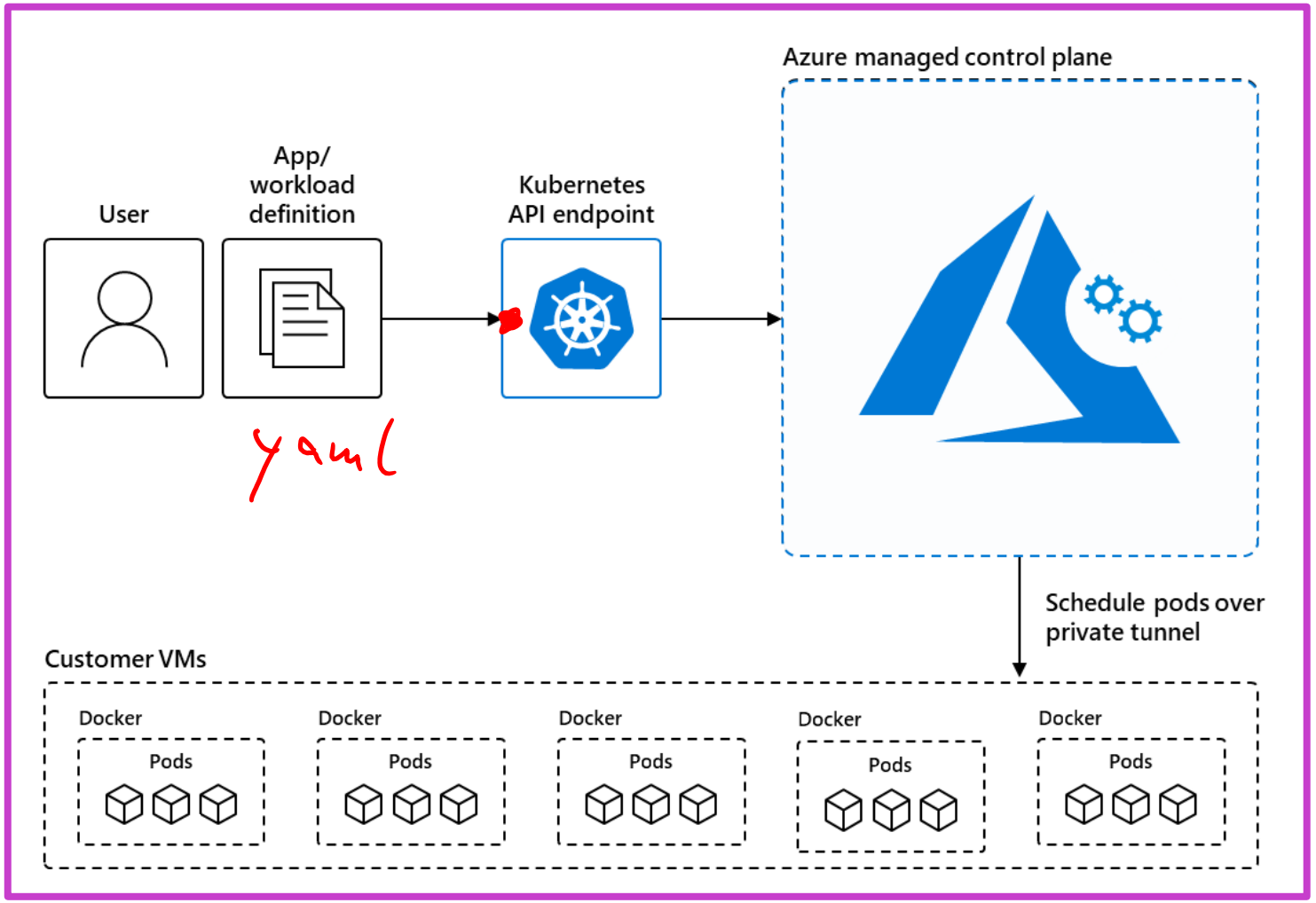


nginx
OS

Fastest way to run a container in Azure without provisioning a VM

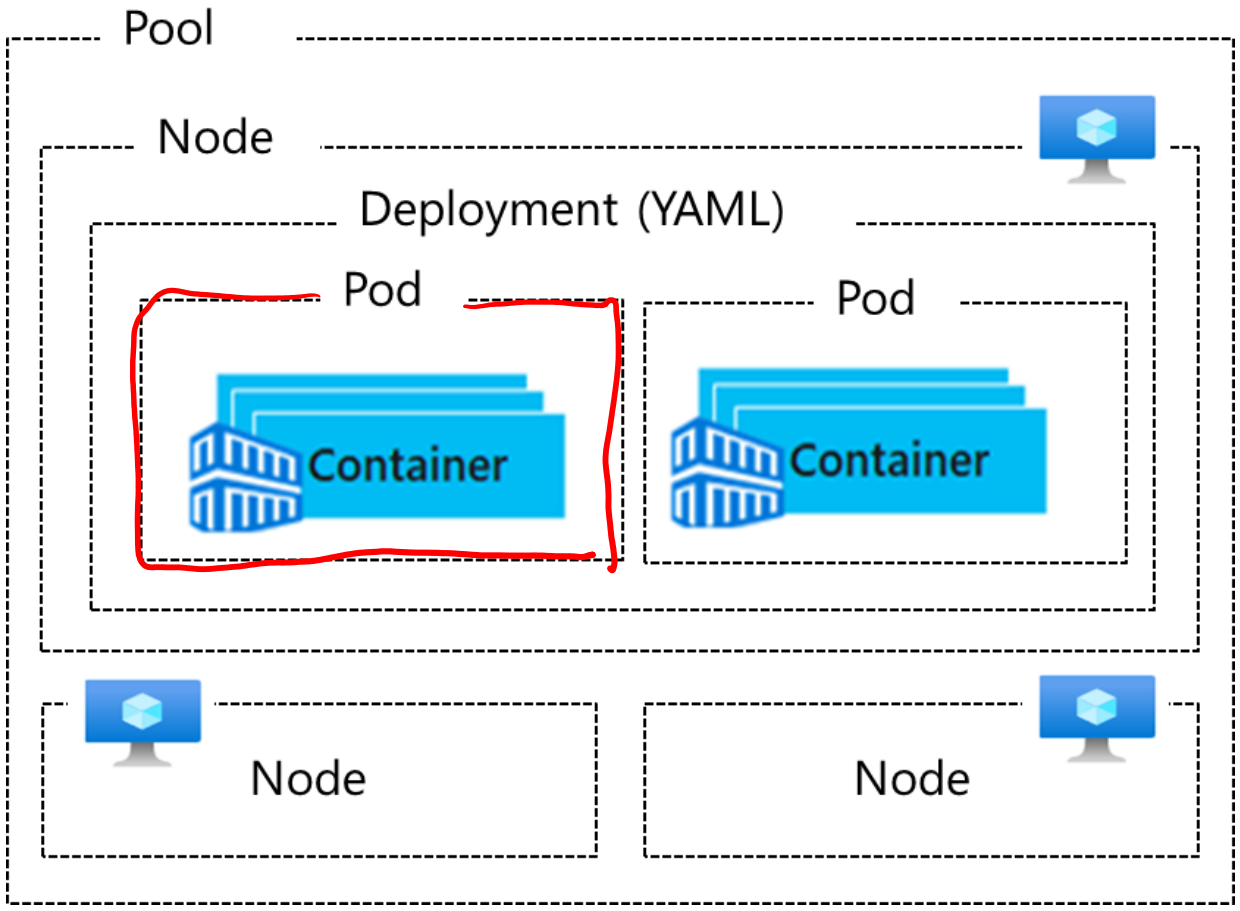
Azure Kubernetes Service (AKS)

- AKS simplifies Kubernetes management, providing high availability, scalability, and integration with DevOps tools.
- Azure manages AKS control plane for free, focusing on health monitoring and maintenance; users pay for nodes.
- AKS use cases include microservices, secure DevOps, data streaming, and running Windows containers.

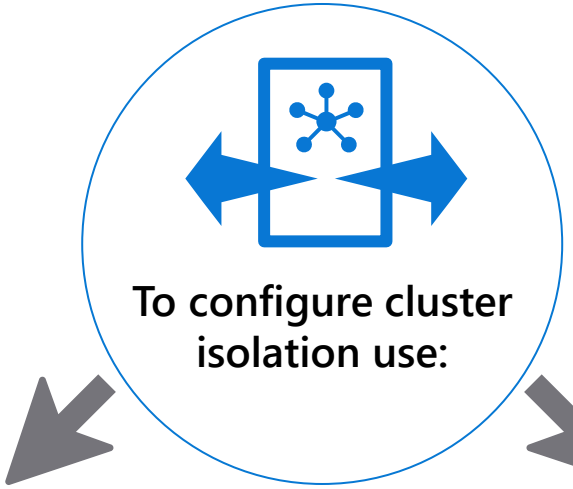


Understand AKS Terminology

Term	Description
Pools	Groups of nodes with identical configurations
Nodes	Individual VMs running containerized applications
Pods	Single instance of an application. A pod can contain multiple containers
Deployment	One or more identical pods managed by Kubernetes
Manifest	YAML file describing a deployment



Configure network isolation for Azure Kubernetes Service



Logical isolation

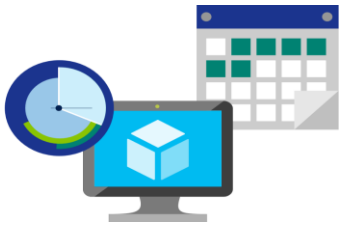
- Has high pod density
- Additional security features, like Kubernetes RBAC for nodes, efficiently block exploit
- For true security when running hostile multi-tenant workloads, you should only trust a hypervisor.

Physical isolation

- Has low pod density
- it adds management and financial overhead.
- Use only for hostile multi-tenant workloads
- For other scenarios, it is recommended to use Logical Isolation.

Cost management

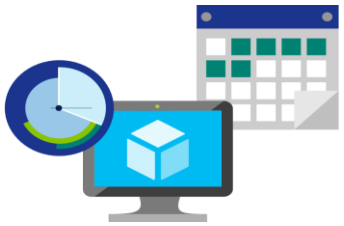
Factors affecting costs (part 1)



These are some of the factors affecting costs:

1) Resource type	2) Consumption	3) Maintenance
Costs are resource-specific, so the usage that a meter tracks and the number of meters associated with a resource, depend on the resource type.	With a pay-as-you-go model, consumption is one of the biggest drivers of costs.	Monitoring your Azure footprint and maintaining your environment can help you identify and mitigate costs that aren't necessary, such as shutting down underused virtual machines.

Factors affecting costs (part 2)



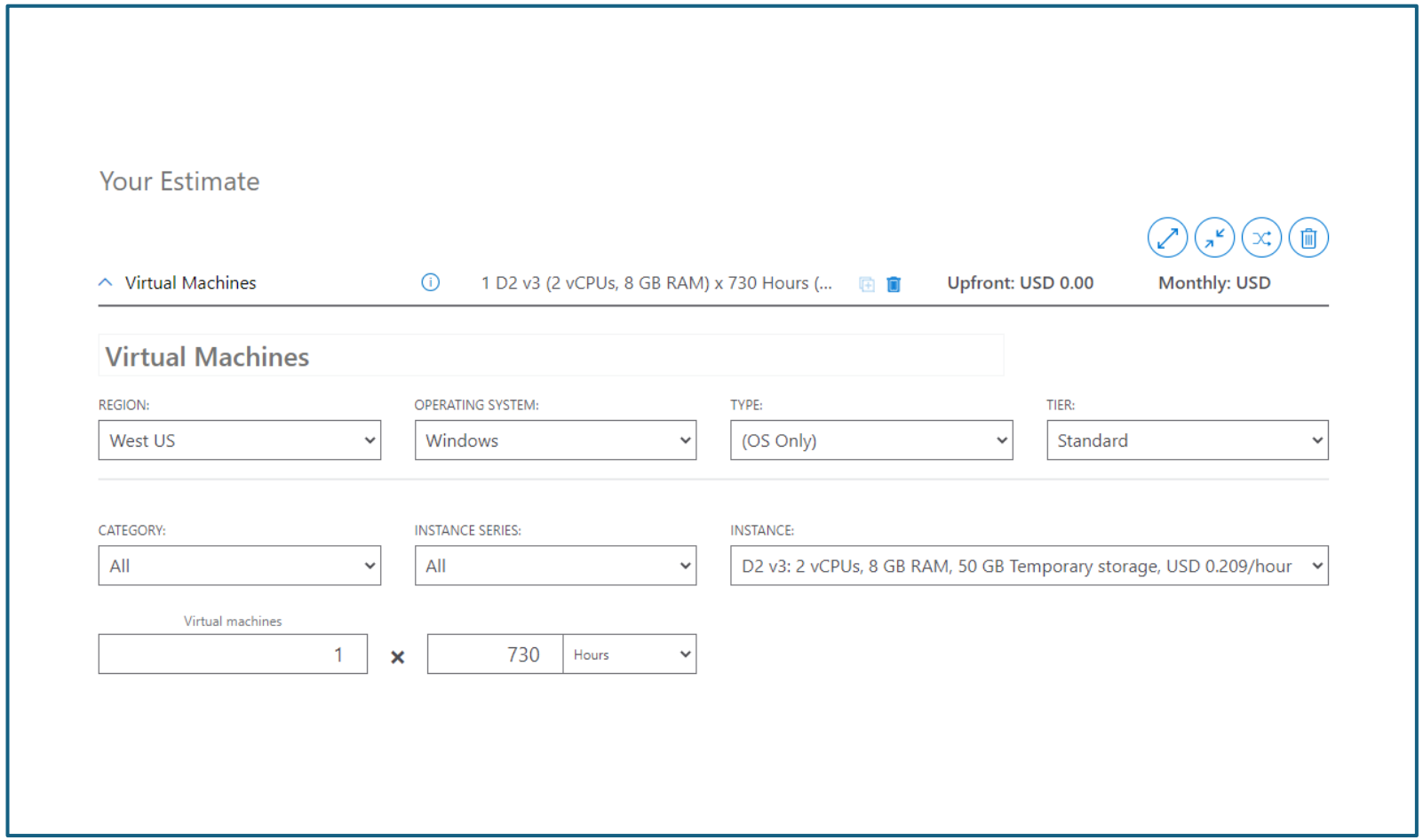
These are some of the factors affecting costs:

4) Geography	5) Network traffic	6) Subscription
The same resource type can cost different amounts depending on the geographic area, which has an impact on Azure costs.	While some inbound data transfers are free, the cost for outbound data or data between Azure resources is impacted by billing zones.	The type and configuration of your subscription can also impact your cost. For example, the free trial lets you explore some Azure resources for free.

Pricing calculator

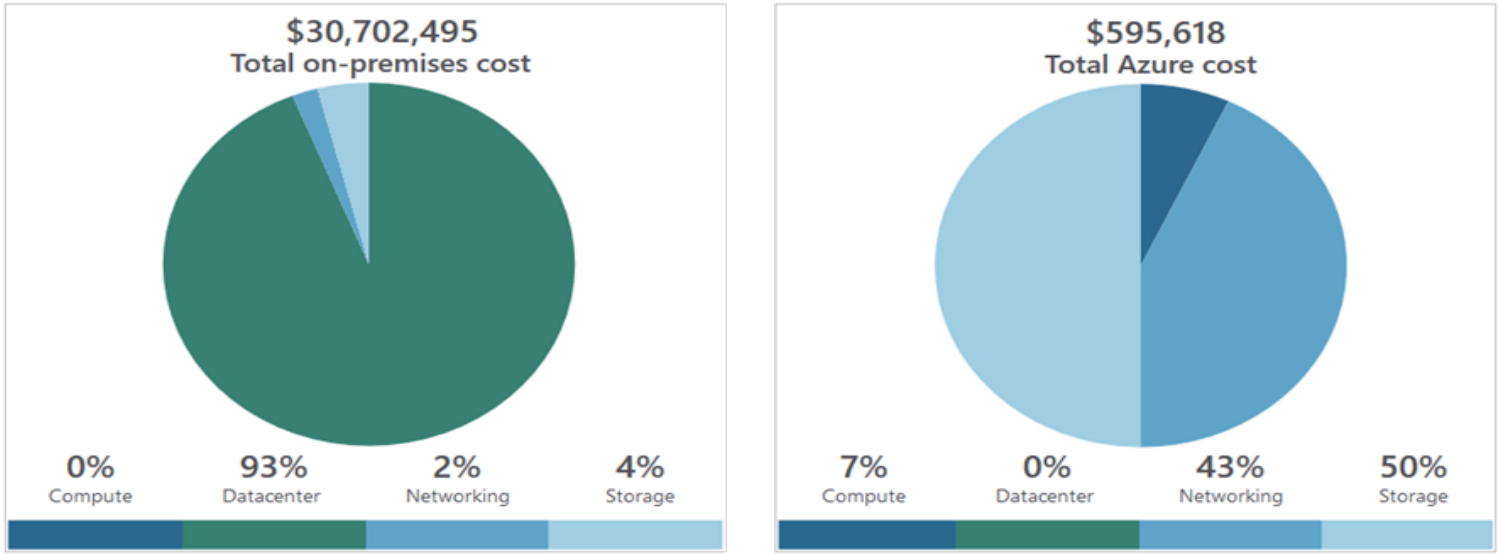
The **pricing calculator** is a tool that helps you estimate the cost of Azure products. The options that you can configure in the pricing calculator vary between products, but basic configuration options include:

- Region
- Tier
- Billing options
- Support options
- Programs and offers
- Azure dev/test



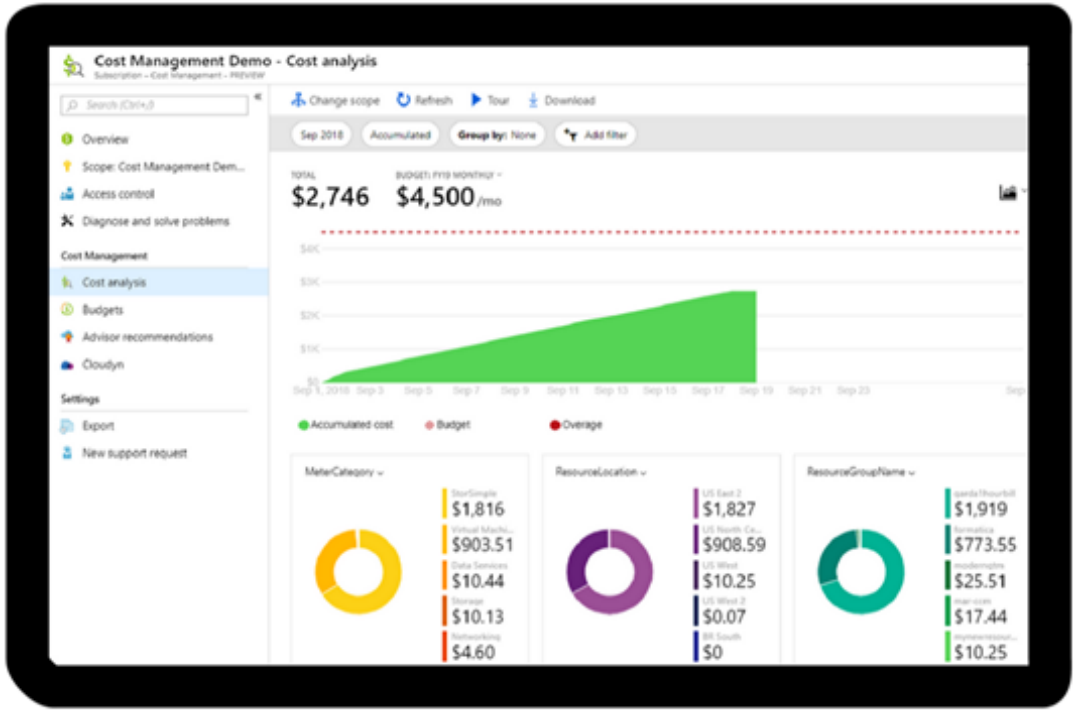
Total Cost of Ownership (TCO) calculator

- A tool to estimate cost savings you can realize by migrating to Azure.
- A report compares the costs of on-premises infrastructures with the costs of using Azure products and services in the cloud.



Azure Cost Management

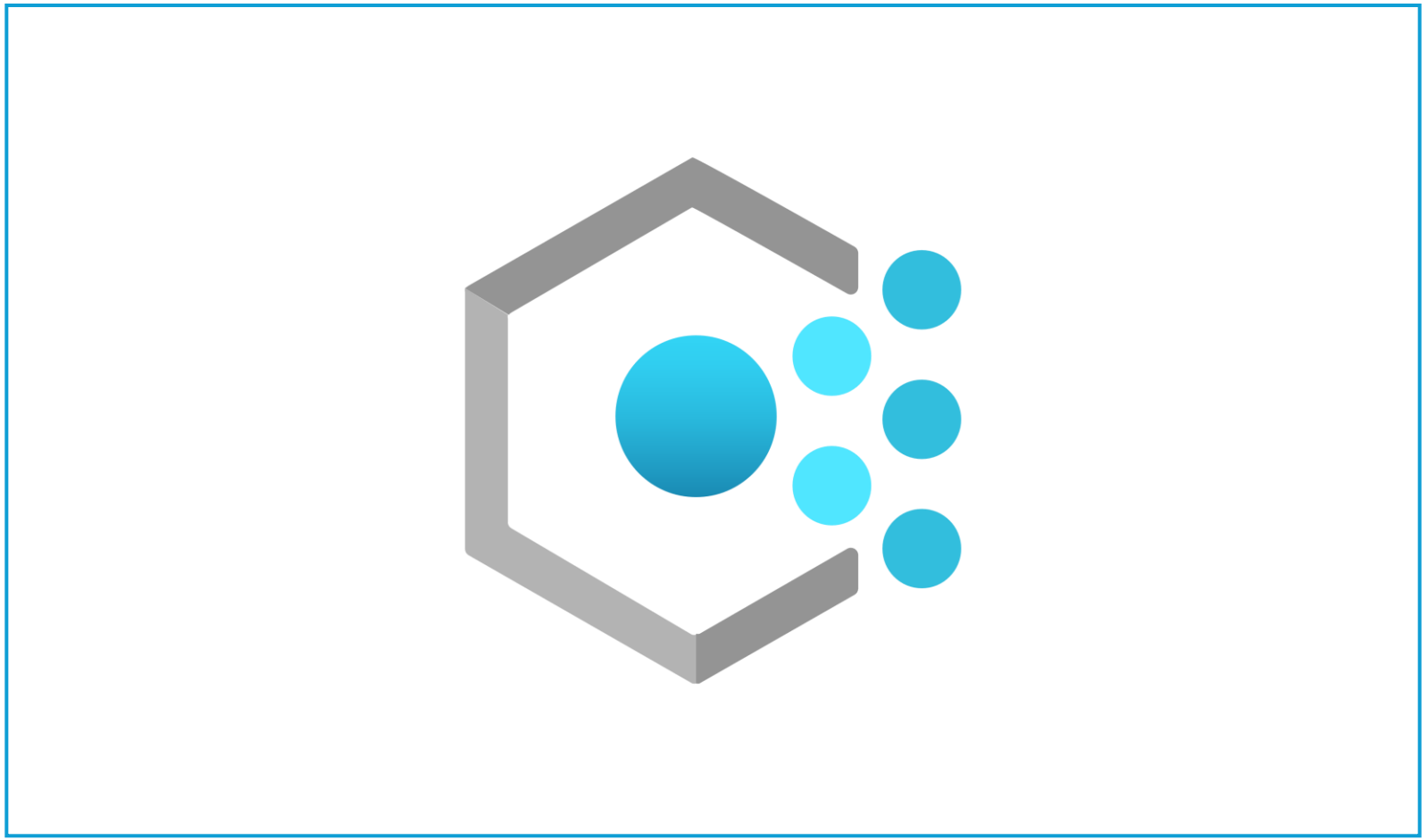
- Reporting: Billing reports
- Data enrichment
- Budgets: Set spend budget
- Alerting: When cost exceed limits
- Recommendation: Cost recommendations



Governance and compliance

Azure Policy

Azure Policy helps to enforce organizational standards and to assess compliance at scale. Provides governance and resource consistency with regulatory compliance, security, cost, and management.



- Evaluates and identifies Azure resources that do not comply with your policies.
- Provides built-in policy and initiative

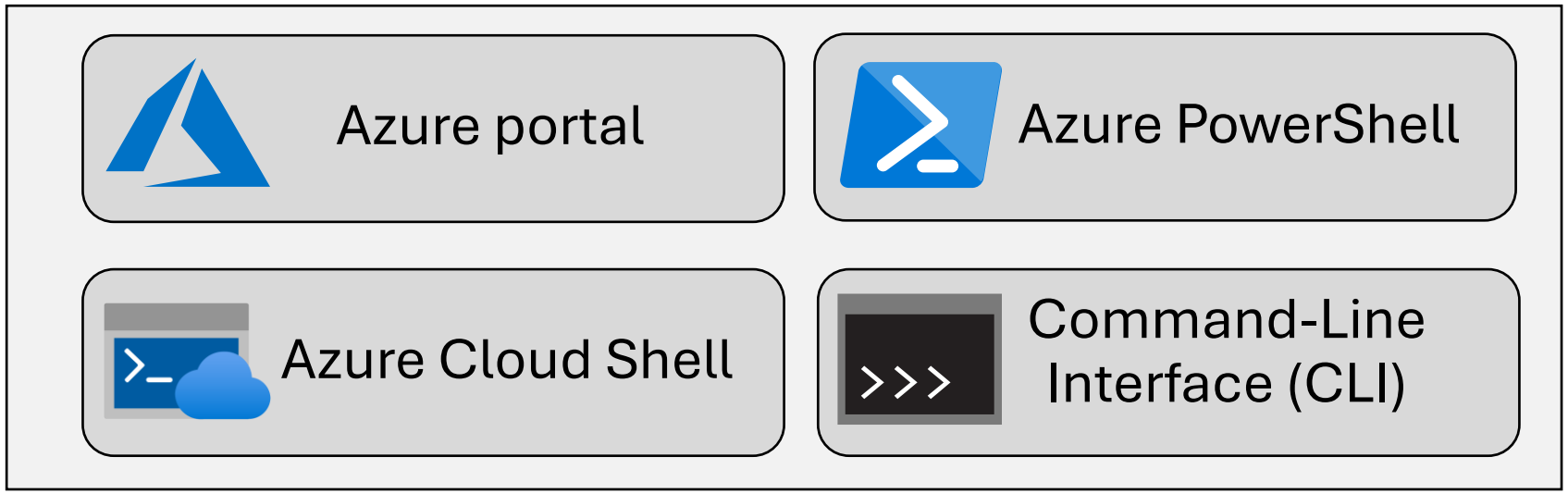
Resource locks

- Protect your Azure resources from accidental deletion or modification.
- Manage locks at subscription, resource group, or individual resource levels within the Azure portal.

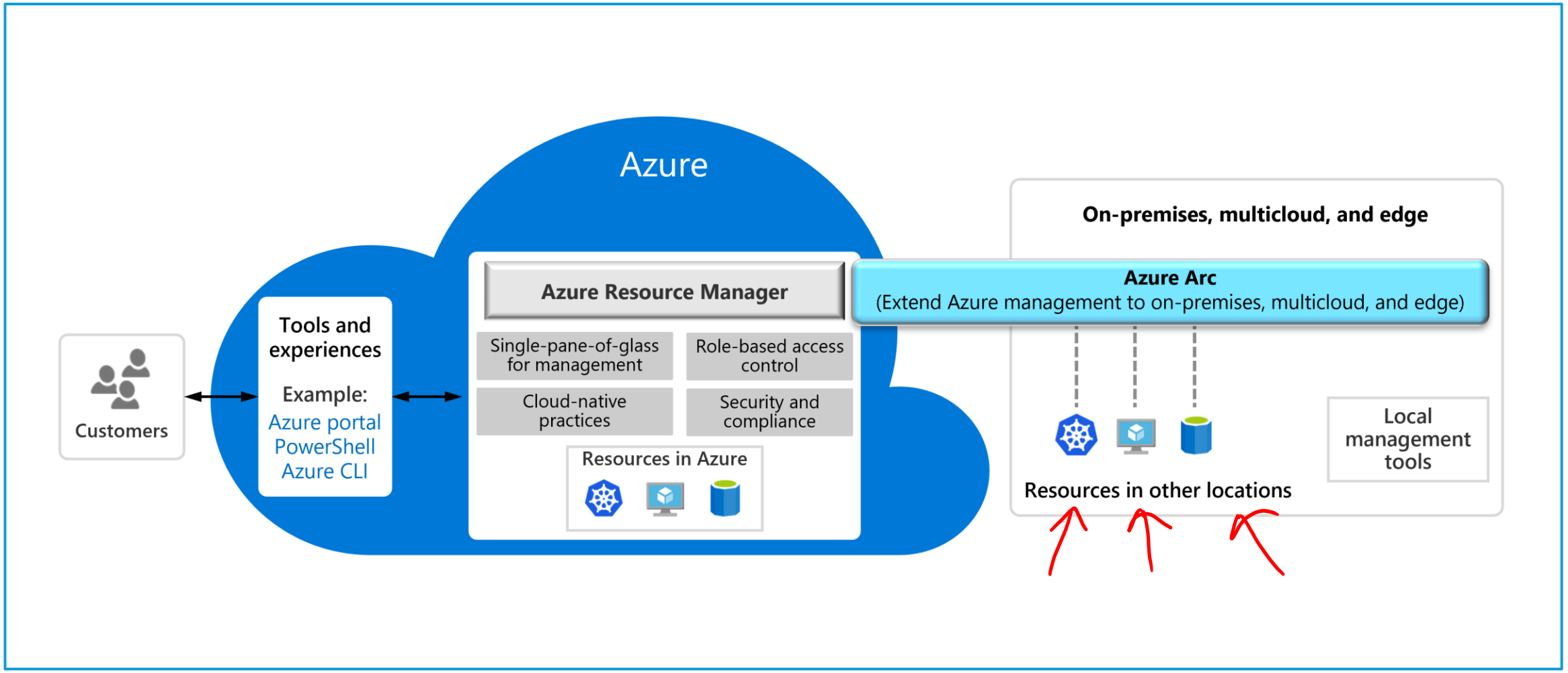
Lock Types	Read	Update	Delete
Delete	Yes	Yes	No
ReadOnly	Yes	No	No

Management and deployment tools

Tools for interacting with Azure

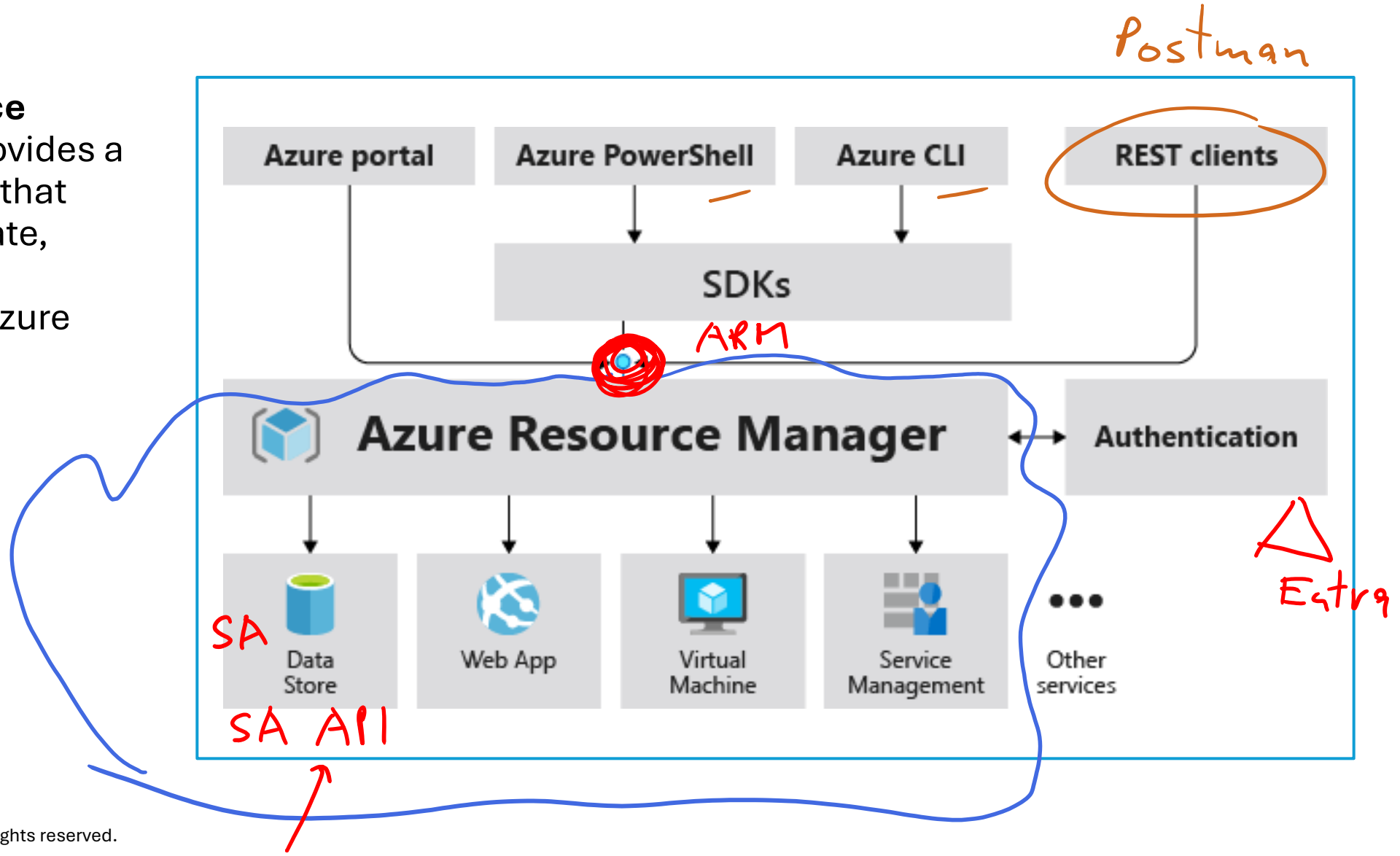


Azure Arc



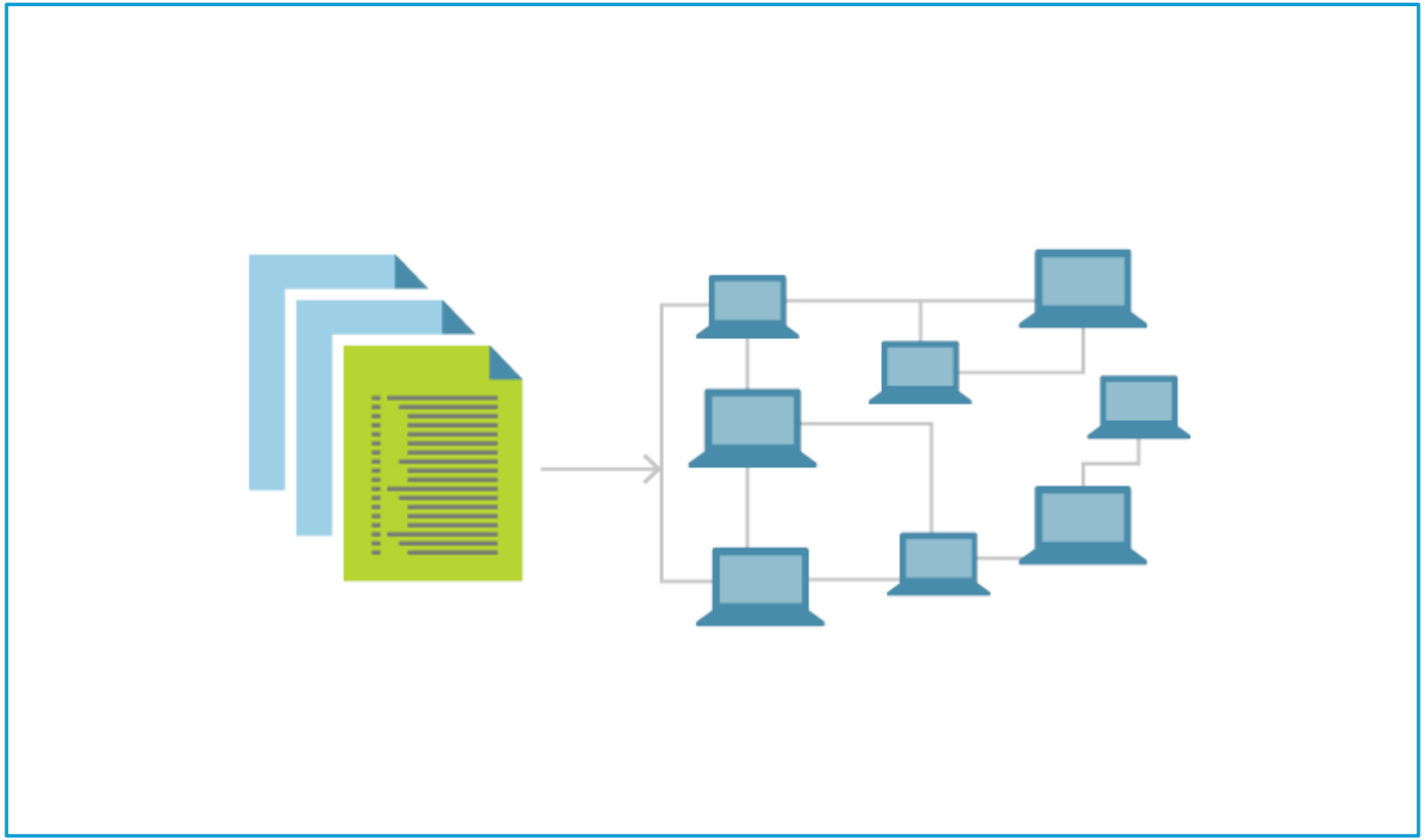
Azure Resource Manager

The **Azure Resource Manager (ARM)** provides a management layer that enables you to create, update, and delete resources in your Azure subscription.



Infrastructure as code

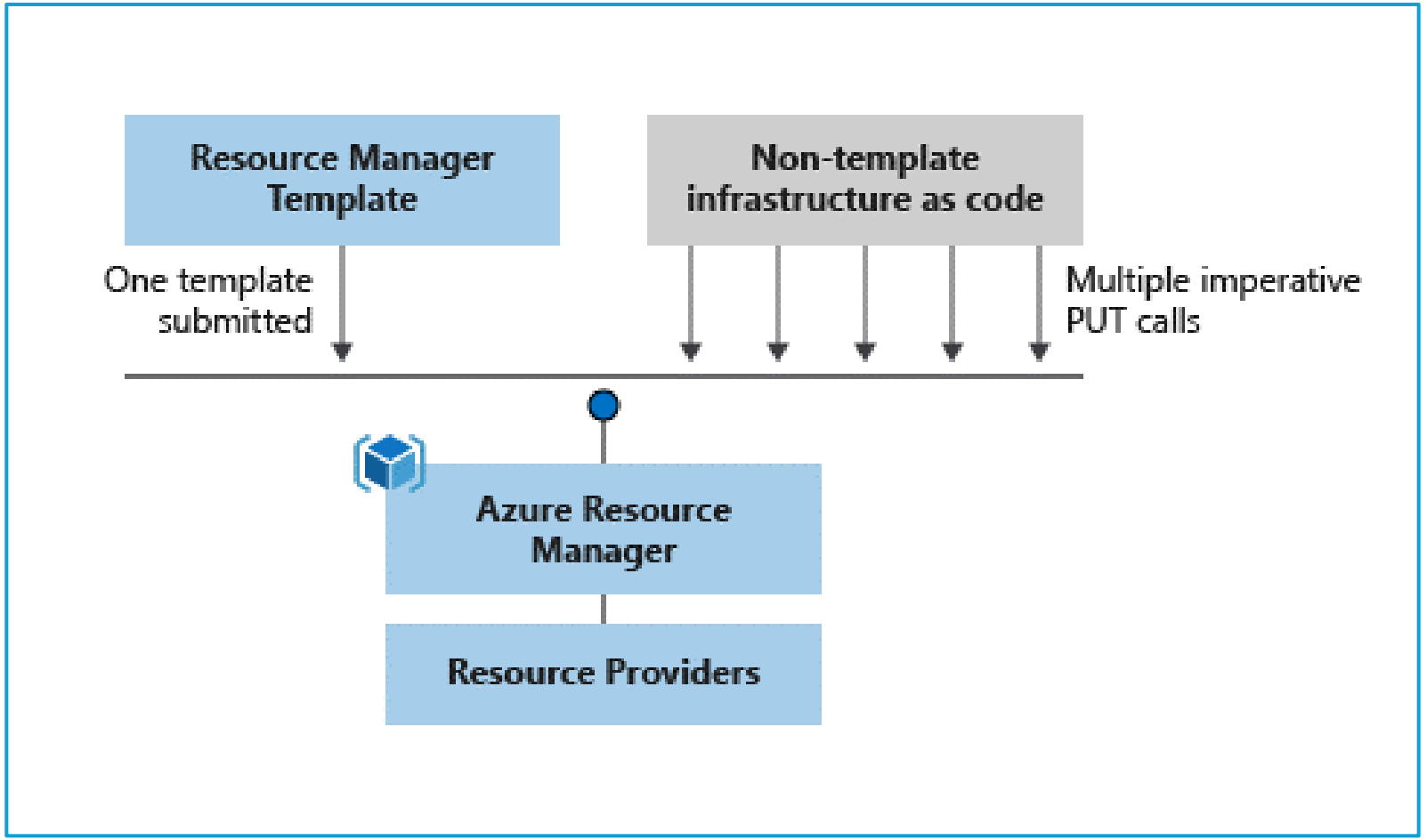
- Ensure consistency in deployment across your cloud ecosystem.
- Manage configuration at scale.
- Rapidly provision additional environments based on a standard configuration and build.



Azure Resource Manager (ARM) templates

Azure Resource Manager (ARM) templates are JavaScript Object Notation (JSON) files that can be used to create and deploy Azure infrastructure without having to write programing commands.

- Declarative syntax
- Repeatable results
- Orchestration
- Modular files
- Built-in validation
- Exportable code



Bicep

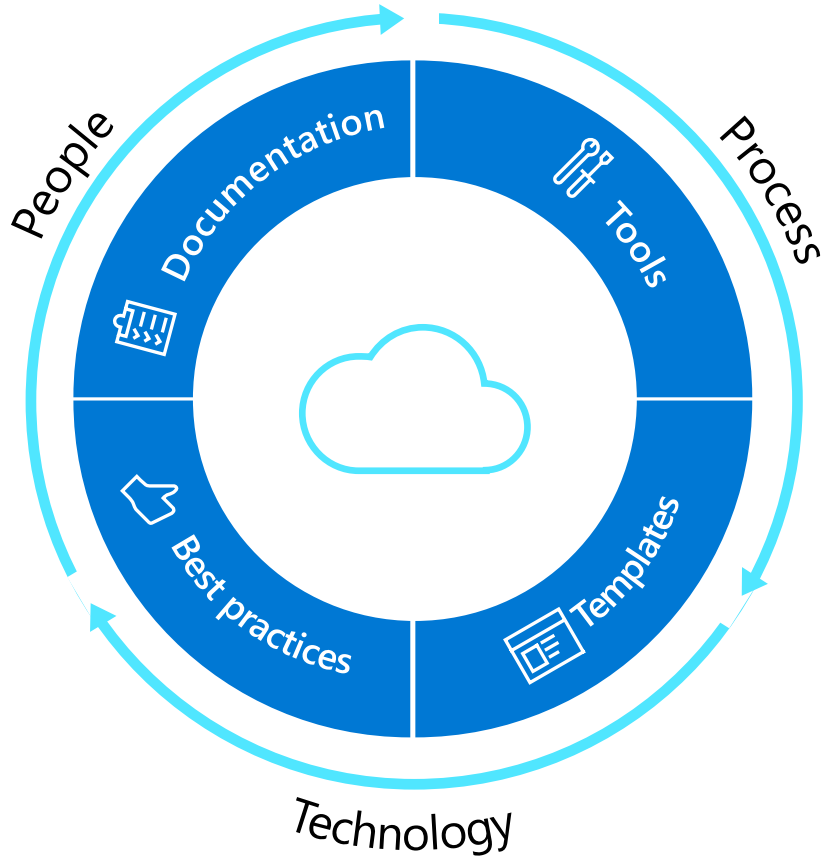
Bicep

```
param location string = resourceGroup().location
param storageAccountName string = 'toylaunch${uniqueString(resourceGroup().id)}'

resource storageAccount 'Microsoft.Storage/storageAccounts@2021-06-01' = {
  name: storageAccountName
  location: location
  sku: {
    name: 'Standard_LRS'
  }
  kind: 'StorageV2'
  properties: {
    accessTier: 'Hot'
  }
}
```

Microsoft Cloud Adoption Framework for Azure

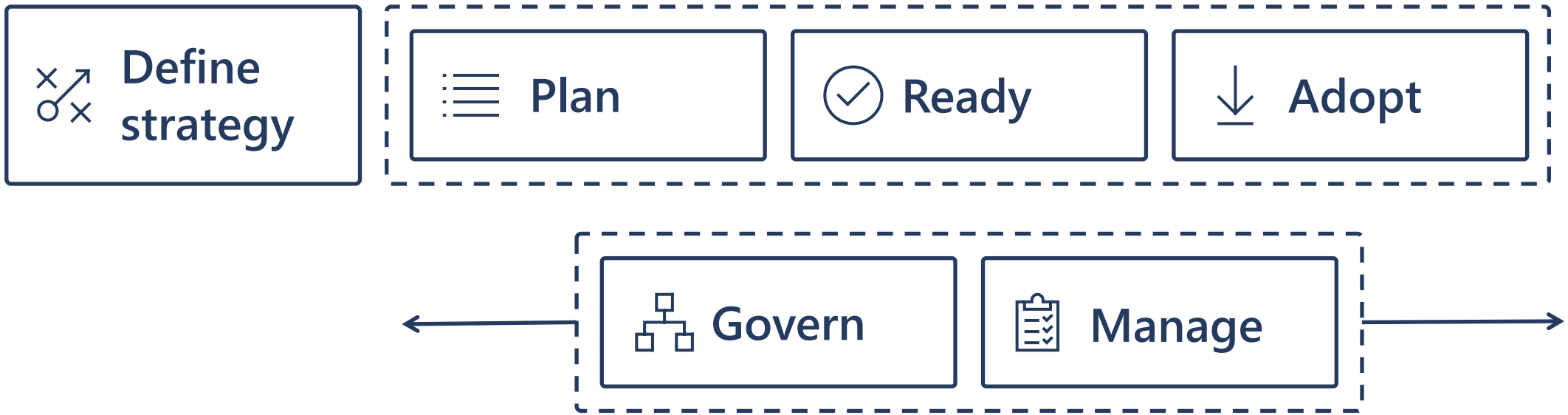
Microsoft Cloud Adoption Framework for Azure



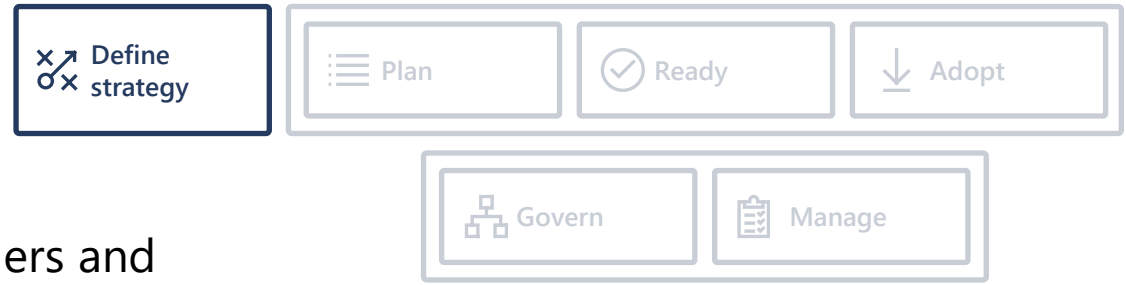
Align **business, people and technology strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

Building the framework

Modular approach, meeting the customer in their journey



Define strategy



Documenting the cloud strategy will help business stakeholders and technicians understand the benefits the organization is pursuing by adopting the cloud.

Motivations

- Executive mandate
- DC Exit
- Merger and acquisitions
- Cost savings
- Optimization
- Agility
- Tech capabilities
- Market demands
- Geo expansion
- Migration
- Innovation

Business outcomes

- **Fiscal:** revenue, cost, profit
- **Agility:** timer to market, provisioning,
- **Reach:** global access, sovereignty
- **Customer engagement:** cycle time, from request to release
- **Performance:** SLAs, Downtime, operations, reliability

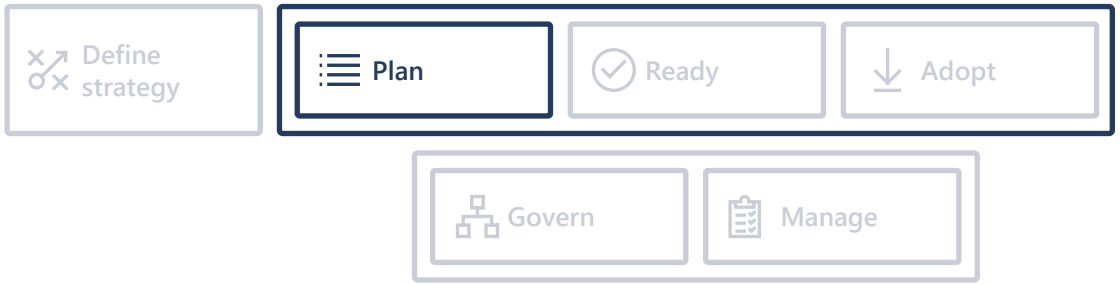
Business justification

- **Business case:** the cloud is not always cheaper, mirroring is not cloud, servers drive cost analysis
- **Financial model:** Capex/ Opex, ROI, gain, cost avoidance/reduction
- **Cloud accounting:** cost center, procurement, profit center, revenue generating, chargeback

First project

- **Business criteria:** workload supported by a BDM
- **Technical criteria:** minimum dependencies and test path, no governance
- **Qualitative analysis:** Current Team analysis

Plan



Cloud adoption plans convert the aspirational goals of the cloud adoption strategy into actions. It will help guide technical efforts, in alignment with the business strategy.

Digital estate

- **Rationalization:** inventory
- **Quantitative analysis:** asset optimized and sized properly
- **Qualitative analysis:** operational process

Initial organization alignment

- **Cloud Strategy Team**
  - Business IT: requirements and needs
  - IT management operations: traditional IT
  - Governance: executive sponsor, finance, business leadership, legal, security, HR
  - Cloud platform vendor: account success team
- **Cost management**
- **IT-business alignment**
- **Governance MVP**

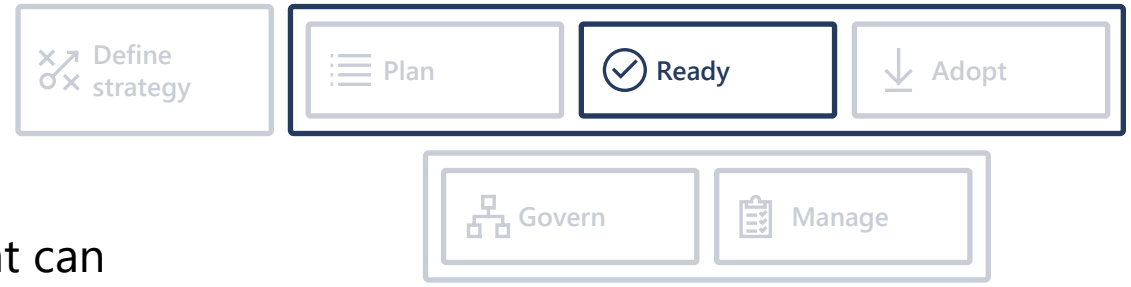
Skill readiness plan

- **Organizational readiness**
- **Governance and security alignment**
- **Initial organization alignment**
- **Building technical skills:** business/technical, and certifications
- **Change management guidance**

Cloud adoption plan

- **5R strategy:** rehost, refactor, rearchitect, rebuild, replace
- **Infrastructure migration:** VM, server, database focus
- **Application innovation:** born in the cloud applications, APIs
- **Data-driven innovation:** Focus on data consolidation and analysis

Ready



Ready establishes a cloud foundation or Adoption Target that can provide hosting for any adoption efforts. This should consist of common denominators across 80–90% of cloud adoption.

Azure readiness guide

- **Resource management:** management groups, subscriptions, resource groups, resources tree hierarchy
- **Naming Standards**
- **Resource tags**

Landing zone infrastructure

- **Network design:** Vnet, hybrid, firewall, hub, front door, endpoints
- **Storage design:** disk, file, blobs, CDN
- **Compute design:** VMs, containers, apps, serverless
- **Data design:** Structured/ unstructured

Landing zone ID

- **Identity and access**
- Role-based access control **RBAC**
- Manage to **least privilege**

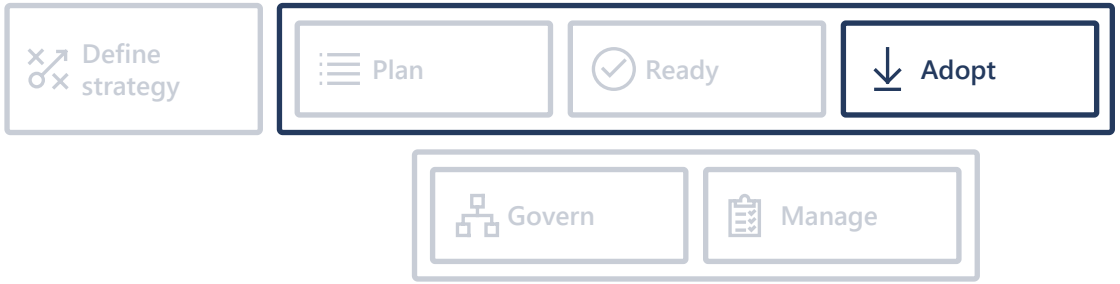
Landing zone cost

- **Costs and billing**
- Analyze **Cloud Costs**
- Monitor with **budgets**
- **Optimize** with recommendations
- **Manage** invoices and payments

Blueprints

- **AI**
- BigData
- Hybrid networks
- **Identity management**
- **IoT**
- **Serverless**
- **SAP**
- VMs
- WebApps
- DevOps

Adopt: Migrate



Cloud adoption will include workloads which do not warrant significant investments in the creation of new business logic. Those workloads could be moved to the migrated to the cloud.

Assess

- **Evaluate** assets and establish a plan
- **Validate pre-requisites:** landing zone, skilling
- **Drivers:** reducing capex, freeing up DC
- **Quantitative factors:** VMs, networking, compatibility
- **Qualitative factors:** process dependencies, critical business events

Migrate: rehost

- **Replicate** (lift and shift) on-prem functionality using cloud native technology
- Leverage **Azure Migration Guide**

Optimize

- **Balance performance and price**
- Deliver the right experience **within budget**
- **Resize VM size, resize storage, resize database**

Secure and manage

- Prepare the migrated asset for ongoing operations: **security, monitoring, configuration**

Adopt: Innovate

Older apps can take advantage of many of the same cloud-native benefits by modernizing the solution or components of the solution. Modern DevOps invites into the process to create shorter feedback loops and better customer experiences.

Infrastructure abstraction

- Cloud native applications built from the ground up **optimized for cloud:**
- Resiliency
- Global scale
- Agility
- Security
- Autoscaling

Innovate: refactor

- Refactoring an application to fit a **PaaS/Serverless-based model** or refactoring code to deliver on new business opportunities.
- **Drivers:** faster and shorter updates, code portability, greater cloud efficiency (resources, speed, cost)

Innovate: rearchitect

- Modify existing applications into managed **containers** to take advantage of cloud native benefits
- **Drivers:** application scale and agility, easier adoption of new cloud capabilities, mix of technology stacks

Innovate: rebuild

- A new code base is created to align with a **cloud-native** approach. **App Data and AI Services**
- **Drivers:** accelerate innovation, build apps faster, reduce operational cost

DevOps

- Culture
- Development
- Testing
- Release
- Monitoring
- Management

Govern

Policy definition ensures consistency across adoption efforts. Alignment to governance/compliance requirements is key to maintain a well-managed cross-cloud environment.

Business risk

- **Document** evolving business risk
- Document risk tolerance based on **data classification**, and **application criticality**

Policy & compliance

- Convert risk decisions into **policy statements**
- Establish cloud adoption boundaries

Processes

- Establish processes to **monitor violations**
- Adhere to corporate policies
- **Cloud Center of Excellence**

Cost management

- Evaluate and monitor cost
- Limit IT spend
- Scale based on business demand
- Create cost accountability

Security baseline

- Compliance with IT Security requirements
- Apply security baseline to all adoption efforts

Resource consistency

- Consistency in resource configuration
- Enforce on boarding, recovery and discoverability practices

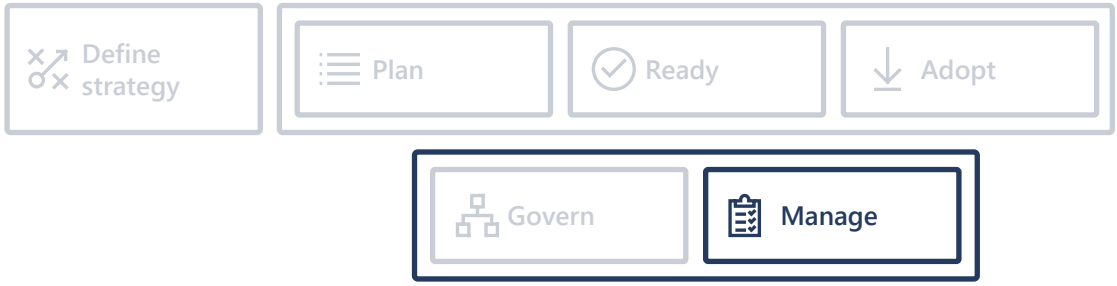
Identity baseline

- Enforce identity and access baseline
- Apply role definitions and assignments

Deployment acceleration

- Centralize templates
- Drive consistency and standardization

Manage and operations



Manage and operations enumerates, implements, and iteratively reviews related to the expected operational behavior of the service.

Management

- Identify critical operations for business operations
- Map operations to services
- Analyze services dependencies
- Create high level view service dashboards

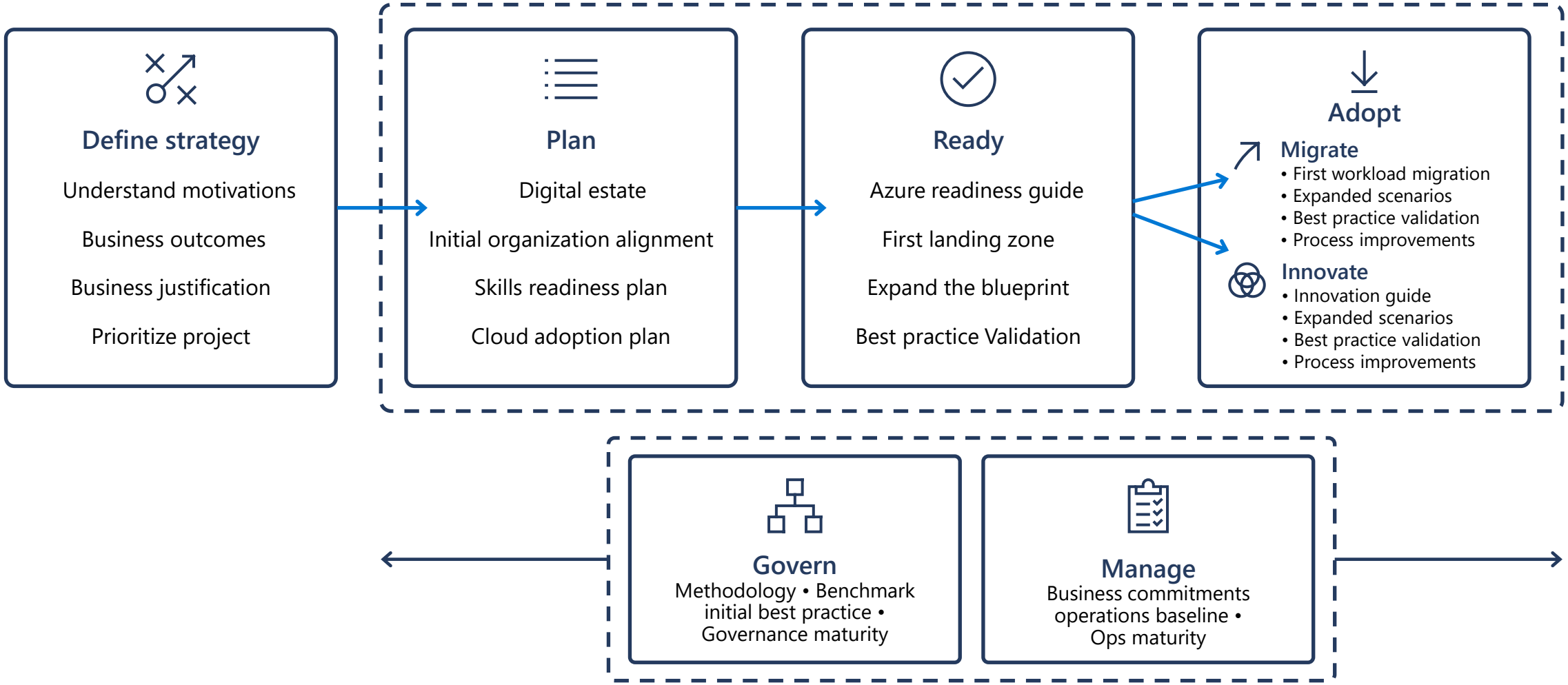
Monitoring

- Enable data collection
- Identify operations baseline
- Generate alerts
- Measure Service Metrics and generate SLAs

Resiliency

- **Enable a resilient** platform
- Recover from failures with minimal downtime and minimum data loss before
- **Evolve to a highly available platform**

Microsoft Cloud Adoption Framework for Azure



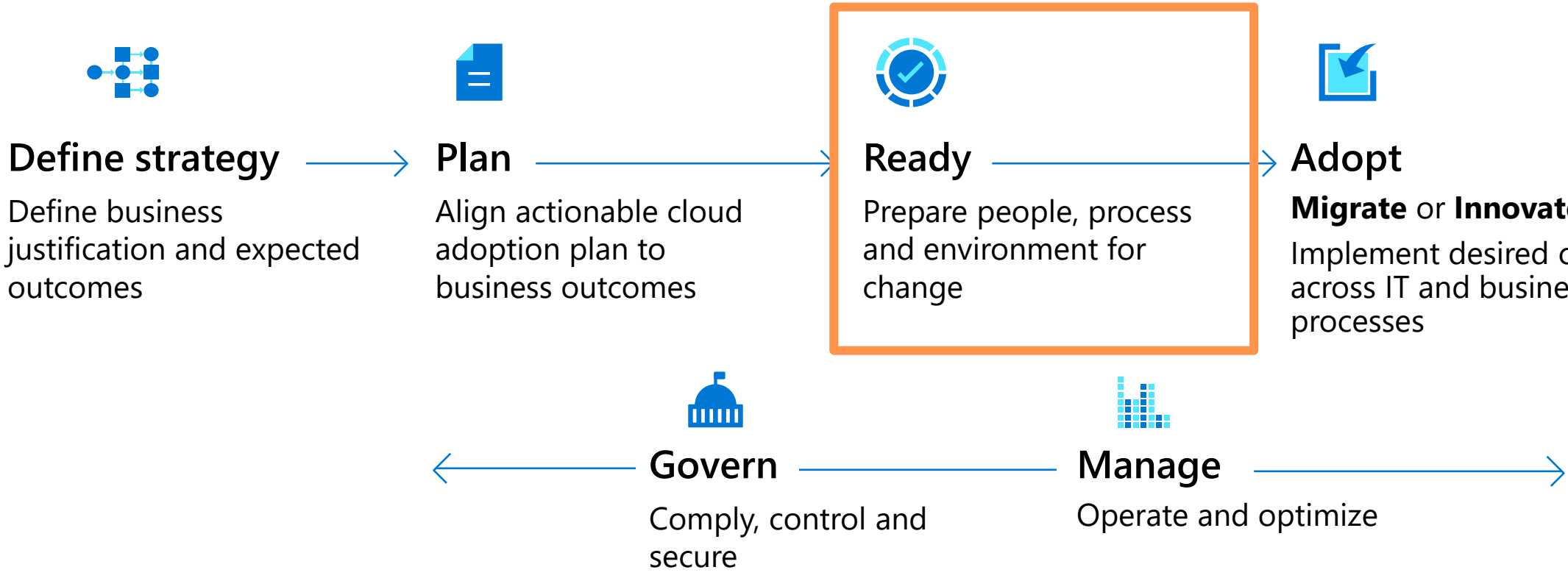
Microsoft

Enterprise-scale landing zones

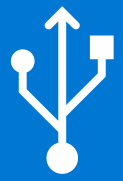
Getting ready to deploy workloads on Azure

Microsoft Cloud Adoption Framework for Azure

*Proven business and technical guidance to help customers create and implement the **business and technology strategies** necessary to succeed in the cloud*



Key Challenges



Architecture Complexity: Customers lack the required level of understanding and experience on Azure. The mismatch between on-premises infrastructure and cloud-design considerations creates dissonance and friction with respect to defining architectures and standards for their migration to the cloud. They are struggling with the translation of their requirements to Azure concepts, capabilities, constructs and security model.

Operating Compatibility: Existing approaches and functions for the traditional delivery and management of IT services are not compatible with the Azure platform and cloud operating models. When combined with a lack of skills and experience, customers are struggling to define and therefore transform their operating model to manage and support large-scale cloud infrastructure.

Lack of Trust and Desire for Control: The absence of a precise and detailed cloud architecture that is compliant with their requirements, and the lack of a well-defined operating model to support such a platform, leads IT not to trust Azure and instead strive to maintain full control. This often involves building ‘walls’ and complicated processes which ultimately get in the way of business lines adopting Azure.

Enterprise-scale?

Enterprise-scale is an architecture approach and reference implementation that enables effective construction and operationalization of landing zones on Azure, at scale and aligned with Azure Roadmap and Microsoft Cloud Adoption Framework for Azure.

Authoritative
Provides holistic design decision framework for Azure Platform.

Proven
Based on success of large-scale migration projects at-scale.

Prescriptive
Apply it on clearly plan and design your Azure environment.

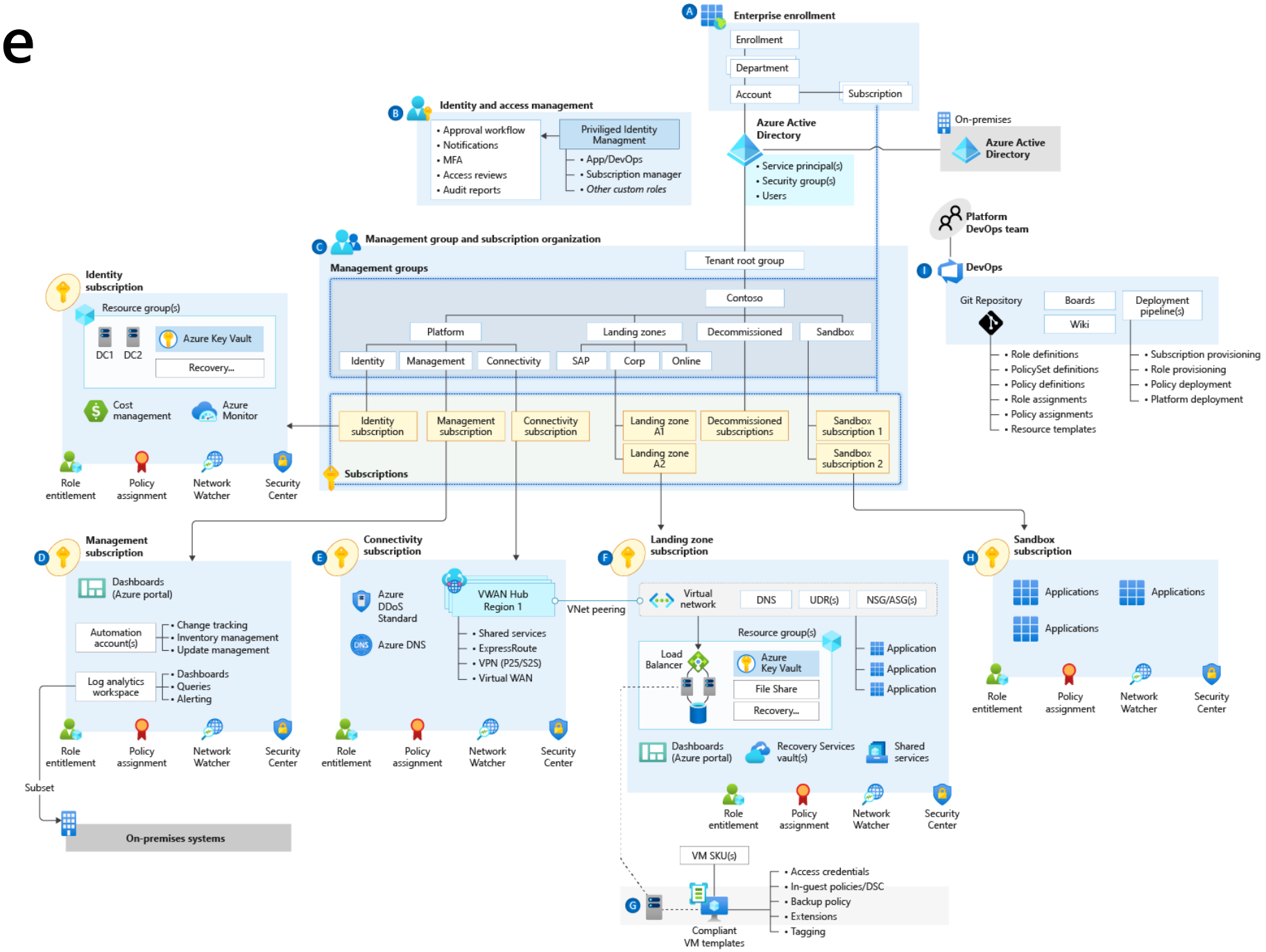
Enterprise-scale Architecture:

- **Enterprise-scale design principles**: Principles to help/guide you customize the design.
- **Enterprise-scale design guidelines**: Guidelines (decisions and recommendations) for the 8 components of the enterprise-scale architecture
- **Enterprise-scale Implementation guide**: The way you create those things using reference implementation in GitHub and the deployment pipeline

Enterprise-scale Reference Implementation:

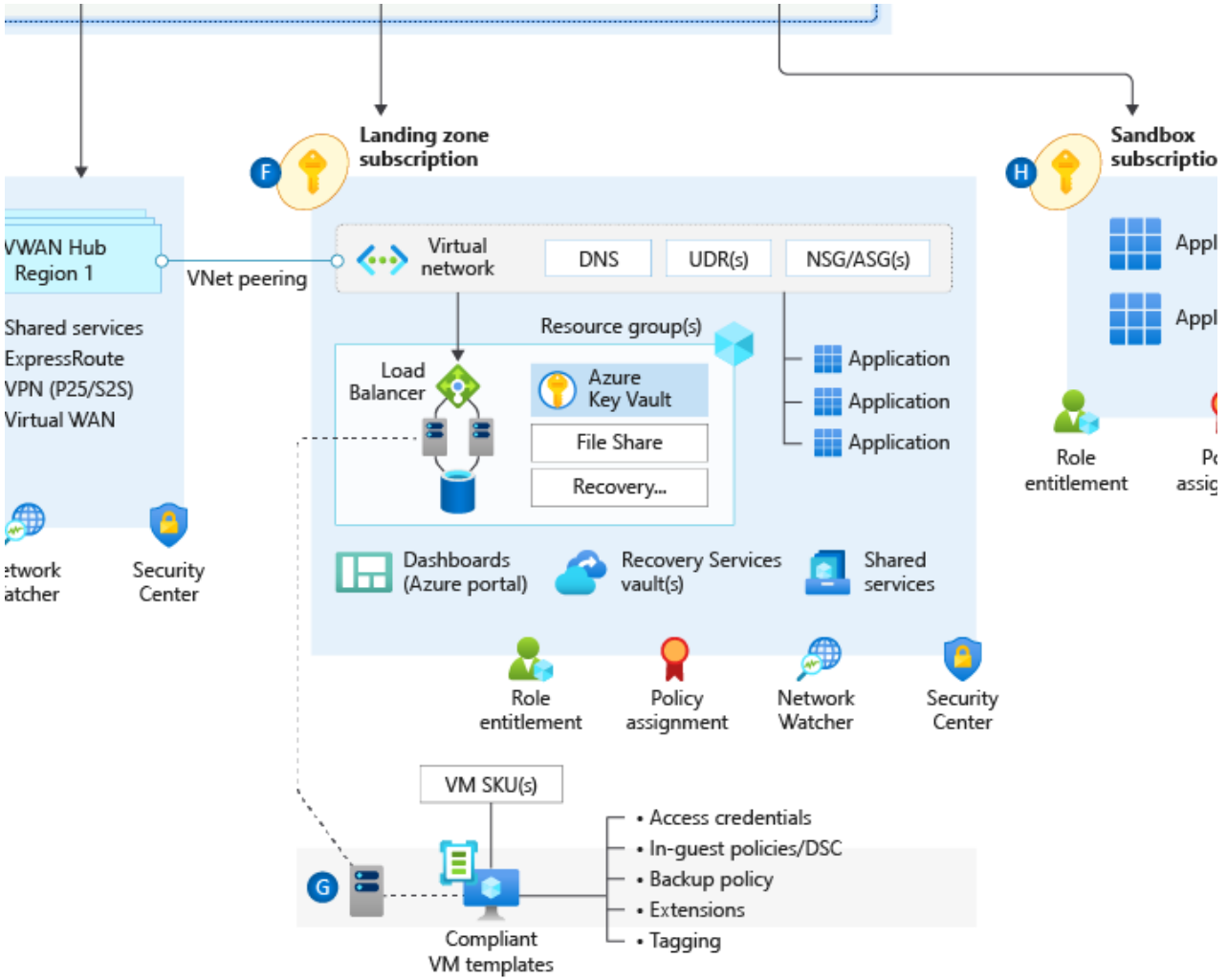
- **Enterprise-scale foundation:** A reference implementation of shared services containing network, security, identity, governance services required to construct and operationalize an enterprise-scale landing zone
- **Enterprise-scale landing zone(s):** A reference implementation of a workload environment conforming to the enterprise-scale architecture (opinionated way to implement, code)

Enterprise-scale



Enterprise-scale landing zone(s)

The principle purpose of the "Landing Zone" is therefore to ensure that when an application or workload lands on Azure, the required "plumbing" is already in place, providing greater agility and compliance with enterprise security and governance requirements.



Enterprise-scale Design Principles

Enterprise-scale Design Principles

Enable Autonomy for Innovation and Transformation

Security and Compliance By-Default

Governance At-Scale with Sustainable Cloud Engineering

Subscription Democratisation

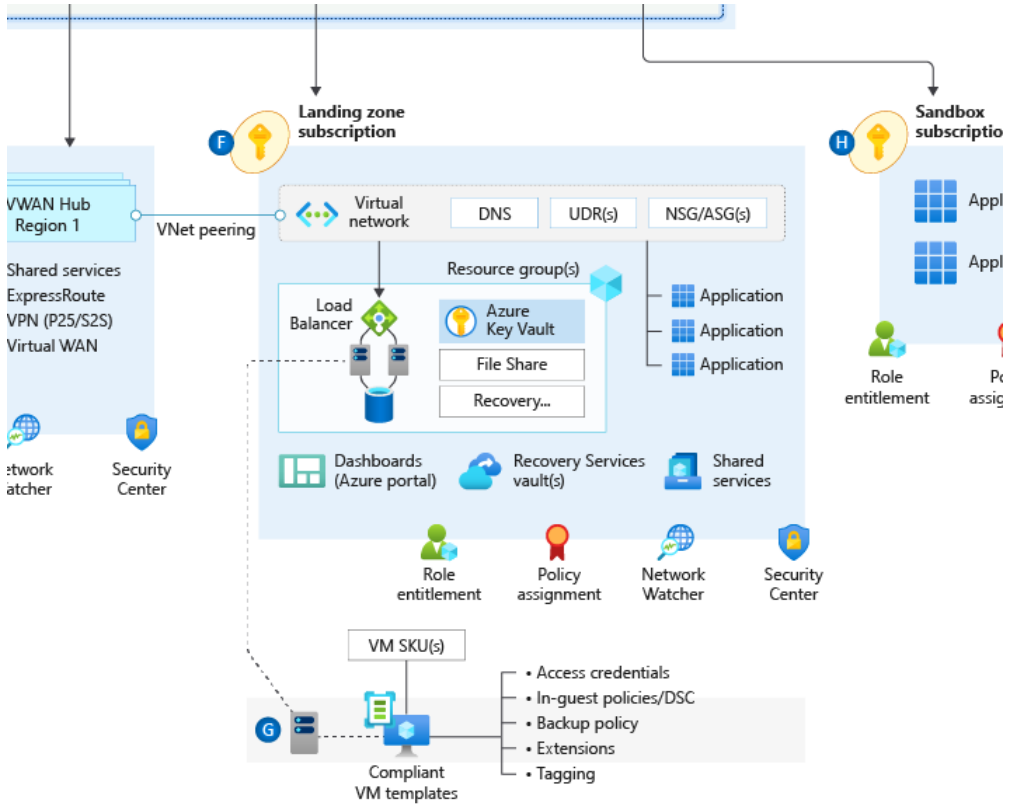
Policy Driven Governance

Single Control and Management Plane

Application Centric and Archetype-Neutral

Azure Native Design and Platform Roadmap Alignment

Enterprise-scale Design Principles

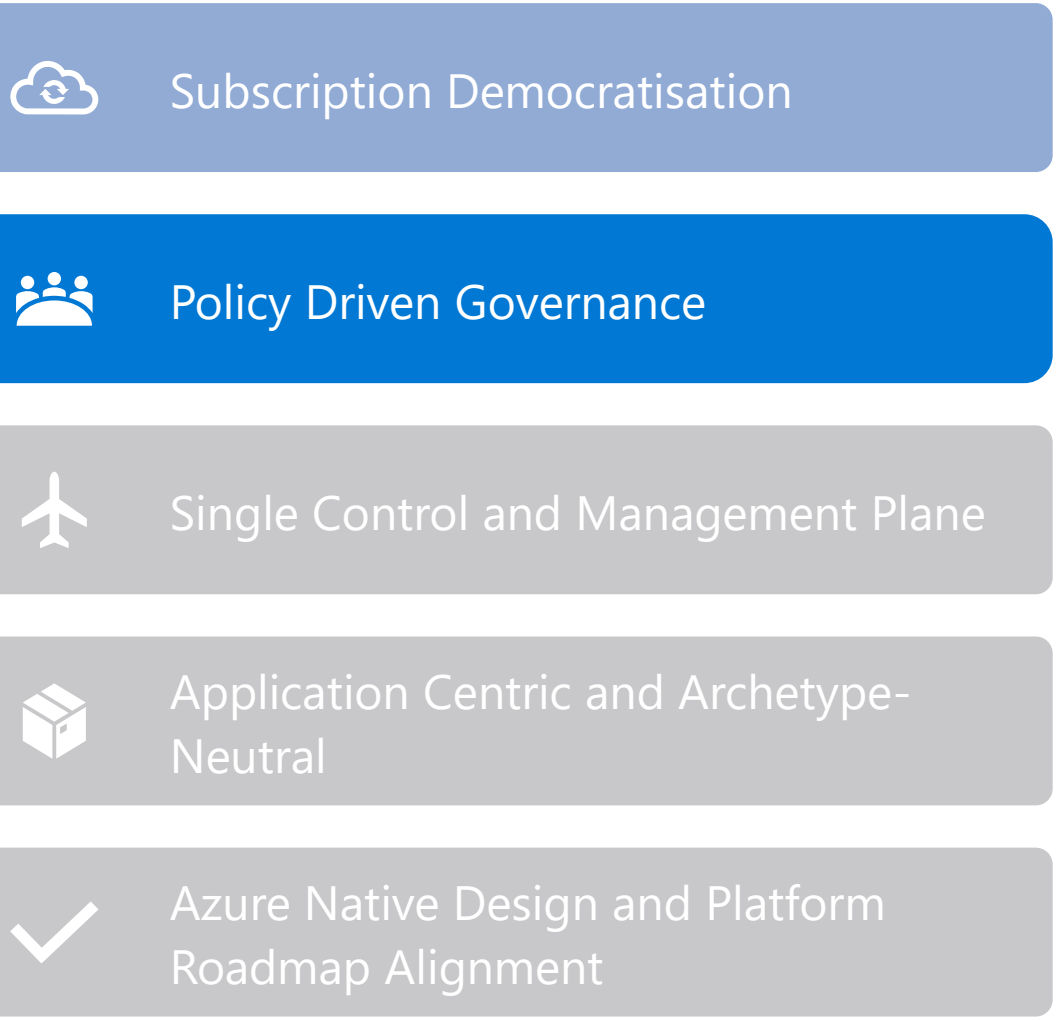


Subscriptions should be used as a unit of management and scale aligned with business needs and priorities, to support business areas and portfolio owners to accelerate application migrations and new application development.

- Subscription Democratization
- Policy Driven Governance
- Single Control and Management Plane
- Application Centric and Archetype-Neutral
- Azure Native Design and Platform Roadmap Alignment

Enterprise-scale Design Principles

Azure Policy should be used to provide the **guard-rails** and ensure the continued compliance of the customer platform and applications deployed onto it, whilst also providing application owners sufficient freedom and a secure unhindered path to cloud.

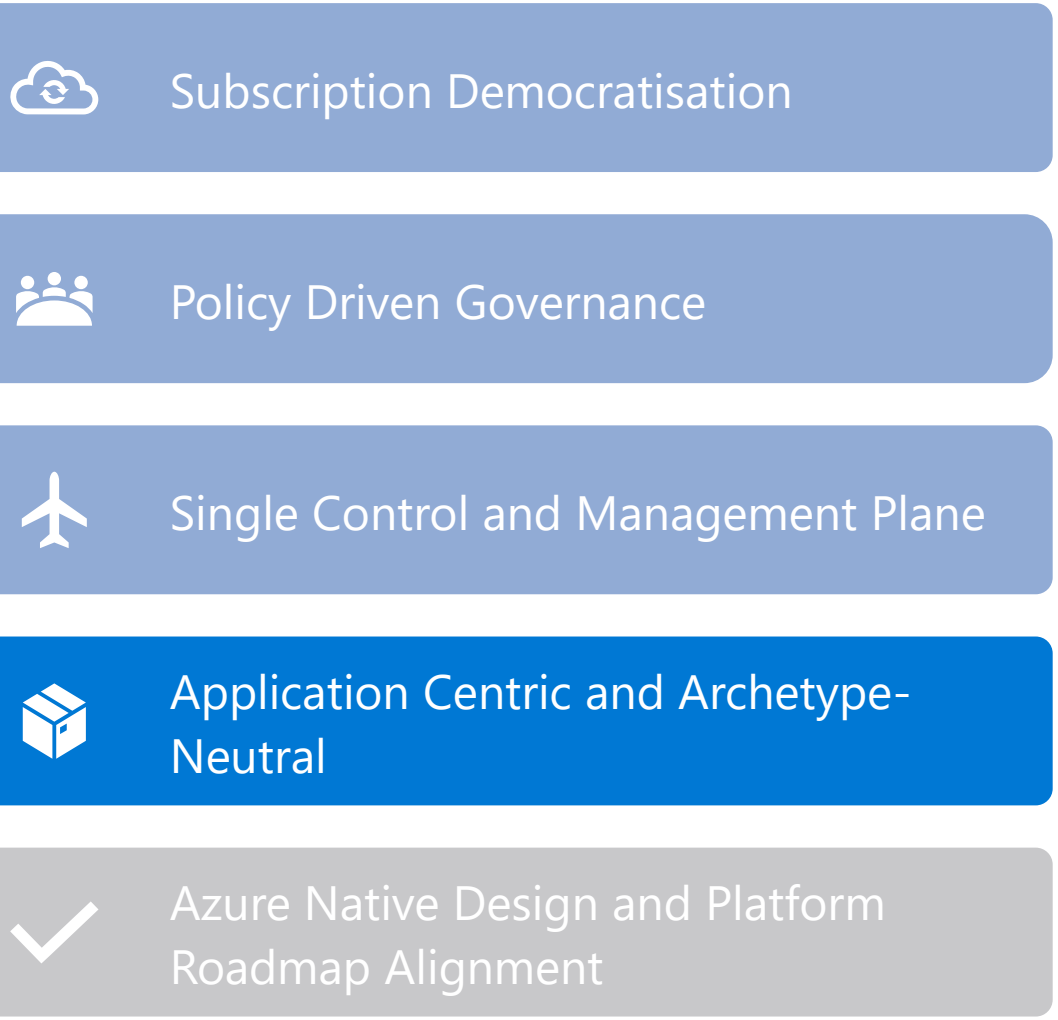


Enterprise-scale Design Principles

The Enterprise-scale architecture should not consider any abstraction layers such as customer developed portals or tooling and should provide a consistent experience for both **AppOps** (centrally managed operation teams) and **DevOps** (dedicated application operation teams).

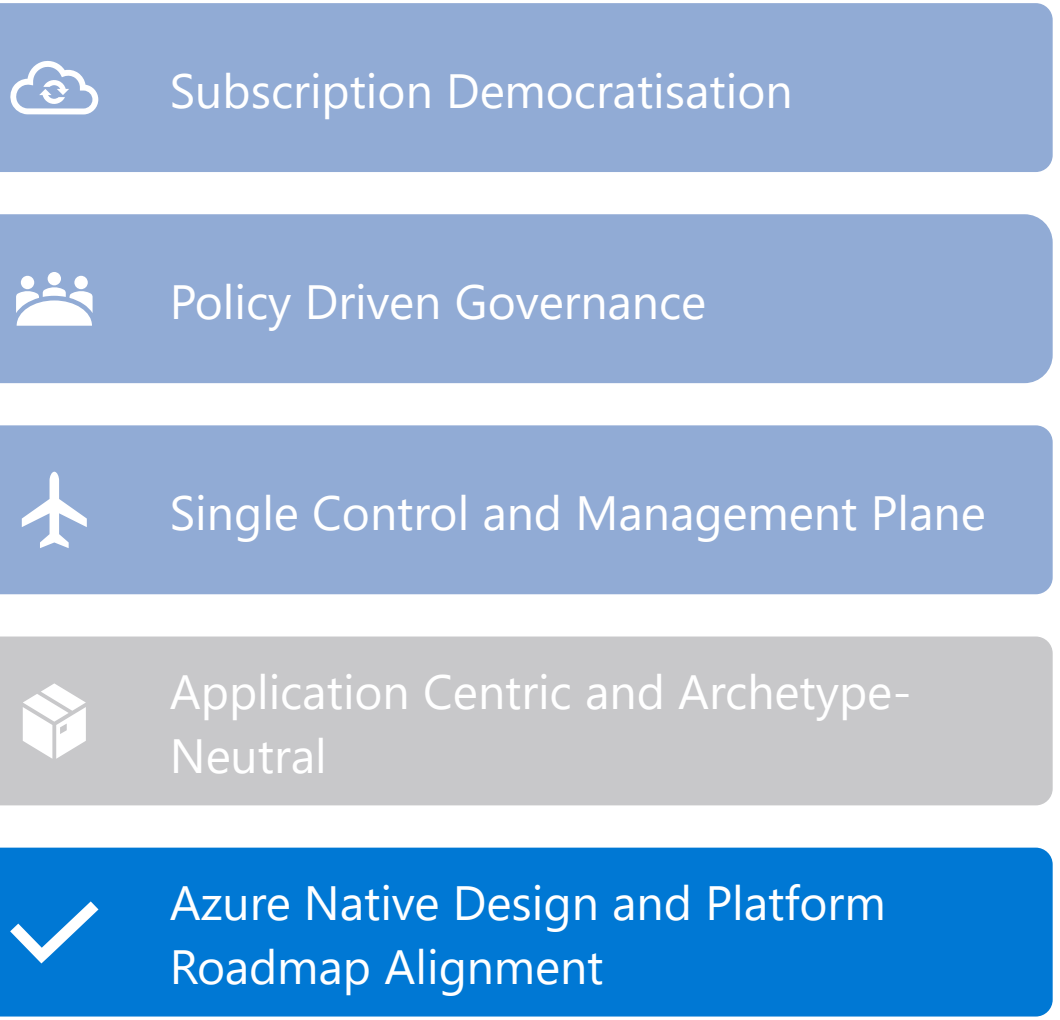
Enterprise-scale Design Principles

We should focus on application centric migrations and development rather than a pure infrastructure "lift and shift" migration (i.e. movement of virtual machines) and should not differentiate between old/new applications or IaaS/PaaS applications.



Enterprise-scale Design Principles

The **Enterprise Scale architecture** approach advocates the use of native platform services and capabilities whenever possible, which should be aligned with Azure platform roadmaps to ensure new capabilities are made available within customer environments.



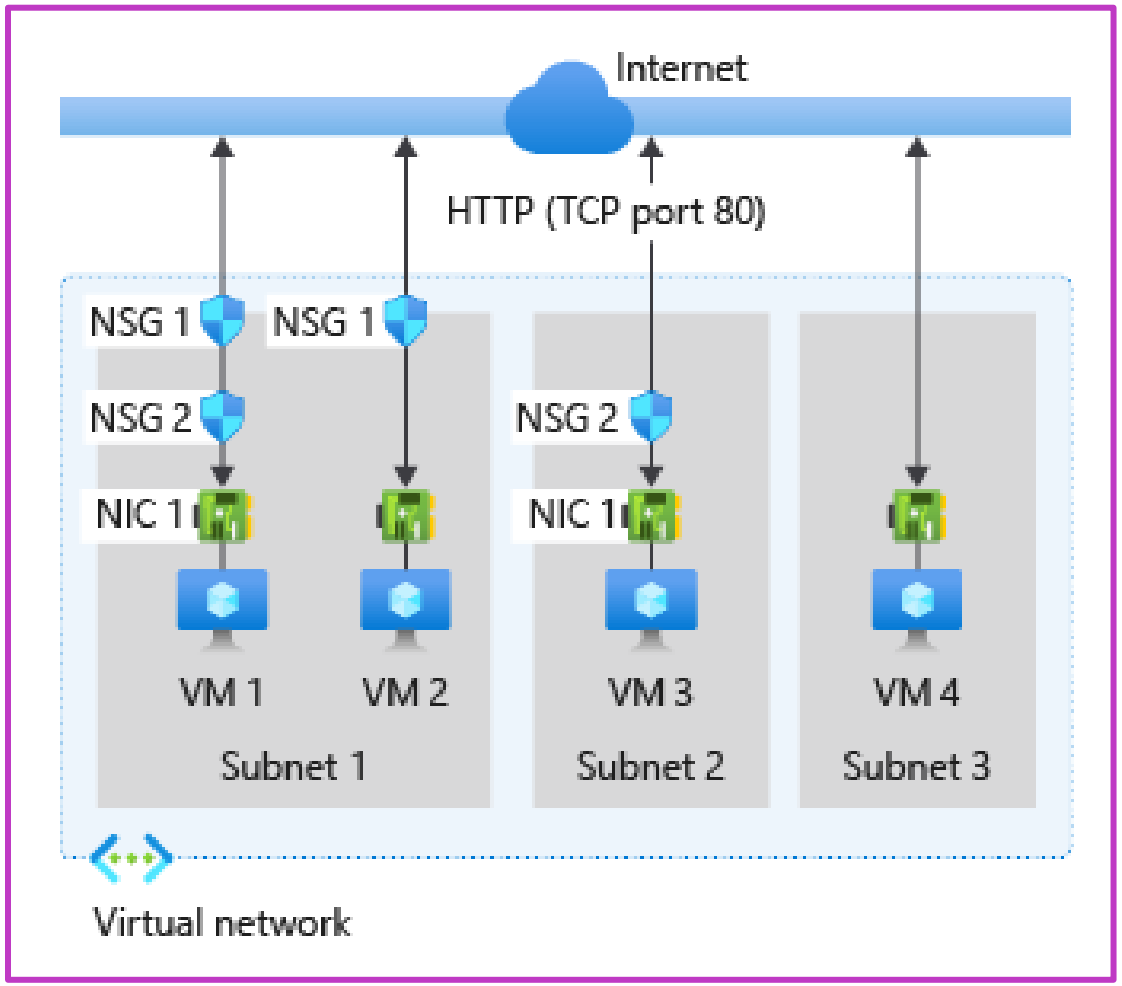
Microsoft Well-Architected Framework - Security

Plan and implement security for virtual networks

Plan and implement Network Security Groups (NSGs)

Network Security Groups

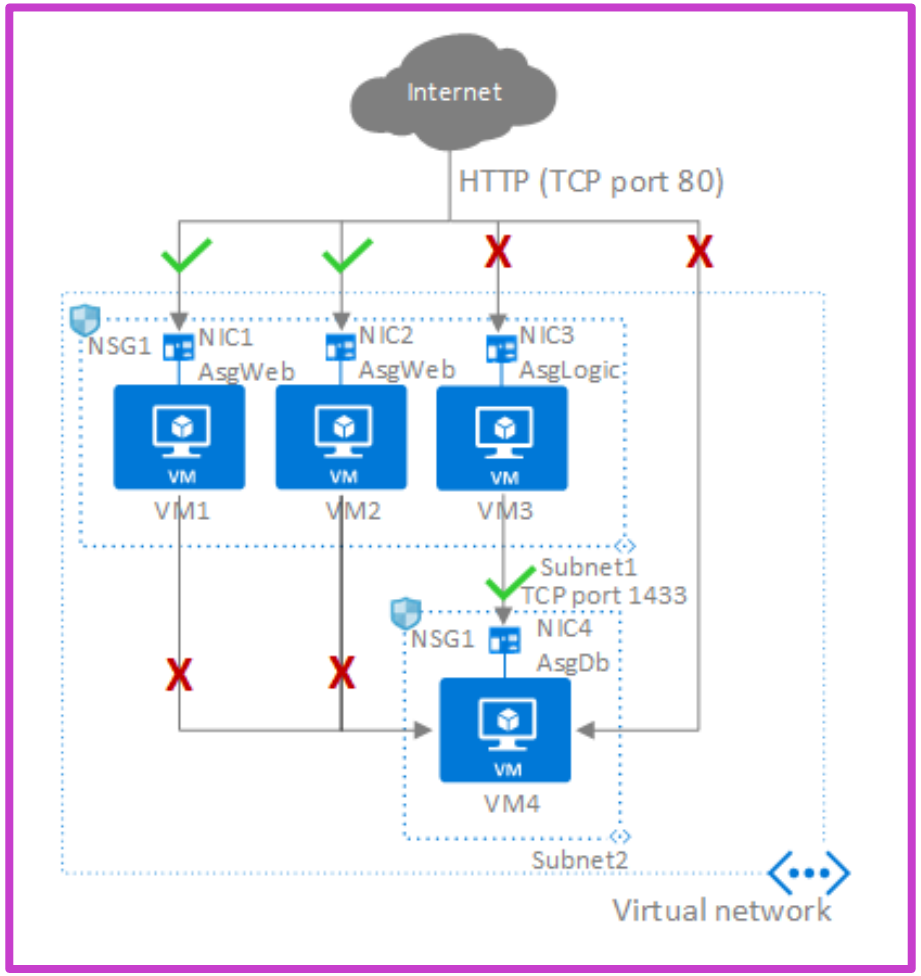
- Filter network traffic between Azure resources like a firewall.
- An NSG can contain any number of rules within Azure subscription limits.
- For each security rule, you can specify source, destination, port, and protocol.
- Rules are evaluated and applied based on the five-tuple (source, source port, destination, destination port, and protocol) information.
- Modifying NSG rules will only impact the new connections that are formed.
- Use augmented security rules to simplify security definition for virtual networks.



Plan and implement Application Security Groups (ASGs)

Application Security Groups

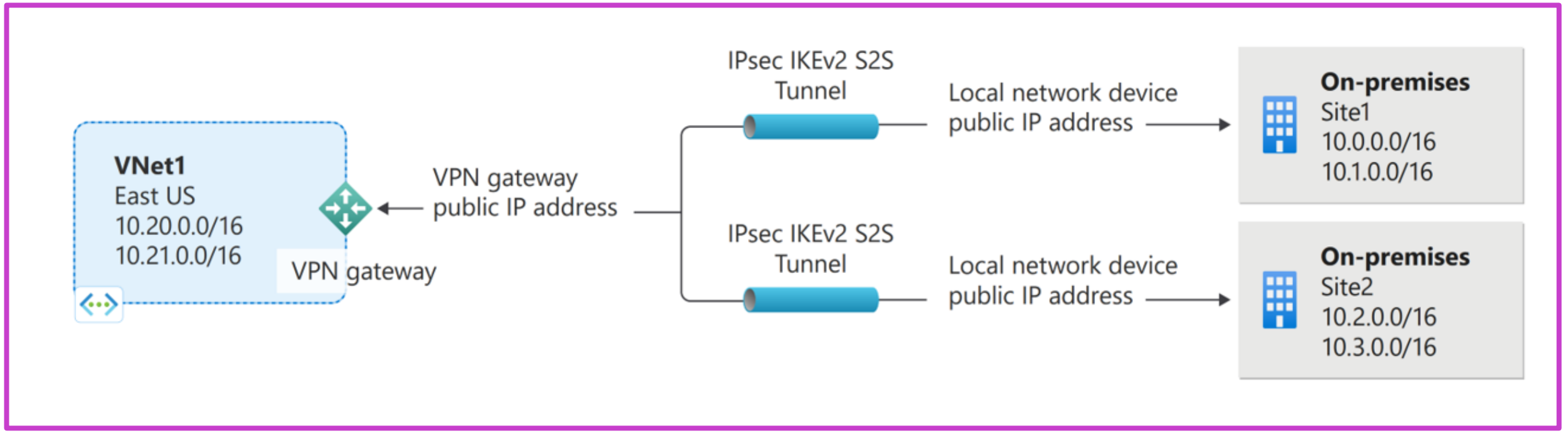
- ASGs enable you to reuse your security policy at scale without manual maintenance of explicit IP addresses.
- The rules that specify an ASG as the source or destination are only applied to the network interfaces that are members of the ASG.
- ASGs have some limitations, such as:
  - All network interfaces assigned to an ASG must exist in the same virtual network that the first network interface assigned to the ASG is in.



VNet1 — Peering — VNet2

Secure VPN connectivity, including a site-to-site VPN with two IPsec IKEv2 tunnels

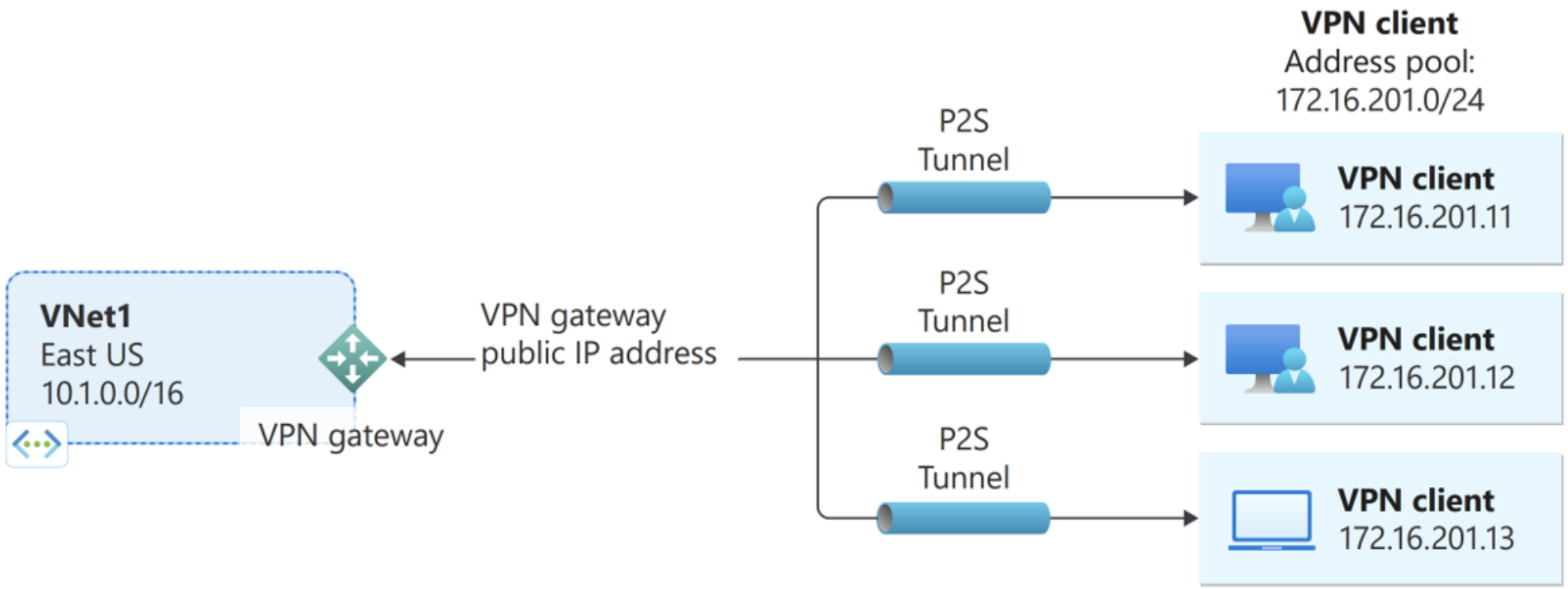
Site-to-site VPN (Two IPsec IKEv2 S2S Tunnels)



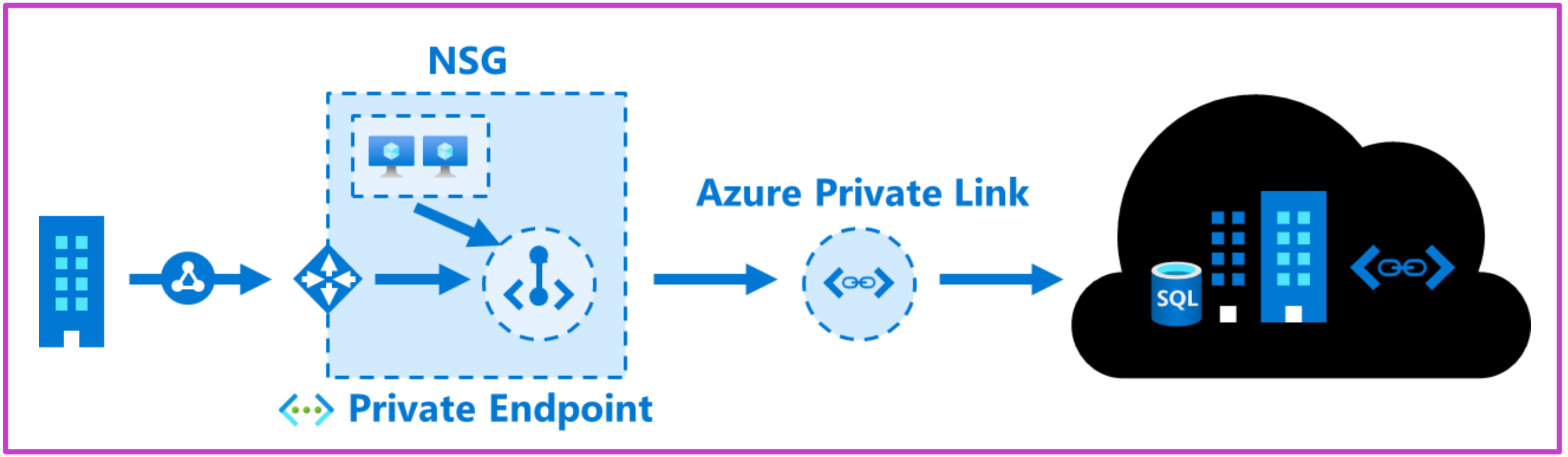
VNet — VNet to VNet Tunnel — VNet2

Point-to-site Virtual Private Network

Point-to-site (P2S) VPN gateway connection

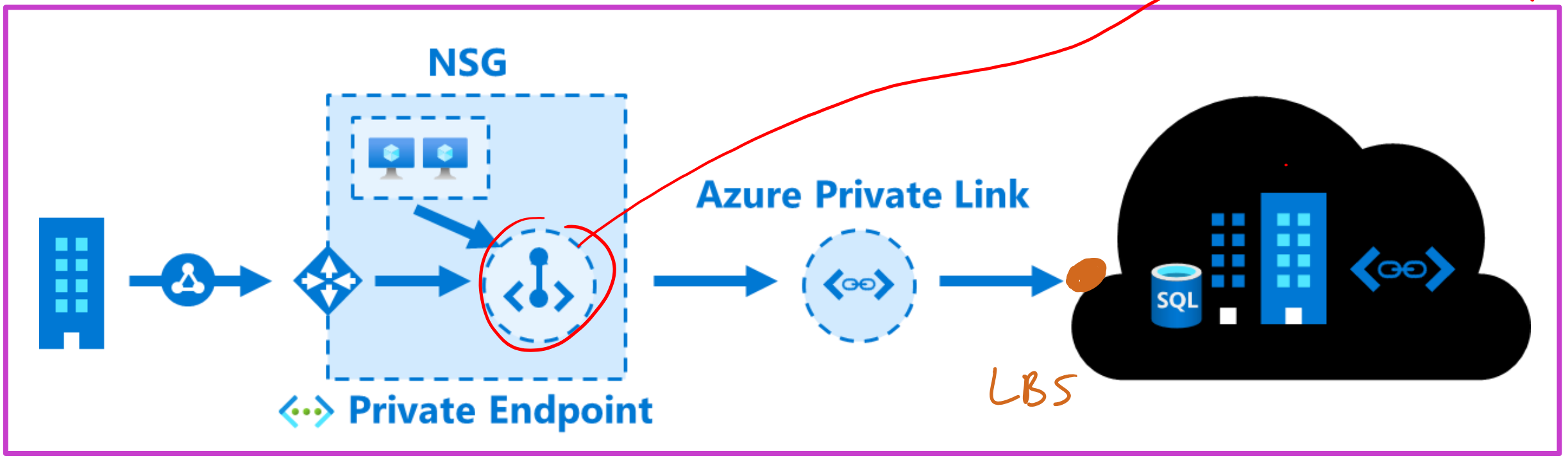


Plan and implement Private Endpoints



- Private connectivity to services on Azure
- Integration with on-premises and peered networks
- Traffic remains on the Microsoft network, with no public internet access
- During a security incident within your network, only the mapped resource would be accessible

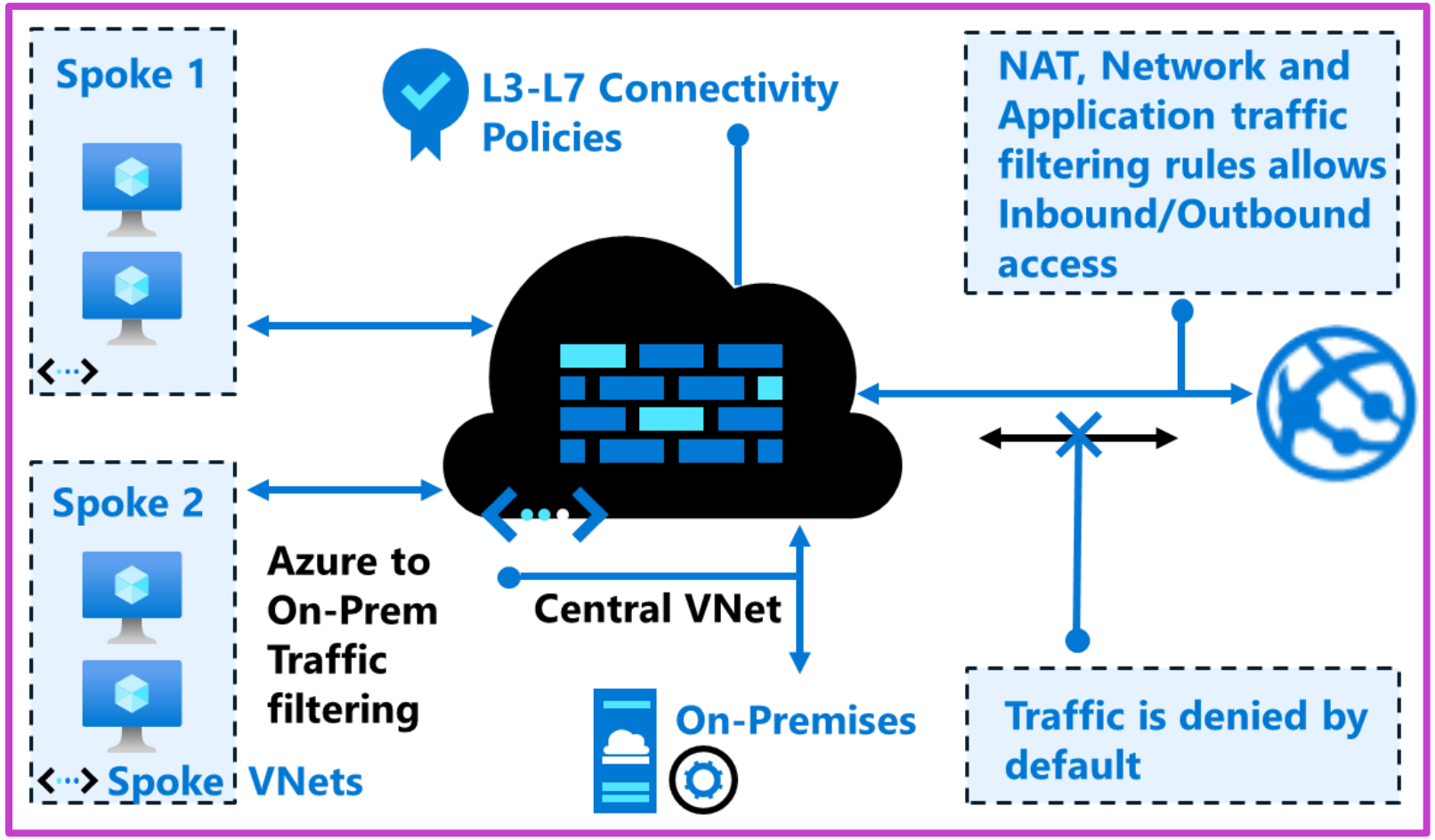
Plan and implement Private Endpoints



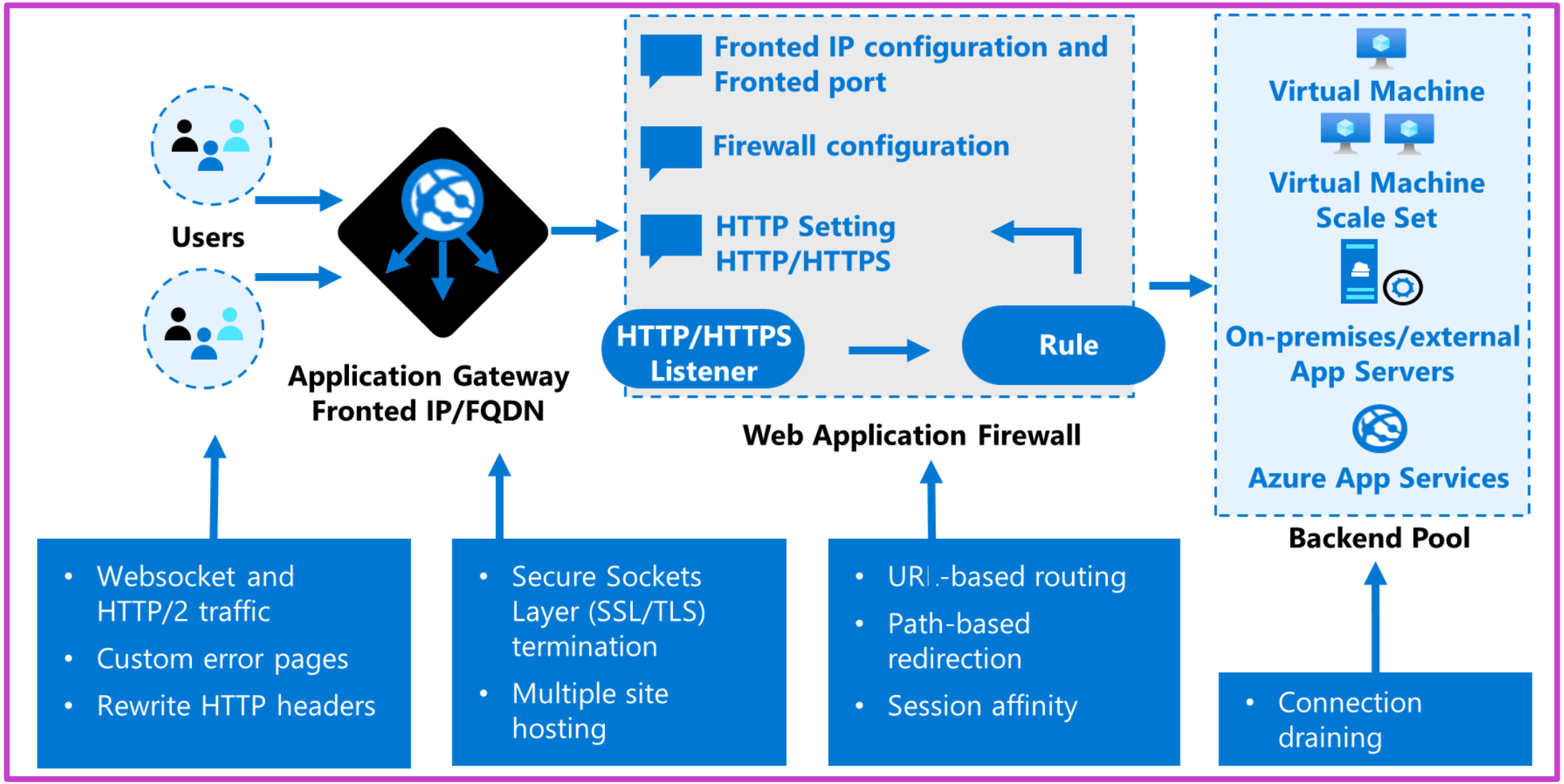
- Private connectivity to services on Azure
- Integration with on-premises and peered networks
- Traffic remains on the Microsoft network, with no public internet access
- During a security incident within your network, only the mapped resource would be accessible

Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies

- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN tags
- Outbound SNAT
- Inbound DNAT support
- L3-L7 connectivity policies
- Separate firewall subnet
- Static public IP address
- Forced tunnelling – Push all internet Traffic for specific next hop (example – on-premises device).



Plan and implement an Azure Application Gateway



"Owner" Key 1 Container - Blob HTTPS SMB

Azure Storage

RBAC "owner" No Data Action

Share - Files HTTPS 443 445

Queues

Tables

- Azure Storage offers durable, scalable, and secure cloud storage for diverse data objects, accessible globally via HTTP/HTTPS.
- It supports a variety of data services like Blob, Files, Elastic SAN, and integrates with Azure services for enhanced functionality.
- Azure Storage is managed by Azure, ensuring high availability and redundancy, with various connectivity and security options for developers and IT professionals.

Key 1

Key 2

Configure access control for storage accounts

Every storage request must be authorized. There are various authorization methods, including anonymous.

Storage	Storage Account Shared Key	Shared access signature	Microsoft Entra ID	Active Directory Domain Services (on-prem ADDS)	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Not supported	Supported
Azure Files (SMB)	Supported	Not supported	Supported, only with Microsoft Entra Domain Services	Supported, credentials must be synced to Microsoft Entra ID	Not supported
Azure Files (REST)	Supported	Supported	Supported	Not supported	Not supported
Azure Queues	Supported	Supported	Supported	Not supported	Not supported
Azure Tables	Supported	Supported	Supported	Not supported	Not supported

Manage storage account access keys

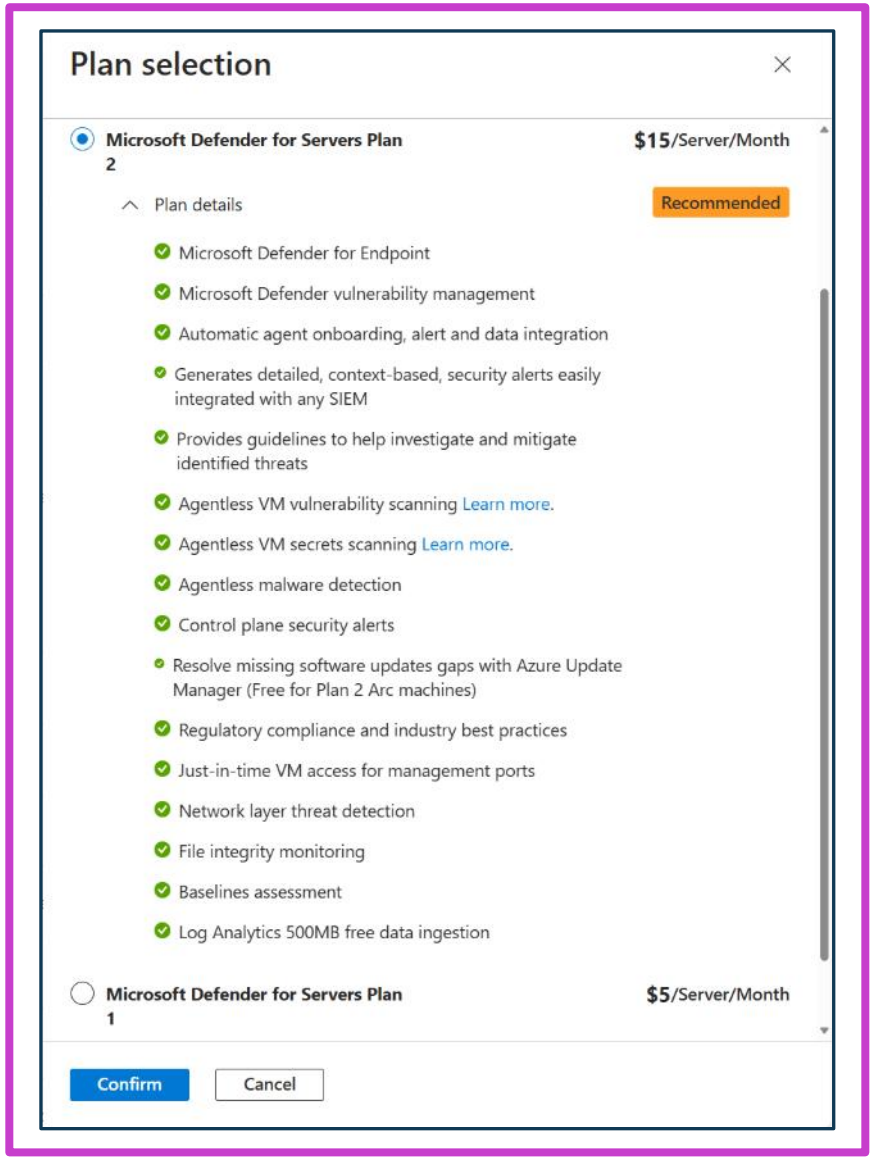
- Key Management: Use Azure Key Vault to securely manage, rotate, and protect storage access keys.
- Enhanced Authorization: Leverage Microsoft Entra ID and managed identities for superior security over shared keys.
- Key Rotation and Monitoring: Regularly rotate keys, set expiration policies, and monitor compliance using Azure Policy.

Implement Microsoft Defender for Cloud

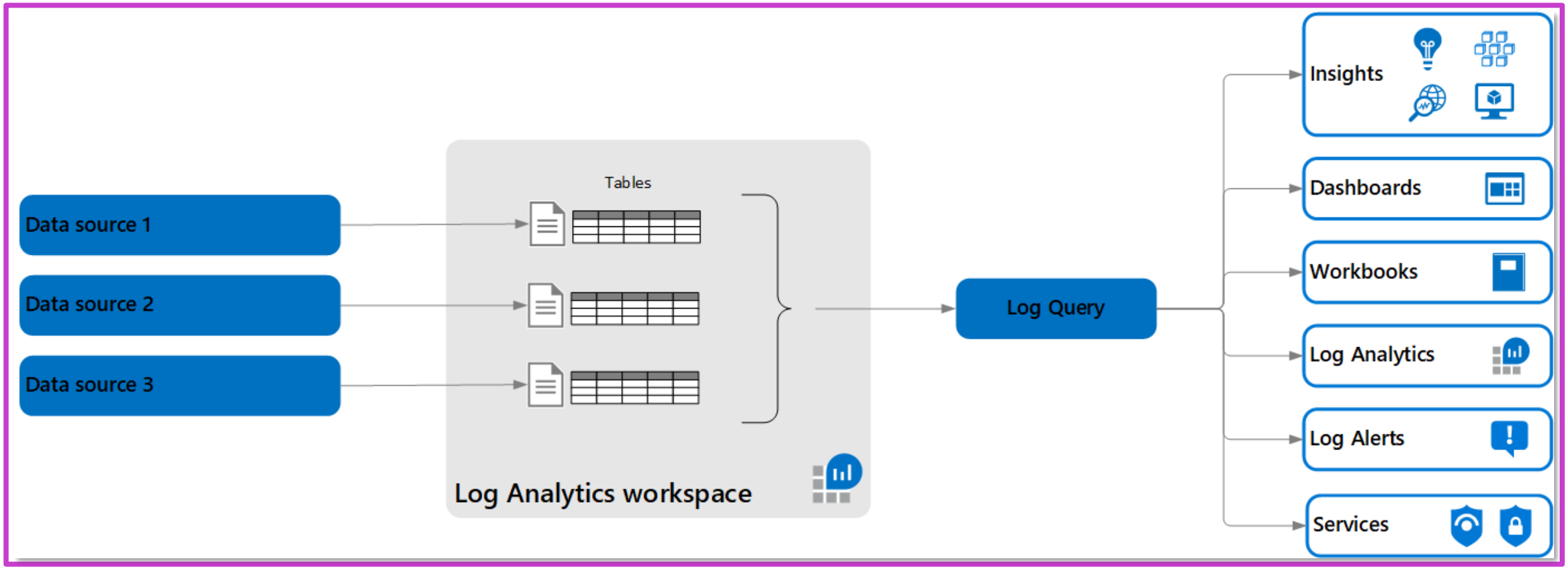
- Protect cloud apps and workloads: Secure resources with DevSecOps, CSPM, and CWPP solutions.
- Enhance security posture: Identify and remediate risks using Secure Score and compliance tools.
- Respond to threats: Detect, prioritize, and mitigate attacks with advanced threat detection capabilities.

Microsoft Defender for Servers

- Defender for Servers protects multicloud and on-premises machines, improving security posture and reducing risks.
- Plan 2 includes advanced features: agentless scanning, malware detection, and file integrity monitoring.
- Flexible deployment supports subscriptions and resources with integrated compliance and threat detection tools.

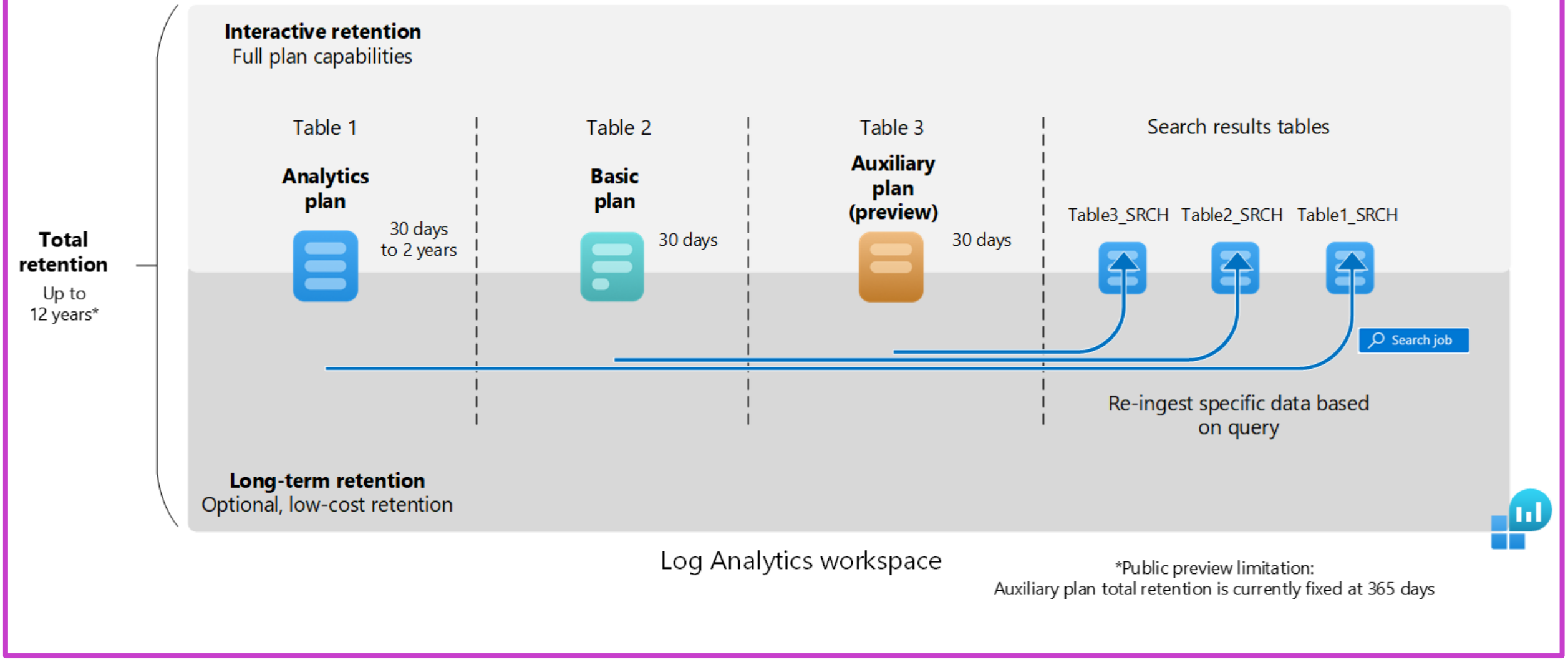


Log Analytics workspace



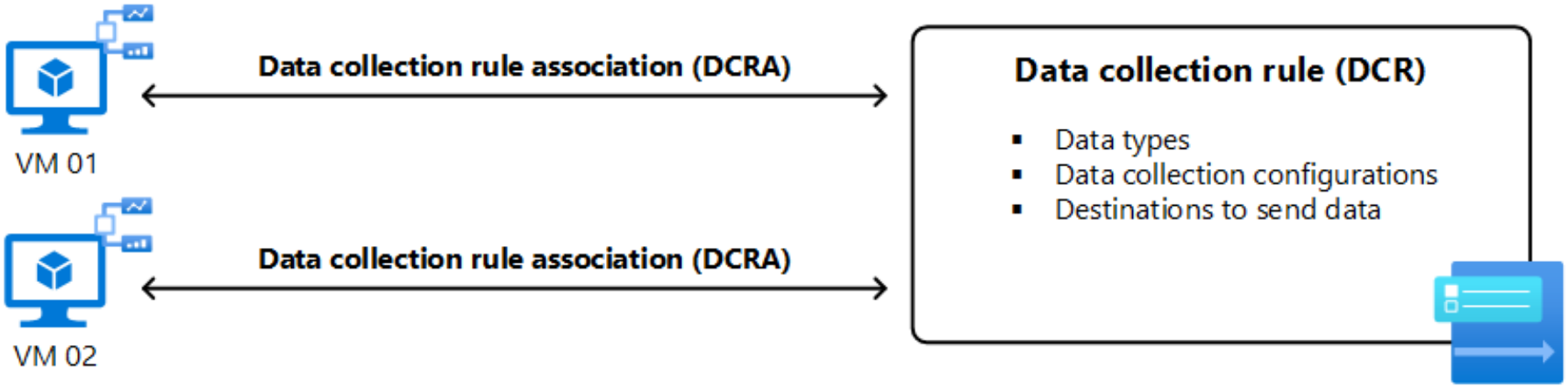
- A Log Analytics workspace is a centralized, configurable environment for Azure Monitor log data, allowing data collection and retention management across multiple Azure services.

Manage data retention in a Log Analytics workspace

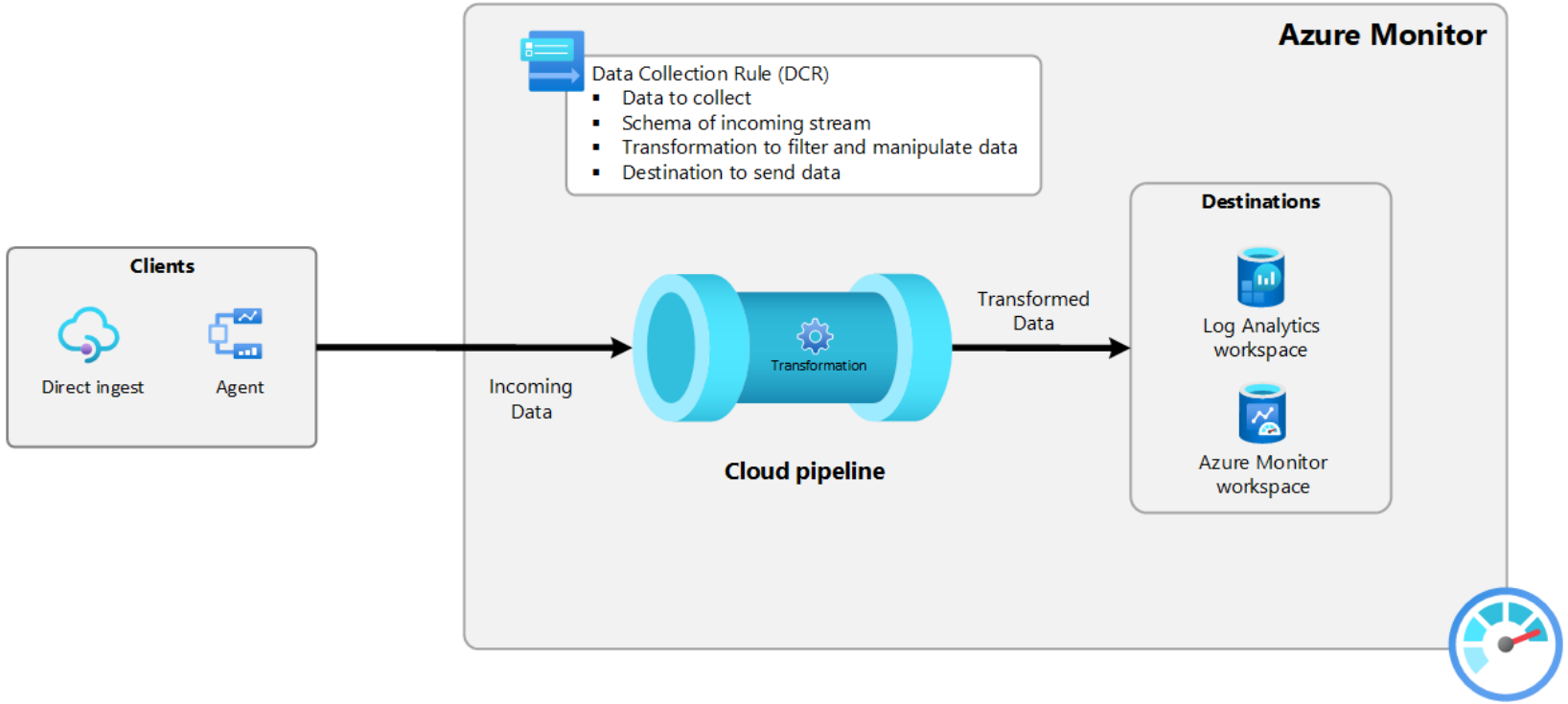


Deploy the Azure Monitor Agent

- Azure Monitor Agent gathers data from guest operating systems across Azure, hybrid, and on-premises environments.
- Data Collection Rules (DCRs) manage data types, transformations, and destinations for flexible monitoring.
- Supports insights and services like Microsoft Sentinel and Defender for Cloud for enhanced security and compliance.



Data collection rules (DCRs) in Azure Monitor



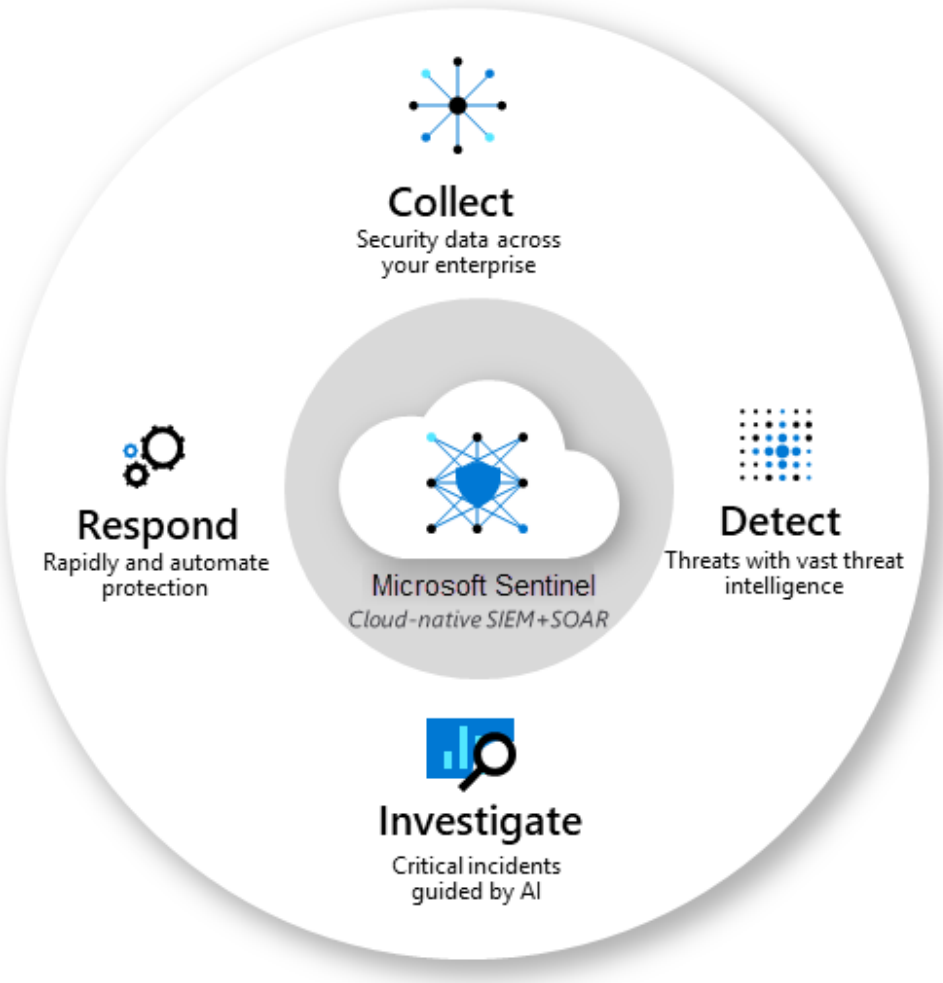
- DCRs improve Azure Monitor data collection with scalable, configurable, and centralized management.
- DCRs replace legacy methods like Log Analytics agent and Data Collector API.
- Edge pipeline enables scalable, offline data collection for environments with connectivity challenges.

Microsoft Sentinel explained

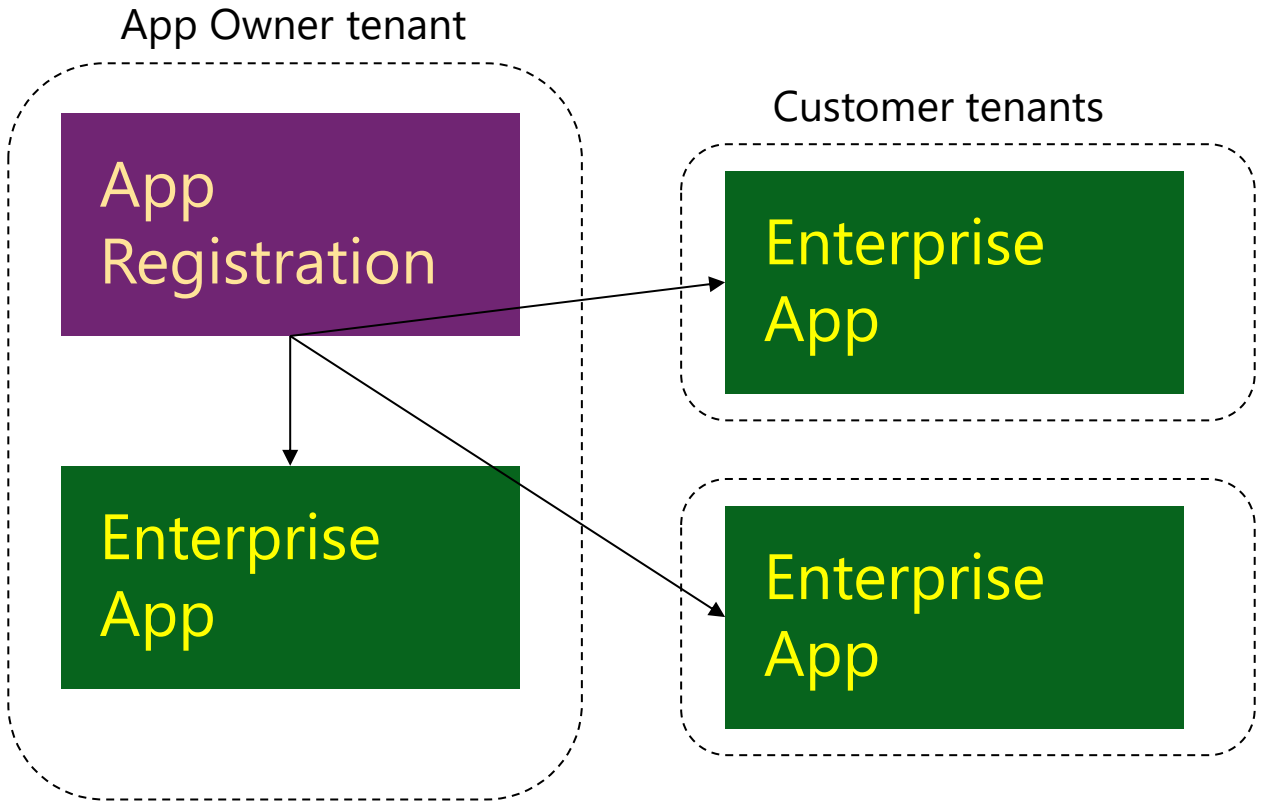
Microsoft Sentinel is a scalable, cloud-native solution that provides a Security information and event management (SIEM), and a Security orchestration, automation, and response (SOAR)

With Microsoft Sentinel your organization can:

- Collect data (using Data connectors)
- Detect previously undetected threats using threat intelligence and analytics
- Investigate threats with artificial intelligence
- Respond to incidents rapidly with built-in orchestration and automation of common tasks



Register an App in Microsoft Entra ID



Global

- Unique application ID
- Redirect URI
- Branding
- API permissions
- Role definitions

Tenant-specific service principal

- Reference to application
  - + unique object ID
- User / group assignments
- Role assignments
- Visibility in portals

Microsoft Defender for Cloud Apps architecture

- **Cloud Discovery**
  Find apps
- **Sanctioning**
  Allow/deny apps
- **Connectors**
  Extend protection into the app
  with APIs
- **Conditional Access** – Set access requirements
- **Policy control** – Define user behavior with apps