AZ-304

Microsoft Azure Architect Design

Program

1. **Design Authentication and Authorization**
2. **Design a Network Solution**
3. **Storage**
4. **Design a Compute Solution**
5. **Design a Database Solution**

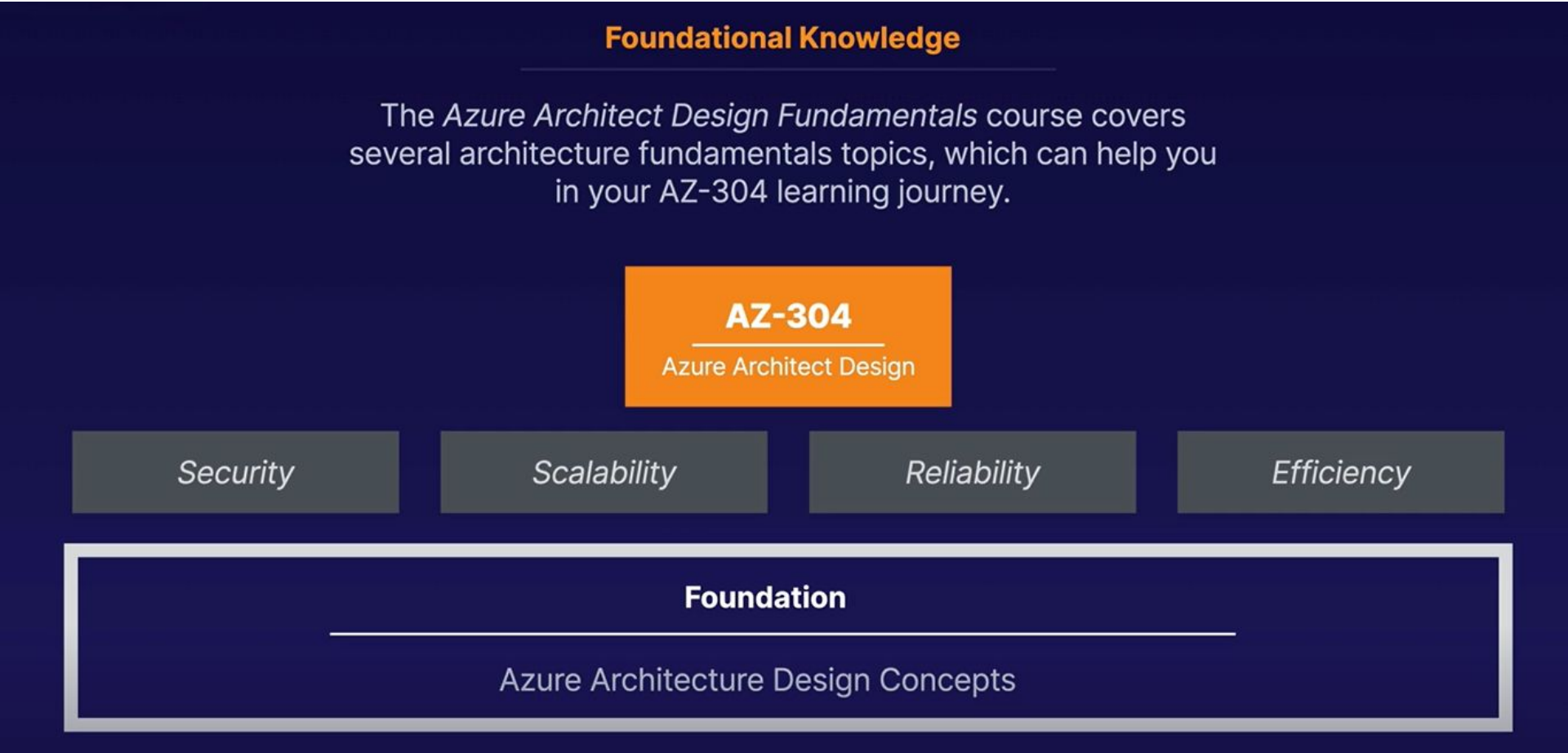
Introduction

Azure Architecture Design Concepts

This course covers several fundamental design concepts of:

- Important architecture concepts
- Requirements, analysis, and design
- Optimizing solutions

AZ-304 pillars



AZ-304 Exam

The AZ-304 has several business case scenario questions.

There will be approximately 40 - 60 questions.

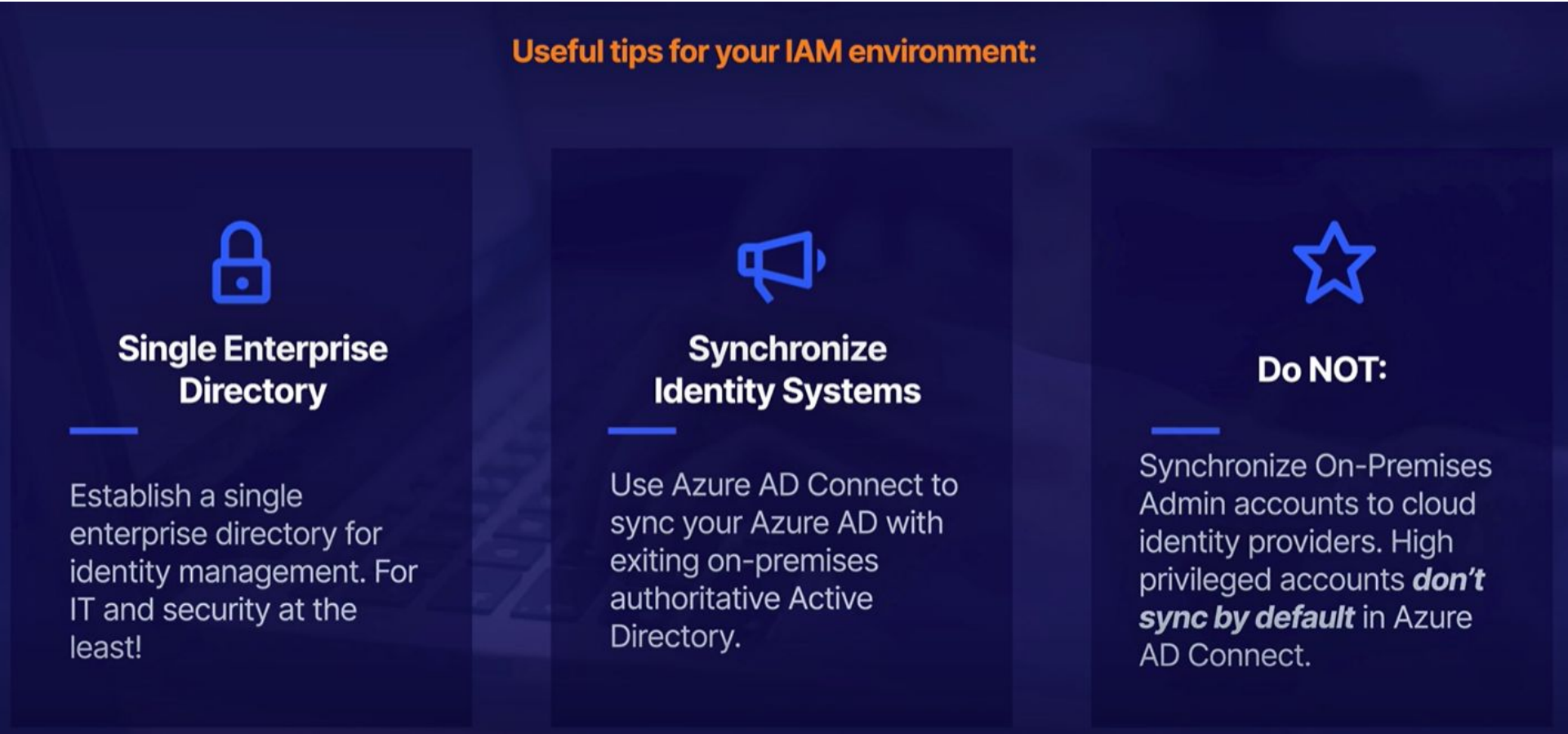
You are allowed 120 minutes to take the AZ-304.

No time limit for scenario questions.

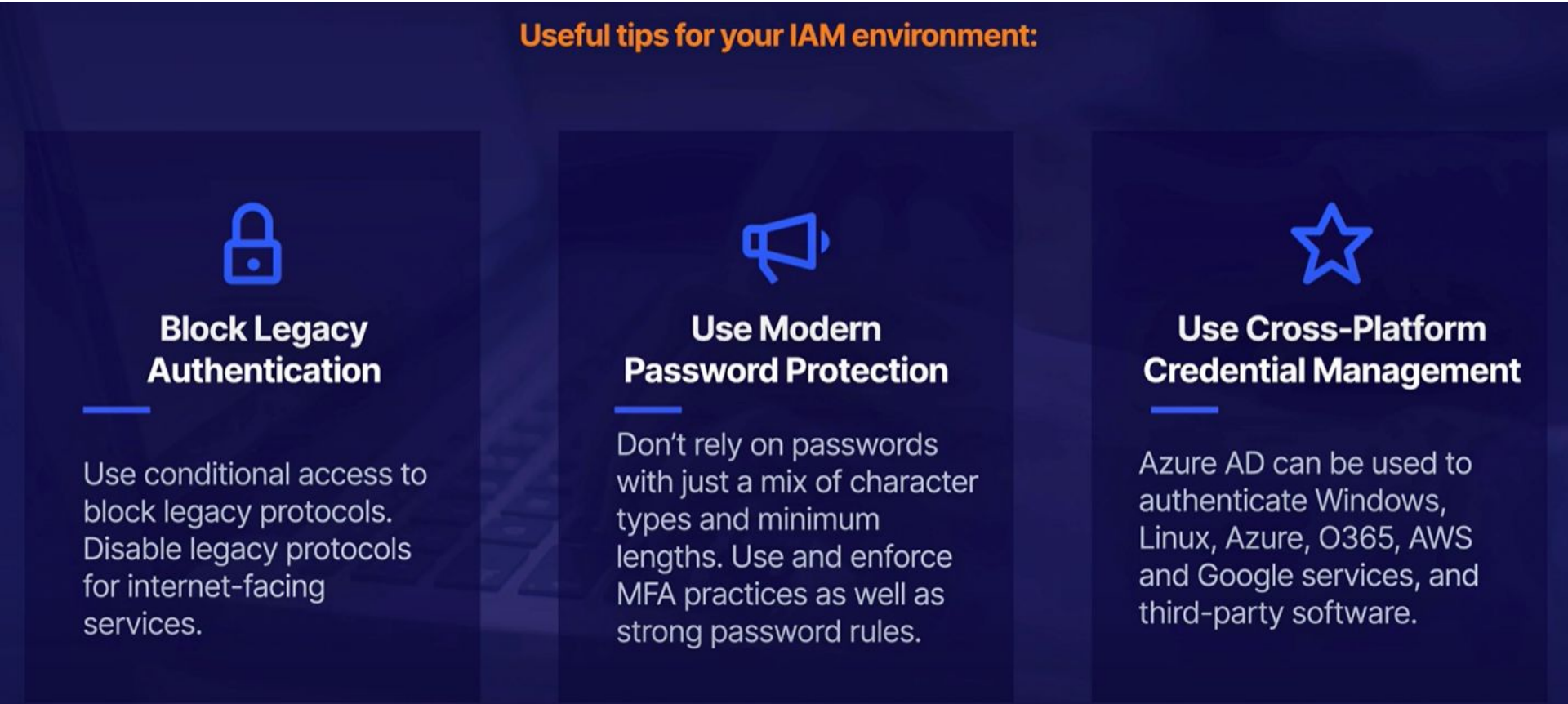
Design Authentication and Authorization

Authentification and Authorization

Identity and Access Management

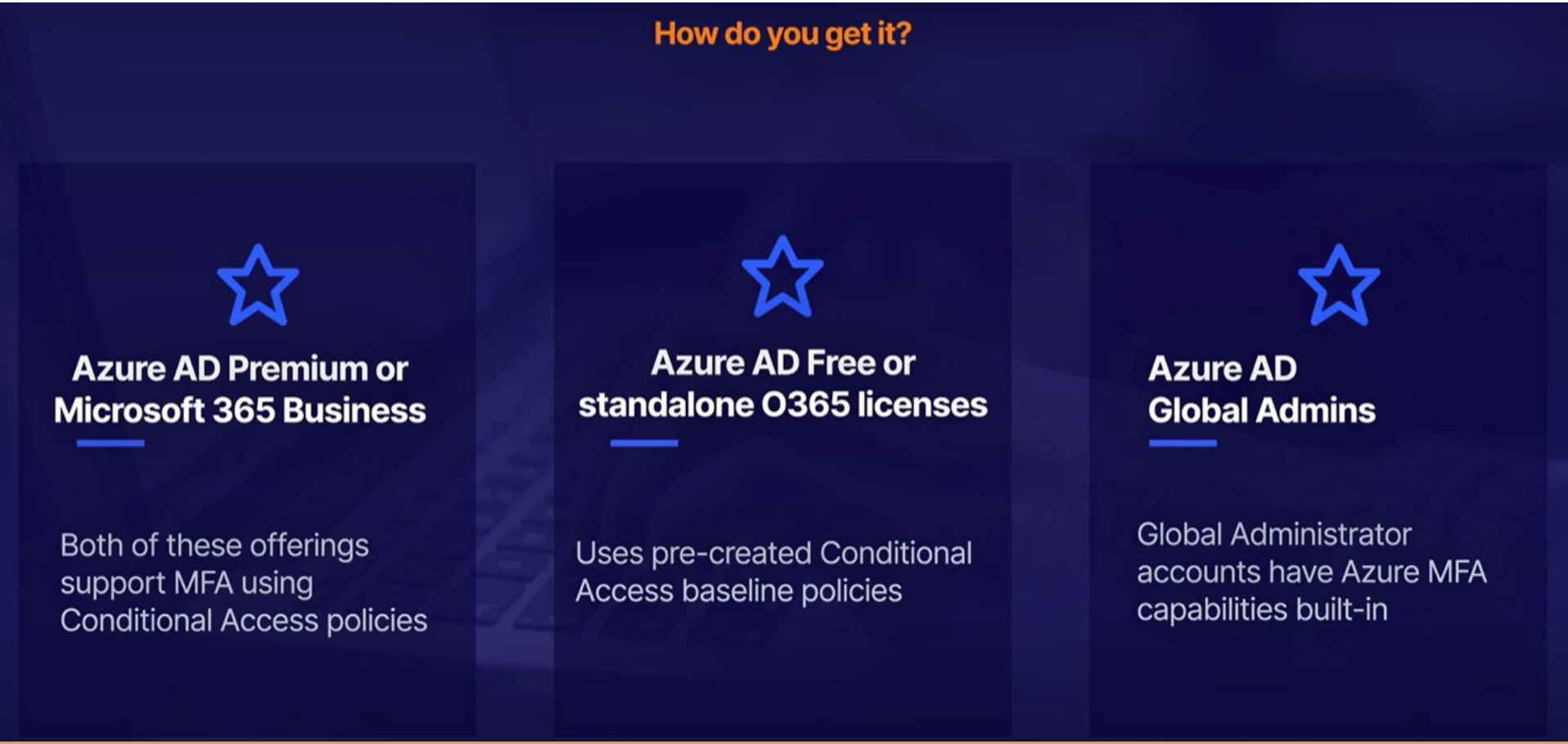


Identity and Access Management



Multi-Factor Authentication

Multi-Factor Authentication



Azure MFA

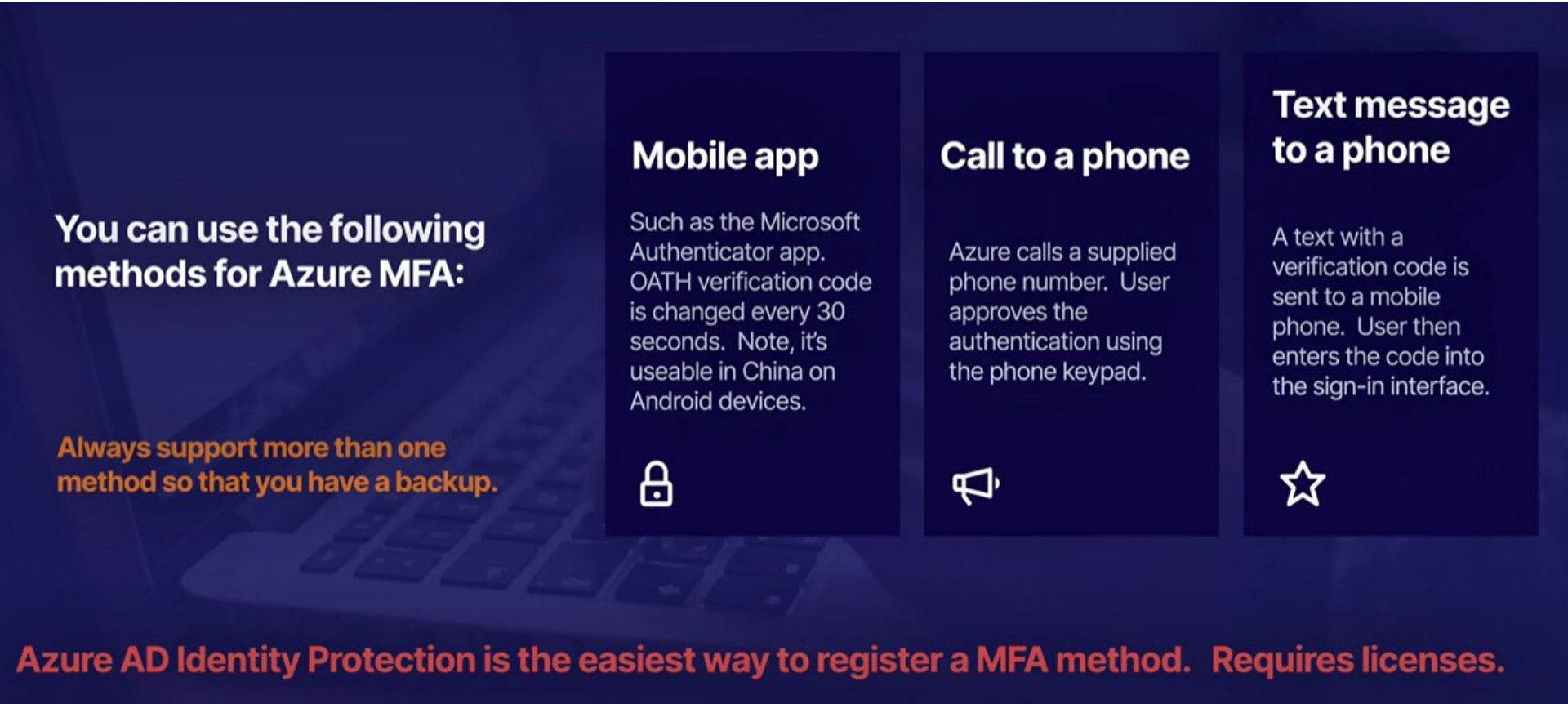
Azure MFA is enforced with Conditional Access policies.

These are If-THEN statements

Common access requests that might require MFA:

- IF a specific cloud app is accessed
- IF a user is accessing a specific network
- IF a user is registering a new device on your network
- IF a user is in a particular geographic area

Supported Authentication Methods



Steps for securing your identity structure

Strengthen credentials

Use strong authentication methods

Azure AD's security defaults enforce MFA for all users and blocks legacy protocol sign-ins. Super easy! Enable with one click.

Turn off traditional complexity and expiration rules

- Use Azure AD's dynamic banned password feature.
- Require passwords of at least 8 characters.
- Disable expiration rules.
- Disable character-composition requirements.

Protect against leaked credentials

- Azure AD has a leaked credentials report that reports ID/password pairs exposed to the "dark web" - but only if you enable password hash sync!
- AD FS Smart Lockout - protects against brute force attacks.
- Use Windows Hello for strong two-factor authentication on PCs and mobile devices.

Reduce Attack Surface

Block invalid authentication in AD FS

Apps using legacy authentication — POP3, IMAP4, SMTP — are easily compromised. Set up SharePoint and Exchange Online to use modern auth methods. If you have Azure AD Premium, use Conditional Access policies to block legacy authentication.

Restrict user consent operations

- Consider disabling user consent operations to help minimize risk.
- Use application assignment and conditional access to restrict users to specific applications.

Implement Azure AD Privileged Identity Management

- Identify and manage users assigned to admin roles.
- Remove unused roles and those with excessive privilege.
- Protect privileged roles with multi-factor authentication.
- Establish rules that ensure privileged roles are granted as-needed.

Automate Threat Response

Use Azure AD Identity Protection

If a user's ID is determined to be "at risk" by the Identity Protection system, that ID can be automatically flagged and set to require a password change.

A "sign-in risk" is the likelihood of someone other than an account holder trying to log in. If the risk is medium or above, set the policy to force MFA or block access.

Use Cloud Intelligence

Monitor Azure AD

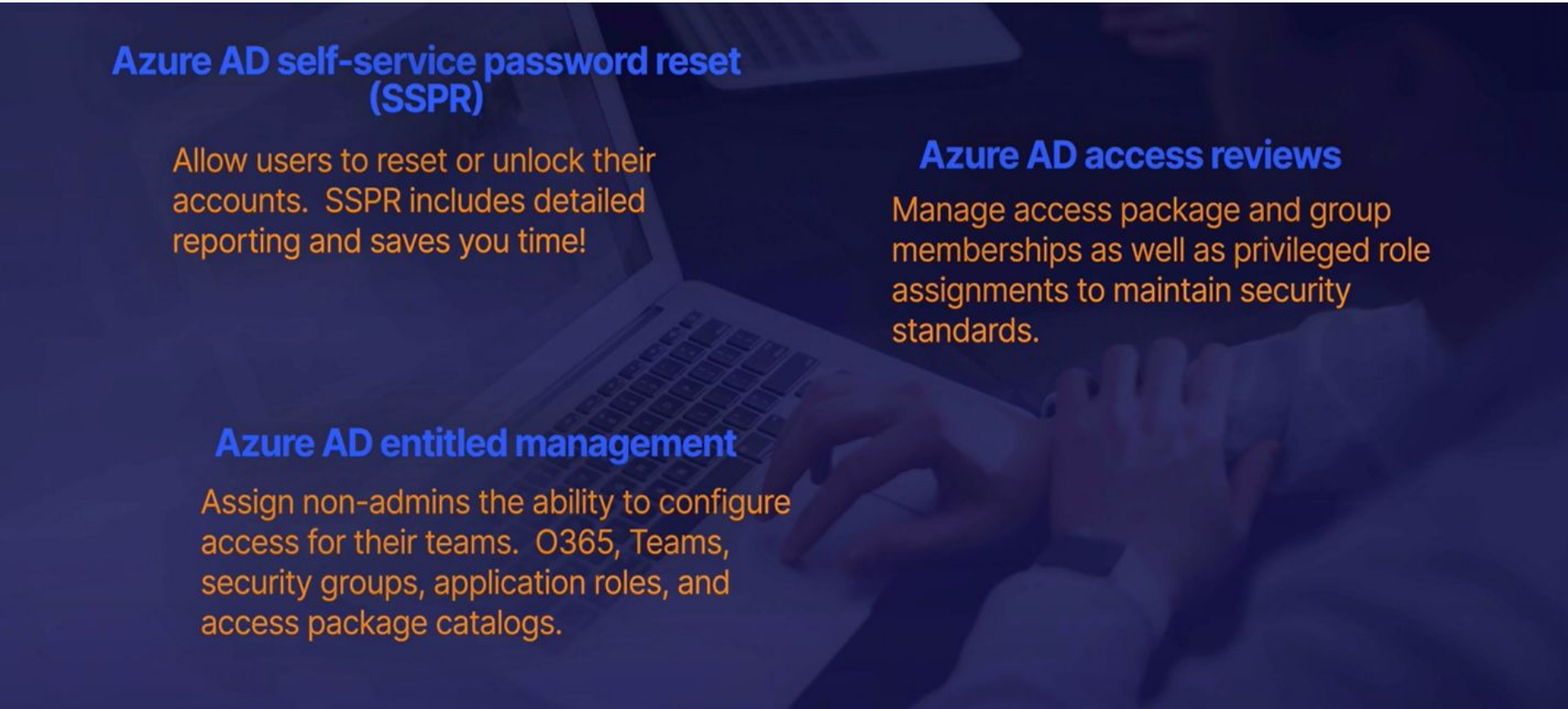
Use Azure logging and auditing to get audit activity reports in the Azure AD portal.

Monitor AD FS with Azure AD Connect Health for hybrid environments.

Azure ID Identity Protection offers two reports that should be monitored daily:

Risky sign-in & **Risky user**

Enable End-User Self-Service



Key Features of Azure Seamless Single Sign-On

Azure Seamless Single Sign-On

Before you recommend Azure Seamless SSO...

Does it work everywhere?

Azure Seamless SSO does **NOT** work in Azure Germany and the Microsoft Azure Government cloud.

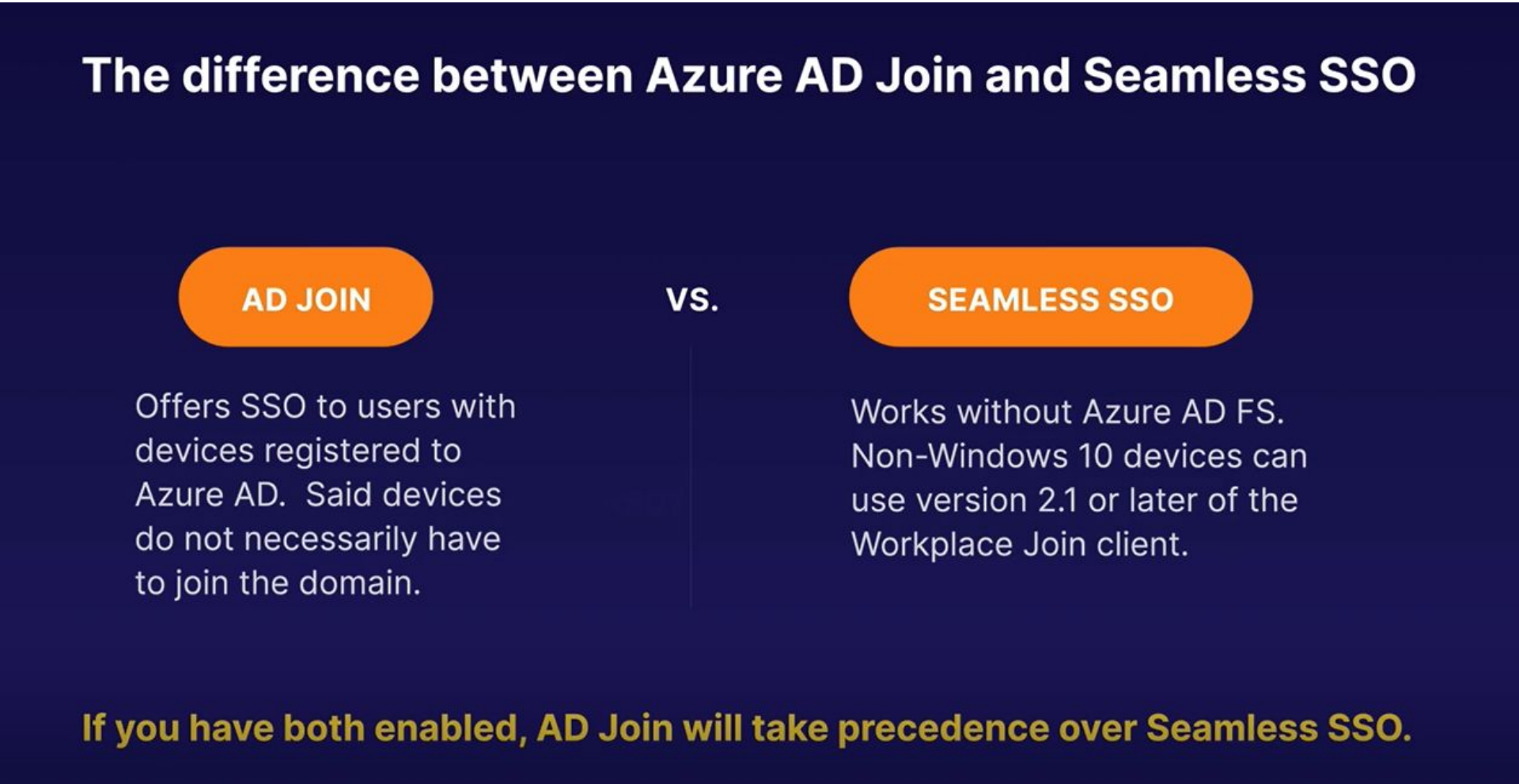
Does Seamless SSO support Alternate ID for the username?

Seamless SSO supports **Alternate ID** as the username when configured in Azure AD Connect. However, not all O365 apps support **Alternate ID**.

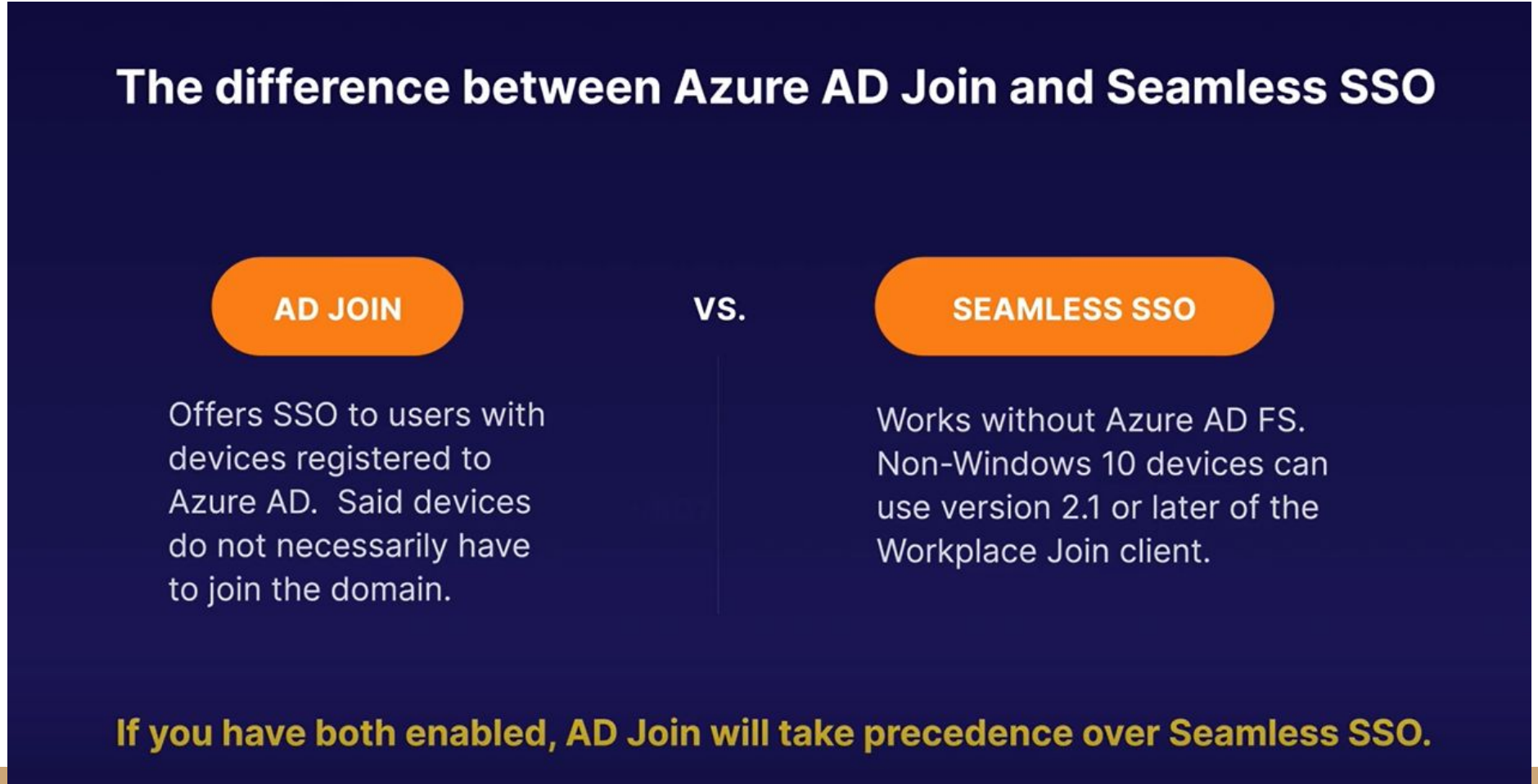
What sign-in methods work with Seamless SSO?

Both password hash synchronization and Pass-through Authentication work with SSO. However, Seamless SSO does **NOT** work with Active Directory Federation Services (ADFS).

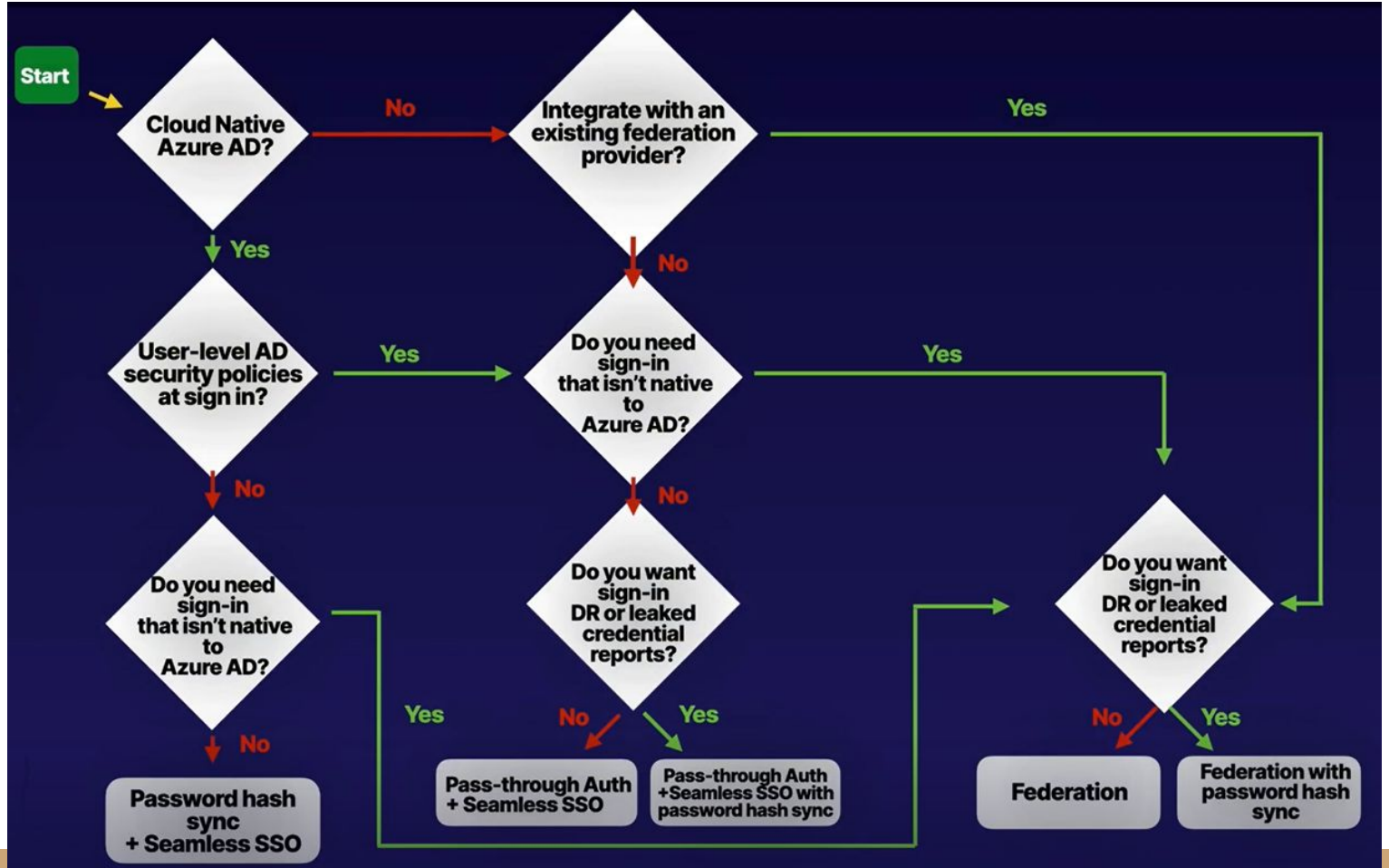
AD Join vs Sleamless SSO



The difference between Azure AD Join and Seamless SSO



Hybrid Identity Decision Tree



Hybrid Identity Decision Tree

Some details on decision tree questions:

- Azure AD can handle sign-in for users without relying on on-premises resources.
- Azure AD can hand off user sign-in to a provider such as AD FS.
- To apply user-level AD security policies, Azure AD requires some on-premises components.

Sign-in features not natively supported by Azure AD:

- Sign-in using smart cards or certificates
- Sign-in using on-premise MFA server
- Sign-in using third-party authentication
- Multi-site on-premises authentication

Note: Azure AD Identity Protection requires password hash sync *regardless of sign-in method*.

Hybrid Identity Decision Tree

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent
What are the requirements for on-premises Internet and networking beyond the provisioning system?	None	Outbound Internet access from the servers running authentication agents
Is there a TLS/SSL certificate requirement?	No	No
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center
Do users get single sign-on to cloud resources from do- main-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO
What sign-in types are supported?	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID
What are the multifactor authentication options?	Azure MFA Custom Controls with Conditional Access	Azure MFA Custom Controls with Conditional Access
What are the Conditional Access options?	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

Hybrid Identity Decision Tree

Some details on decision tree questions:

- Azure AD can handle sign-in for users without relying on on-premises resources.
- Azure AD can hand off user sign-in to a provider such as AD FS.
- To apply user-level AD security policies, Azure AD requires some on-premises components.

Sign-in features not natively supported by Azure AD:

- Sign-in using smart cards or certificates
- Sign-in using on-premise MFA server
- Sign-in using third-party authentication
- Multi-site on-premises authentication

Note: Azure AD Identity Protection requires password hash sync *regardless of sign-in method*.

Comparing Authentication Methods

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent
What are the requirements for on-premises Internet and networking beyond the provisioning system?	None	Outbound Internet access from the servers running authentication agents
Is there a TLS/SSL certificate requirement?	No	No
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center
Do users get single sign-on to cloud resources from do- main-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO
What sign-in types are supported?	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID
What are the multifactor authentication options?	Azure MFA Custom Controls with Conditional Access	Azure MFA Custom Controls with Conditional Access
What are the Conditional Access options?	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

B2B - What Is It?

Business to Business!

Azure AD B2B allows the partner organization to use their own identity management solution.

- Organizations use their own identities and credentials; Azure AD is not required.
- No management of external accounts or passwords.
- No account synchronization or lifecycle management required.
- Guest accounts are created when an external user redeems their access invitation.

Functions of Azure AD B2B

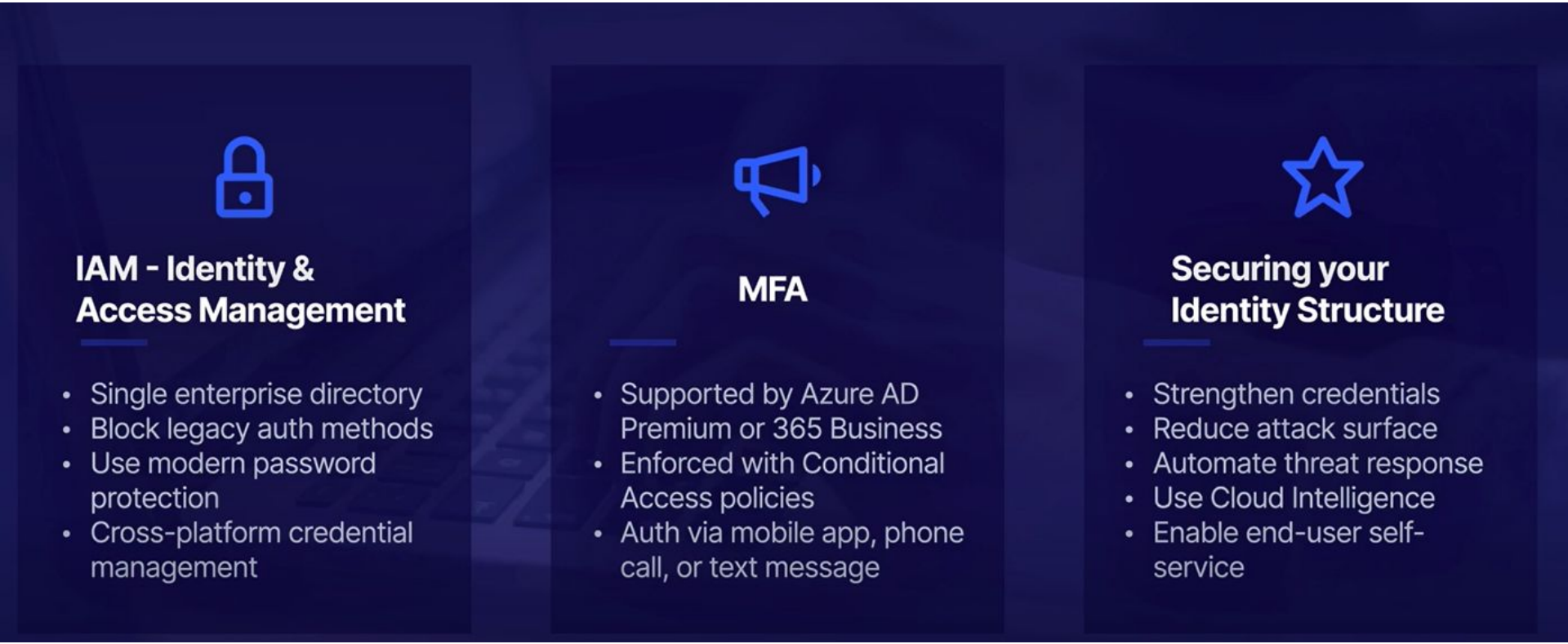
Apps and services are shared via Conditional Access policies.

Application and group owners can manage their own guest users.

Azure AD supports external identity providers (Google, Facebook, etc.).

B2B allows for an external user to utilize the self-service sign-up for application access.

Summary



IAM - Identity & Access Management

- Single enterprise directory
- Block legacy auth methods
- Use modern password protection
- Cross-platform credential management

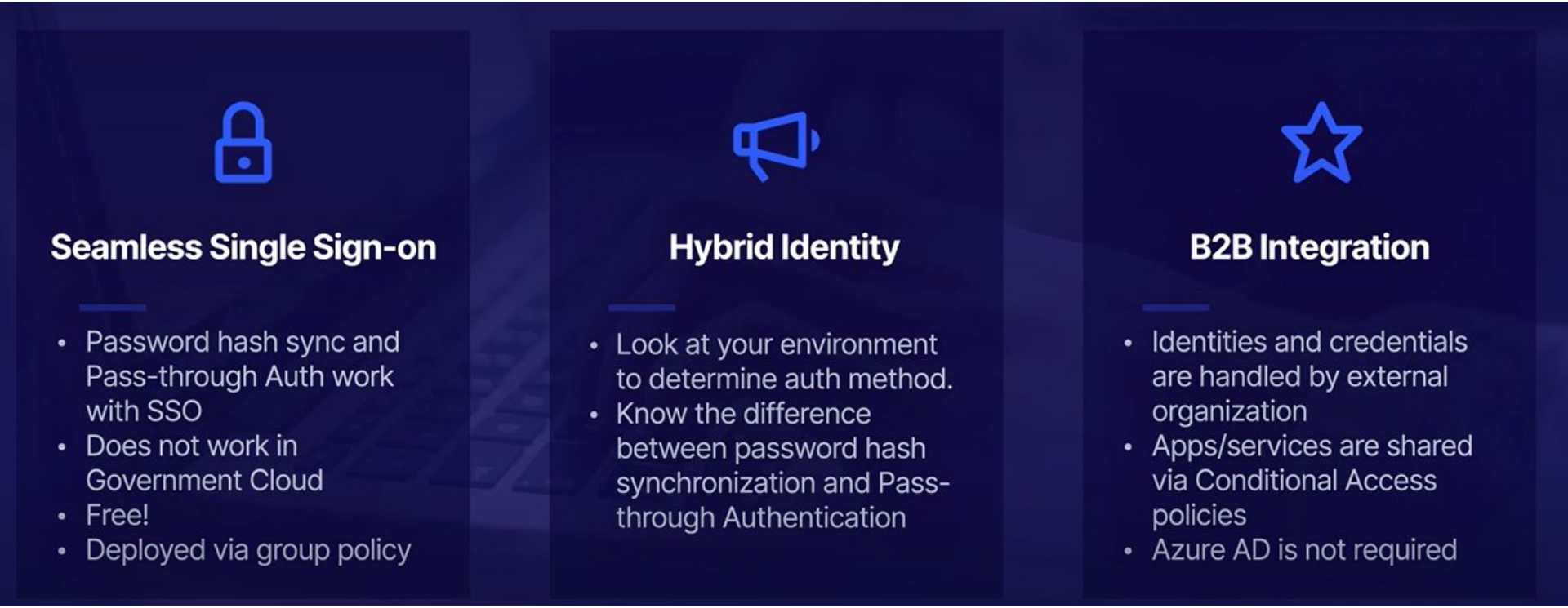
MFA

- Supported by Azure AD Premium or 365 Business
- Enforced with Conditional Access policies
- Auth via mobile app, phone call, or text message

Securing your Identity Structure

- Strengthen credentials
- Reduce attack surface
- Automate threat response
- Use Cloud Intelligence
- Enable end-user self-service

Summary



Seamless Single Sign-on

- Password hash sync and Pass-through Auth work with SSO
- Does not work in Government Cloud
- Free!
- Deployed via group policy

Hybrid Identity

- Look at your environment to determine auth method.
- Know the difference between password hash synchronization and Pass-through Authentication

B2B Integration

- Identities and credentials are handled by external organization
- Apps/services are shared via Conditional Access policies
- Azure AD is not required

Design a Network Solution

Design a Network Solution

Considerations when planning your Virtual Network...

How many network interfaces and private IP addresses do you require in a virtual network? (Remember limits!)

Do you have any organizational administration requirements for resources in different Virtual Networks?

Do any organizational security requirements exist for isolating traffic into separate Virtual Networks or for isolating Virtual Networks into separate regions/subscriptions?

Do you want to connect the Virtual Network to another Virtual Network or on-premises network?

Design a Network Solution

Considerations for subnets...

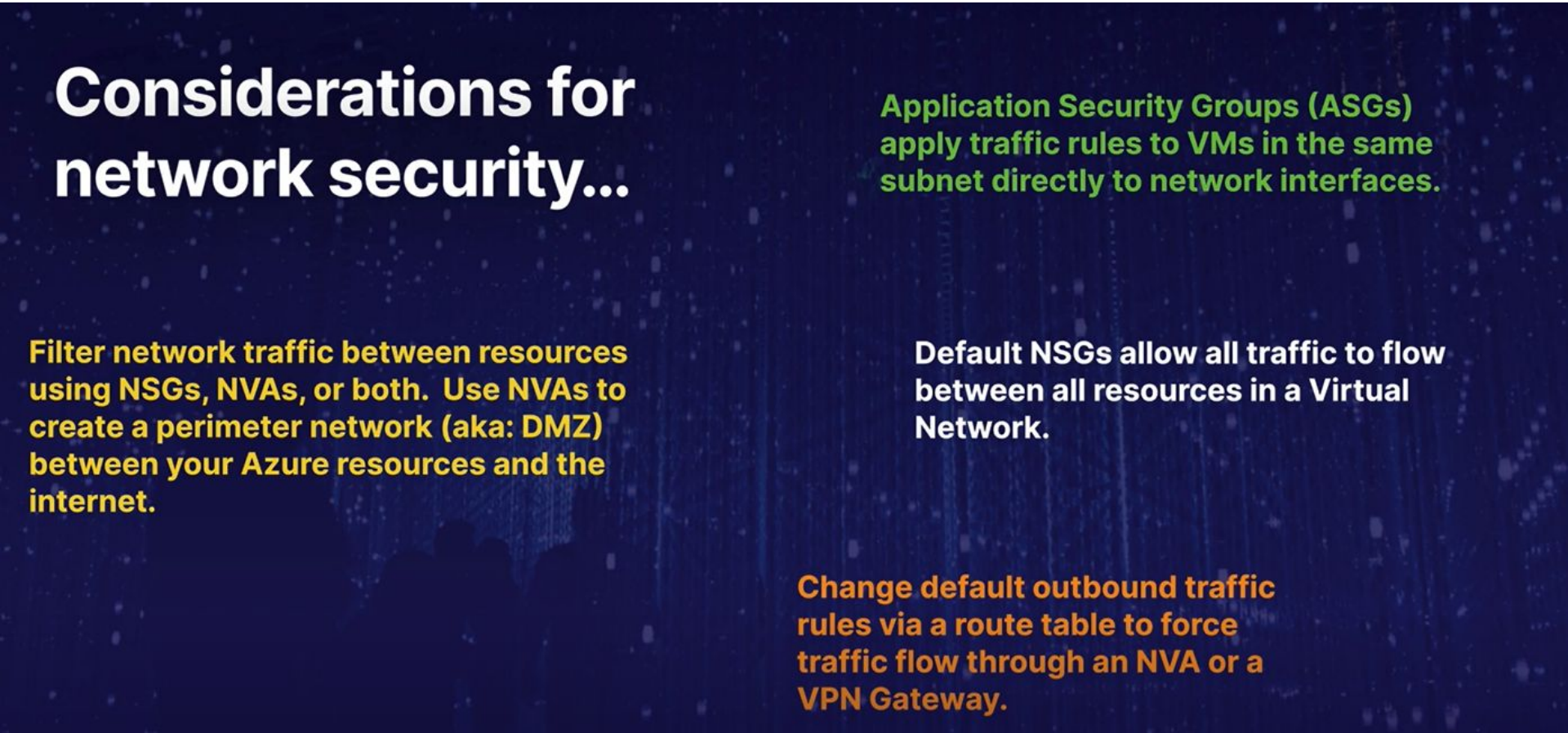
Azure routes traffic between all subnets in a Virtual Network. Deploy resources to different subnet if routing traffic through a Network Virtual Appliance (NVA).

Some Azure service resources (such as VPN Gateways) require and create their own subnets. Make sure you've allowed space for this.

Network Security Groups (NSGs) can be assigned to subnets to control subnet traffic.

Use service endpoints on subnets to limit access to resources like SQL DBs or Storage Accounts.

Design a Network Solution



Design a Network Solution

Connectivity

VPN Gateway:

Used to connect a Virtual Network to your on-premises network using site-to-site VPN or ExpressRoute.

Combing peering and a VPN Gateway to create hub and spoke networks.

Peering:

Virtual Networks can be in the same, or different, supported Azure regions.

Virtual Networks can be in different subscriptions (even those in different AD Tenants).

Name Resolution:

Azure DNS cannot resolve name of resource in a peered network. Deploy a DNS server or use Azure DNS private domains to resolve names for peering. Name resolution between virtual and on-premises networks also requires a DNS server.

Design a Network Solution

Permissions and Policy

Permissions are assigned to a scope in the following hierarchy:

- Management Group
  - Subscription
    - Resource Group
      - Resource

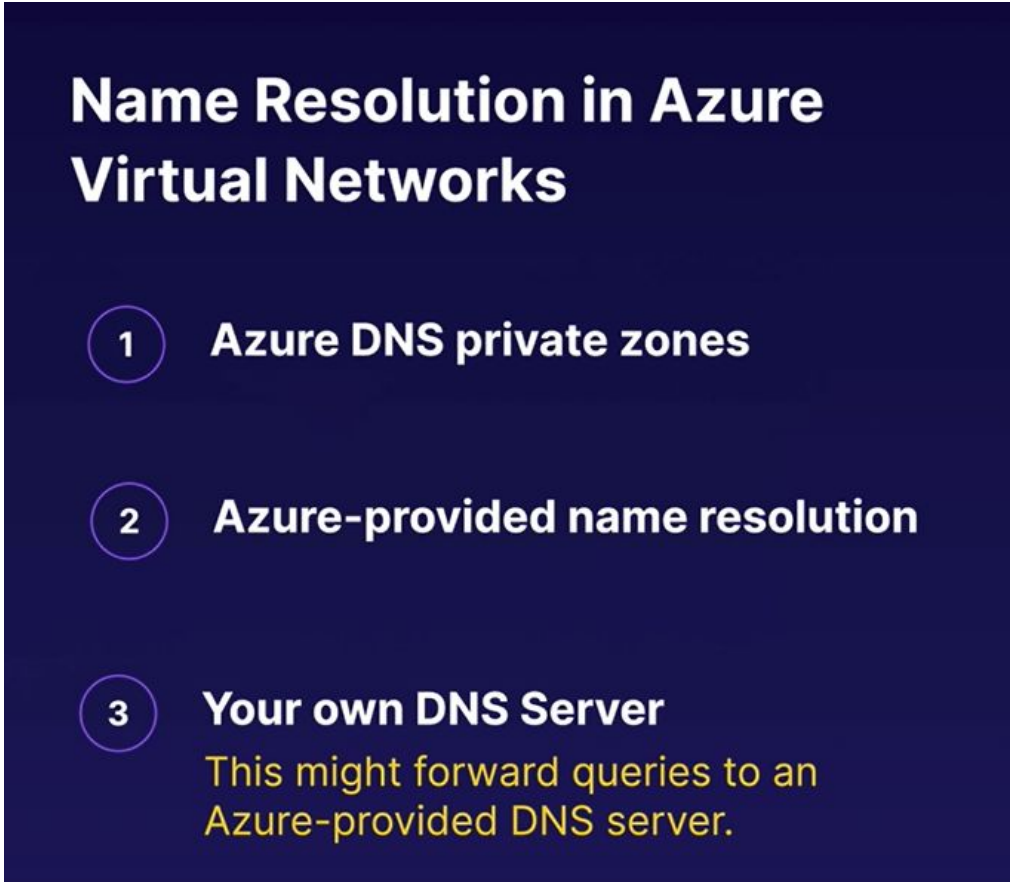
To work with Virtual Networks, use the Owner, Contributor, or Network Contributor roles.

Azure Policy can define and enforce rules over resources to maintain compliance. For example, they can require the use of NSGs or restrict network resource creation to specific regions.

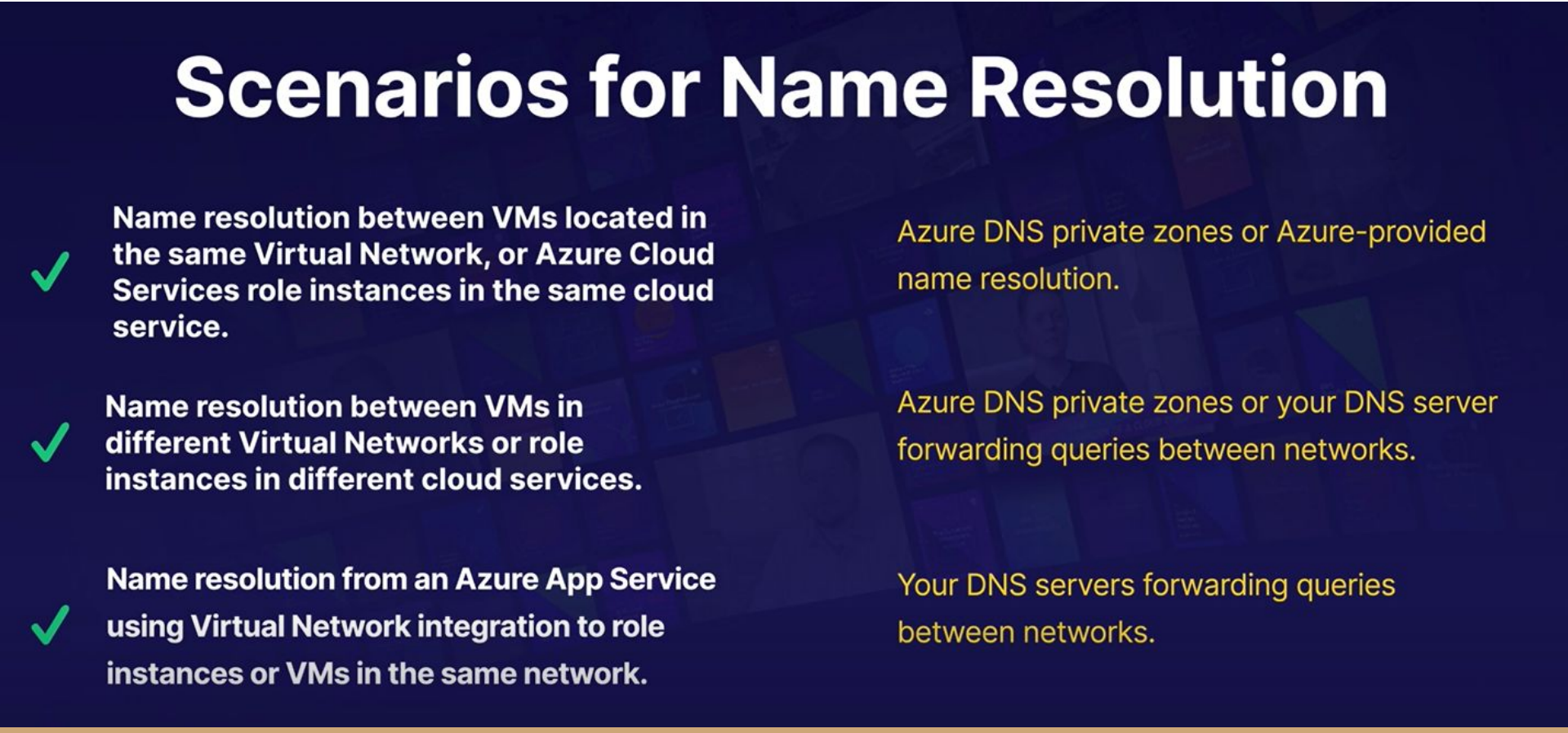
Policies are applied in the following hierarchy:

- Management Group
  - Subscription
    - Resource group
      - Resource

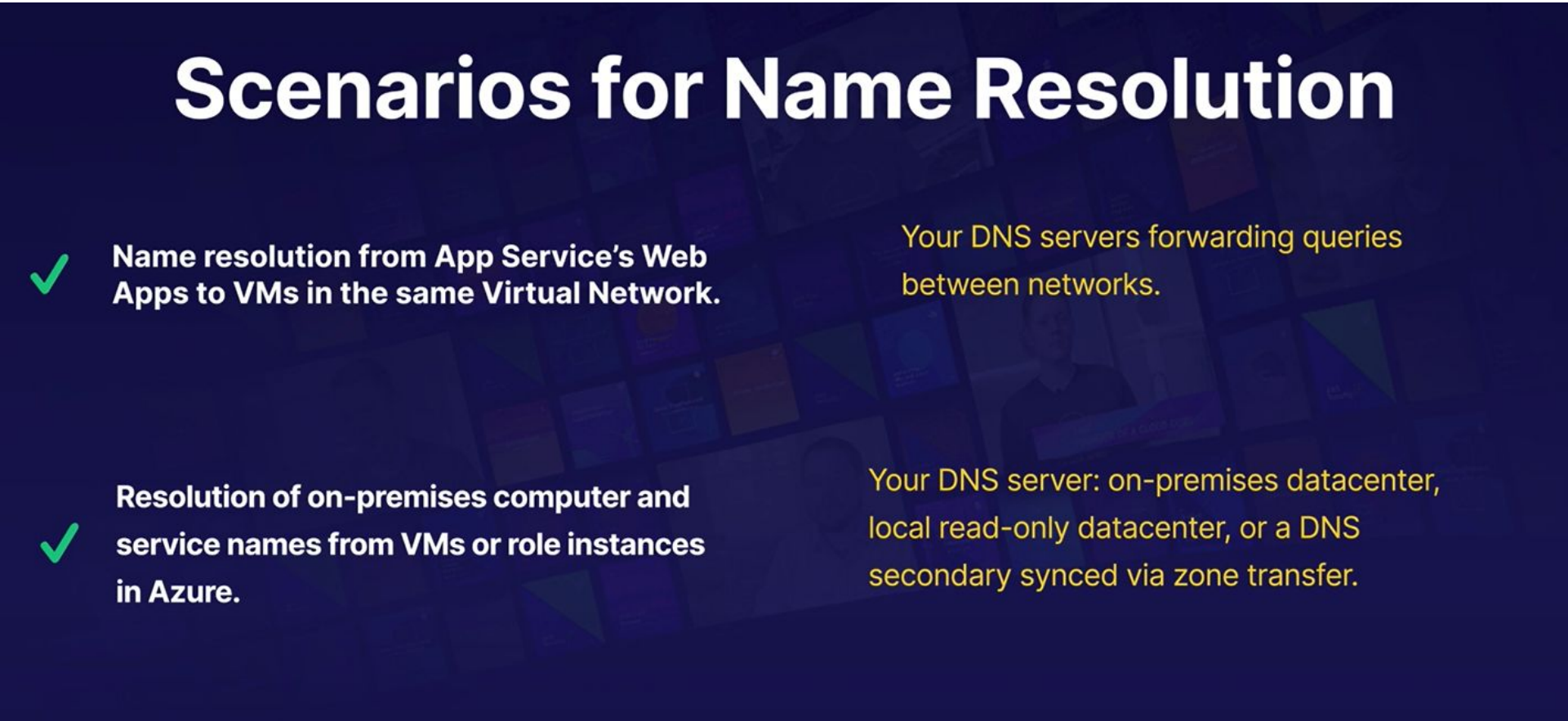
Name Resolution in Azure Virtual Networks



Name Resolution in Azure Virtual Networks



Name Resolution in Azure Virtual Networks



Design a Network Solution

Scenarios for Name Resolution

✓ **Resolution of Azure hostnames from on-premises computers.**	Forward queries to your DNS proxy server in the corresponding Virtual Network.
✓ **Reverse DNS for internal IP addresses.**	Azure DNS private zones, Azure-provided name resolution, or your own DNS server.
✓ **Name resolution between VMs or role instances located in different cloud services, NOT in a Virtual Network.**	Cannot do this outside a Virtual Network.

Understanding Azure-Based Name Resolution

AZURE-PROVIDED NAME RESOLUTION

Provides only basic authoritative DNS capabilities. DNS zone names and records are automatically managed.

Want more control? Use your own DNS servers or Azure DNS private zones!

- Azure provides internal name resolution for VMs and role instances within the same Virtual Network or cloud service.
- VMs and instances in a cloud service share the same DNS suffix, so a hostname is sufficient. No FQDN required.
- Virtual Networks deployed via the classic deployment model give different DNS suffixes to different cloud services.
- Virtual Networks deployed using the Azure Resource Manager model keeps the DNS suffix consistent across all VMs in a Virtual Network, FQDN not needed.

Note: DNS names can be assigned to both VMs and NICs.

Solutions for Hybrid Networks

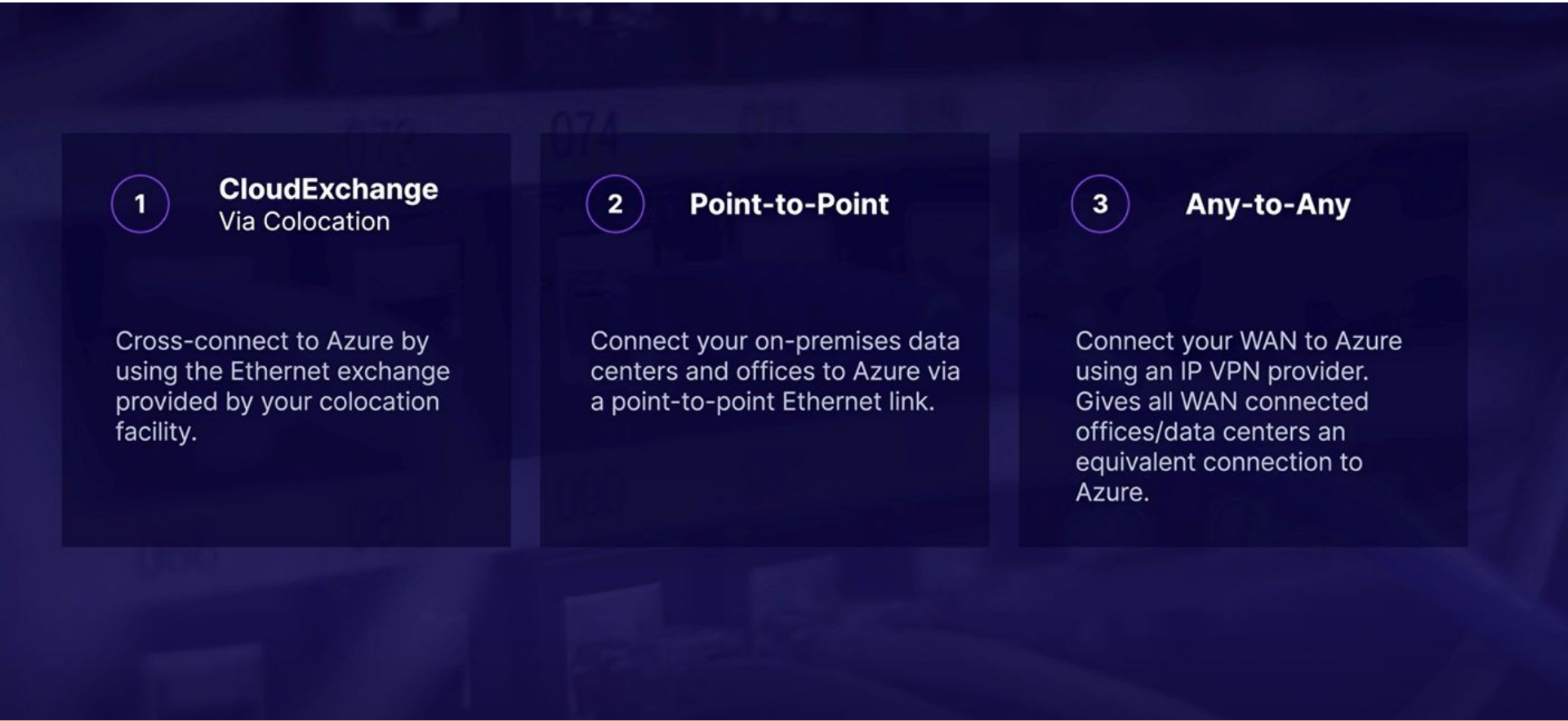
HYBRID NETWORKS

Microsoft says, “Use ExpressRoute!”

ExpressRoute is Azure’s primary solution for extending on-premises networks over a private connection (NSX-T uses it.).

ExpressRoute extends beyond Azure, allowing connections to other Microsoft service, such as Office 365.

ExpressRoute Connectivity Types



1 **CloudExchange**
Via Colocation

Cross-connect to Azure by using the Ethernet exchange provided by your colocation facility.

2 **Point-to-Point**

Connect your on-premises data centers and offices to Azure via a point-to-point Ethernet link.

3 **Any-to-Any**

Connect your WAN to Azure using an IP VPN provider. Gives all WAN connected offices/data centers an equivalent connection to Azure.

Hybrid Networks

Considerations for using ExpressRoute...

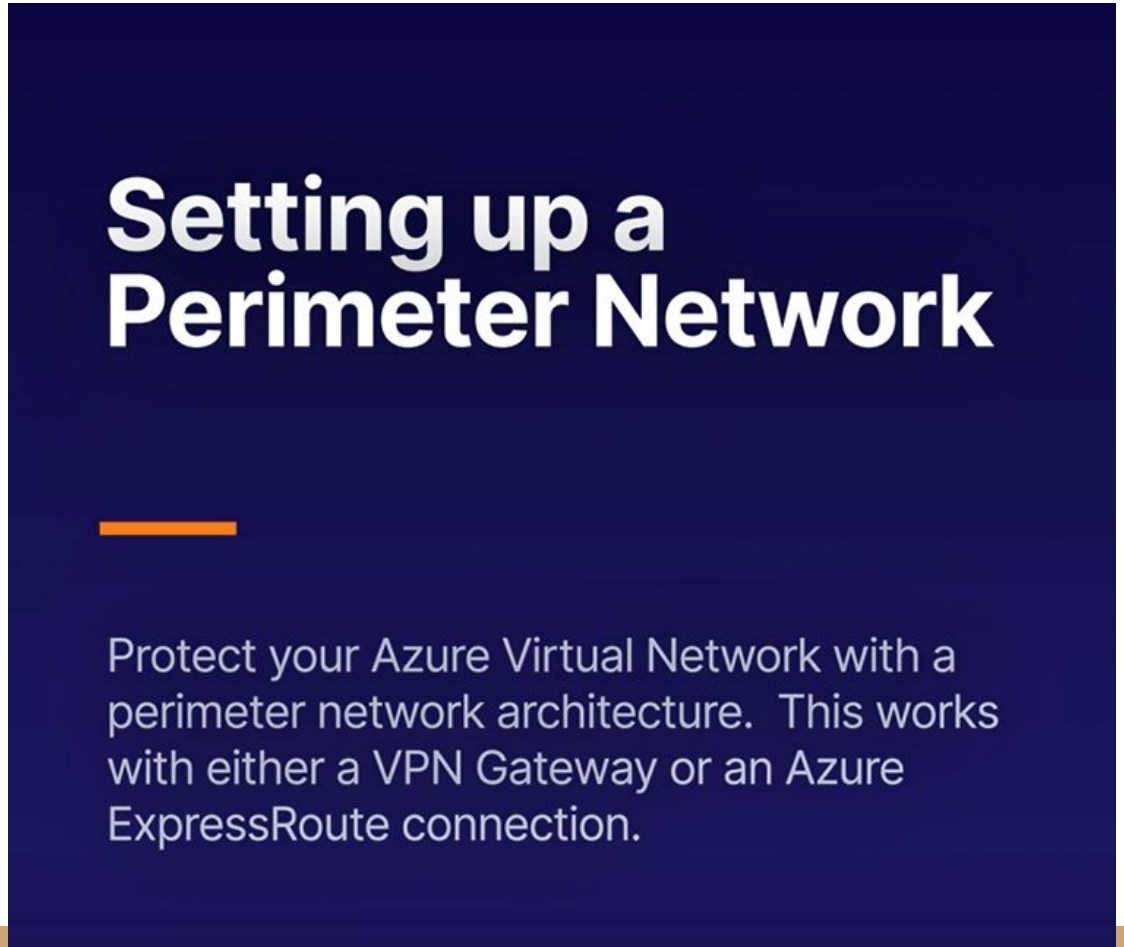
Benefits:

- Uses layer 3 connectivity and security standards.
- Can support up to 100 Gbps bandwidth.
- Suited for high-speed and critical business operations.

Considerations:

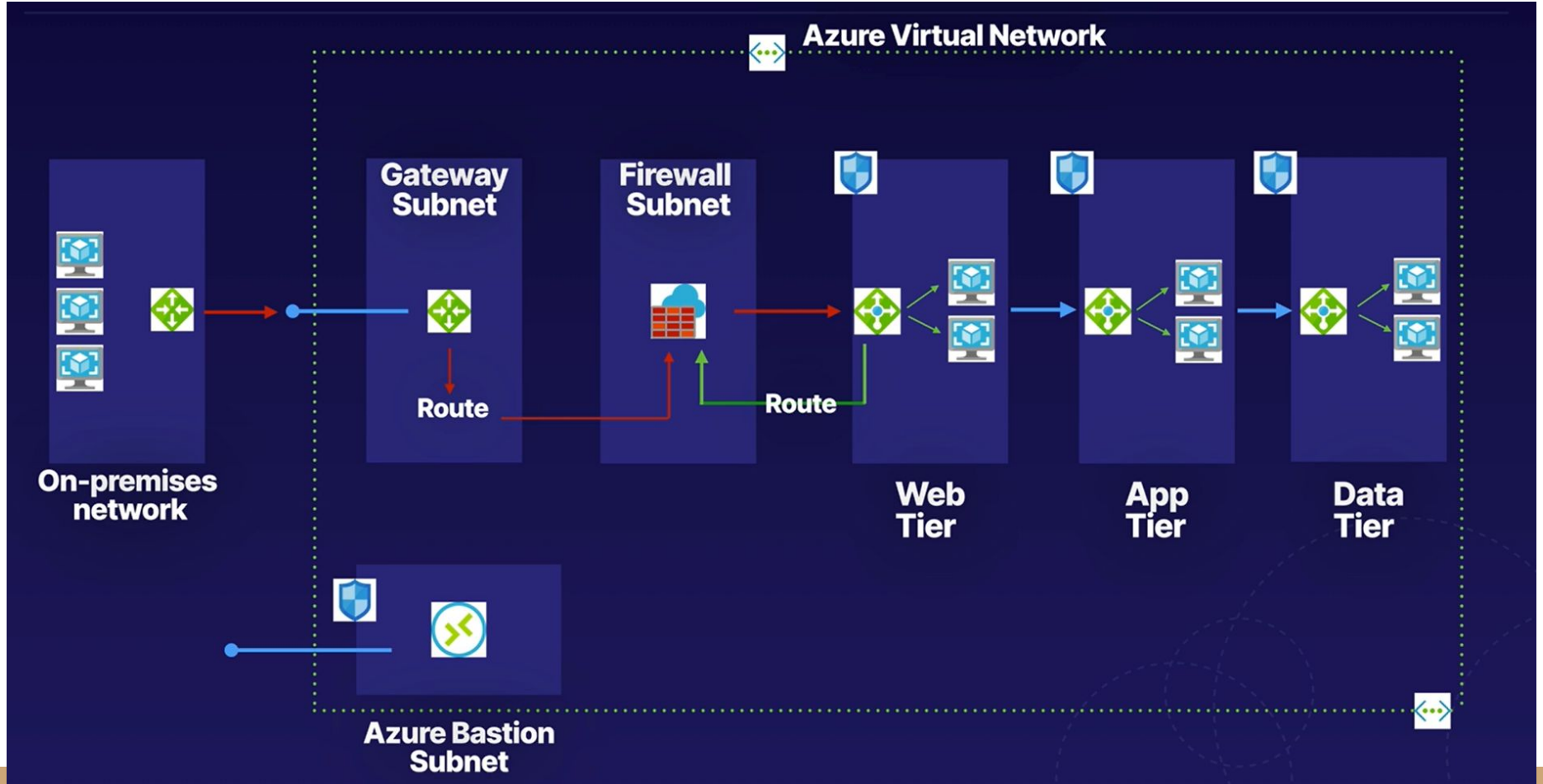
- Somewhat complex, requires collaboration with your ISP.
- On-premise installation of high-bandwidth routers required.
- ISP manages the ExpressRoute circuit.
- Does not support the Hot Standby Router Protocol (HSRP), instead use a Border Gateway Protocol (BGP).
- Layer 3, requires a Network Security Appliance for threats.
- Network Security Appliances should be placed between your ISP edge routers and your on-premises network.
- Connectivity monitoring requires the Azure Connectivity Toolkit.

Recommend Implementations for Secure Hybrid Networks



Components of the Perimeter Network

Secure Hybrid Network



Secure Hybrid Network

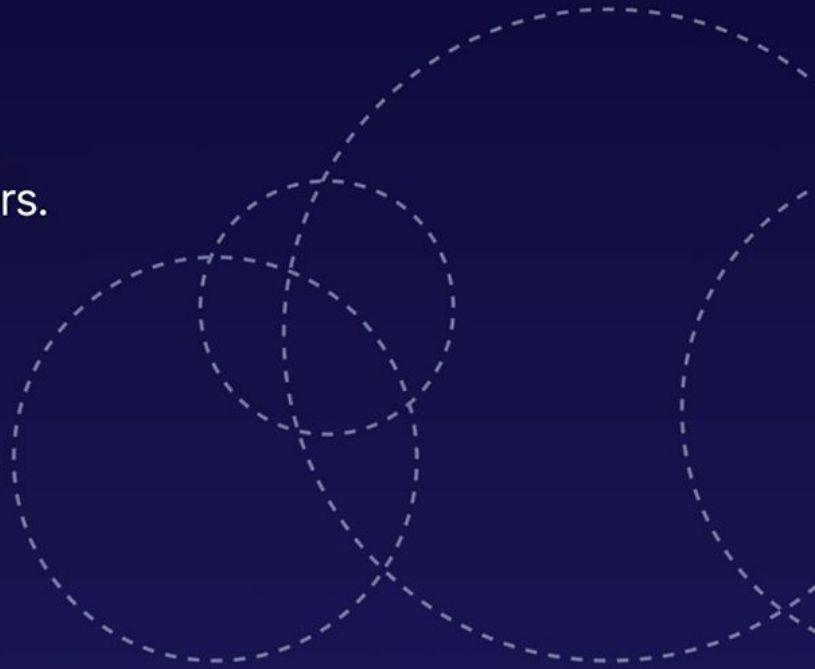
SECURITY CONSIDERATIONS:

Routing on-premises users through the firewall.

Use NSGs to block/pass traffic between application tiers.

Be sure to organize your Virtual Network assets in the same resource group. This will work for both organizational purposes as well as security.

Assign RBAC roles to resource groups to restrict access to resources.



Summary

Planning Virtual Networks

What to keep in mind:

Handling Name Resolution

- Azure private zones
- Azure-provided name resolution
- Customer-managed DNS (your own)

Azure Name Resolution

What it does and doesn't do.

Hybrid Networks

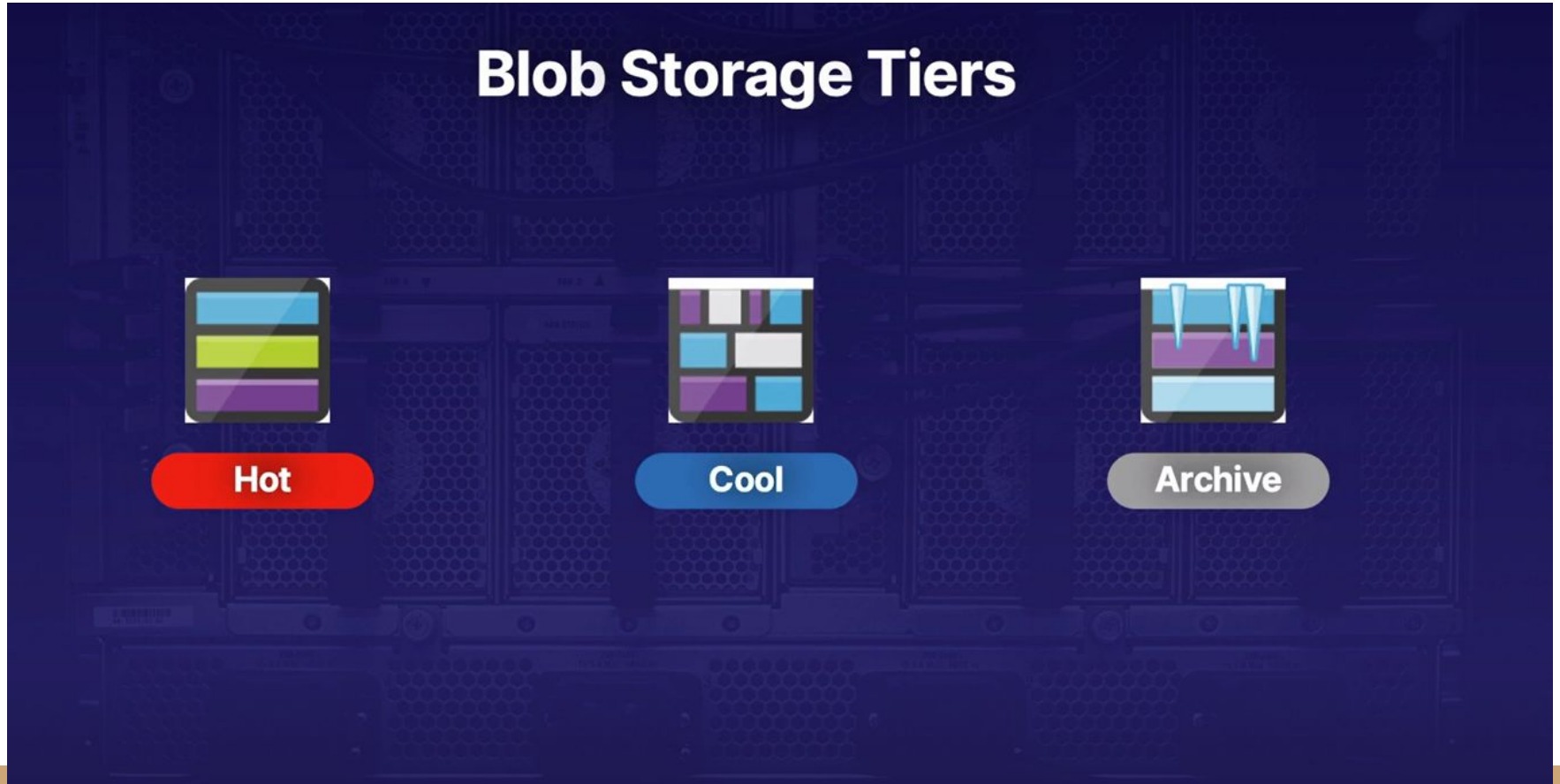
aka: ExpressRoute

Securing a Hybrid Network

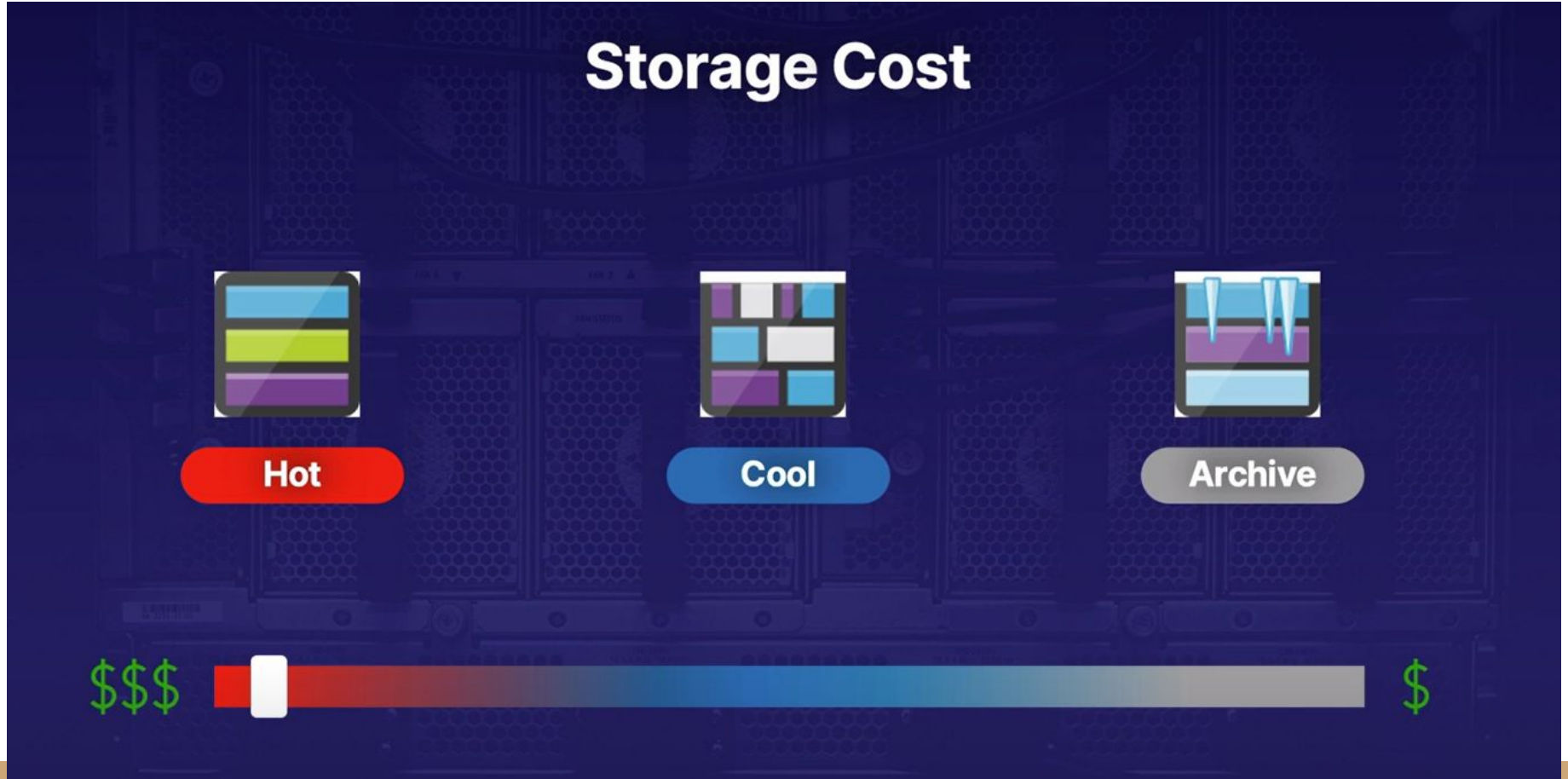
Perimeter Network

Storage

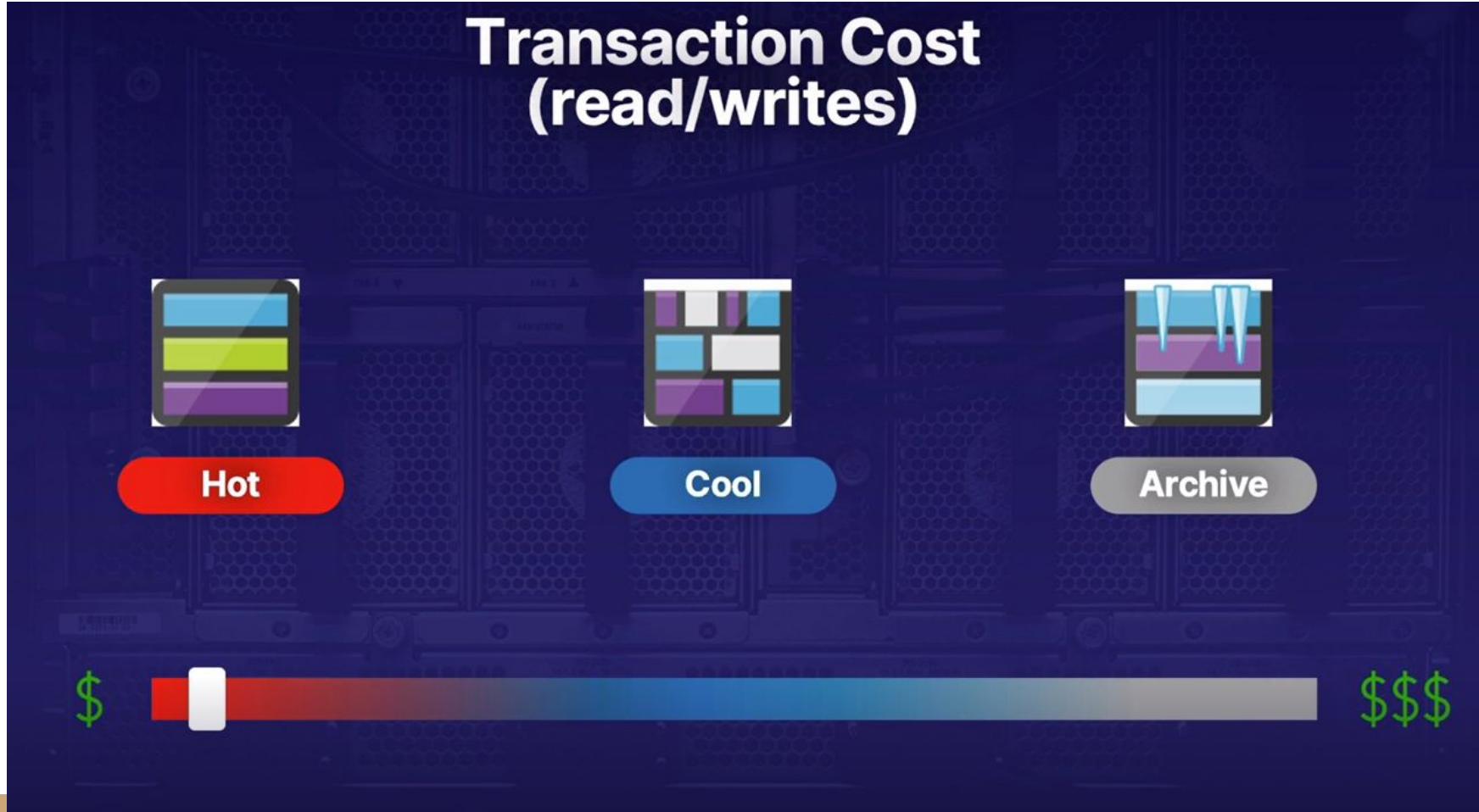
Choosing a storage Tier



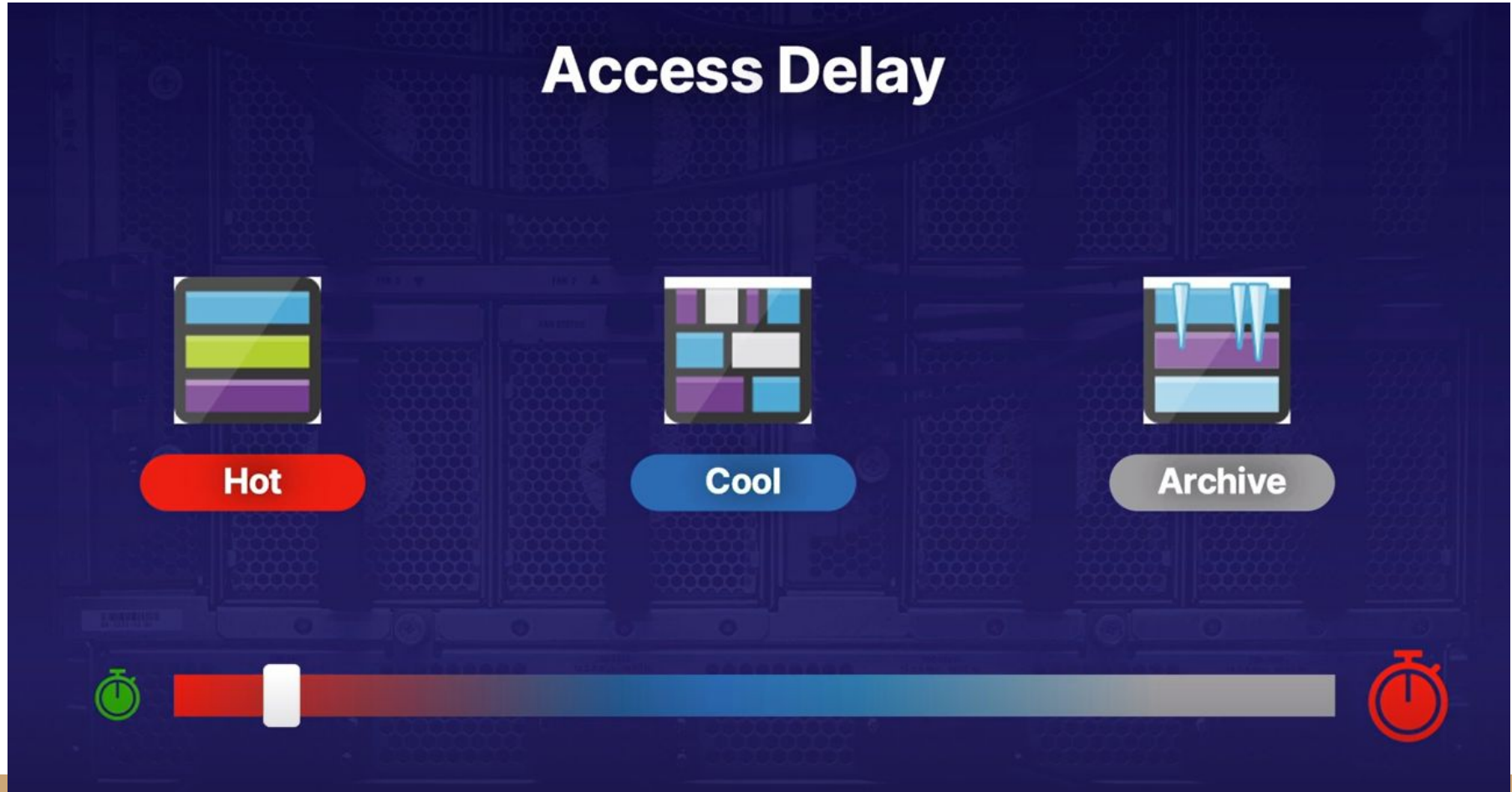
Choosing a storage Tier



Choosing a storage Tier



Choosing a storage Tier



Choosing a storage Tier

Choosing a storage Tier

Best Uses

Hot

- Actively changing data
- Recent backups

Cool

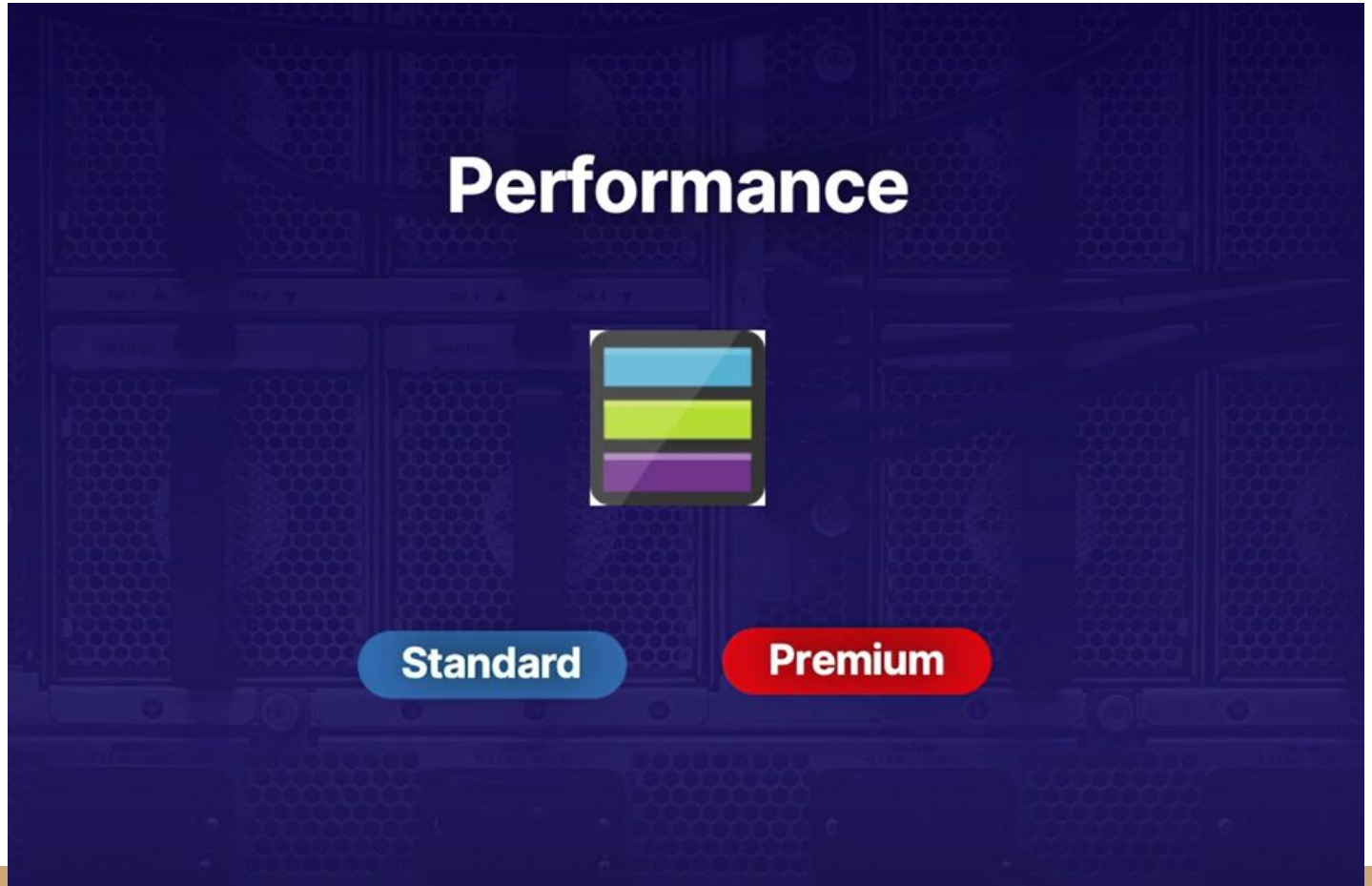
- Older backups
- Storage

Archive

- Long-term backups
- Archive data
- Static/historical/ compliance (e.g. HIPAA)

Choosing a Storage Tier

Support Tiering for Storage Accounts

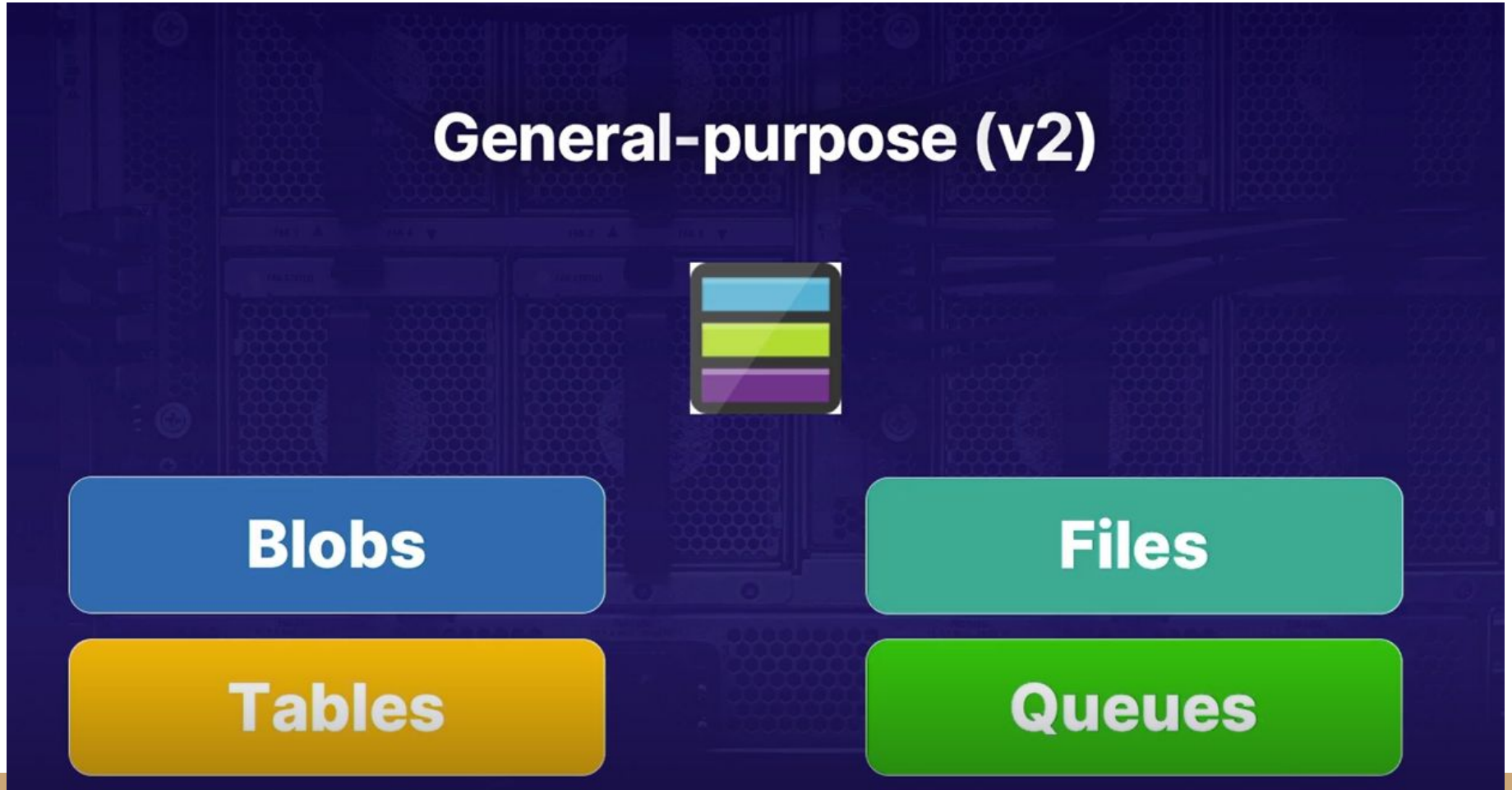


Support Tiering for Storage Accounts

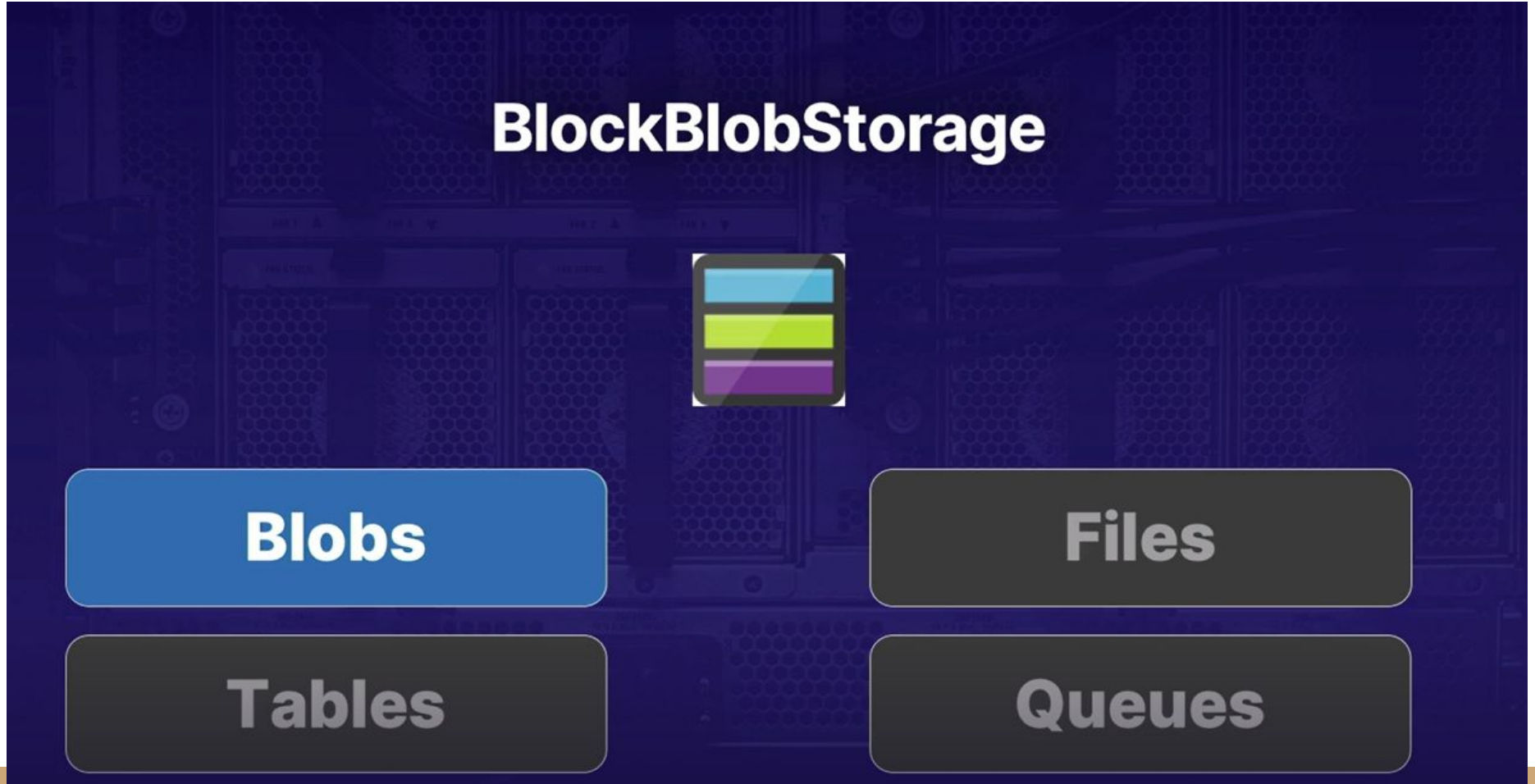
Types of Storage Accounts

- General-purpose v2
- General-purpose v1 (Legacy)
- BlockBlobStorage
- FileStorage
- BlobStorage (Legacy)

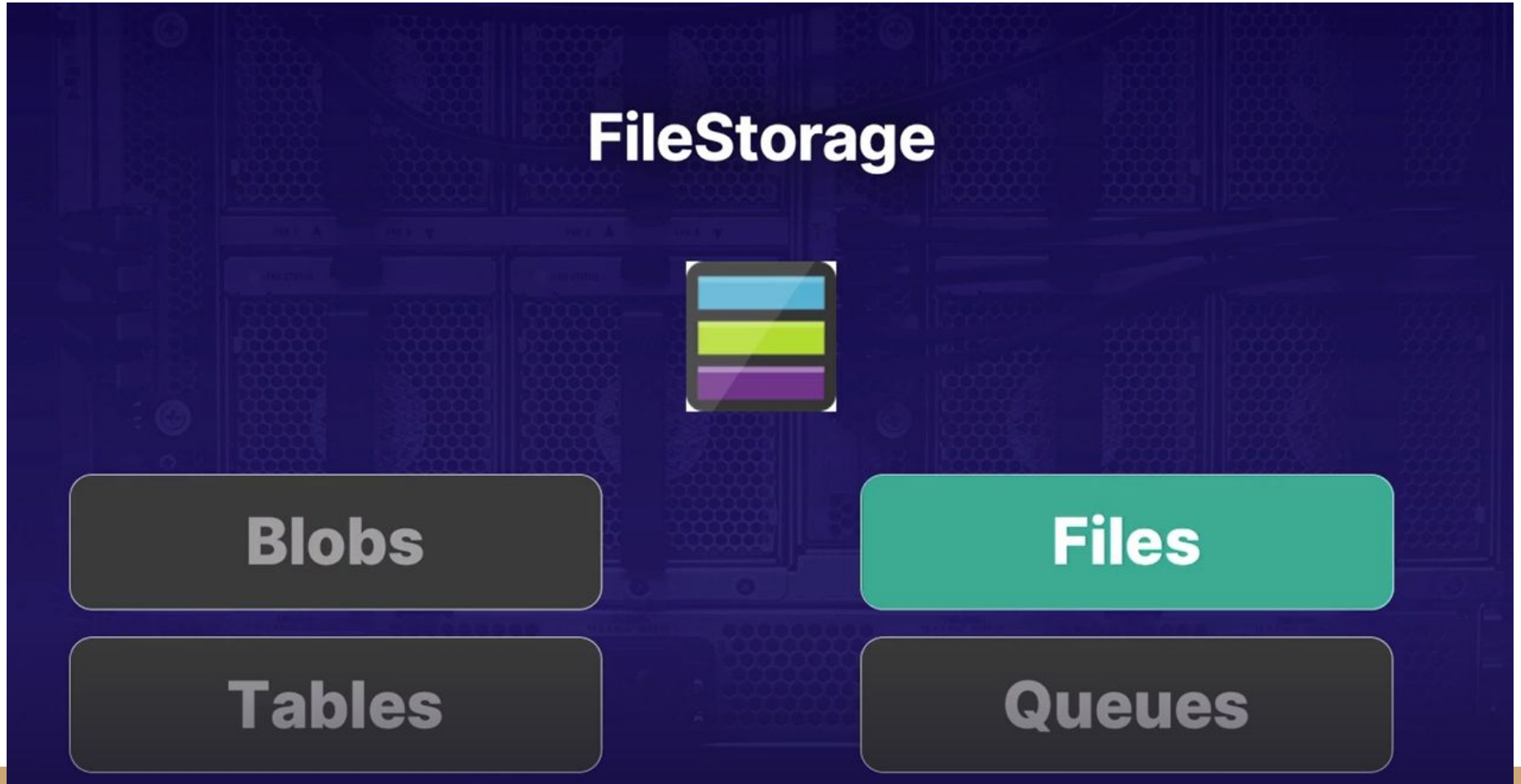
Support Tiering for Storage Accounts



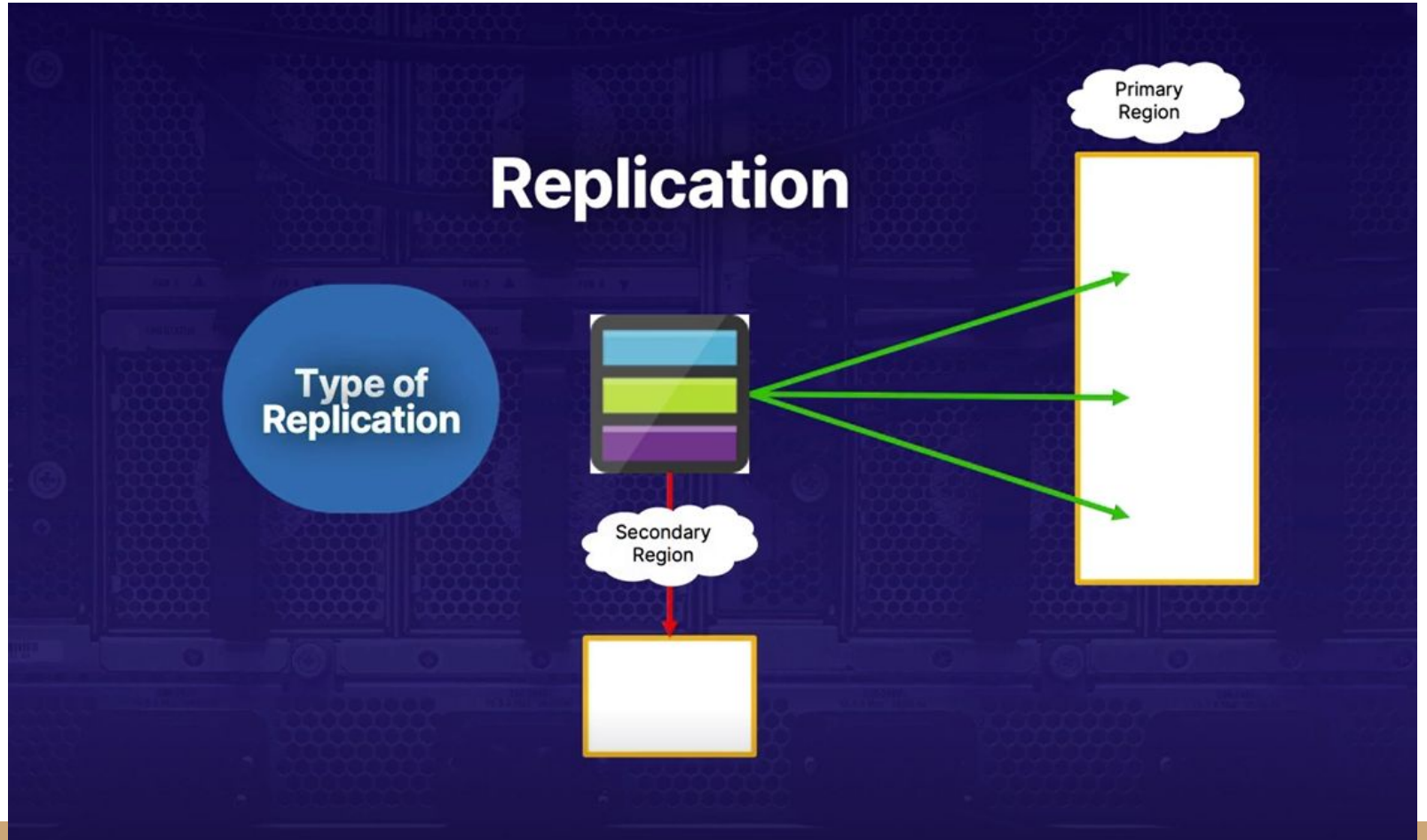
Support Tiering for Storage Accounts



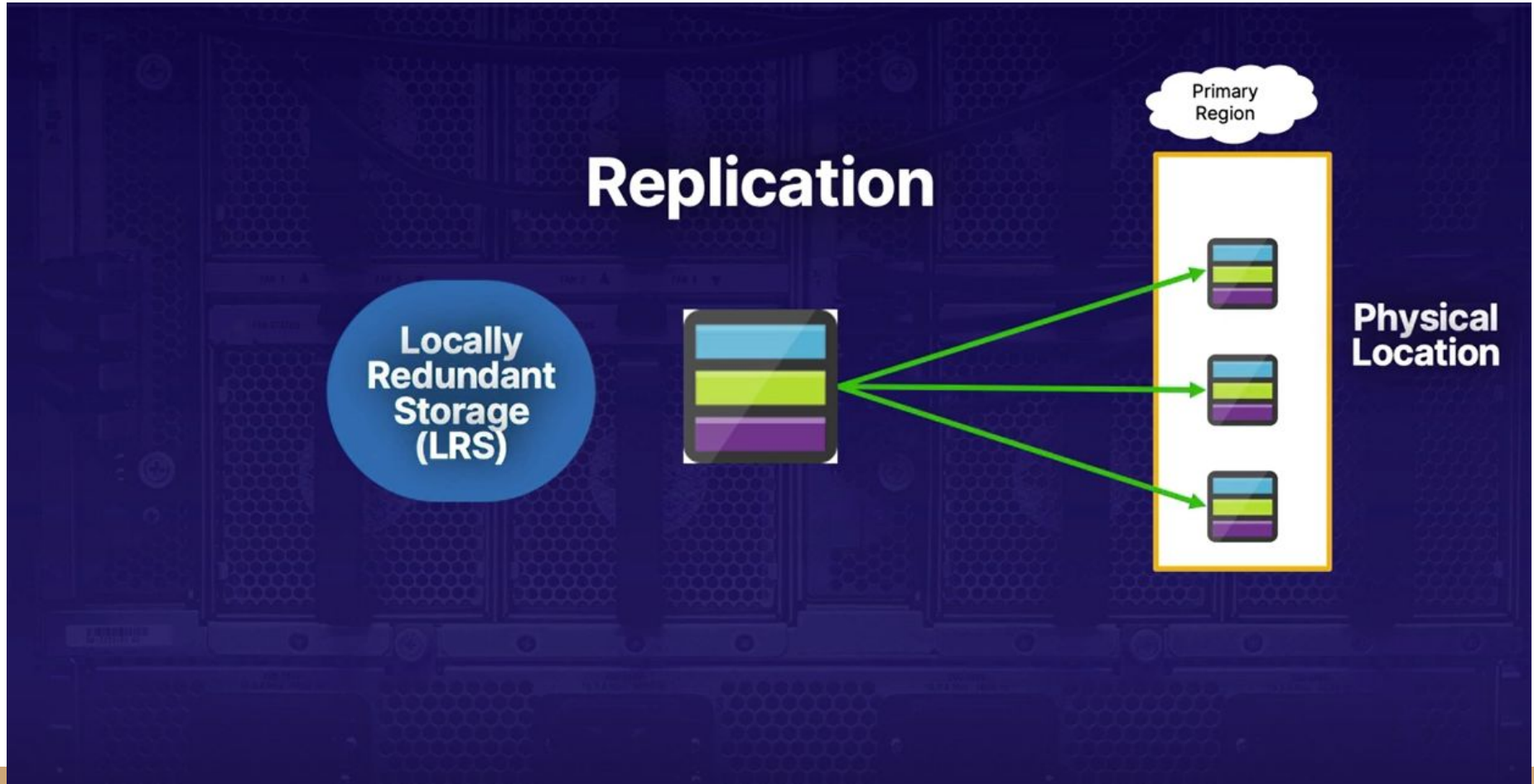
Support Tiering for Storage Accounts



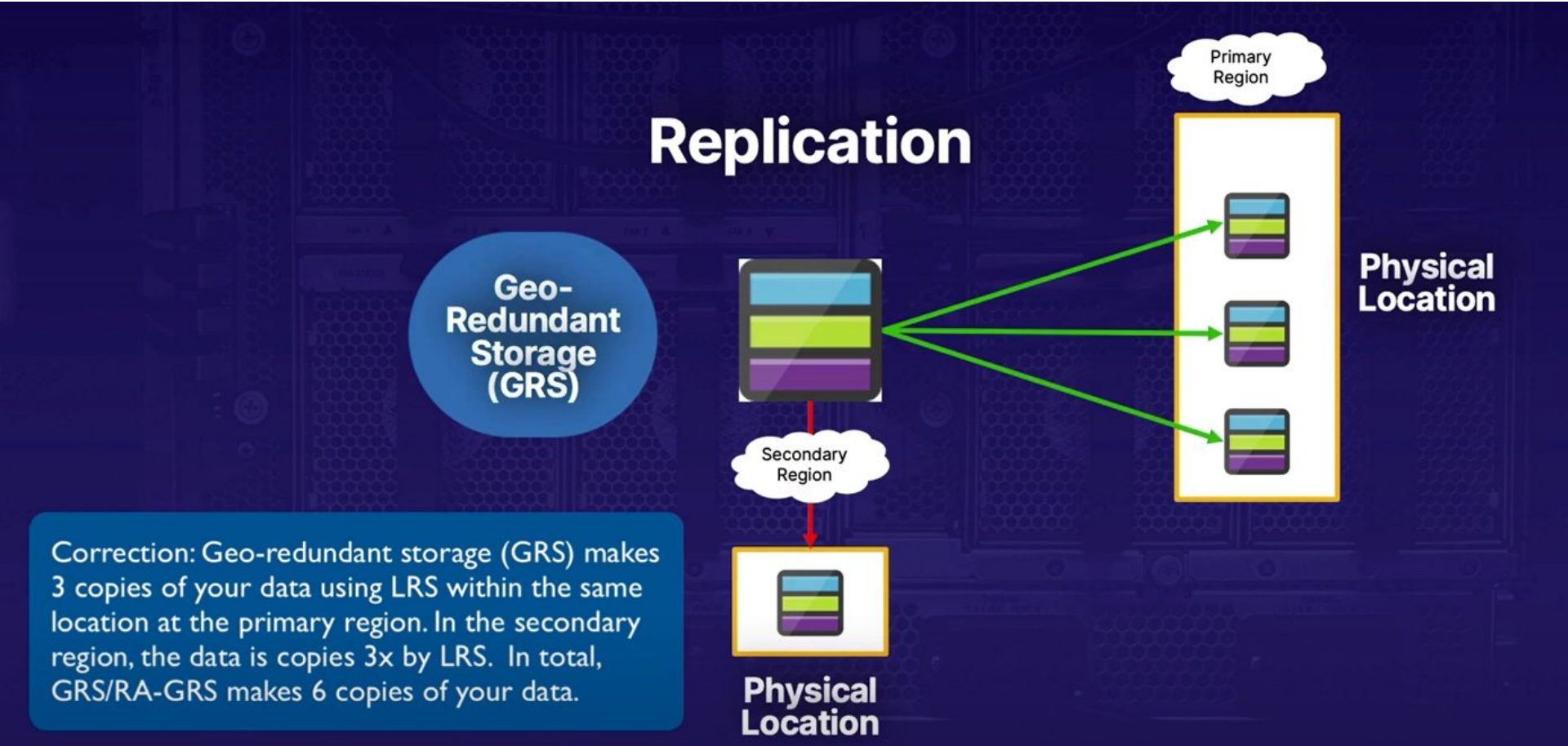
Support Tiering for Storage Accounts



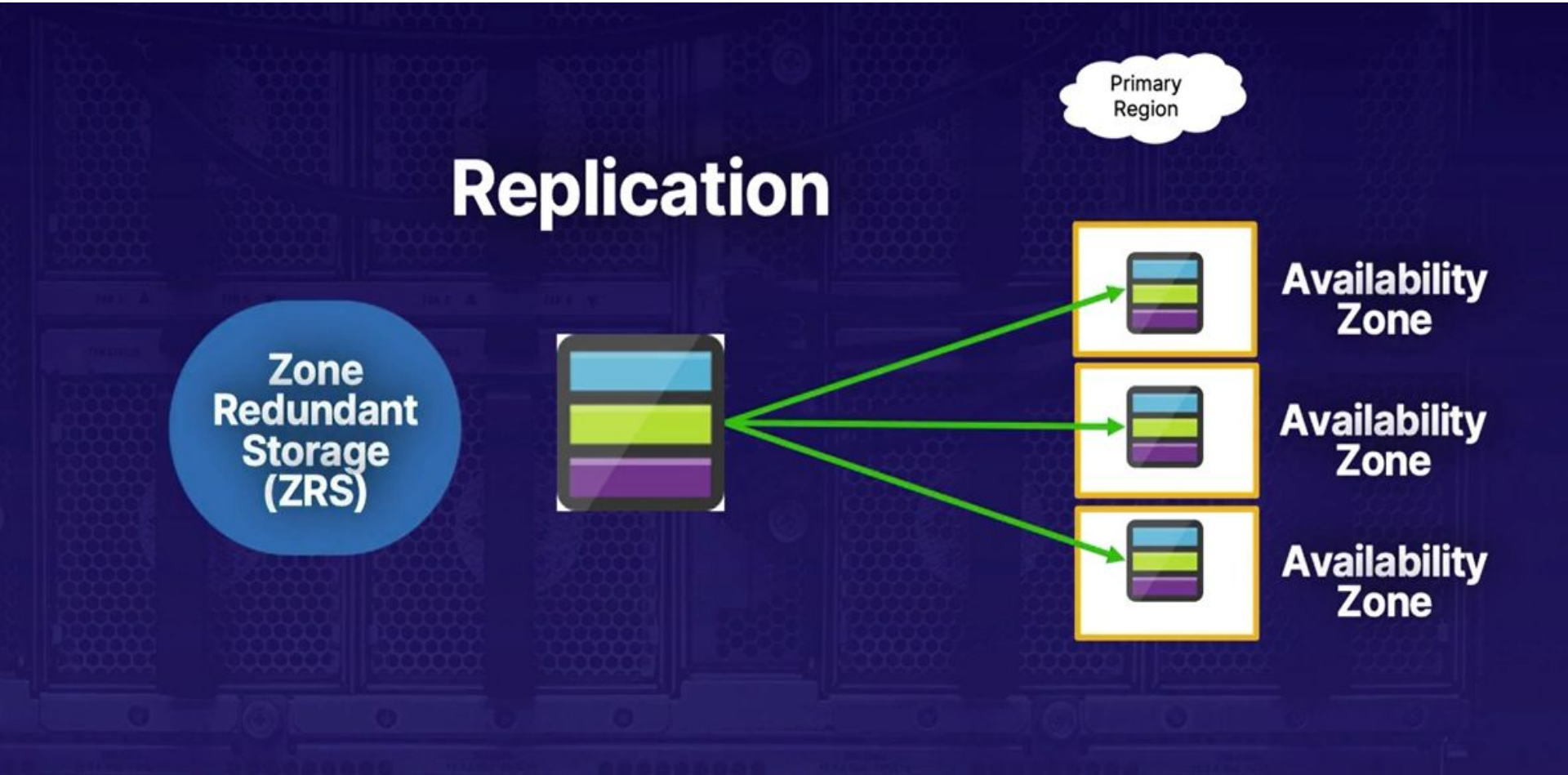
Support Tiering for Storage Accounts



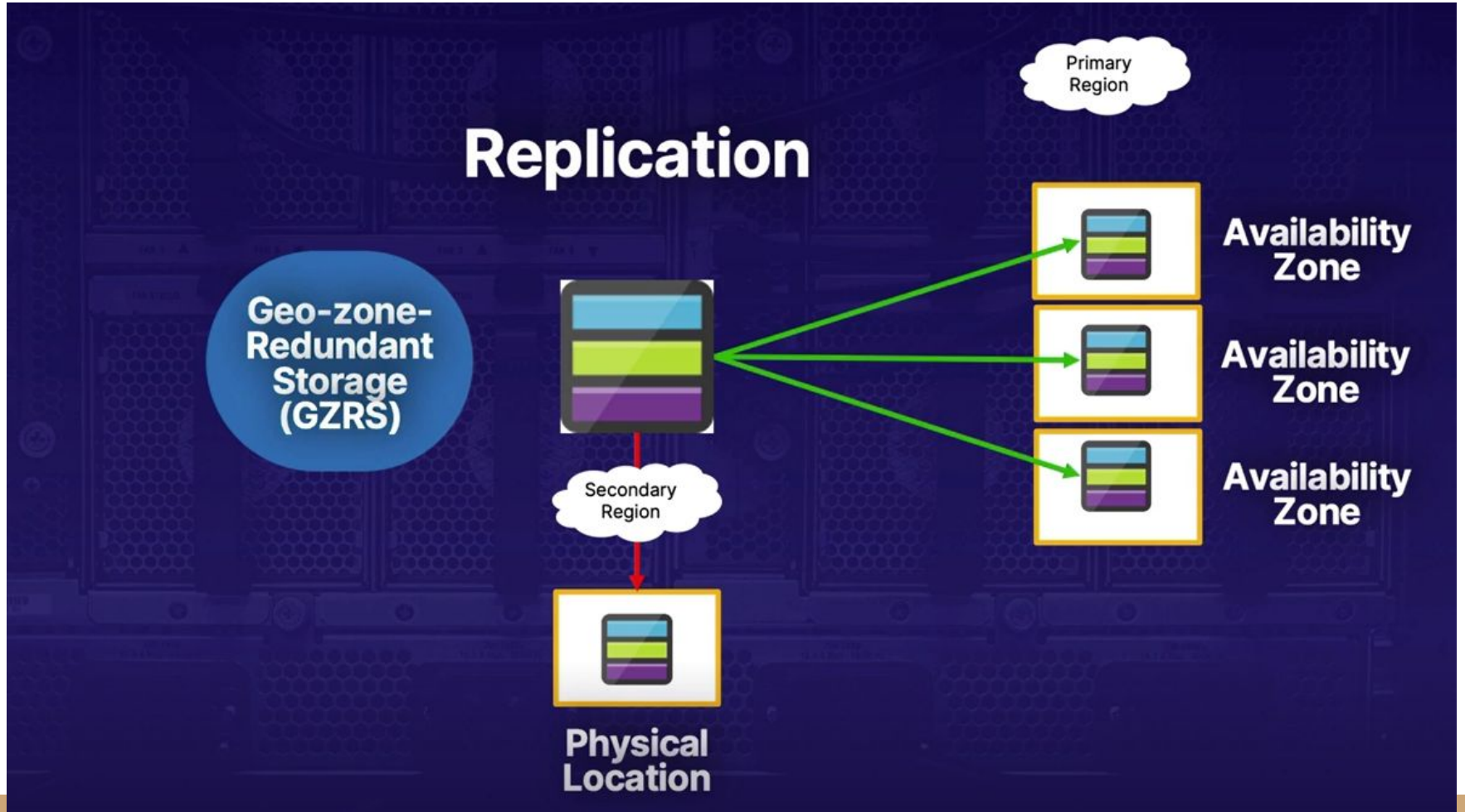
Support Tiering for Storage Accounts



Support Tiering for Storage Accounts



Support Tiering for Storage Accounts

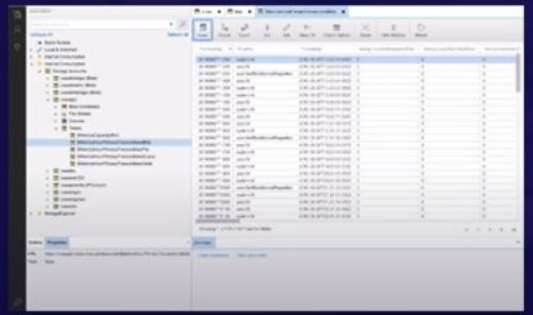


Support Tiering for Storage Accounts

Recommended Storage Management Tools

Tool Types - Recommended Storage Management Tools

Graphical User Interface (GUI)



Command Line

```
Bash
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

mark@Azure:~$
```

Scripting

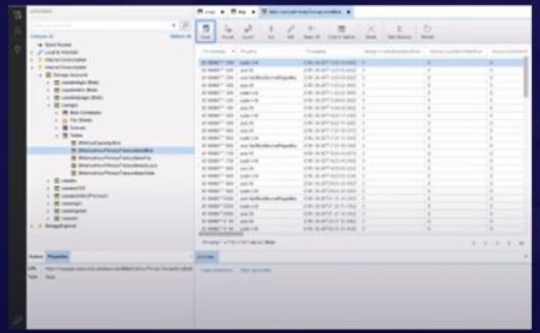
PowerShell

```powershell
# download first blob
Get-AzStorageBlobContent -Blob "Image001.jpg" `
  -Container $containerName `
  -Destination "D:\_TestImages\Downloads\" `
  -Context $ctx

# download another blob
Get-AzStorageBlobContent -Blob "Image002.png" `
  -Container $containerName `
  -Destination "D:\_TestImages\Downloads\" `
  -Context $ctx
```

Tool Types - Recommended Storage Management Tools

Recommended Storage Management Tools

- Azure Portal
- Azure Storage Explorer
- Visual Studio Cloud Explorer



- Azure CLI

```
Bash
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

mark@Azure:~$
```

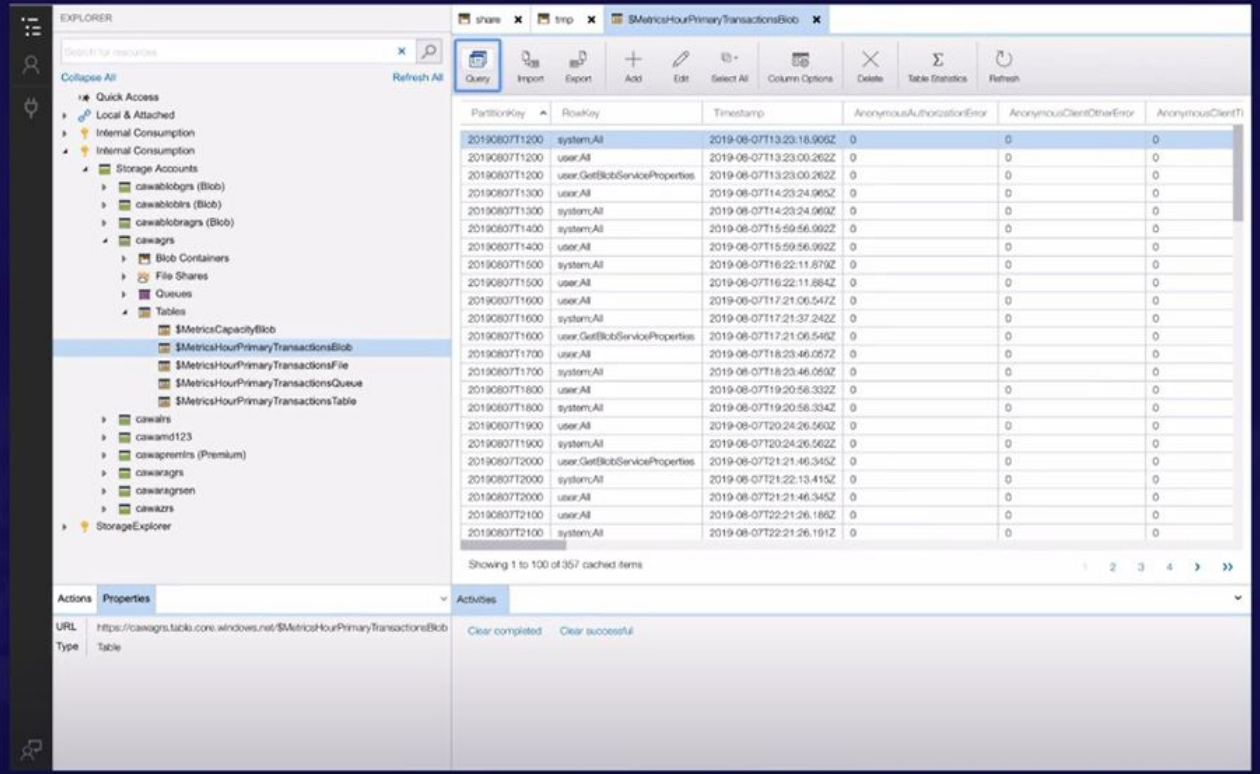
- PowerShell
- .NET
- Java
- Python
- Go
- PHP
- Ruby
- Xamarin

```
PowerShell

# download first blob
Get-AzStorageBlobContent -Blob "Image001.jpg" `
  -Container $containerName `
  -Destination "D:\_TestImages\Downloads\" `
  -Context $ctx

# download another blob
Get-AzStorageBlobContent -Blob "Image002.png" `
  -Container $containerName `
  -Destination "D:\_TestImages\Downloads\" `
  -Context $ctx
```

Azure Storage Explorer

Recommended Storage Management Tools

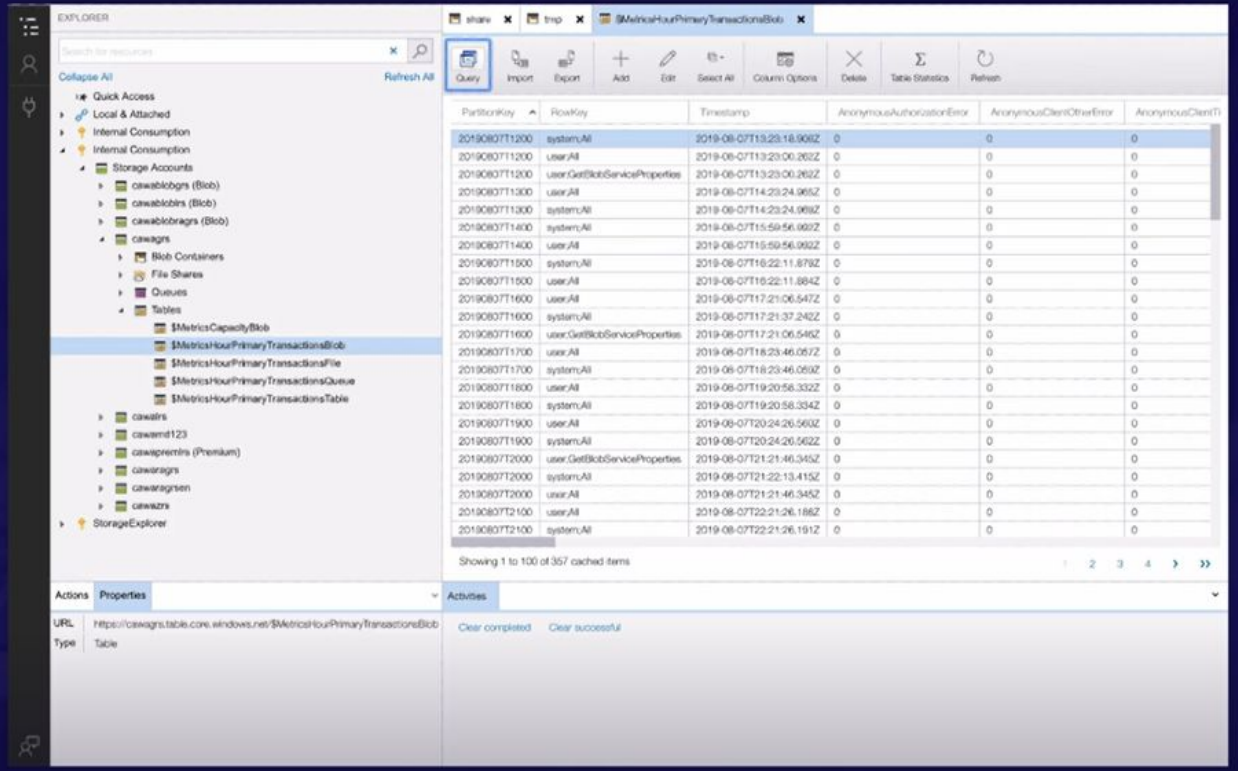
- Blobs, Files, Queues, Tables
- Azure Cosmos DB
- Azure Data Lake
- Virtual Machine Disks



Tool Types - Recommended Storage Management Tools

Recommended Storage Management Tools

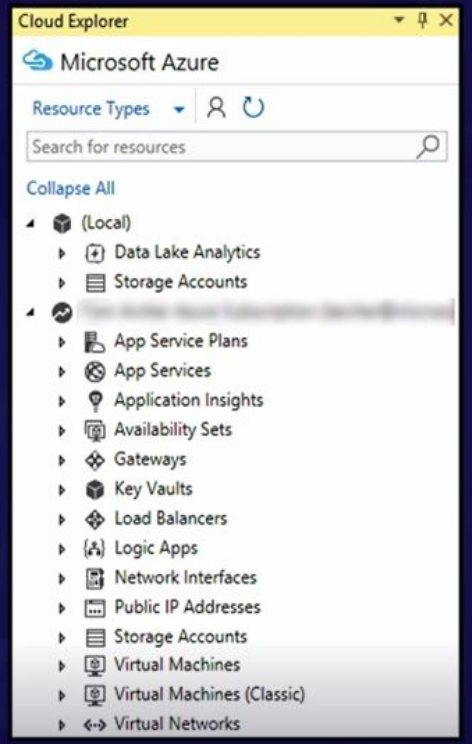
- Multiple Subscriptions
- Azure
- Azure Stack
- Government Cloud



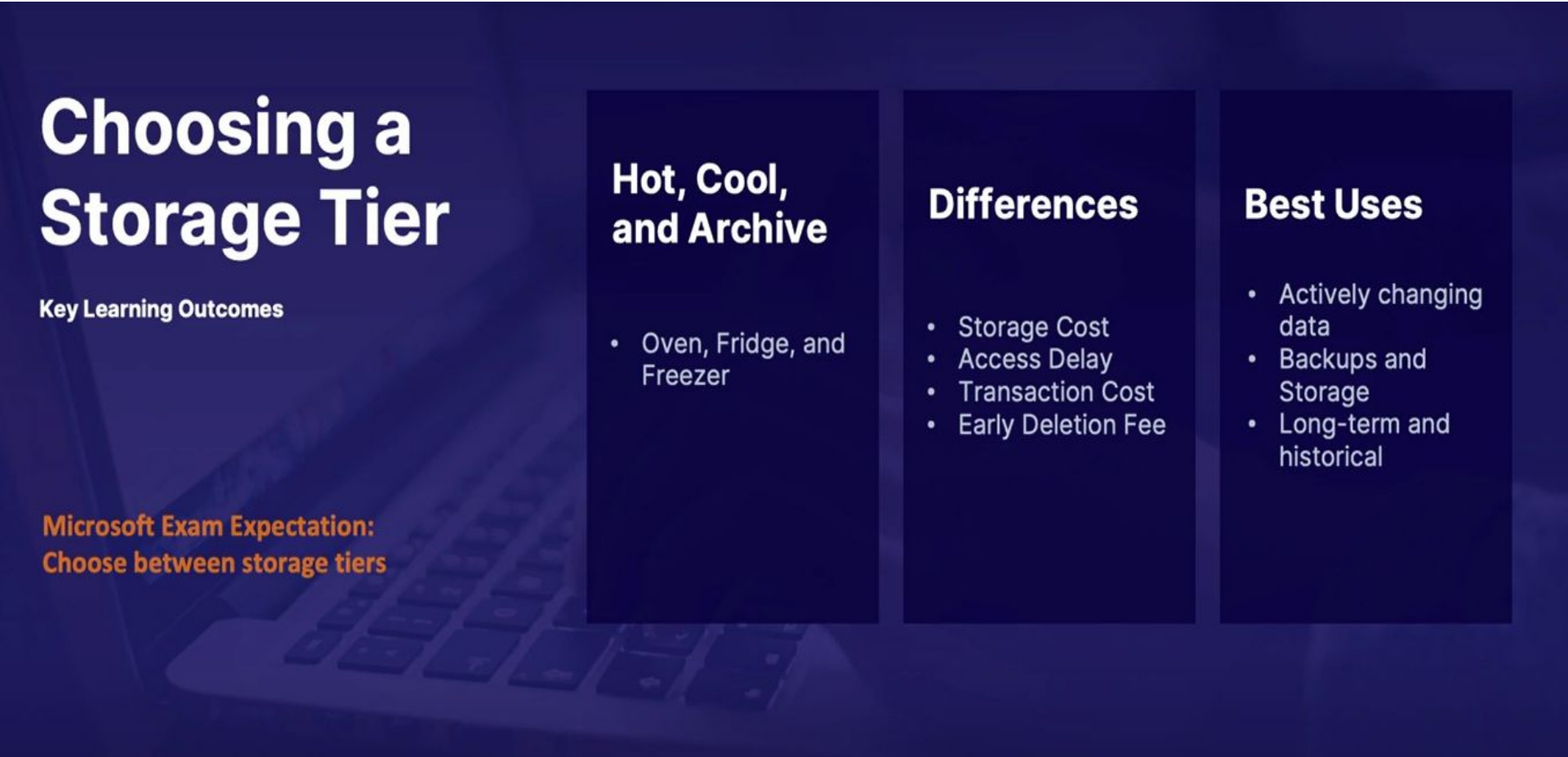
Tool Types - Recommended Storage Management Tools

Recommended Storage Management Tools

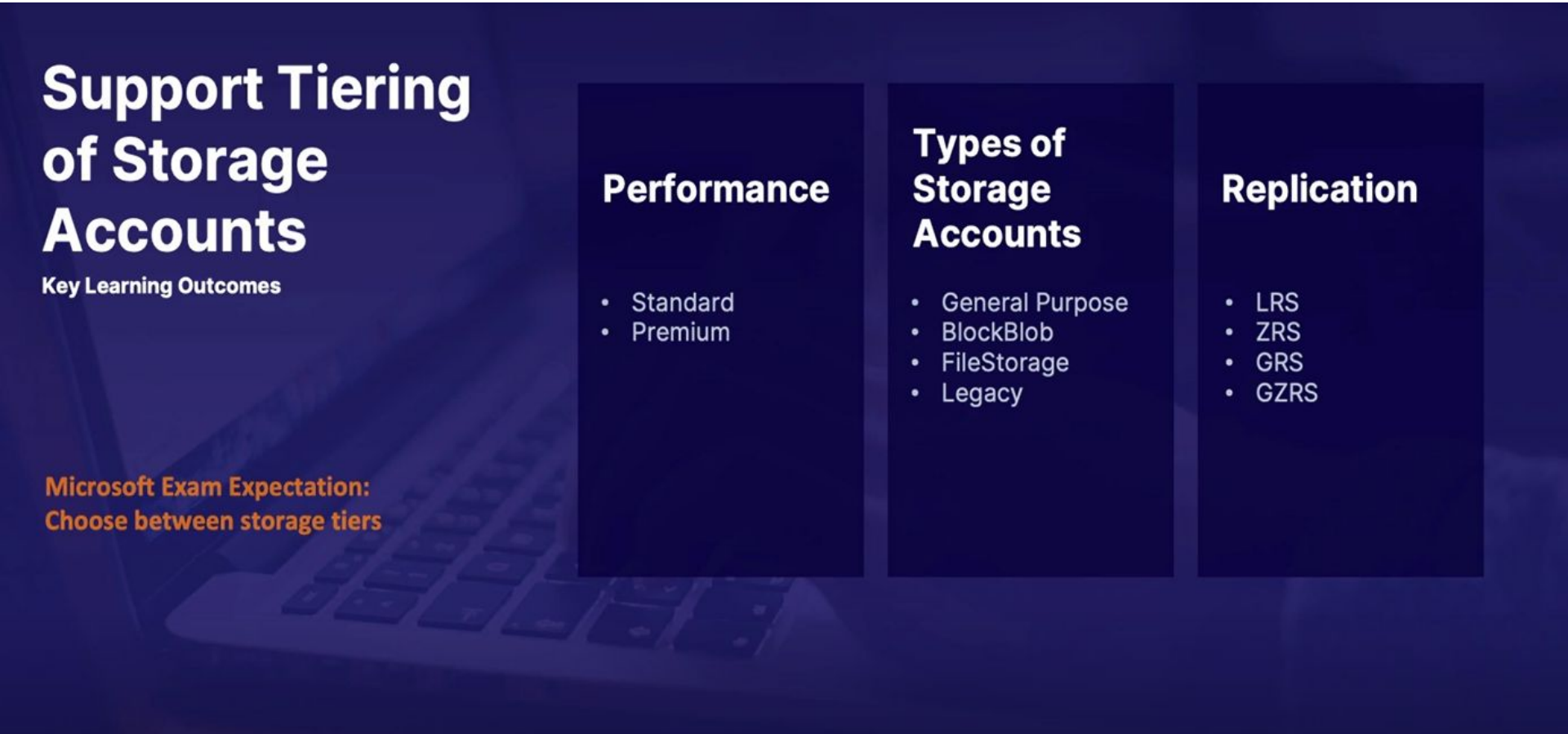
- Built on Azure Resource Manager Stack
- View Resources and Groups
- Inspect Properties
- Perform Key Developer Diagnostics within Visual Studio



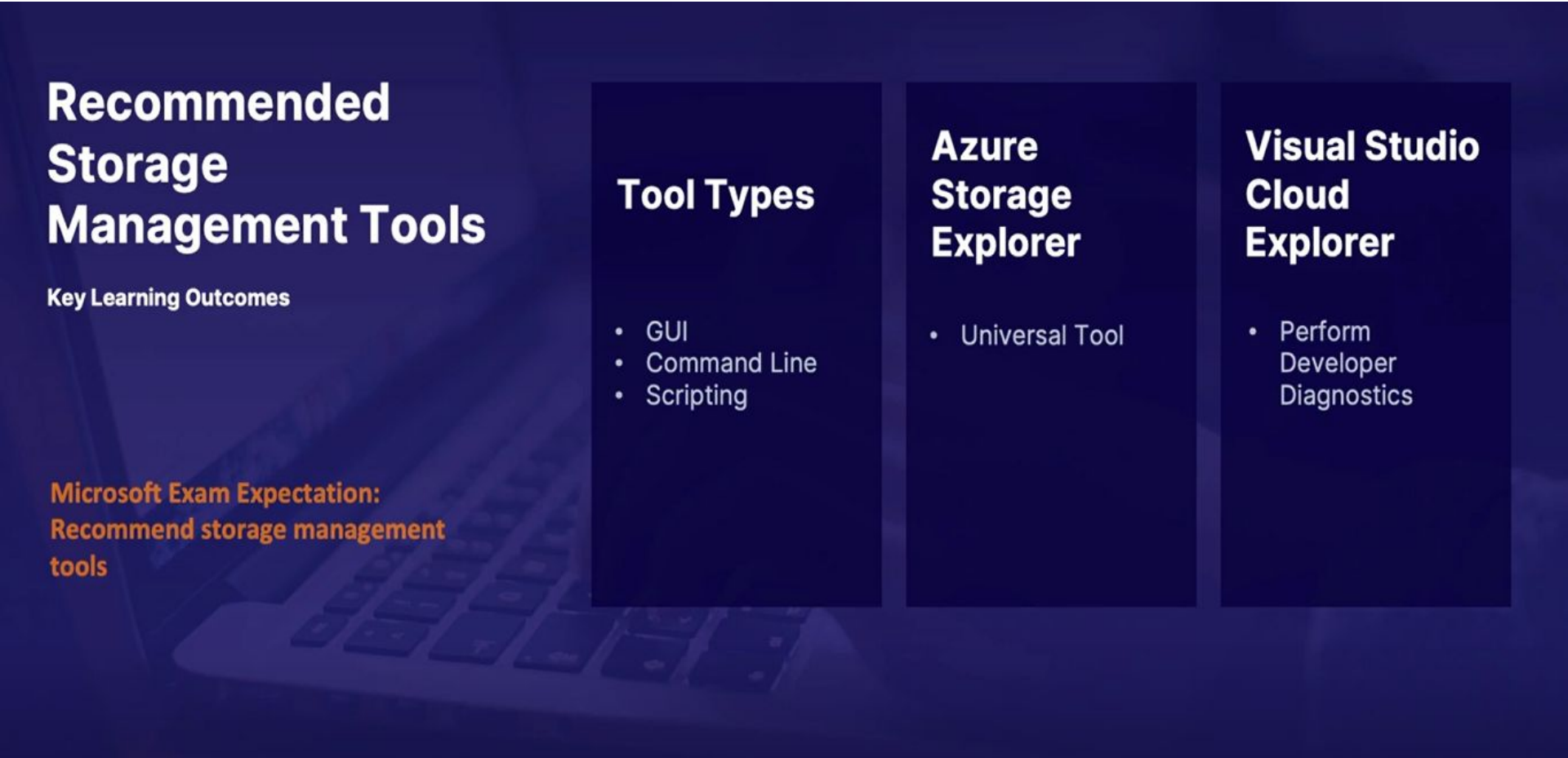
Summary


Choosing a Storage Tier
Key Learning Outcomes
Microsoft Exam Expectation:
Choose between storage tiers
Hot, Cool, and Archive
• Oven, Fridge, and Freezer
Differences
• Storage Cost
• Access Delay
• Transaction Cost
• Early Deletion Fee
Best Uses
• Actively changing data
• Backups and Storage
• Long-term and historical

Summary


Support Tiering of Storage Accounts
Key Learning Outcomes
Microsoft Exam Expectation:
Choose between storage tiers
Performance
Standard
Premium
Types of Storage Accounts
General Purpose
BlockBlob
FileStorage
Legacy
Replication
LRS
ZRS
GRS
GZRS

Summary


Recommended Storage Management Tools
Key Learning Outcomes
Microsoft Exam Expectation: Recommend storage management tools
Tool Types
GUI
Command Line
Scripting
Azure Storage Explorer
Universal Tool
Visual Studio Cloud Explorer
Perform Developer Diagnostics

Summary

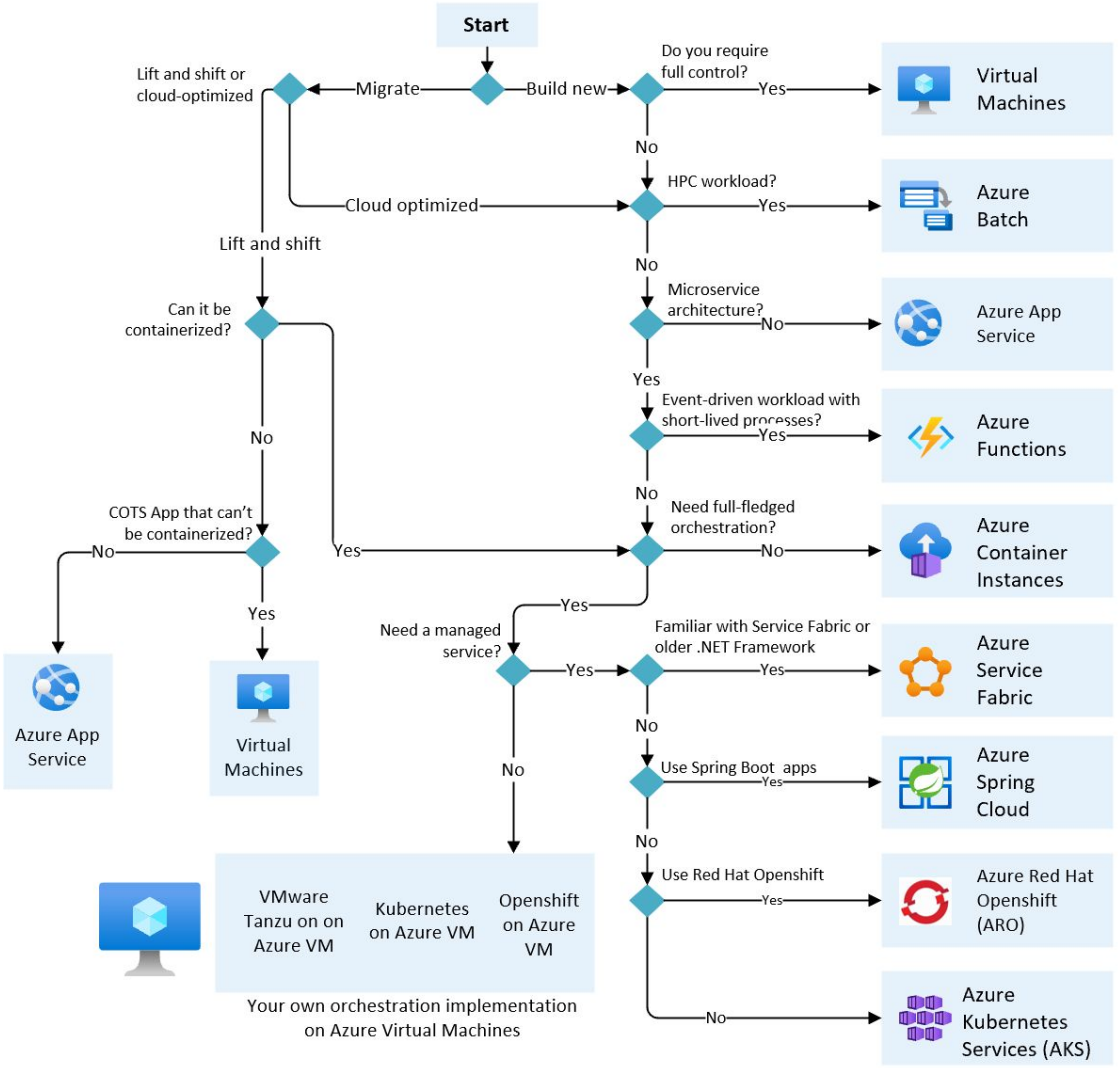
Storage Redundancy

Keep a close eye on the regions end users need to access an application.

Sometimes "Read-Access" isn't so apparent!

Design a Compute Solution

Choose an Azure compute service for your application

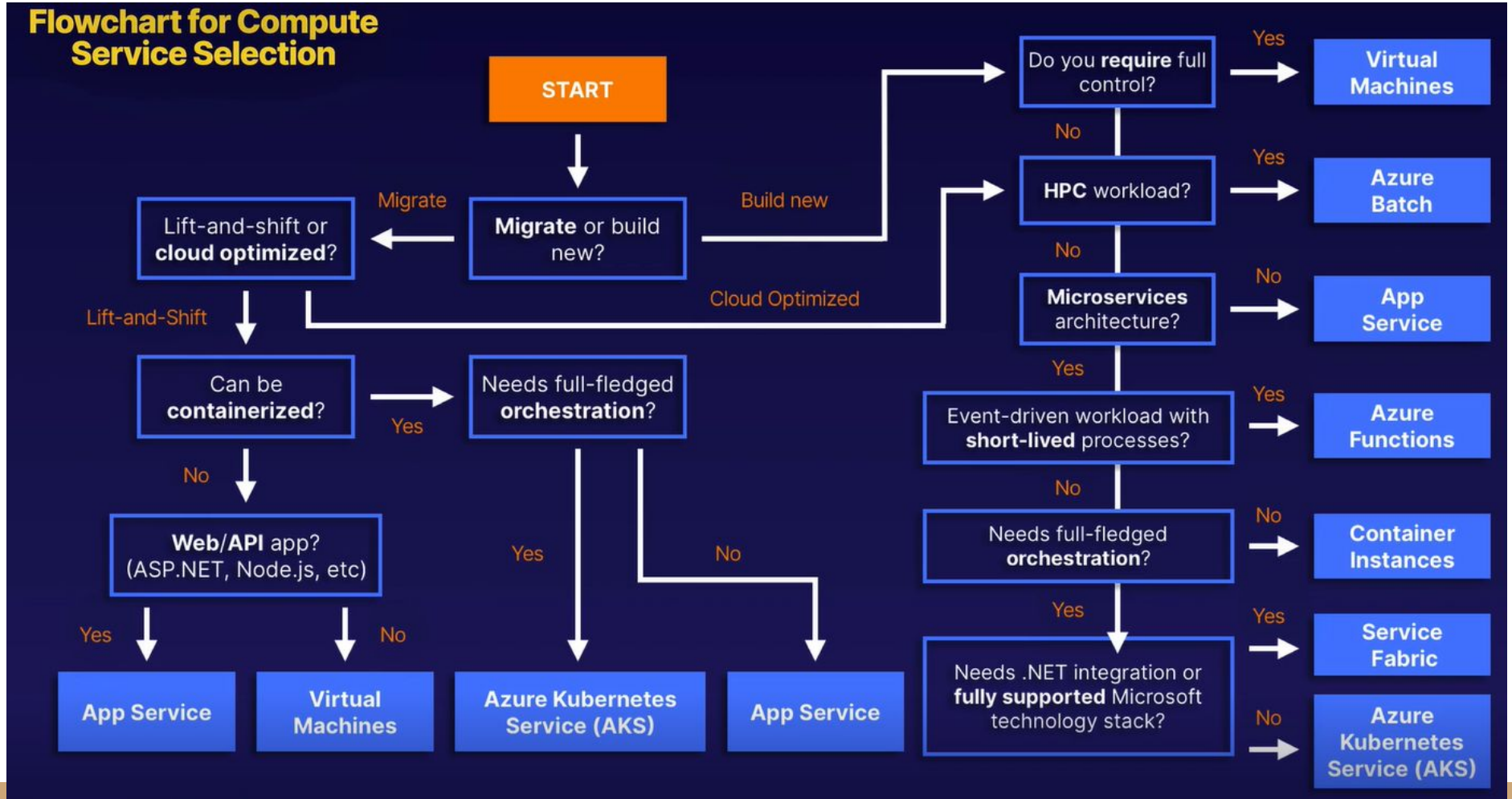


Choosing an Azure Compute Service

Compute: hosting model for the computing resources on which your application runs.

As with all planning and review activities, you'll need to know your end goal.
Always choose services with performance, availability, and cost in mind.

Choosing an Azure Compute Service



Choosing a Compute Service

Hosting Models:

Infrastructure as a Service (IaaS)	Provision VMs and associated network/storage components.
Platform as a Service (PaaS)	Managed hosting - deploy app without VMs or dedicated networking.
Functions as a Service (FaaS)	Deploy code and the service runs it. e.g. Azure Functions

SaaS: considered a subset of PaaS

Choosing an Azure Compute Service

Features:

Virtual Machines:
'nuff said.

Kubernetes (AKS):
service for running containerized apps

Container Instances:
quick and simple container setup. No VMs required. Includes Service Fabric

App Service:
for hosting web apps, RESTful APIs, mobile back-ends, or automated business processes.

Batch:
service for running large-scale parallel and high-performance computing (HPC) operations.

Functions:
Azure Functions as a Service (FaaS)

Determine Compute Options for Microservices

Microservices - What are they?

Applications are composed of small, independent modules which communicate using well-defined API contracts. These modules are decoupled "building blocks" that generally implement a single purpose function.

How does this apply to compute design?

You'll want to design an environment suited to the operations that your microservices will accomplish.

Choosing an Azure Compute Option for Microservices

Two of the most popular approaches:

SERVERLESS

Azure Functions:

Deploy your code and the hosting service puts it onto a VM to execute. Service Bus queues, Event Hub events, message processing...

VS.

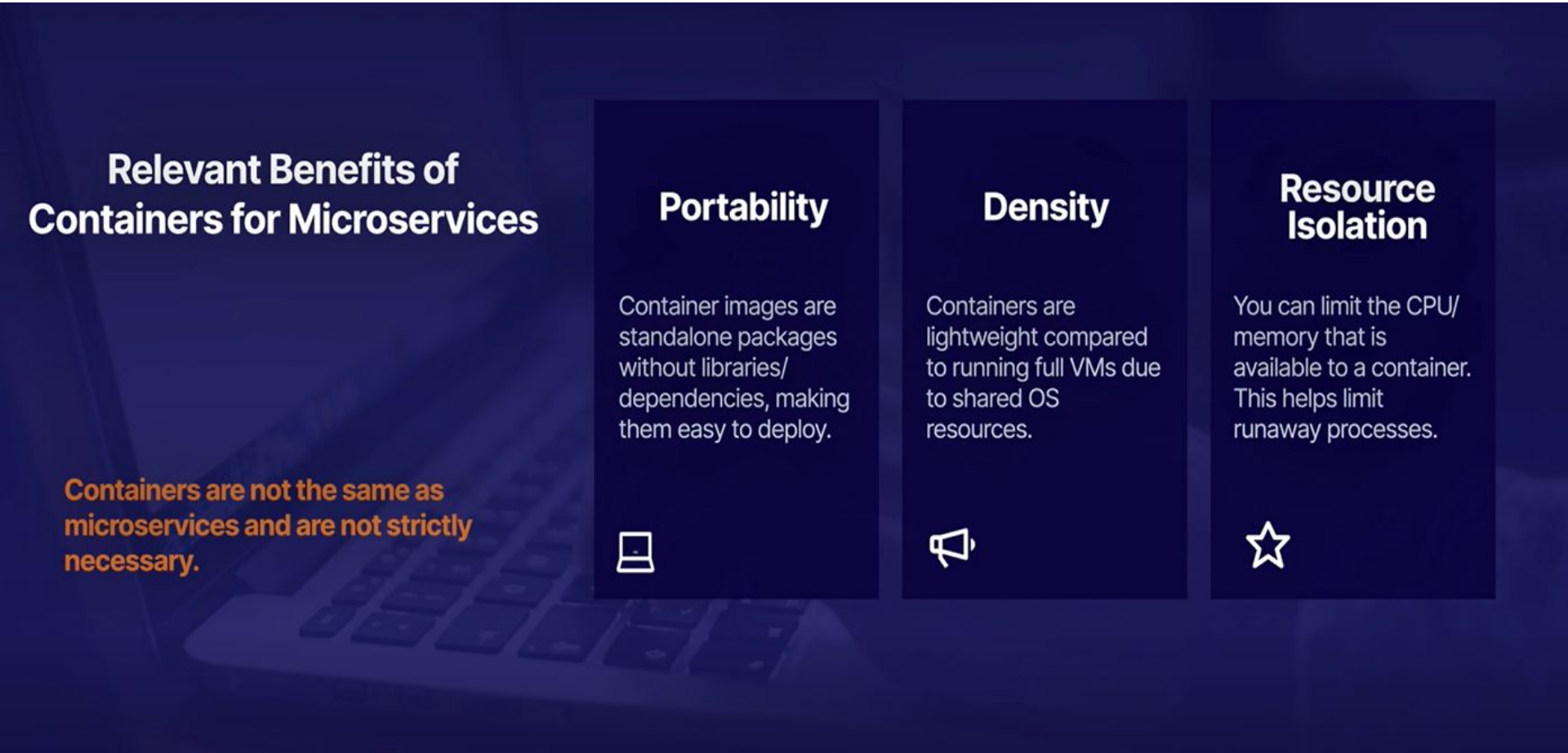
SERVICE ORCHESTRATOR

AKS & Service Fabric:

"Kubernetes APIs as a service" - limited to containers.

Service Fabric packages, deploys, and manages microservices. Can also run processes (binary executables).

Containers

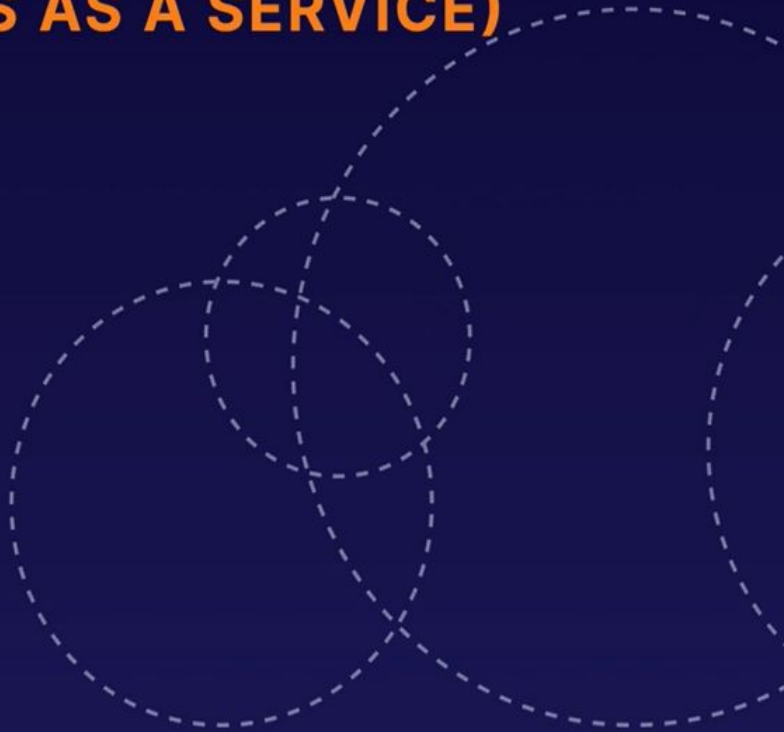

Relevant Benefits of Containers for Microservices
Containers are not the same as microservices and are not strictly necessary.
Portability
Container images are standalone packages without libraries/ dependencies, making them easy to deploy.
Density
Containers are lightweight compared to running full VMs due to shared OS resources.
Resource Isolation
You can limit the CPU/ memory that is available to a container. This helps limit runaway processes.

Serverless

SERVERLESS (FUNCTIONS AS A SERVICE)

No need to manage VMs or Virtual Network infrastructure.

Types of triggers can include schedules, HTTP, Blob storage, Event Hub events, Azure Queue storage, and Service Bus queues.



So, Which to choose

When choosing between an orchestrator and a serverless approach, keep these factors in mind:

Manageability

Serverless - platform manages all compute resources.
Orchestrator - you'll need to consider load balancing, CPU and memory usage, as well as networking.

Flexibility and Control

Orchestrator - lots of control over configuring and managing your services and the cluster.
Serverless - less control since many details are abstracted.

Portability

All orchestrators (Kubernetes, DC/OS, Docker Swarm, and Service Fabric) can run on-premises or in multiple public clouds.

Application Integration

Serverless - architecture can be challenging to manage. Logic Apps can help coordinate a set of functions.

Cost

Orchestrator - you pay for the VMs in the cluster.
Serverless - pay only for actual compute resources consumed.
In both cases, factor in the costs of other services (storage, databases, messaging, etc.).

Scalability

Azure Functions scales automatically.
Orchestrator - scale by increasing the number of service instances in the cluster. You can also add VMs.

Choosing Kubernetes

As mentioned before, consider green field or lift-and-shift when evaluating AKS

Identity and security management

Configure an AKS cluster to integrate with Azure AD and use existing IDs and groups.

Cluster node upgrades

AKS manages Kubernetes software upgrades. Cordons of nodes one by one and drains them before upgrading.

Integrated logging and monitoring

AKS includes Azure Monitor for containers. Custom Kubernetes installs normally required a monitoring solution needing install and config.

GPU enabled nodes

AKS supports GPU enabled node pools for compute or graphic intensive workloads.

Auto Cluster node and pod scaling

AKS supports two scaling options: Horizontal pod autoscaler or cluster autoscaler.

Choosing Kubernetes

As mentioned before, consider green field or lift-and-shift when evaluating AKS

Storage volume support

AKS supports both static and dynamic storage volumes. Pods can attach/reattach to these volumes as they are created or rescheduled on different nodes.

Virtual network support

An AKS cluster can easily be deployed into an existing virtual network.

Ingress with HTTP app routing support

Do your apps need to be publicly available? HTTP application routing allows easy access to deployed apps.

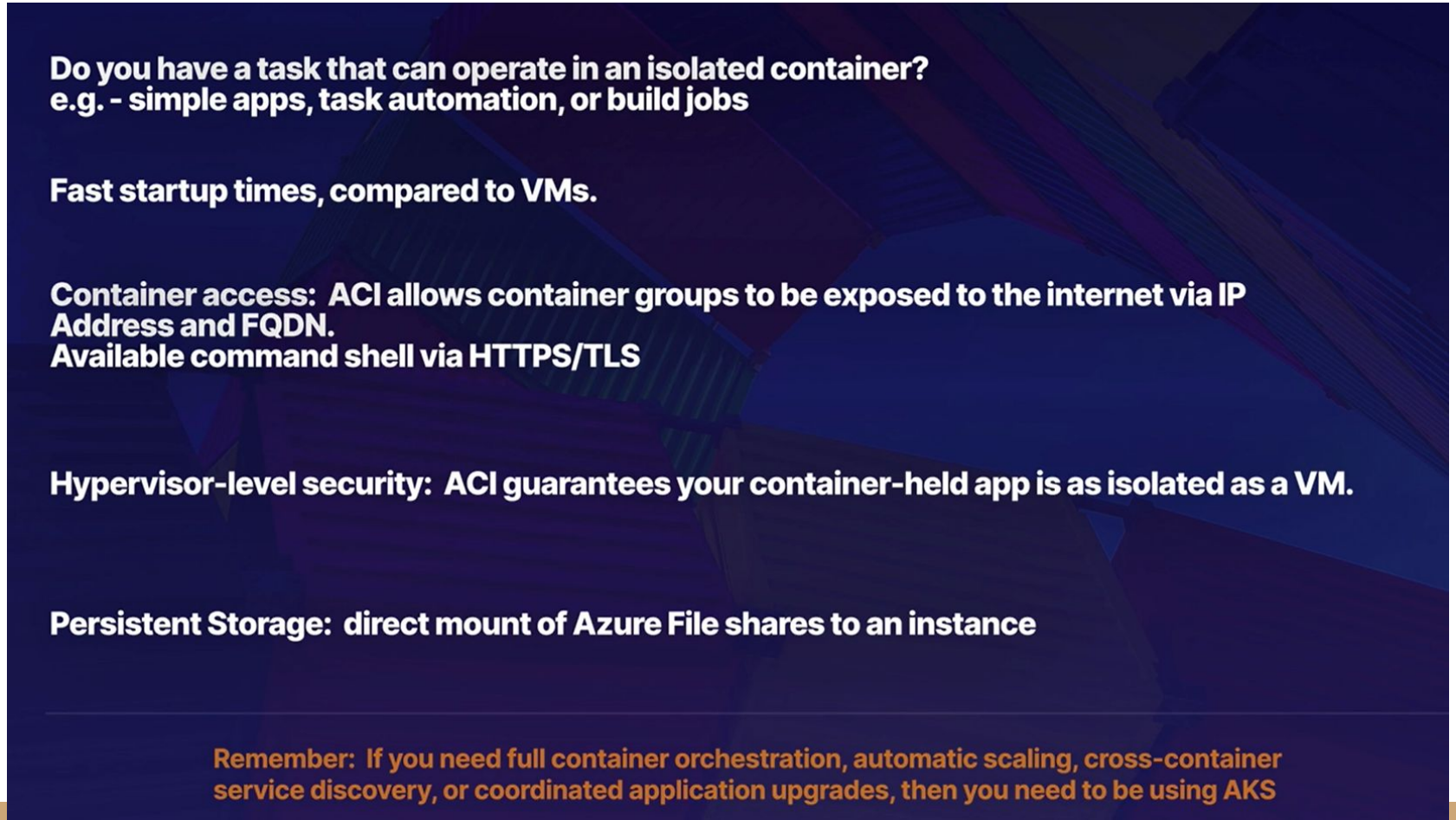
Private container registry

Do you need a private container registry? AKS integrates with Azure Container Registry. You can also use other public or private container repos.

Docker image support

AKS supports the Docker file image format.

When & why to use ACI (Azure Container Instances)



When & why to use ACI (Azure Container Instances)

Custom sizing: adjust your Instance to meed the needs of your application.

Linux and Windows support: ACI can run both operating systems with the same API.

Co-scheduled groups: multi-container groups that share a host machine, local network, storage, and lifecycle . Combine main app container with supporting role containers.

Virtual network deployment: put container instances into an Azure virtual network as you would a VM, with the same benefits.

Remember: If you need full container orchestration, automatic scaling, cross-container service discovery, or coordinated application upgrades, then you need to be using AKS

Design a Compute Solution

Solutions to provision your Azure compute infrastructure...

Use automation to provision and manage compute resources.

For each VM you deploy, you normally have to manually do the following:

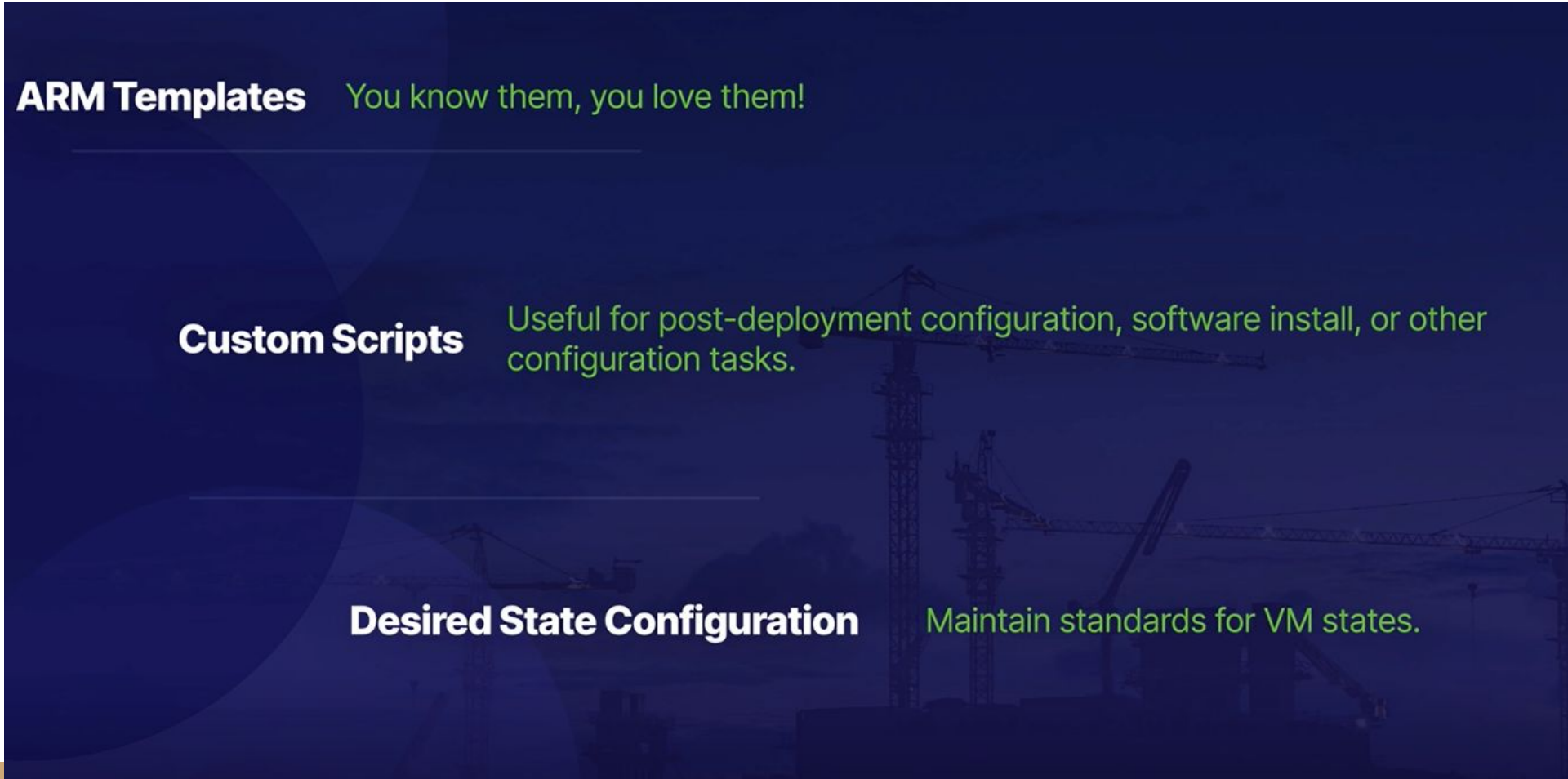
Configure the VM: tier, SKU, IP address, disk, etc.

Configure the OS: set OS level firewalls, partitions, security, etc.

Install Software: anti-malware, agents, backup software, etc.

Apply Updates: an important part of every OS install.

Automation Tools



Automation Tools

Automation State Configuration — Manage and deploy DSC configurations.

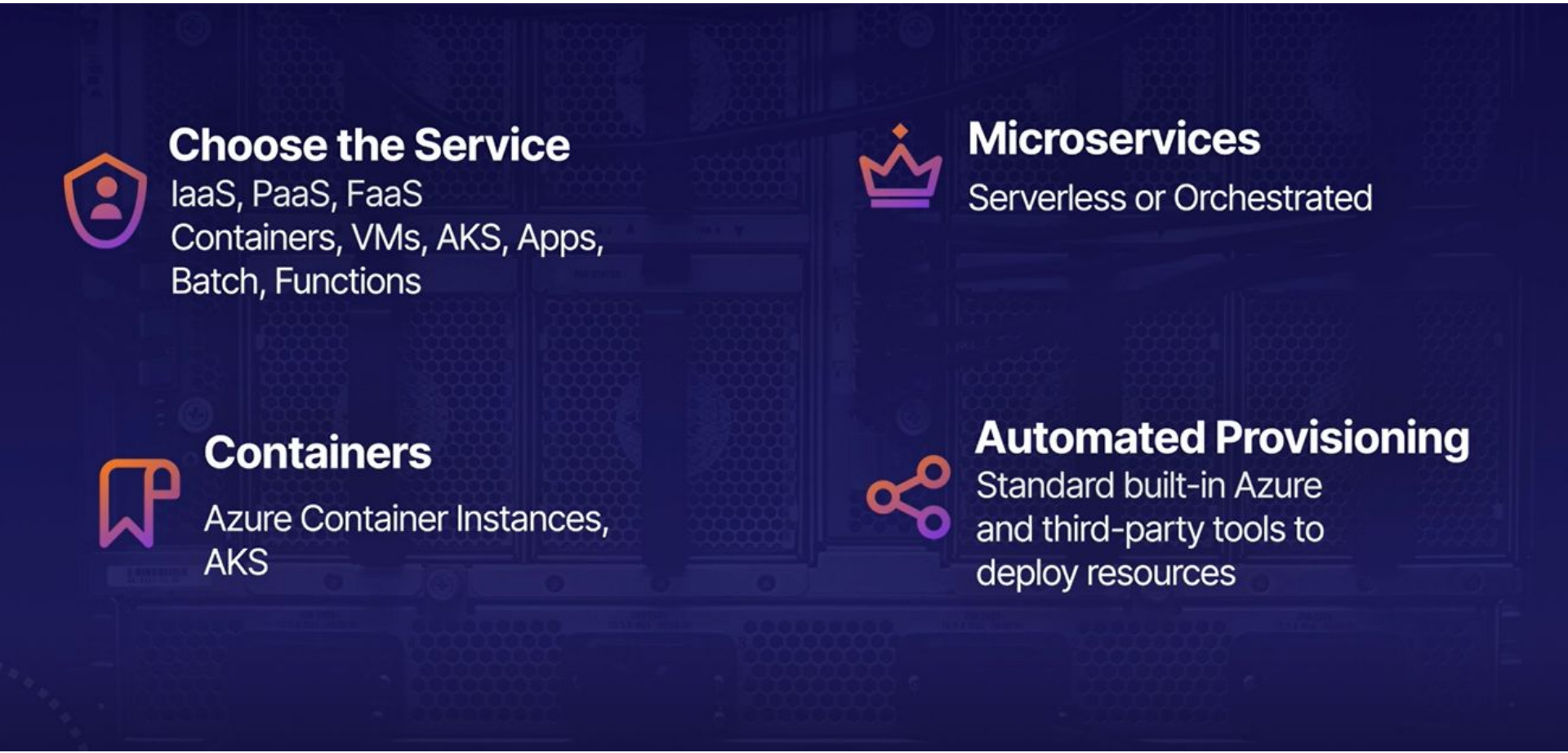
Chef

On-premises or cloud deployment tool.
Typically hosted.
Recipes can add the Chef extension to ARM templates.

Terraform

Open-source infrastructure-as-code (IAC) tool.
Multi-cloud functional.
Can run directly from the Azure CLI.

Compute Solution Design



Design a Database Solution

Selecting a Database Platform - Types of Data

Stuctured

- Azure SQL Database
- MySQL
- PostgreSQL on Azure
- Data Lake

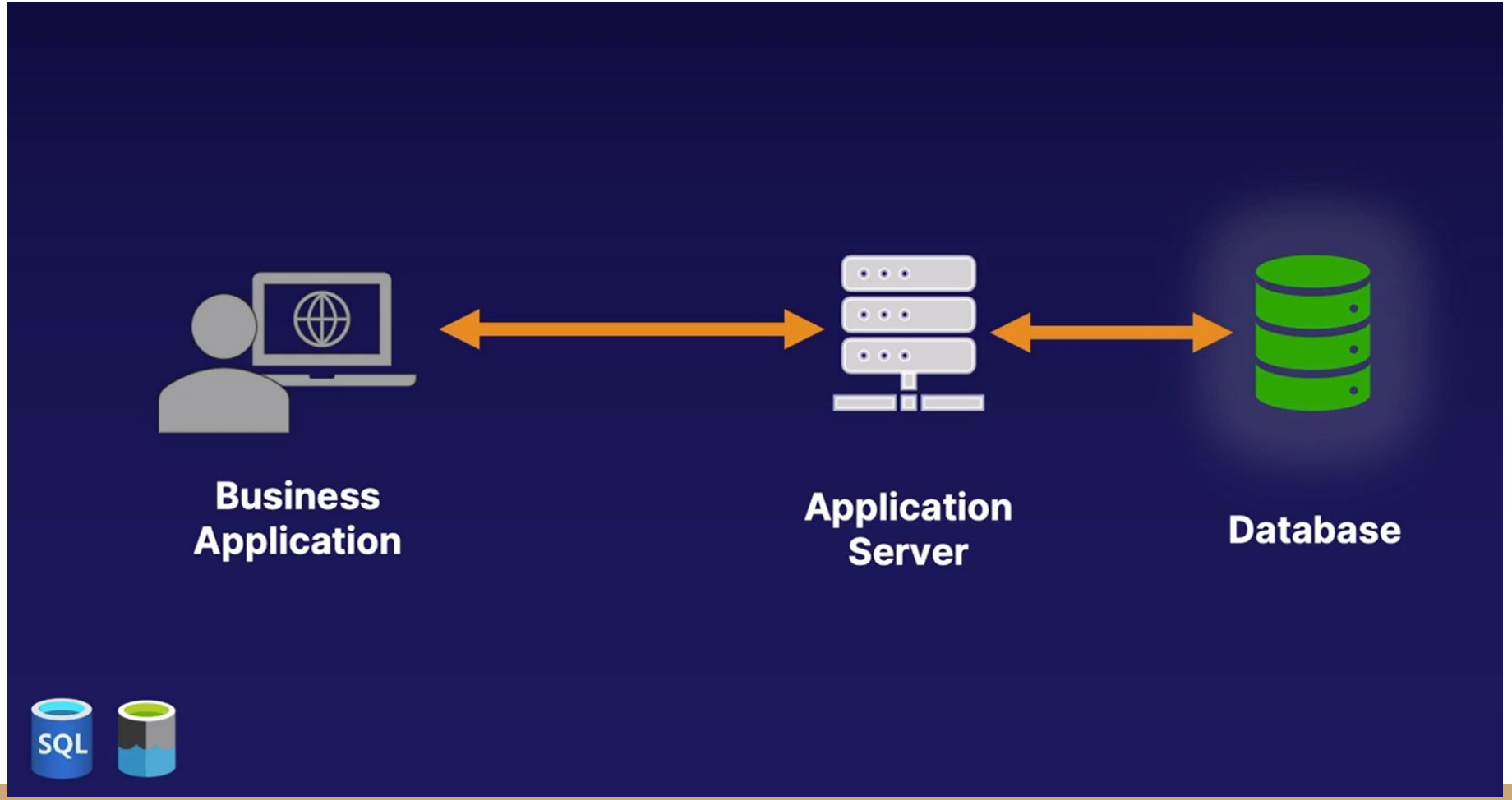
Semi-Structured (NoSQL)

- Azure Cosmos DB
- Data Lake

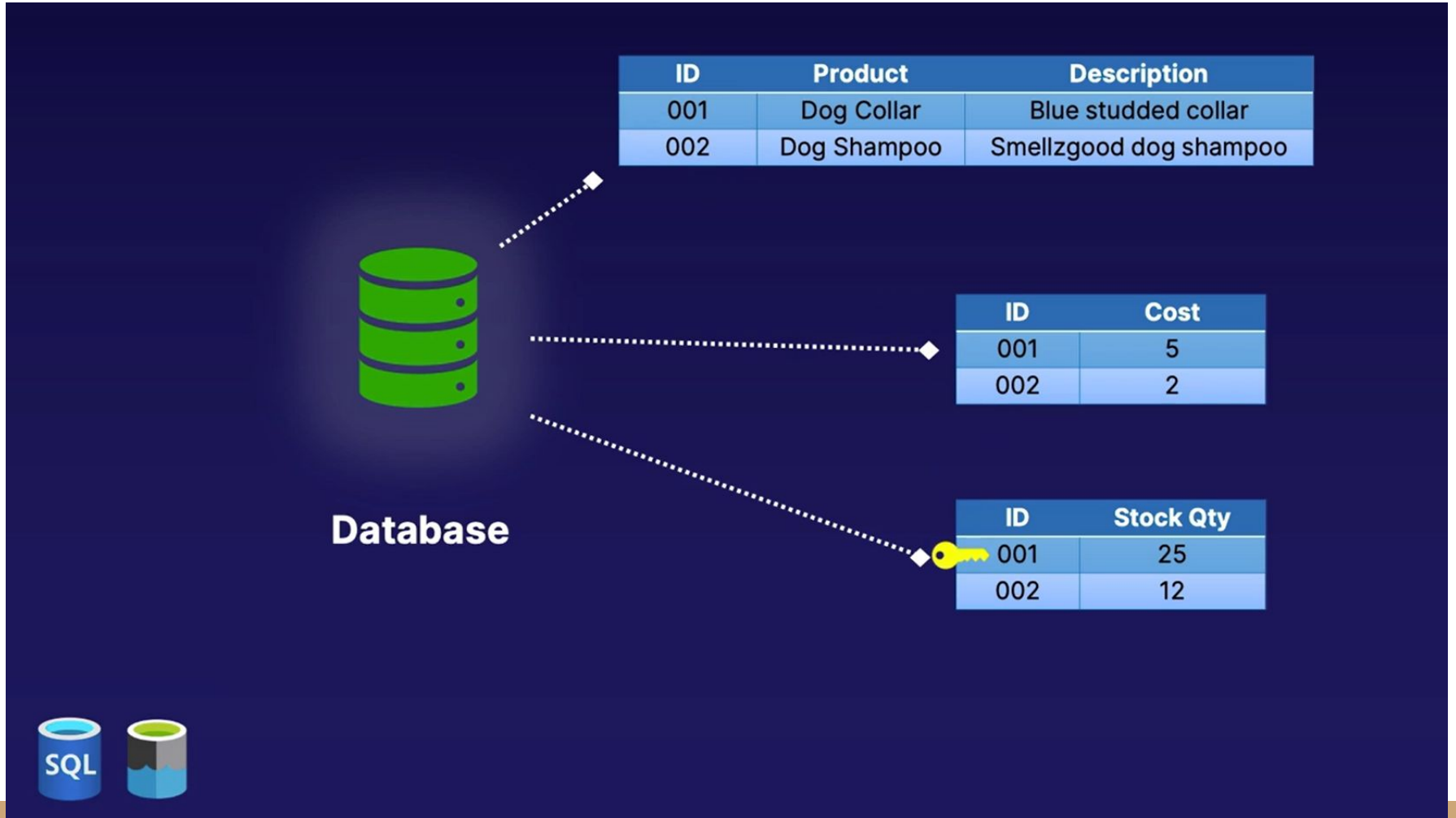
Unstructured

- Table storage
- Blob storage
- File storage

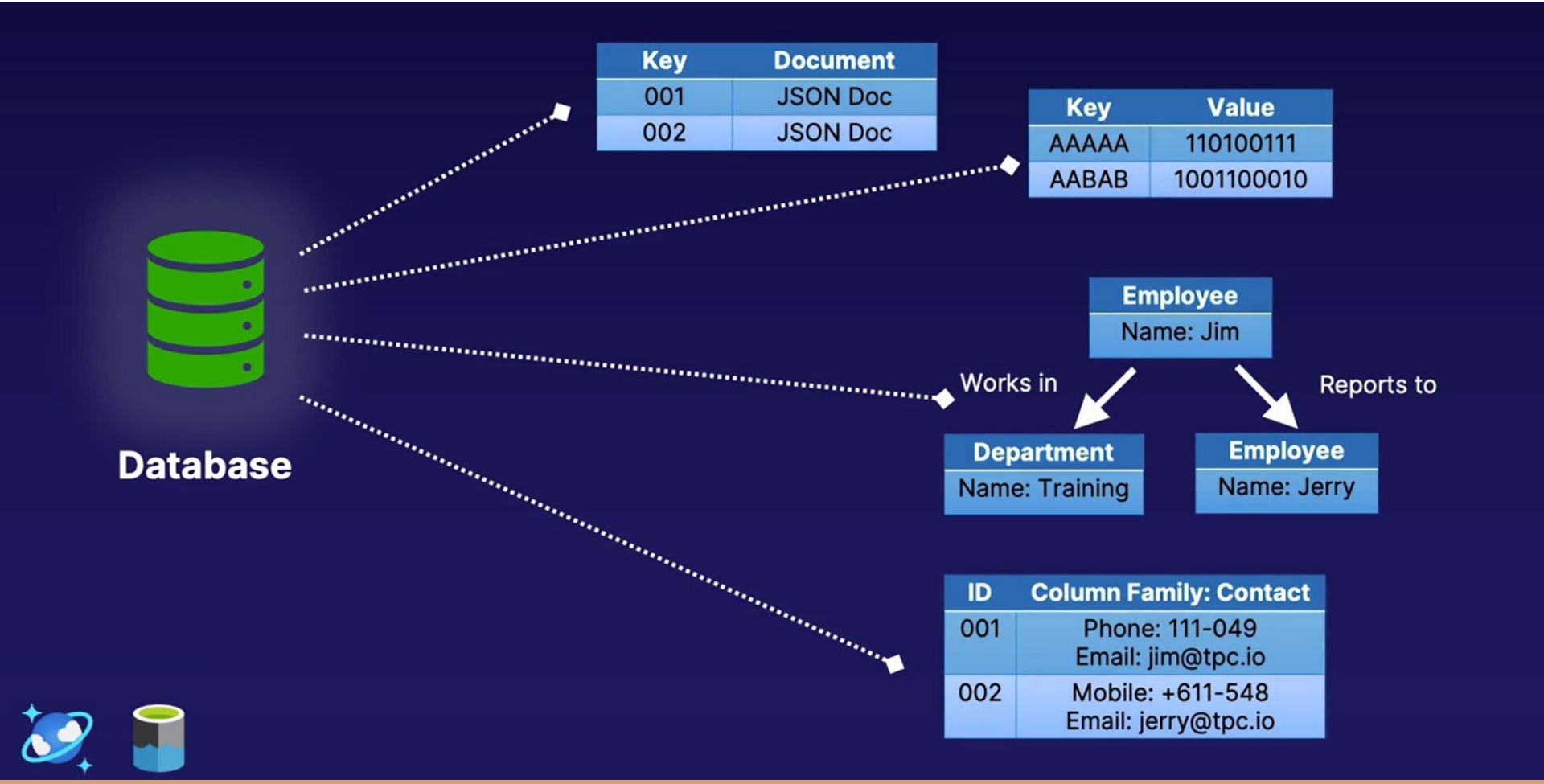
Structured Data: Relational Database



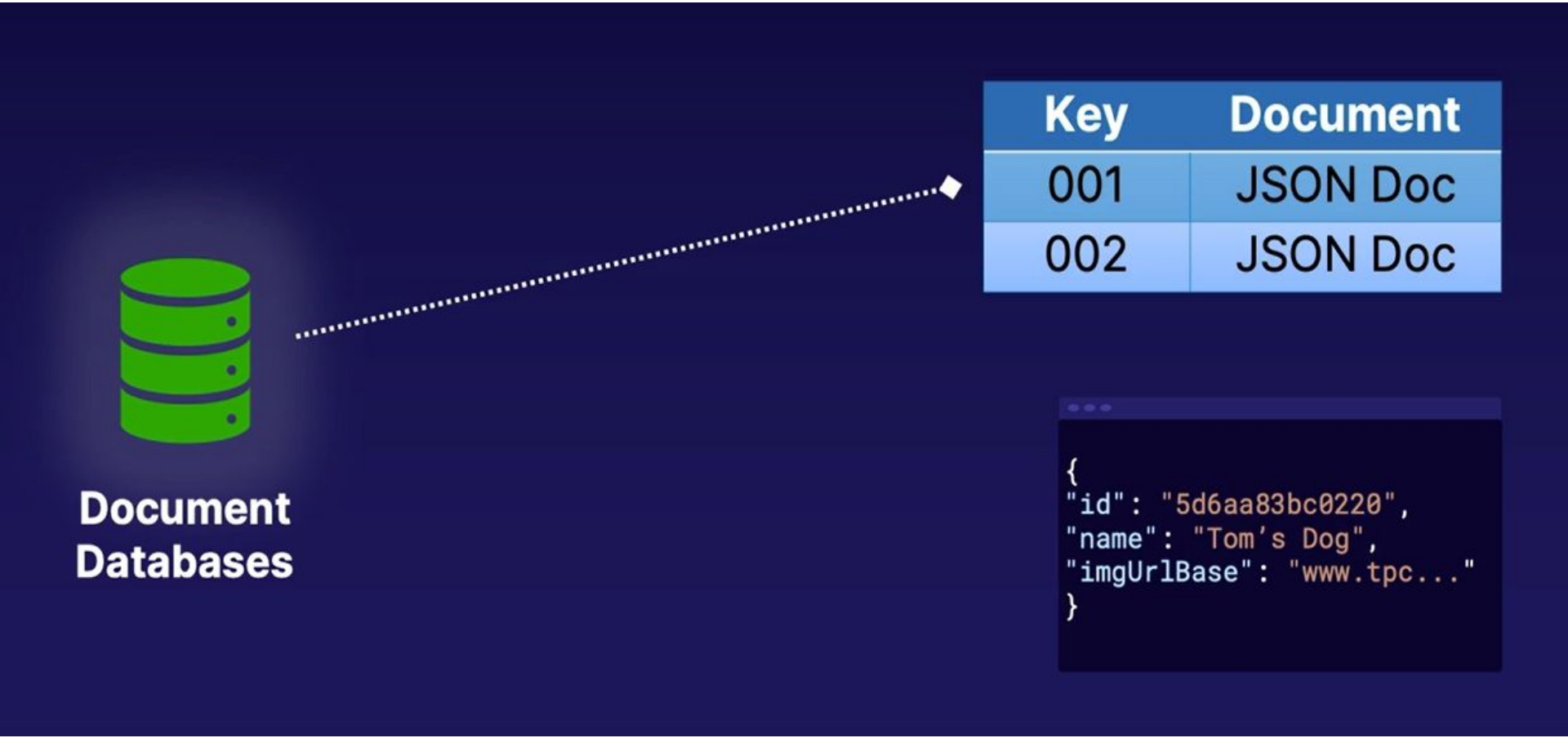
Structured Data: Relational Database



Non-Relational Data Models



Non-Relational Data Models



Non-Relational Data Models

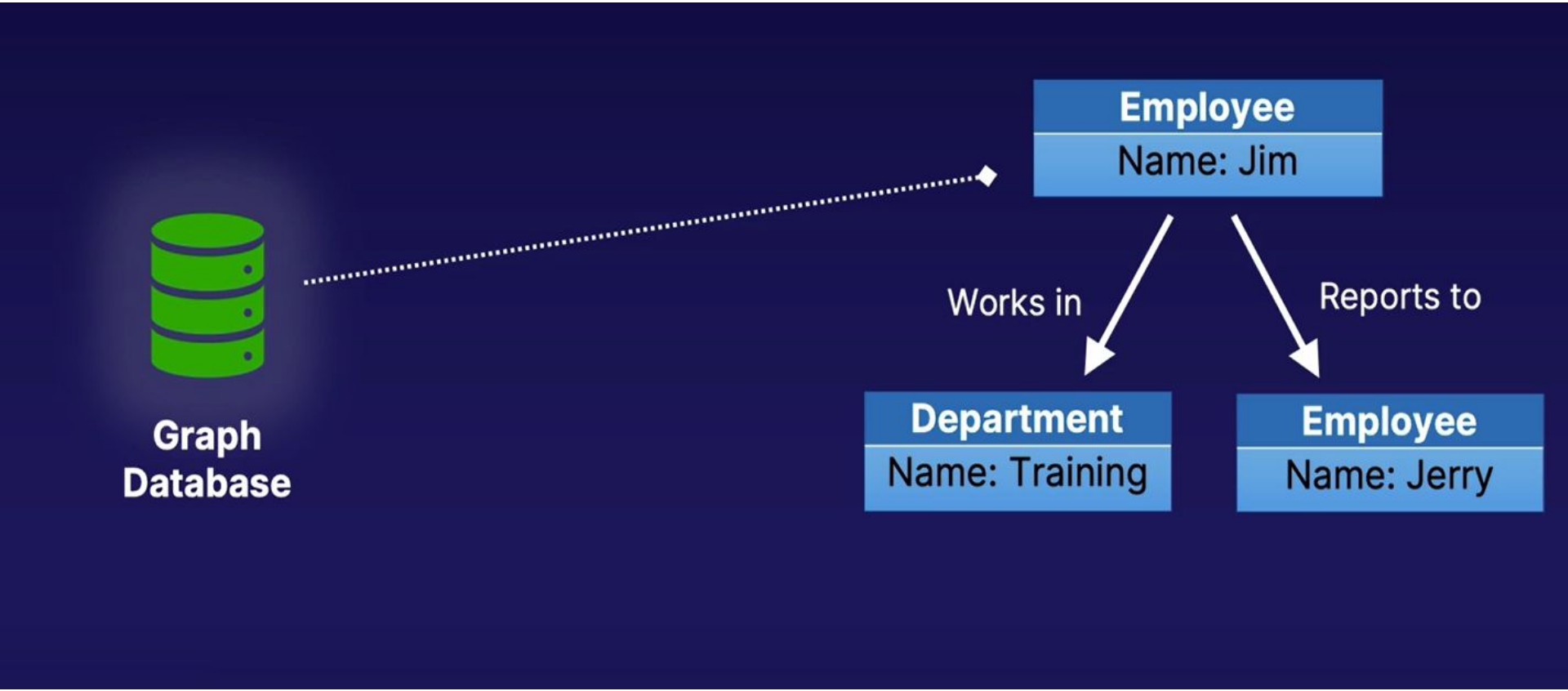
Key Value Stores

Key	Value
AAAAA	110100111
AABAB	1001100010

Optimized for:

- Simple lookups only
- Lookup by key

Non-Relational Data Models



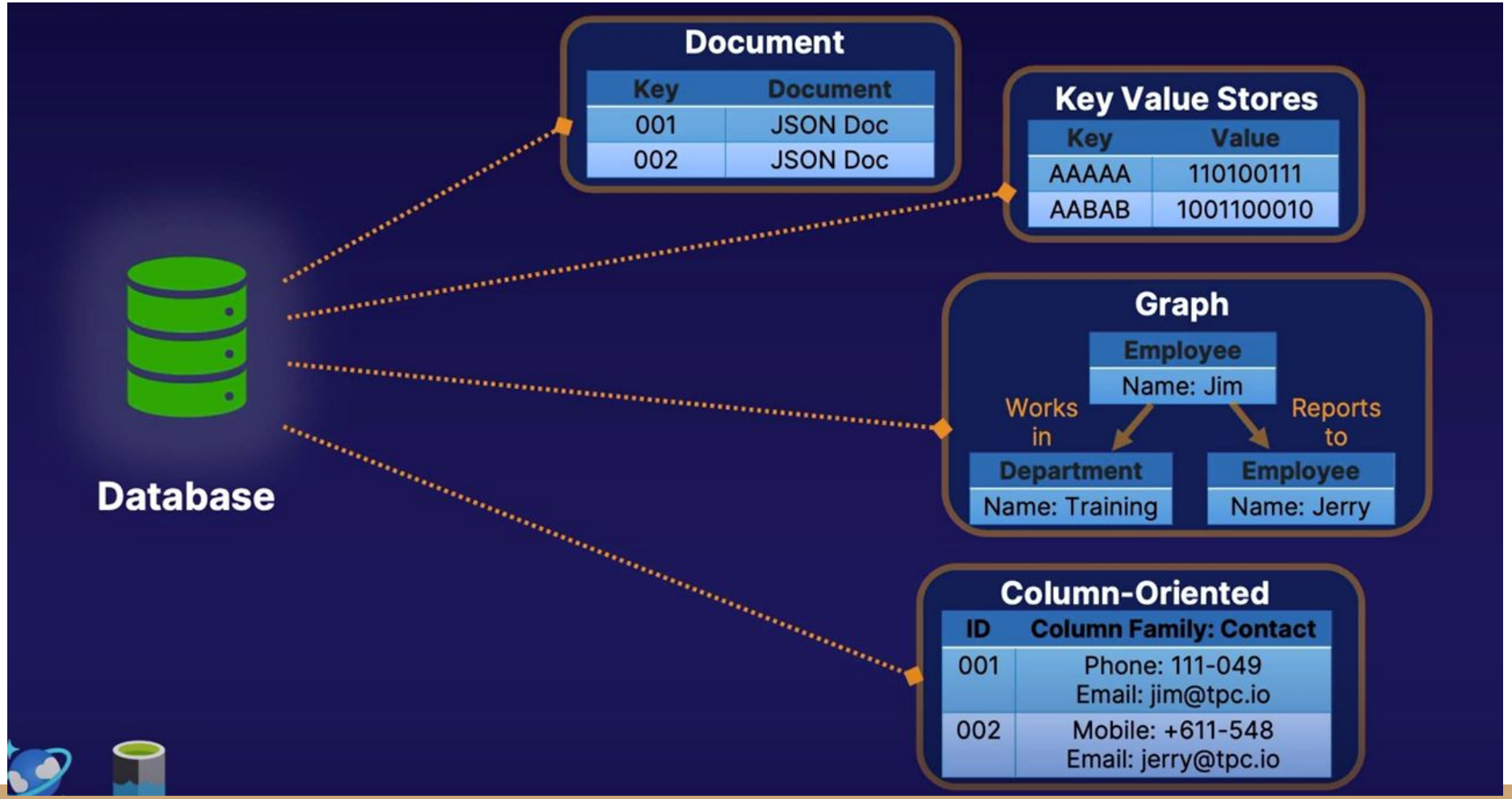
Non-Relational Data Models

Column-Oriented Databases

ID	Column Family: Contact
001	Phone: 111-049 Email: jim@tpc.io
002	Mobile: +611-548 Email: jerry@tpc.io

- Arranged by columns and rows
- Rows contain families of data

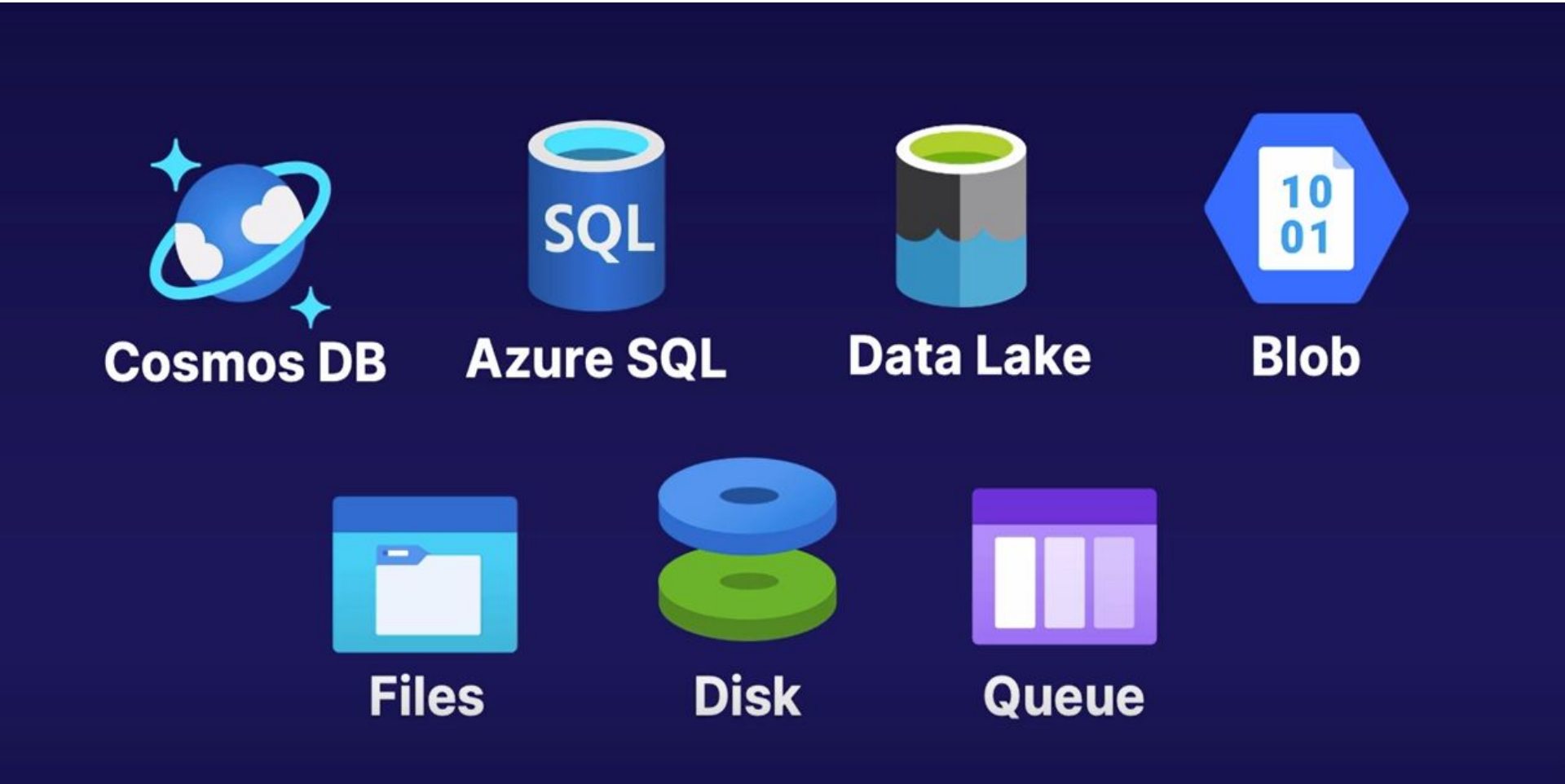
Non-Relational Data Models



Summary


Selecting a Database Platform
Types of Data
• Structured, Semi-Structured, Unstructured
Relational Databases
Non-relational Data Models
• Document, Key Value Stores, Graph, Column-Oriented

Azure Data Storage Solutions - Type of Storage



Types of Storage

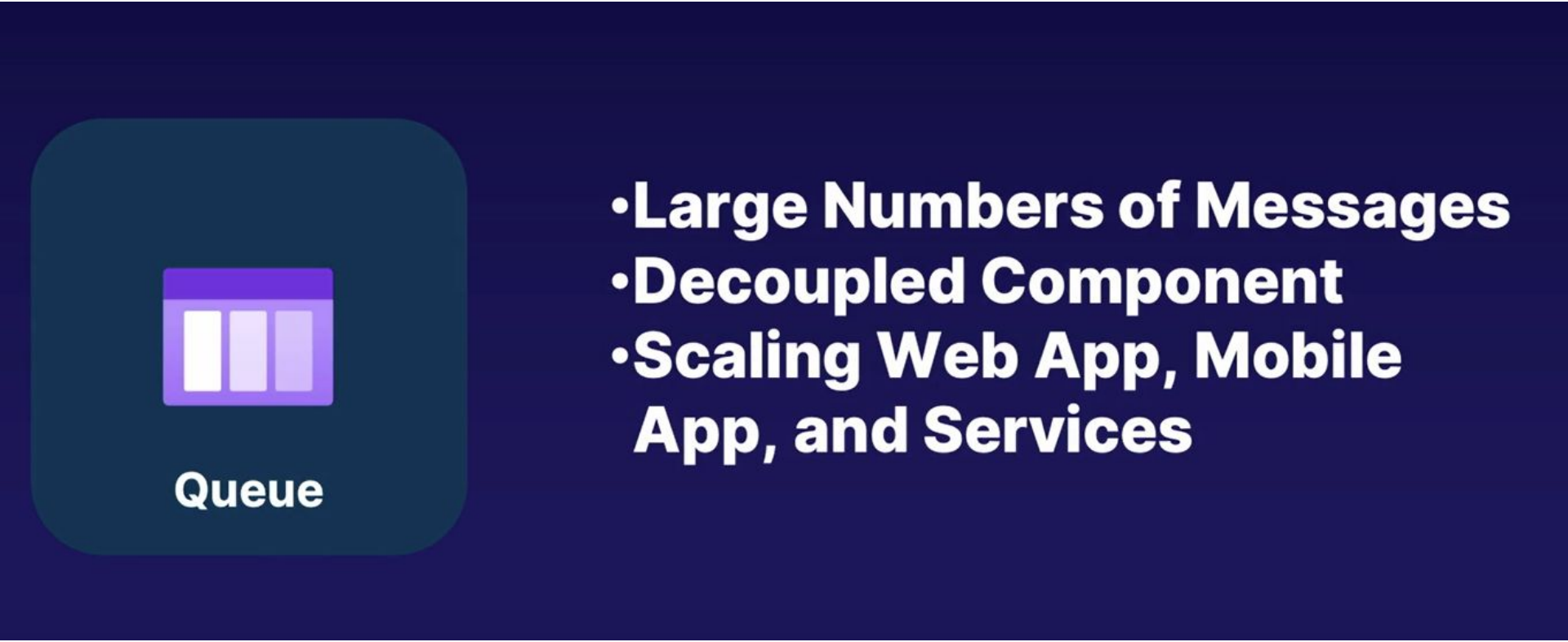
Types of Storage

- Structured + Unstructured
- Object Storage + Big Data
- Analysis

Types of Storage

- Unstructured
- Highly Scalable

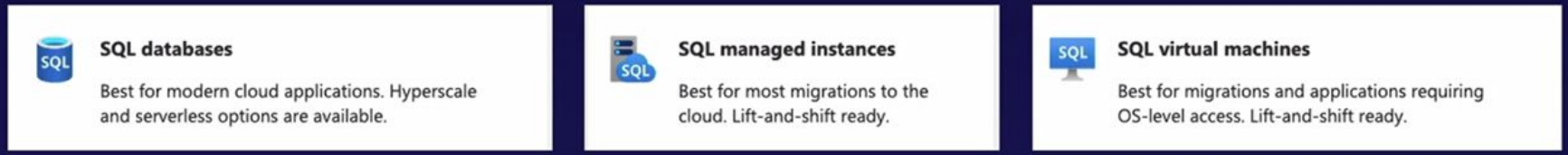
Types of Storage



Types of Storage

Database Service Tier Sizing

First Time Replication Provisioning



SaaS Solution

- Single database, elastic pool, database server

PaaS Solution

- Single instance

IaaS Solution

- Select image of SQL and Windows/Linux Server versions

SQL Virtual Machines

Basics | Disks | Networking | Management | Advanced | SQL Server settings | Tags | Review + create

SQL virtual machines

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Select a VM size

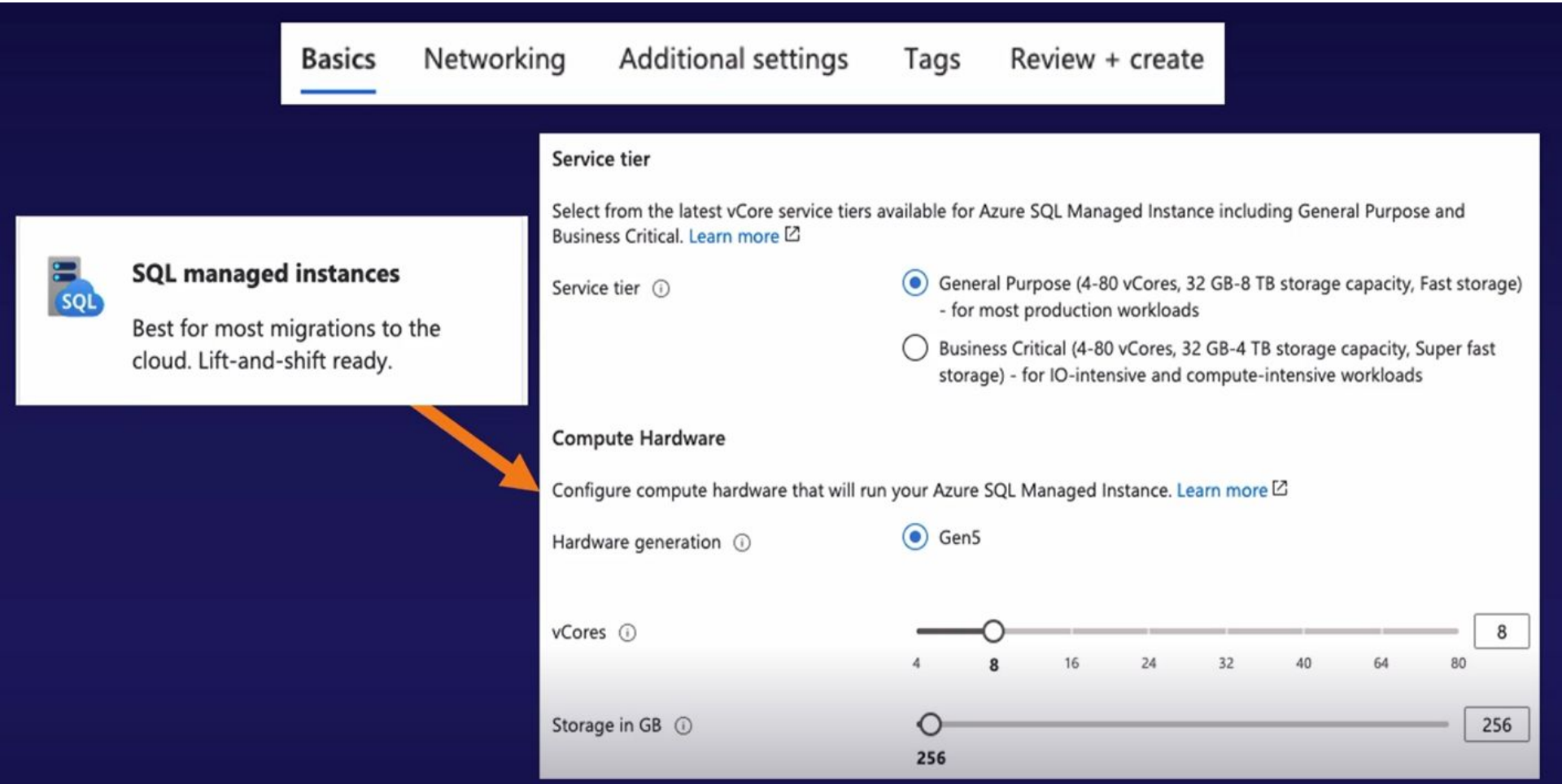
Search by VM size... | Display cost : **Monthly** | vCPUs : **All** | RAM (GiB) : **All** | Add filter

Most used sizes by Azure users

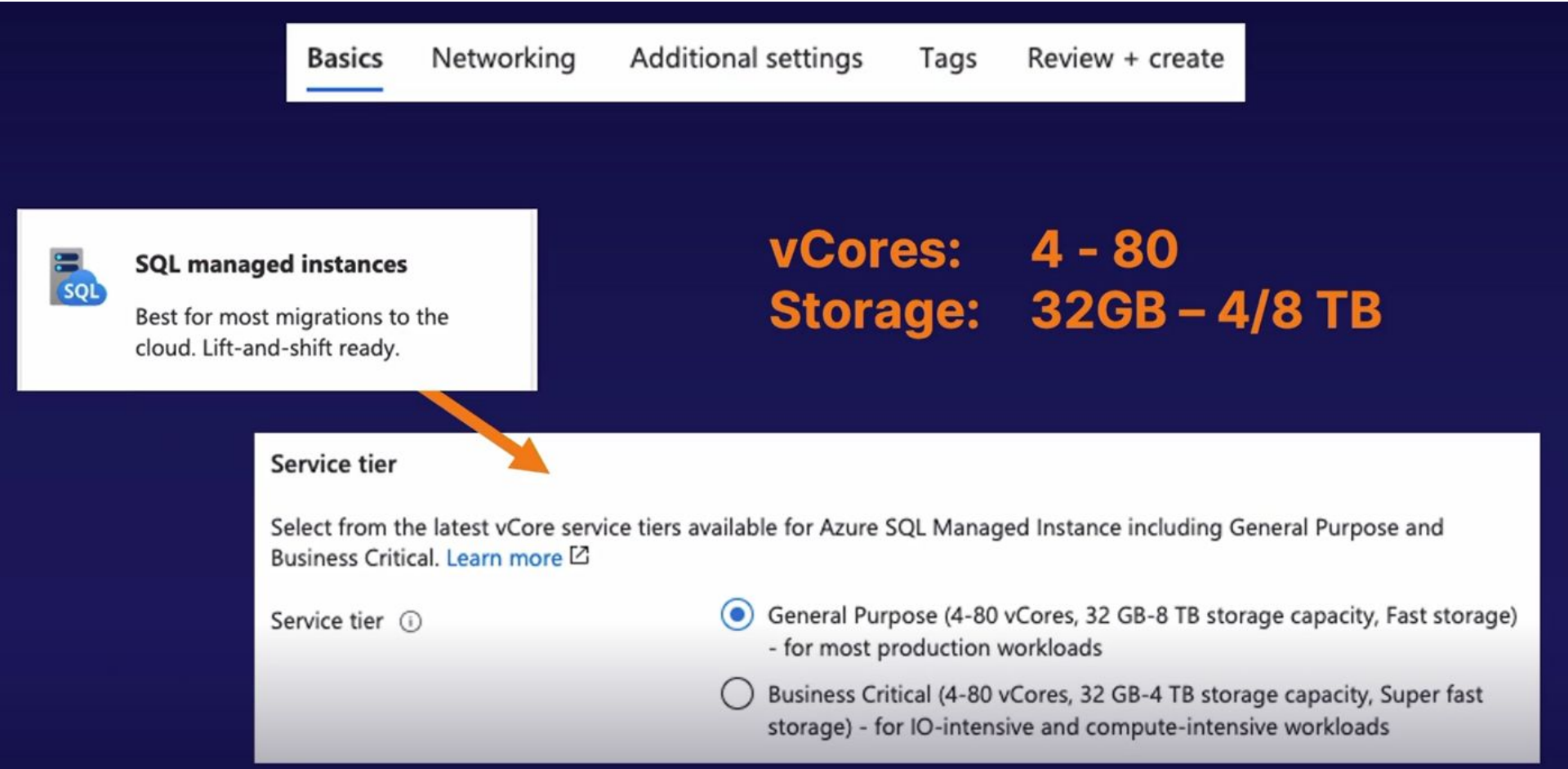
Showing 363 VM sizes. | Subscription: Visual Studio Enterprise | Region: South Central US | Current size: Standard_D2_v2 | Ima 201

VM Size	Family	vCPUs	RAM (GiB)	Data disks	Max IOPS
Most used by Azure users		**The most used sizes by users in Azure**			
DS1_v2	General purpose	1	3.5	4	3200
D2s_v3	General purpose	2	8	4	3200
B2s	General purpose	2	4	4	1280
B1s	General purpose	1	1	2	320
B2ms	General purpose	2	8	4	1920
B1ms	General purpose	1	2	2	640
DS2_v2	General purpose	2	7	8	6400
B4ms	General purpose	4	16	8	2880
D4s_v3	General purpose	4	16	8	6400

Azure SQL Managed Instances



Azure SQL Managed Instances



SQL Databases - Single Database

Basics | Networking | Additional settings | Tags | Review + create

SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.

Basic	Standard	Premium
For less demanding workloads	For workloads with typical performance requirements	For IO-intensive workloads.
General Purpose	**Hyperscale**	**Business Critical**
Scalable compute and storage options	On-demand scalable storage	High transaction rate and high resiliency
500 - 20,000 IOPS 2-10 ms latency	500 - 204,800 IOPS 1-10 ms latency	5,000 - 204,800 IOPS 1-2 ms latency

SQL Databases - Single Database Sizing Models

DTU
(Database Transaction Unit)

Bundled compute, storage, and I/O

Simple, preconfigured resource options

vs.

vCore

Choose compute and storage resources

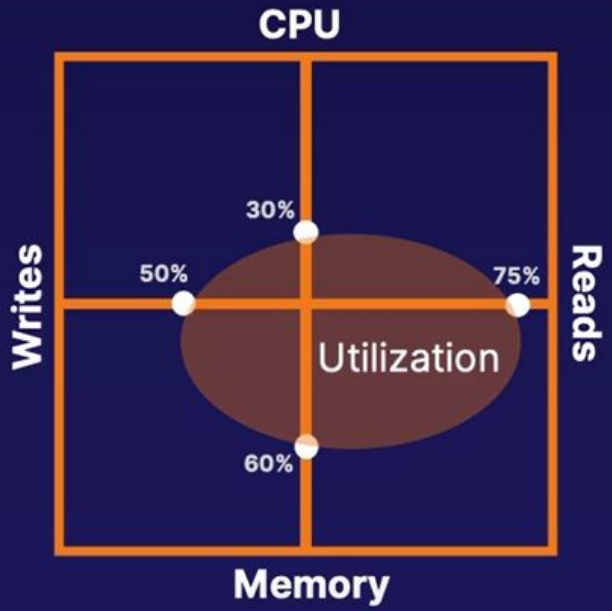
Flexibility, control, and transparency

What is a DTU?

Database Transaction Unit

Bundled compute, storage, and I/O

- Represents resources assigned to the database
- CPU, memory, and read-write rates
- Compare the power across performance levels
- Simplifies talking about performance



SQL Databases - Single Database Sizing Models

DTU Model vs. vCore Model

DTU Model

1. **Basic**
   Less demanding workloads
2. **Standard**
   Typical performance requirements
3. **Premium**
   I/O-intensive workloads

vCore Model

1. **General Purpose**
   Scalable compute and storage options
2. **Hyperscale**
   On-demand scalable storage
3. **Business Critical**
   High transaction rate and high resiliency

SQL Databases - Single Database Sizing Models

DTU Model

1 Basic

DTU	5
Data Max Size	100 MB – 2 GB

2 Standard

DTU	10 - 3000
Data Max Size	100 MB – 250 GB

3 Premium

DTU	125 - 4000
Data Max Size	100 MB – 1 TB

SQL Databases - Single Database Sizing Models

vCore Model

1 General Purpose

IOPS	500 – 20,000
Latency	2 – 10 ms
vCores	2 - 80
Data Max Size	1 GB – 4 TB
Replicas	1 Read-Write

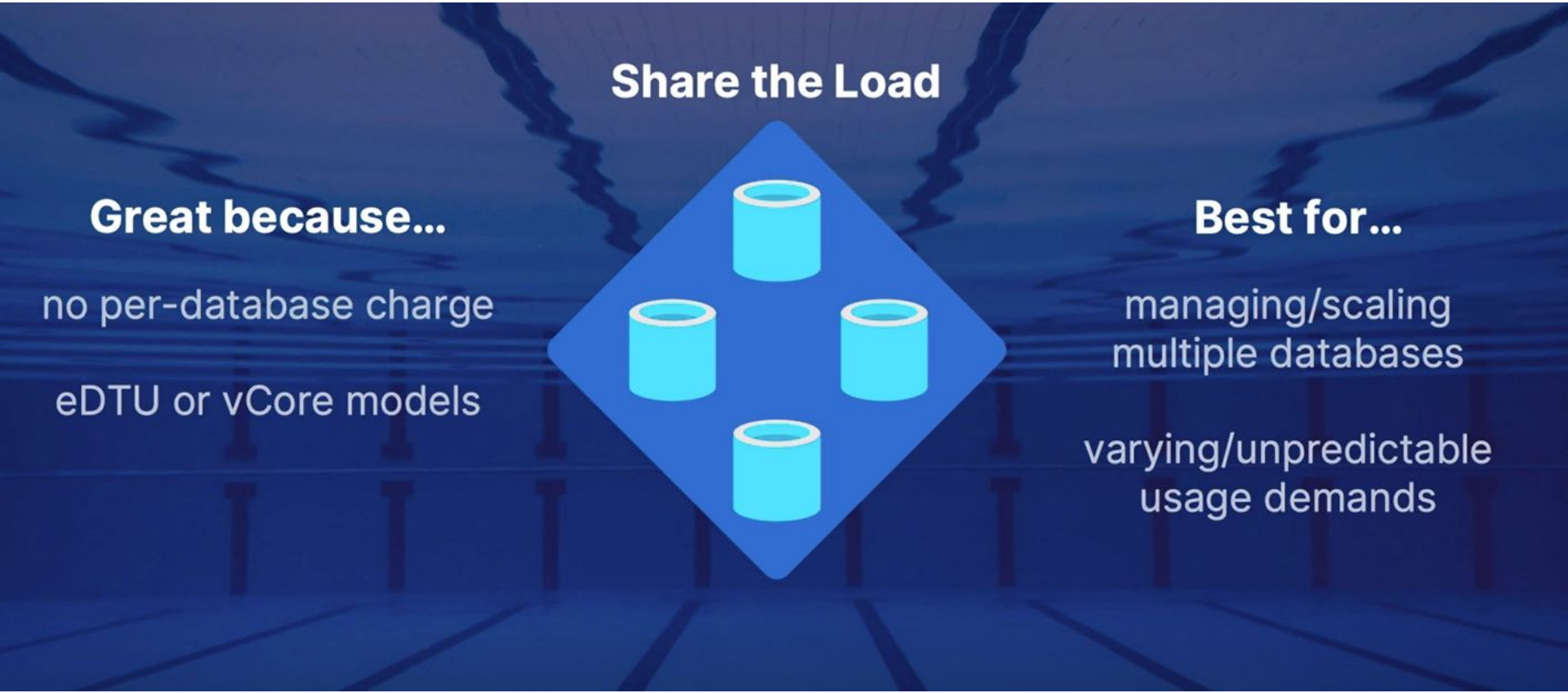
2 Hyperscale

IOPS	500 – 204,800
Latency	1 – 10 ms
vCores	2 - 80
Data Max Size	100 TB
Replicas	1 Read-Write 0 – 4 Read-Scale

3 Business Critical

IOPS	5,000 – 204,800
Latency	1 – 2 ms
vCores	2 - 80
Data Max Size	1 GB – 4 TB
Replicas	3 Read-Write 1 Read-Scale

SQL Databases - Elastic Pools



SQL Databases - Elastic Pool Sizing Models

eDTU Model

1 Basic

Pool	50 - 1600
Database	0 - 5
Data Max Size	4.88 – 156.25 GB

2 Standard

Pool	50 - 3000
Database	0 - 10
Data Max Size	50 GB – 4 TB

3 Premium

Pool	125 - 4000
Database	0 - 25
Data Max Size	50 GB – 4 TB

SQL Databases - Elastic Pool Sizing Models

vCore Model

1 General Purpose

IOPS	500 – 20,000
Latency	2 – 10 ms
vCores	2 - 80
Data Max Size	1 GB – 4 TB

2 Hyperscale

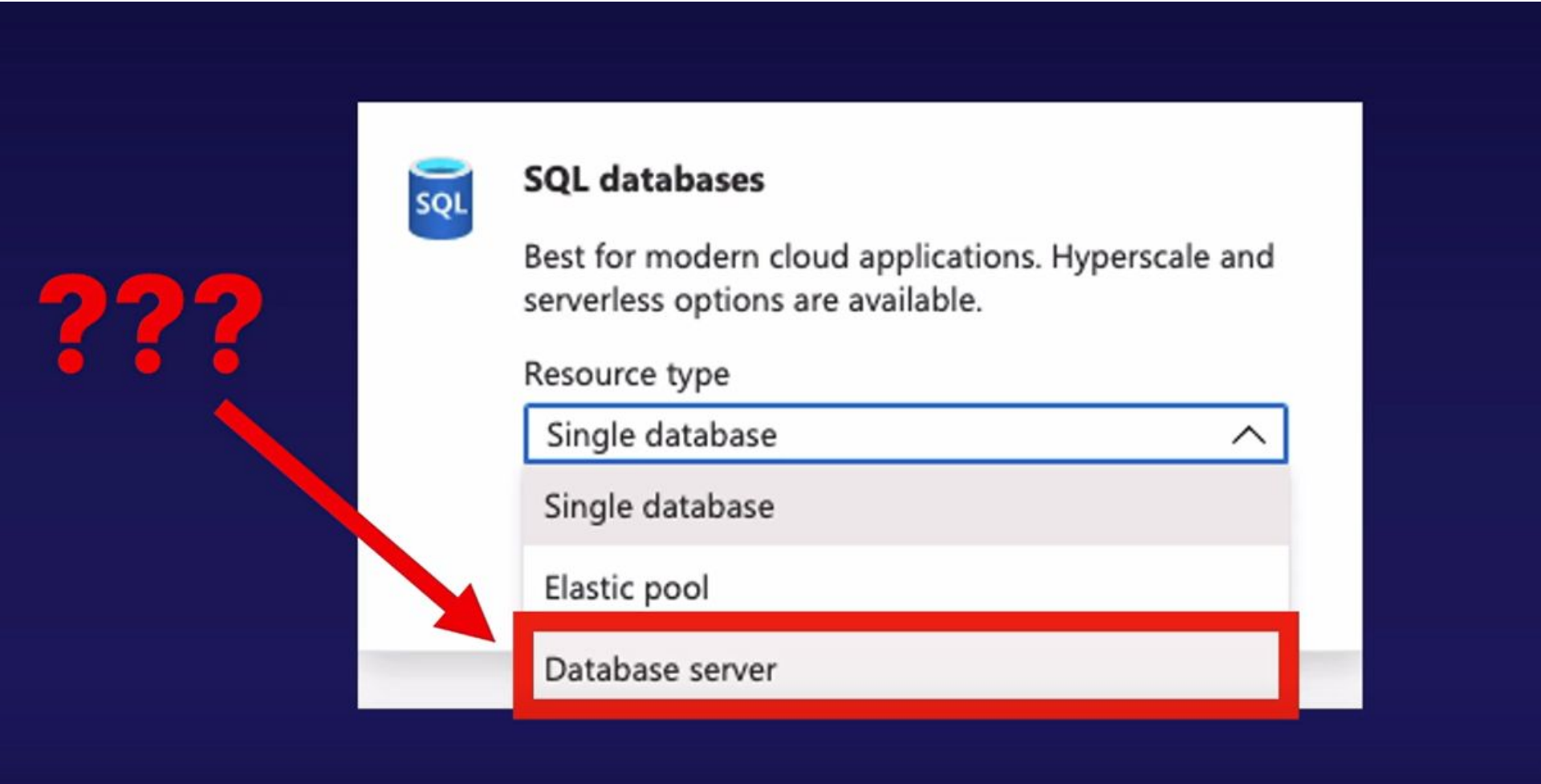
IOPS	500 – 204,800
Latency	1 – 10 ms
vCores	2 - 80
Data Max Size	100 TB

Secondary Replicas	0 - 4

3 Business Critical

IOPS	5,000 – 204,800
Latency	1 – 2 ms
vCores	2 - 80
Data Max Size	1 GB – 4 TB

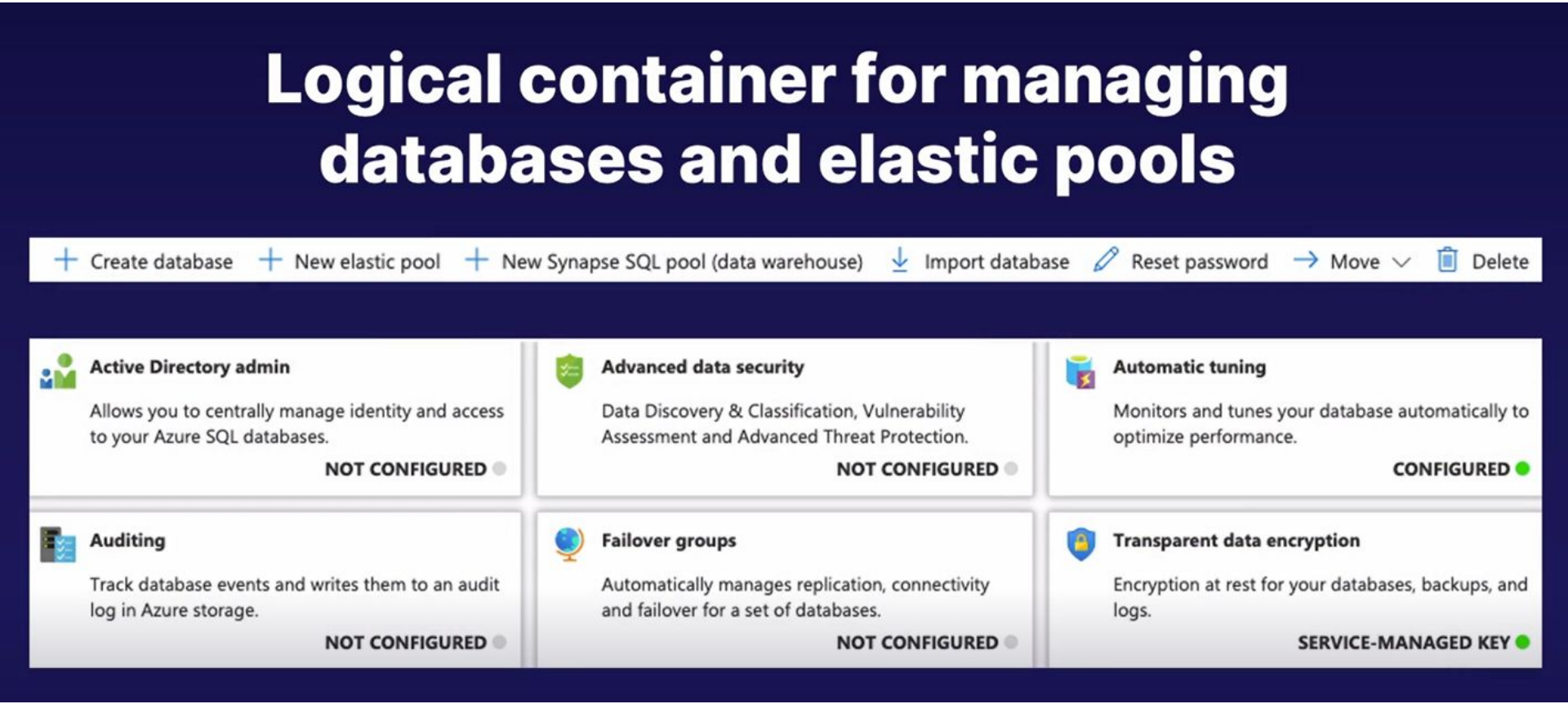
SQL Databases - Database Server



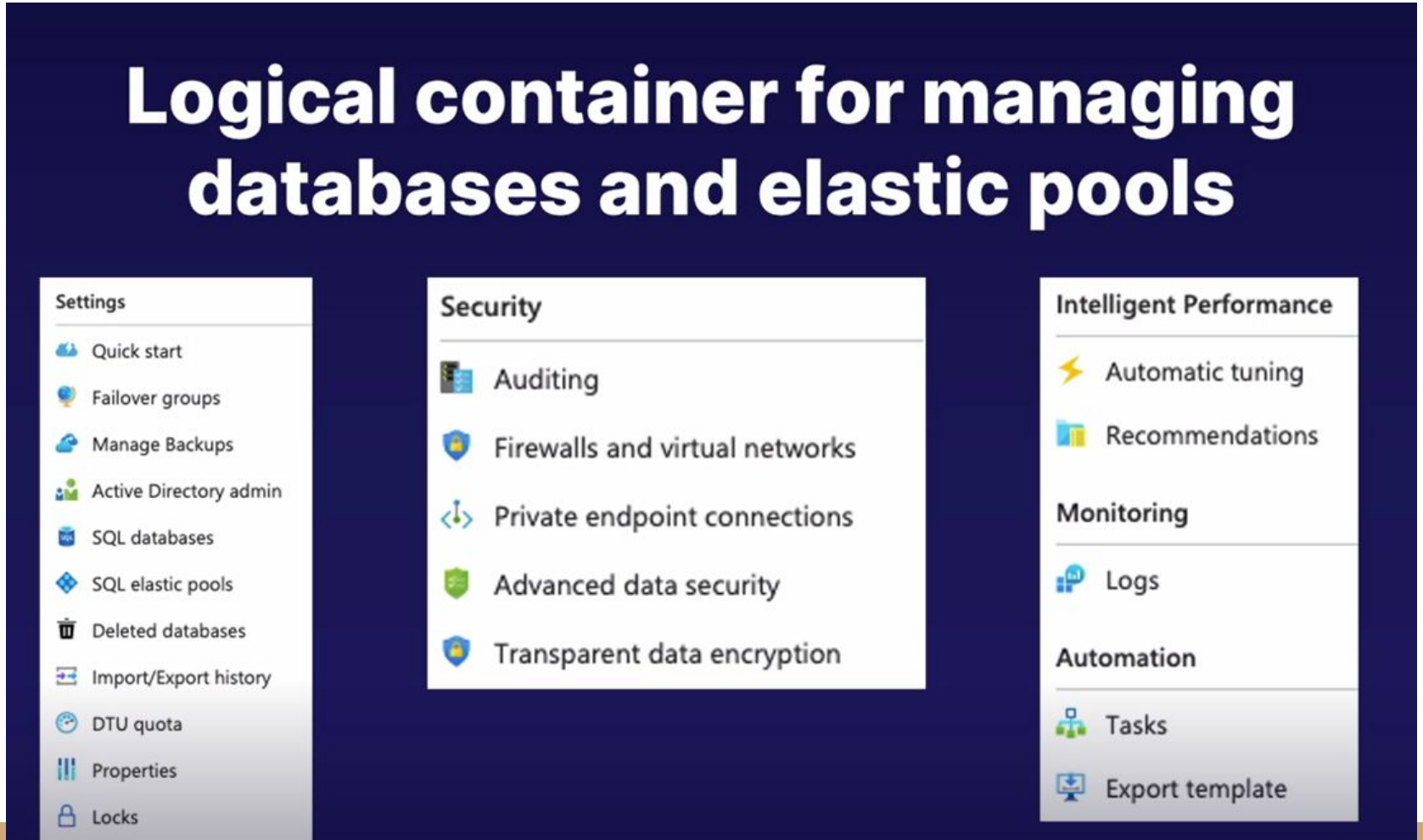
SQL Databases - Database Server

Logical container for managing databases and elastic pools

SQL Databases - Database Server



SQL Databases - Database Server



Database Service Tier Sizing

Dynamically Scale Azure SQL DB and SQL Managed Instances - Types of Scaling

Scaling Up and Down

- Memory
- CPU
- Disk Space

Dynamically Scale Azure SQL DB and SQL Managed Instances - Types of Scaling

Scaling Up

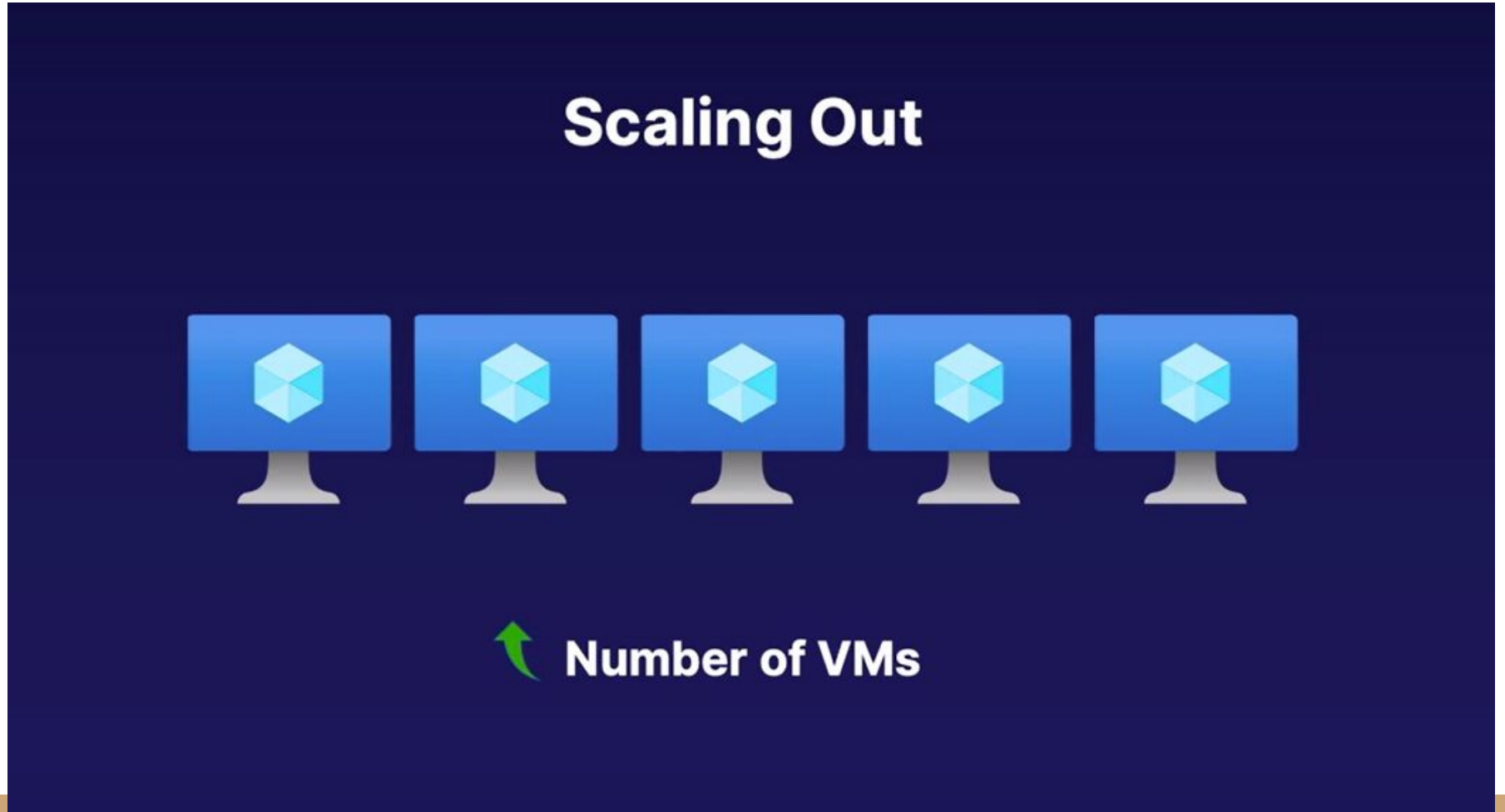
- Memory
- CPU
- Storage

Dynamically Scale Azure SQL DB and SQL Managed Instances - Types of Scaling

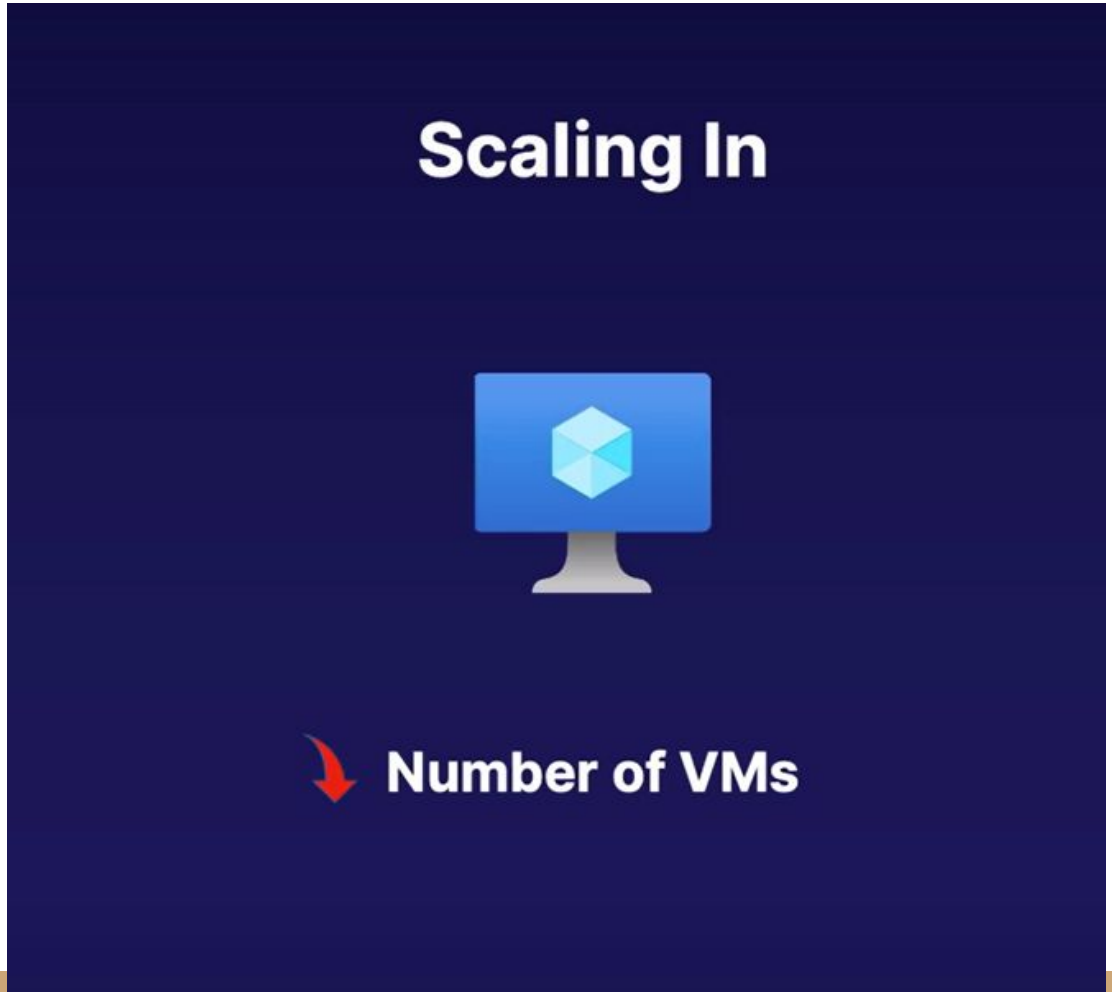
Scaling Down

- Memory
- CPU
- Storage

Dynamically Scale Azure SQL DB and SQL Managed Instances - Types of Scaling



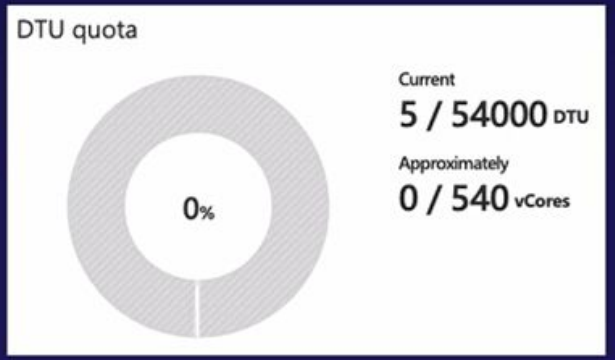
Dynamically Scale Azure SQL DB and SQL Managed Instances - Types of Scaling



Scaling with Azure SQL Database

Scaling (DTU Model)

- DTU
- Data Max Size
- Read Scale Out



Scaling with Azure SQL Database

Basic
For less demanding workloads

Standard
For workloads with typical performance requirements

Premium
For IO-intensive workloads.

DTUs What is a DTU?

125 250 500 1000 1750 4000

125 (P1)

Data max size

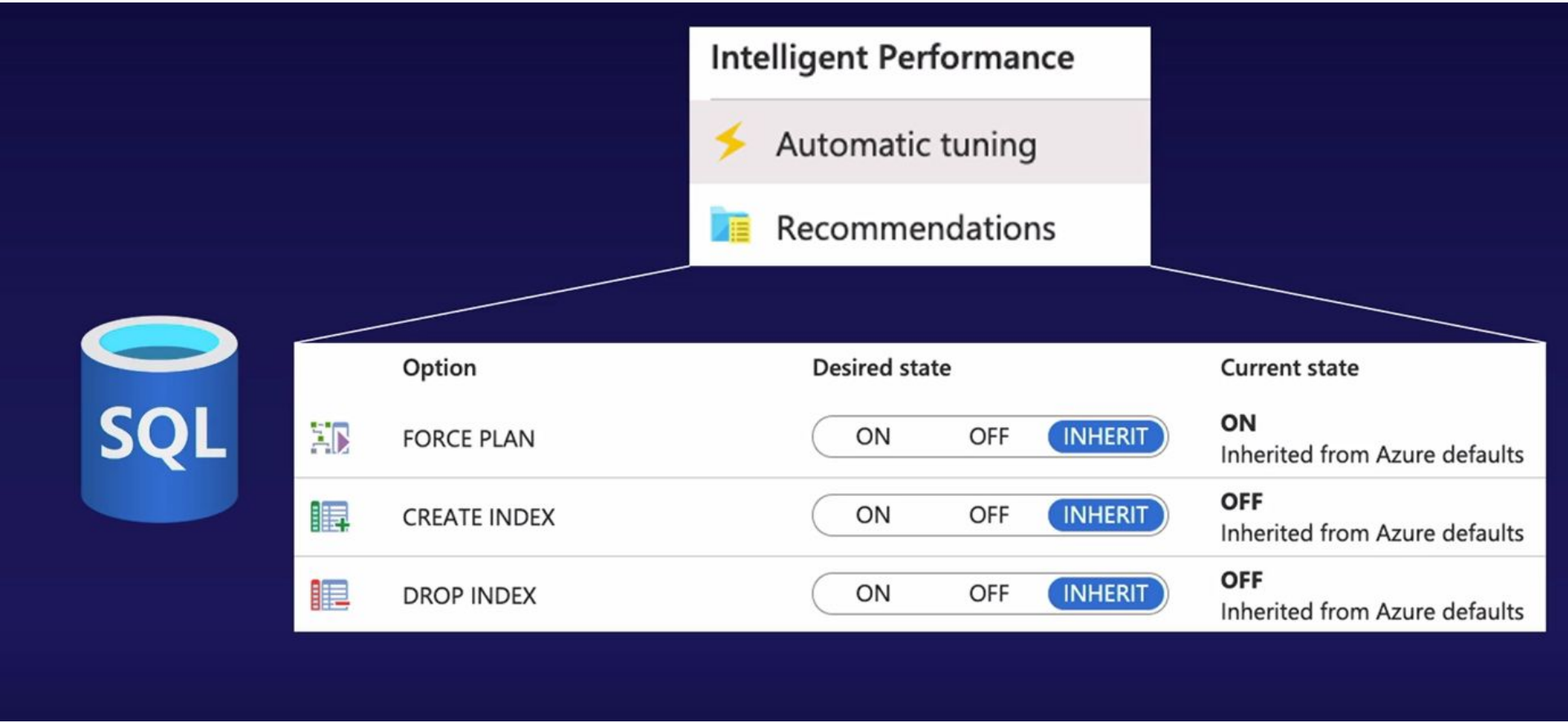
100 MB 1 TB

100 MB

Read scale-out
(•) Enabled ( ) Disabled

Would you like to make this database zone redundant? ⓘ
( ) Yes (•) No

Bonus: Automatic Tuning



Bonus: Automatic Tuning

Tuning Options

1 Create Index

- Identifies indexes that may improve performance
- Creates indexes
- Automatically verifies that performance has improved

2 Drop Index

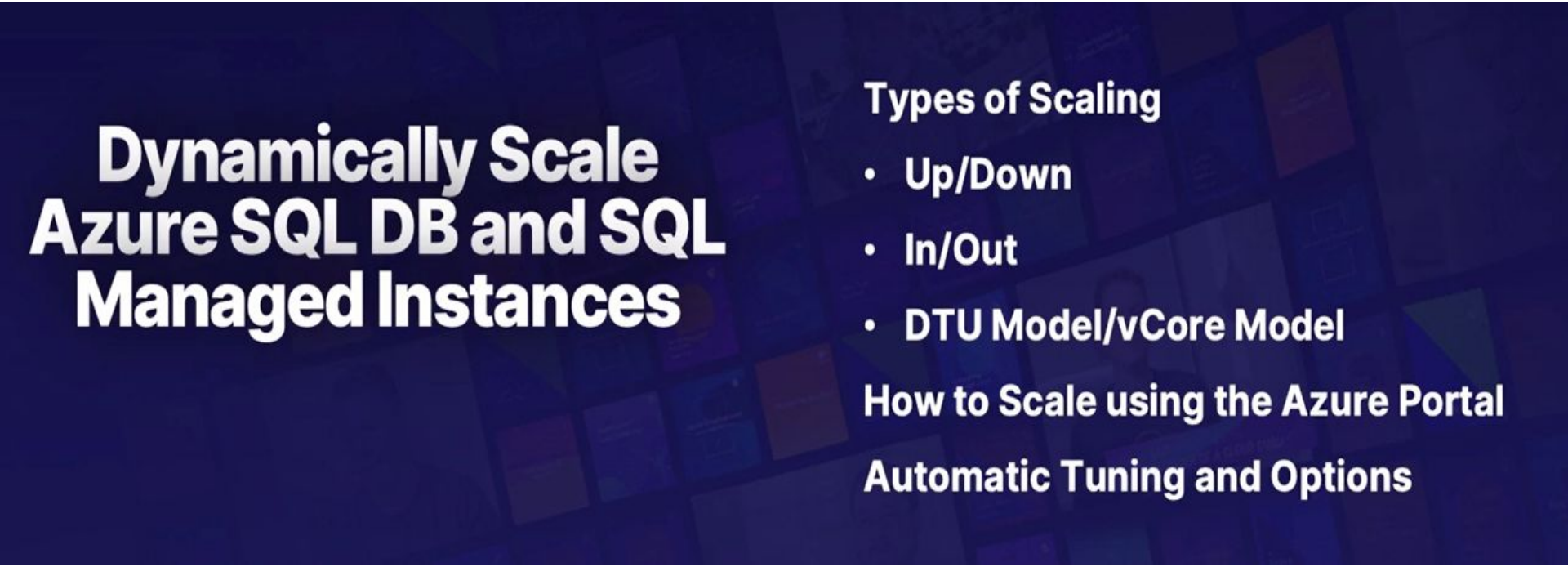
- Identifies redundant and duplicate indexes (without unique indexes)
- Identifies indexes not used for > 90 days

*Not compatible with apps using partition switching and index hints

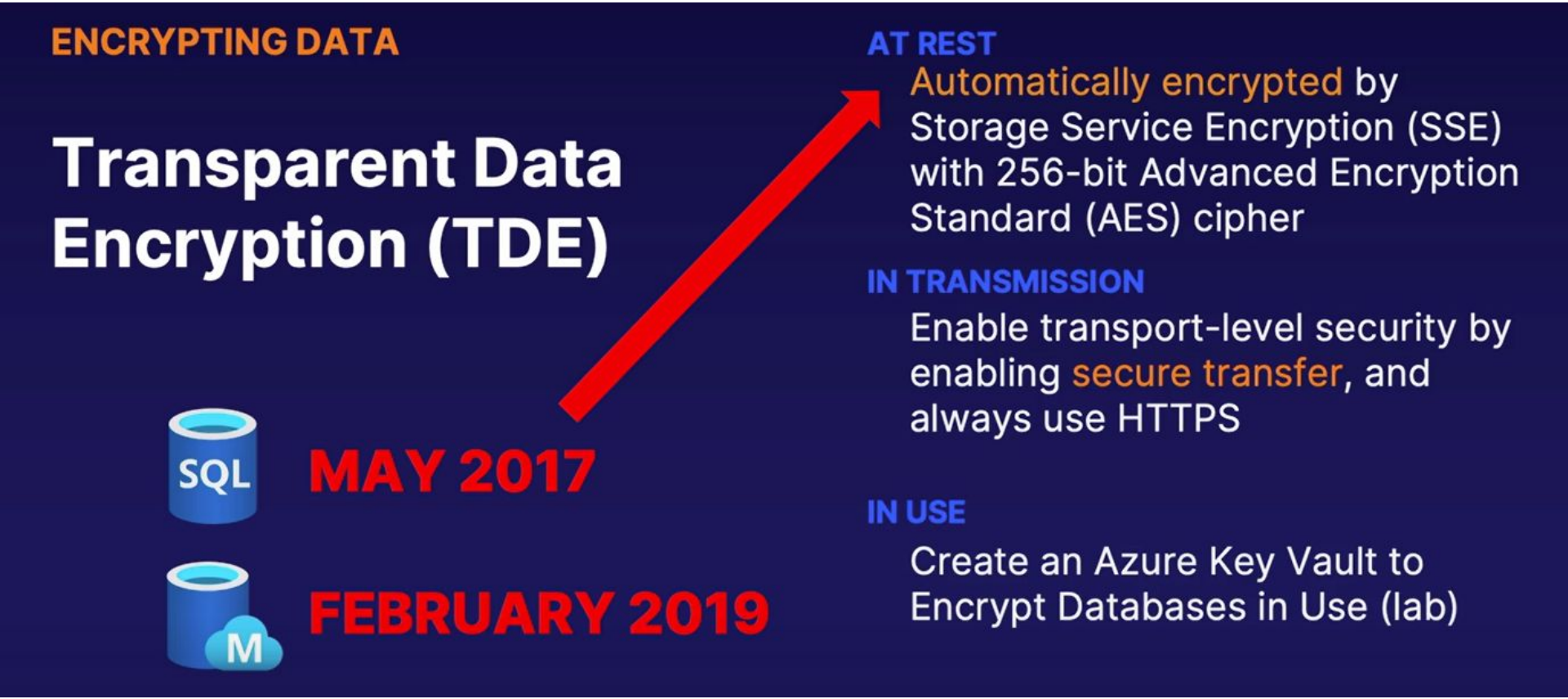
3 Force Last Good Plan

- Identifies queries using execution plan that is slower than the previous good plan
- Queries using the last known good plan instead of regressed plan

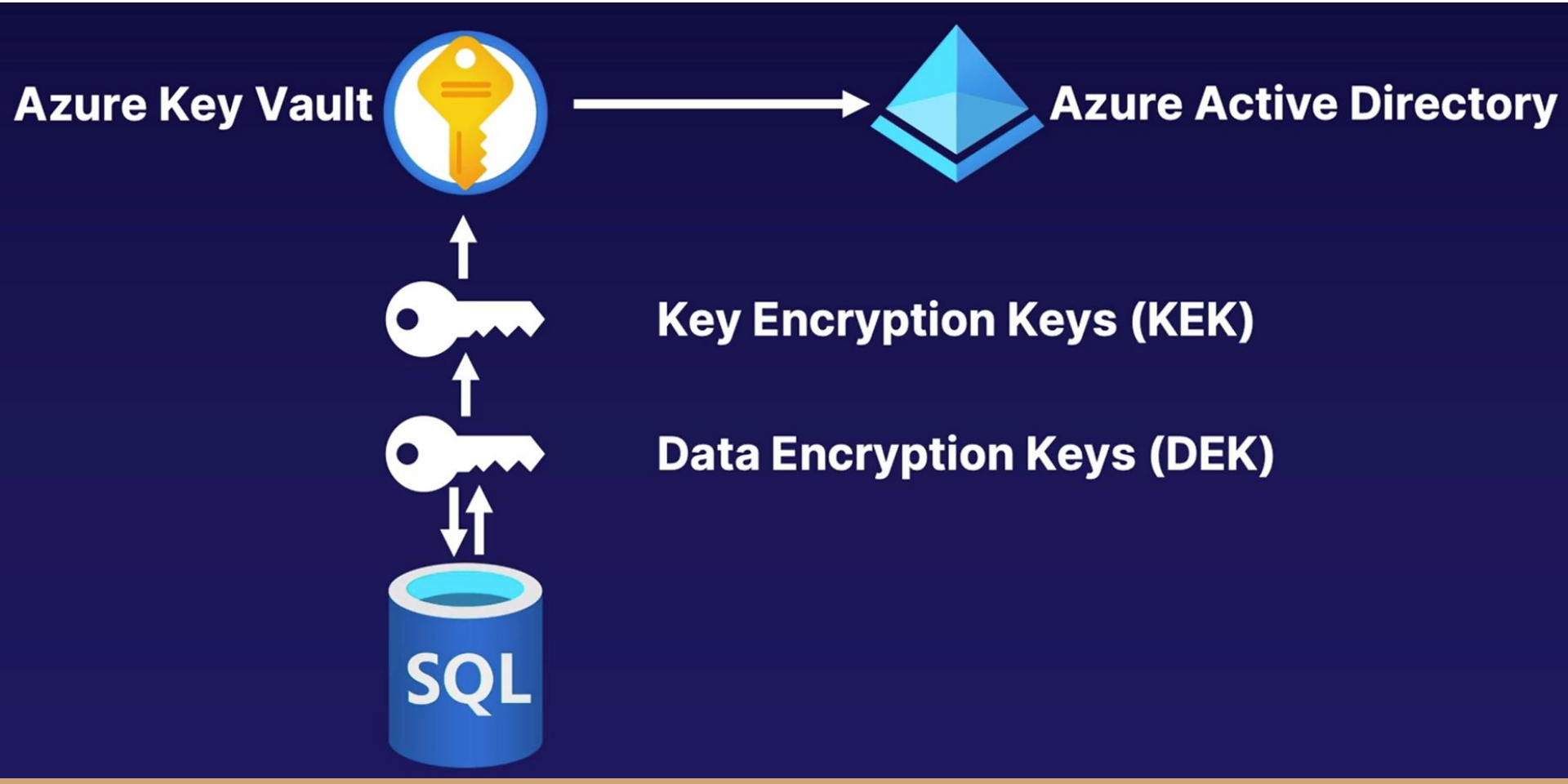
Summary


Dynamically Scale Azure SQL DB and SQL Managed Instances
Types of Scaling
• Up/Down
• In/Out
• DTU Model/vCore Model
How to Scale using the Azure Portal
Automatic Tuning and Options

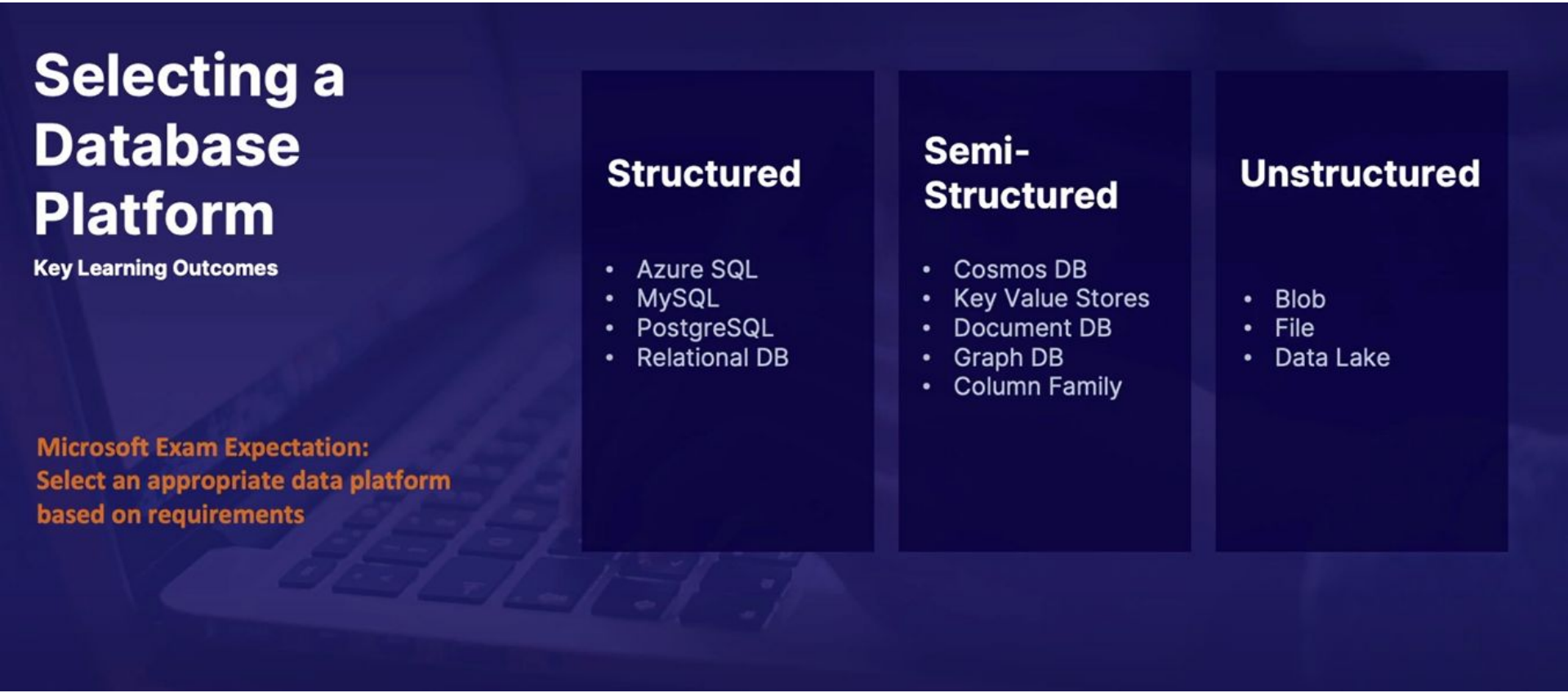
Encrypting Data at Rest, in Transmission, and in Use



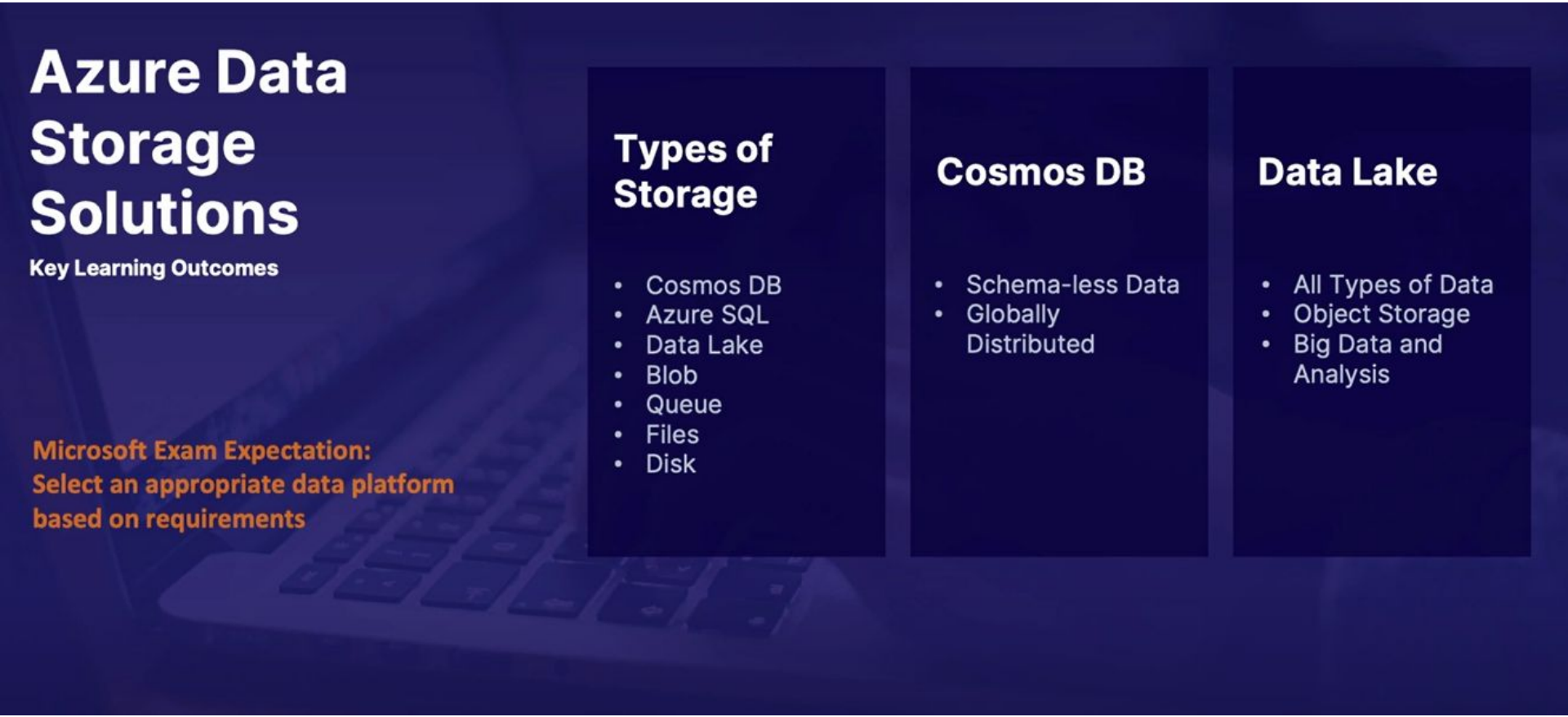
How Azure Key Vault Encrypts SQL



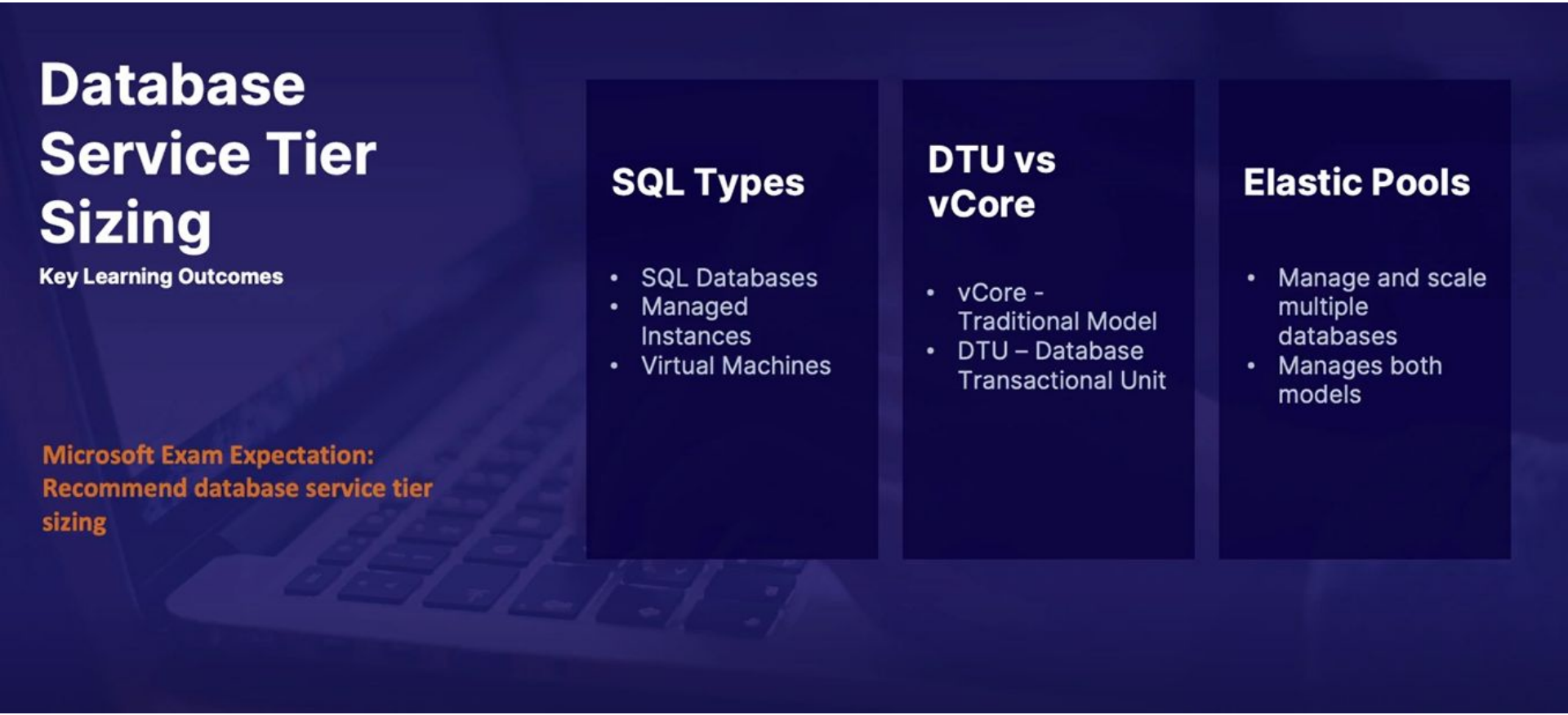
Summary


Selecting a Database Platform
Key Learning Outcomes
Microsoft Exam Expectation:
Select an appropriate data platform based on requirements
Structured
Azure SQL
MySQL
PostgreSQL
Relational DB
Semi-Structured
Cosmos DB
Key Value Stores
Document DB
Graph DB
Column Family
Unstructured
Blob
File
Data Lake

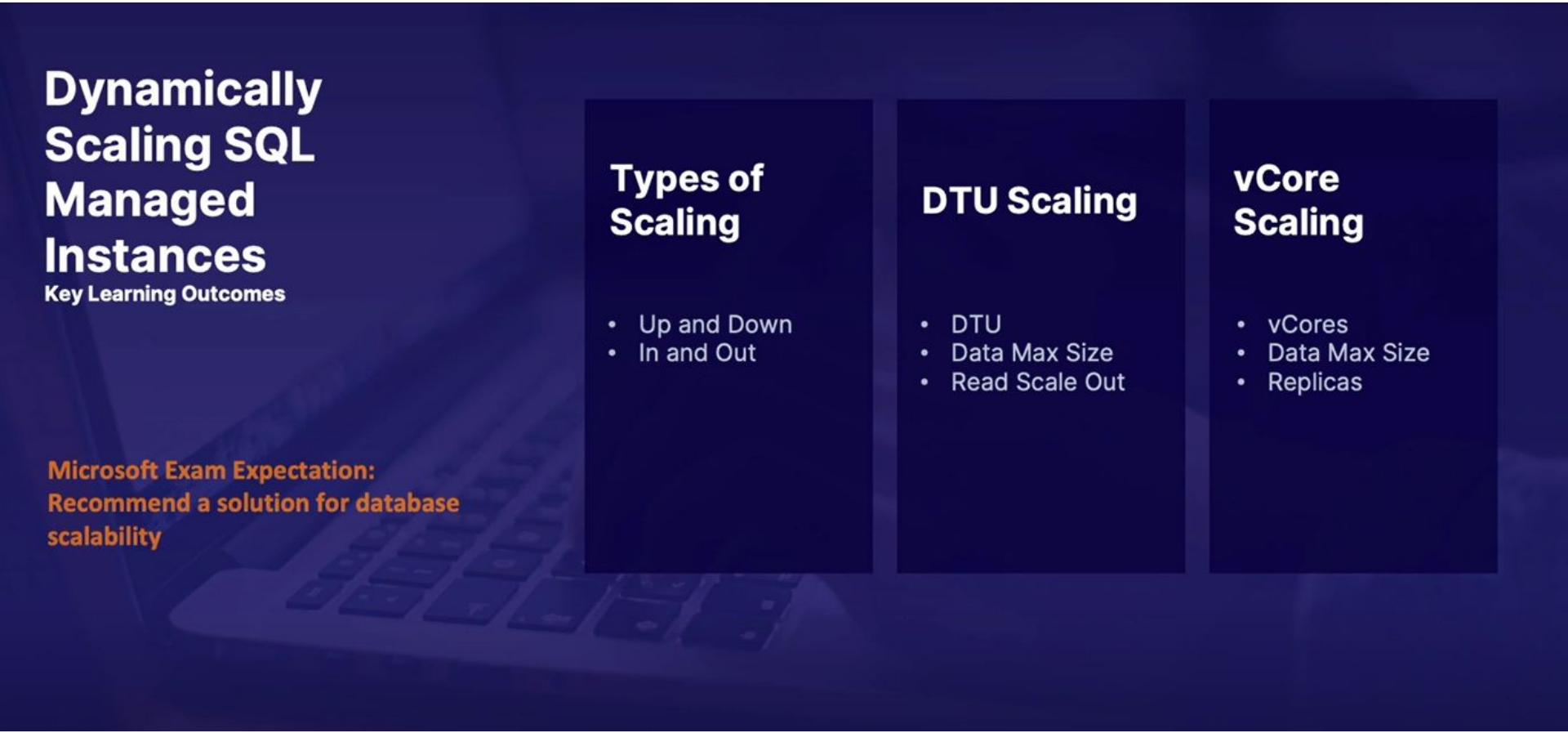
Summary


Azure Data Storage Solutions
Key Learning Outcomes
Microsoft Exam Expectation:
Select an appropriate data platform based on requirements
Types of Storage
Cosmos DB
Azure SQL
Data Lake
Blob
Queue
Files
Disk
Cosmos DB
Schema-less Data
Globally Distributed
Data Lake
All Types of Data
Object Storage
Big Data and Analysis

Summary


Database Service Tier Sizing
Key Learning Outcomes
Microsoft Exam Expectation: Recommend database service tier sizing
SQL Types
SQL Databases
Managed Instances
Virtual Machines
DTU vs vCore
vCore - Traditional Model
DTU – Database Transactional Unit
Elastic Pools
Manage and scale multiple databases
Manages both models

Summary


Dynamically Scaling SQL Managed Instances
Key Learning Outcomes
Microsoft Exam Expectation: Recommend a solution for database scalability
Types of Scaling
• Up and Down
• In and Out
DTU Scaling
• DTU
• Data Max Size
• Read Scale Out
vCore Scaling
• vCores
• Data Max Size
• Replicas

Summary


Encrypting SQL Data
Key Learning Outcomes
Microsoft Exam Expectation: Recommend a solution for encrypting data at rest, data in transmission, and data in use
At Rest
• Transparent Data Encryption (TDE)
In Transmission
• Transport Layer Security
• SSL Certificates
In Use
• Always Encrypted

Summary

Quick Notes

SQL Managed Instances support Common Language Runtime (CLR)

Elastic Pools and Azure SQL Database servers can handle many databases

Deterministic supports more querying vs Randomized Encryption

Thank you