Microsoft

AZ-900

Learning path 02: Azure architecture and services

Learning path 02—outline

You will learn the following concepts:

1. **Azure architectural components**
   - Regions and availability zones
   - Subscriptions and resource groups
2. **Compute and networking**
   - Compute types
   - Application hosting
   - Virtual networking
3. **Storage**
   - Storage services
   - Redundancy options
   - File management and migration
4. **Identity, access, and security**
   - Directory services
   - Authentication methods
   - Security models

Azure accounts

- Azure account
- Azure free account
- Azure free student account
- Microsoft Learn sandbox

Azure architectural components

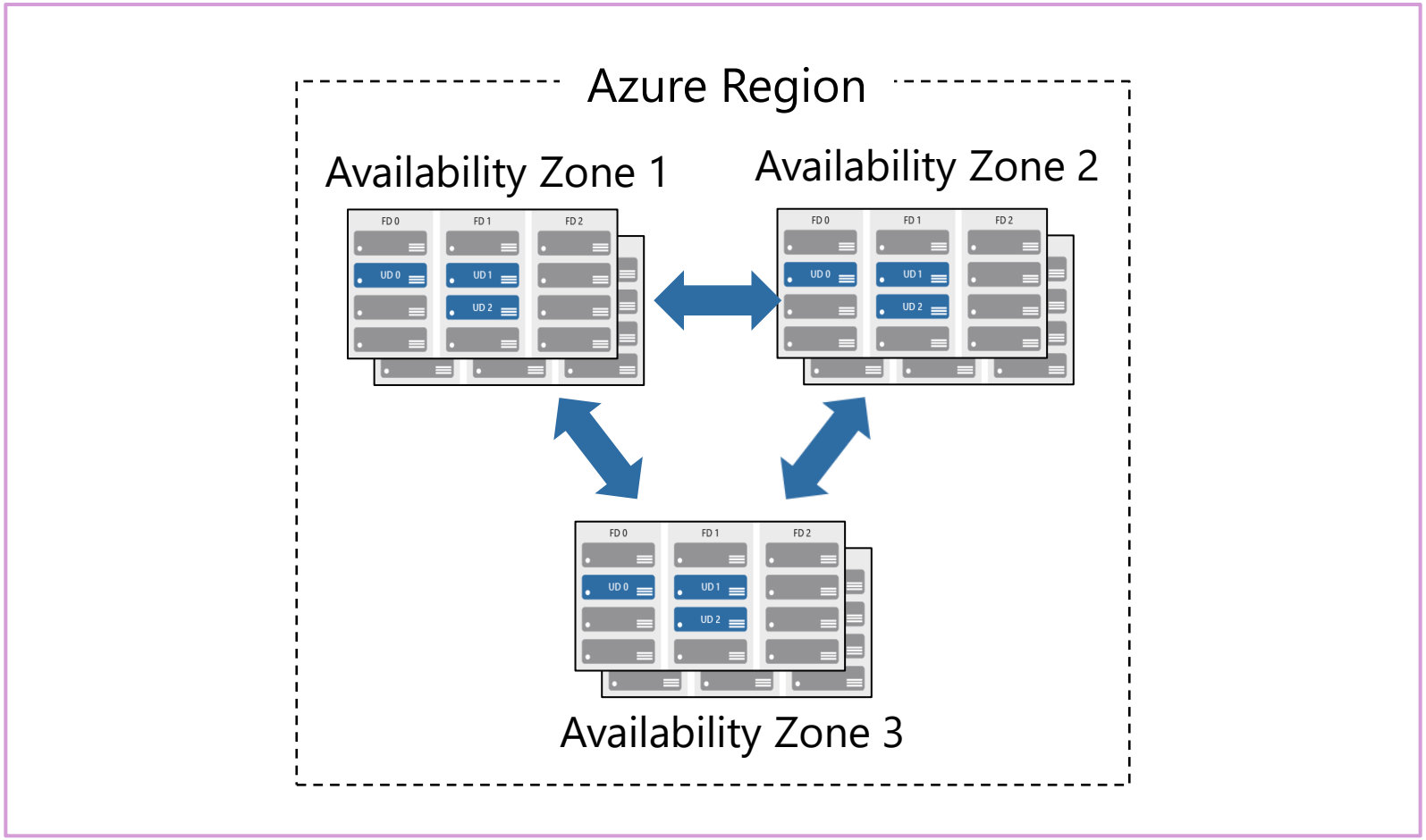
Regions

Azure offers more global regions than any other cloud provider with 60-plus regions representing over 140 countries

- Regions are made up of one or more datacenters in close proximity.
- They provide flexibility and scale to reduce customer latency.
- Regions preserve data residency with a comprehensive compliance offering.

Availability zones

- Provide protection against downtime due to datacenter failure.
- Physically separate datacenters within the same region.
- Each datacenter is equipped with independent power, cooling, and networking.
- Connected through private fiber-optic networks.



Region pairs

- At least 300 miles of separation between region pairs.
- Automatic replication for some services.
- Prioritized region recovery in the event of outage.
- Updates are rolled out sequentially to minimize downtime.

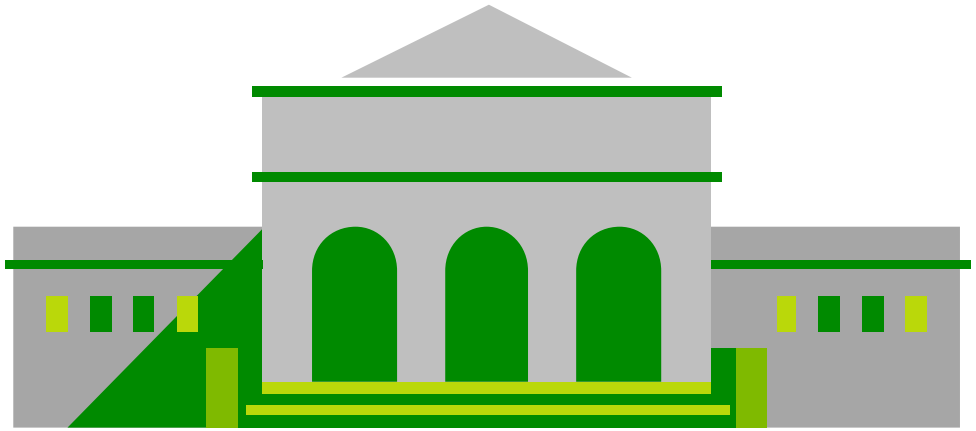
Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe
UK West	UK South
Germany Central	Germany Northeast
South East Asia	East Asia
East China	North China
Japan East	Japan West
Australia Southeast	Australia East
India South	India Central
Brazil South (Primary)	South Central US

Azure sovereign regions (US government services)

Meets the security and compliance needs of US federal agencies, state and local governments, and their solution providers.

Azure government:

- Separate instance of Azure.
- Physically isolated from non-US government deployments.
- Accessible only to screened, authorized personnel.



Azure sovereign regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

Azure China features:

- Physically separated instance of Azure cloud services operated by 21Vianet.
- All data stays within China to ensure compliance.

Azure resources

Azure **resources** are components like storage, virtual machines, and networks that are available to build cloud solutions.

Virtual machines

Storage accounts

Virtual networks

App services

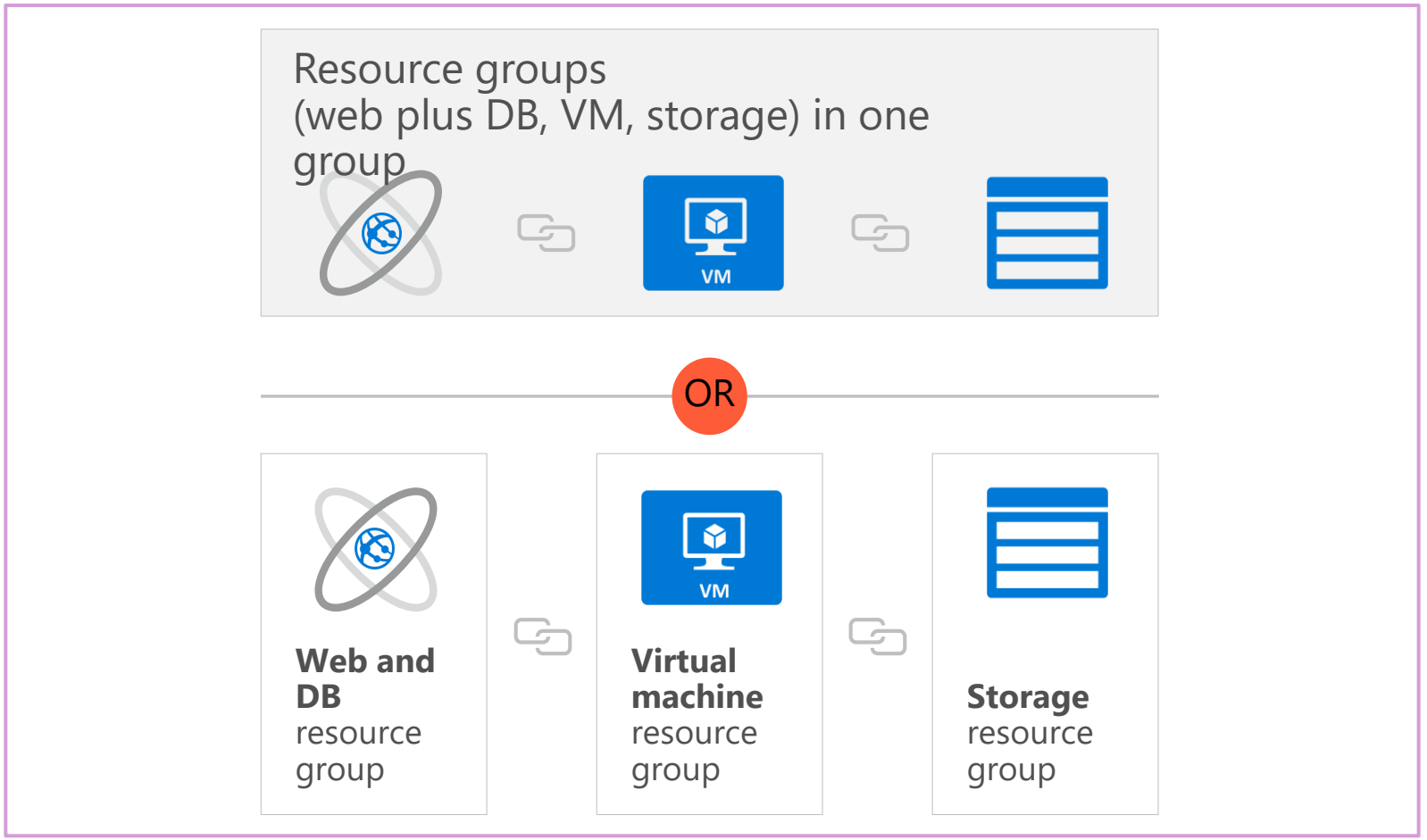
SQL databases

Functions

Resource groups

A **resource group** is a container you use to manage and aggregate resources in a single unit.

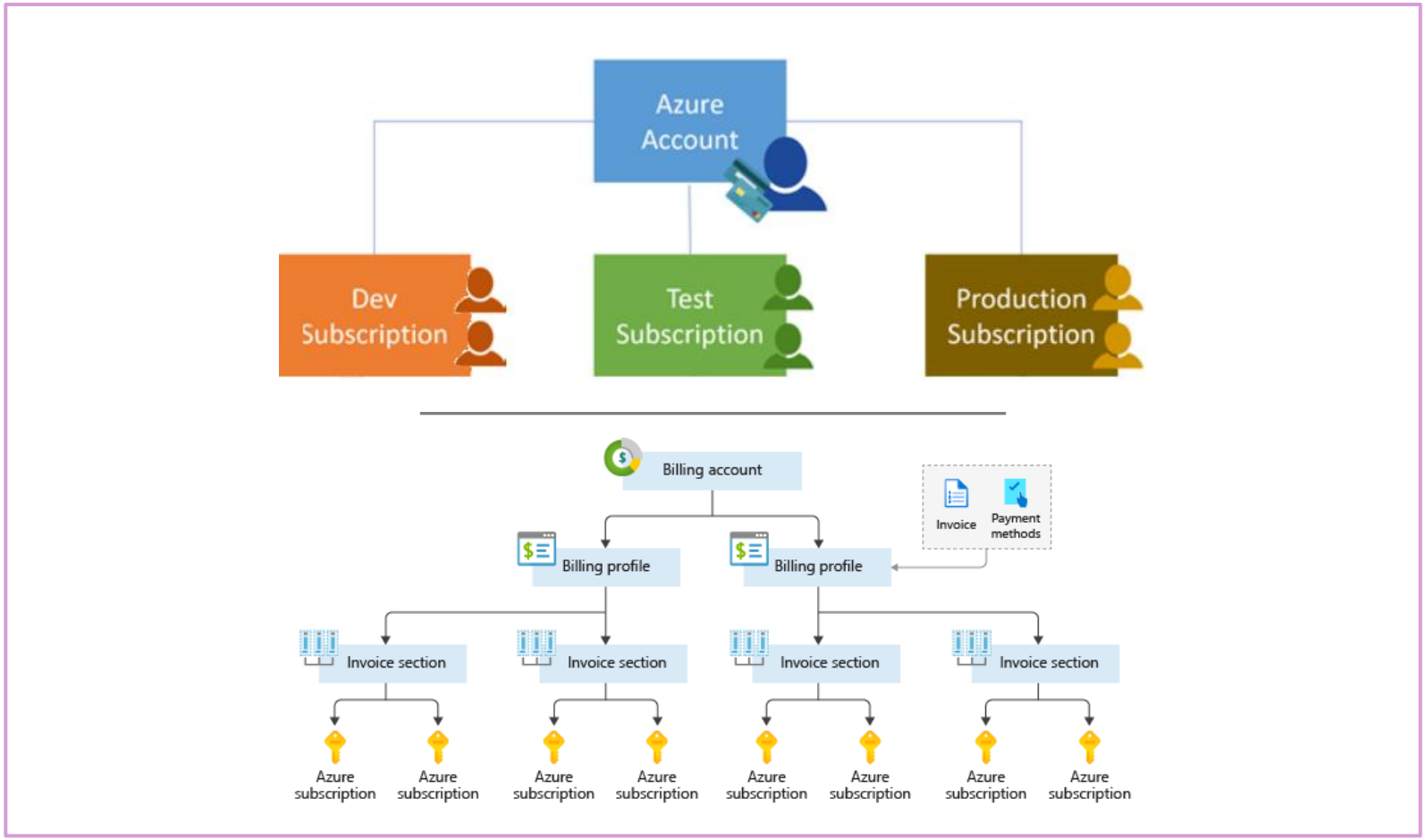
- Resources can exist in only one resource group.
- Resources can exist in different regions.
- Resources can be moved to different resource groups.
- Applications can utilize multiple resource groups.



Azure subscriptions

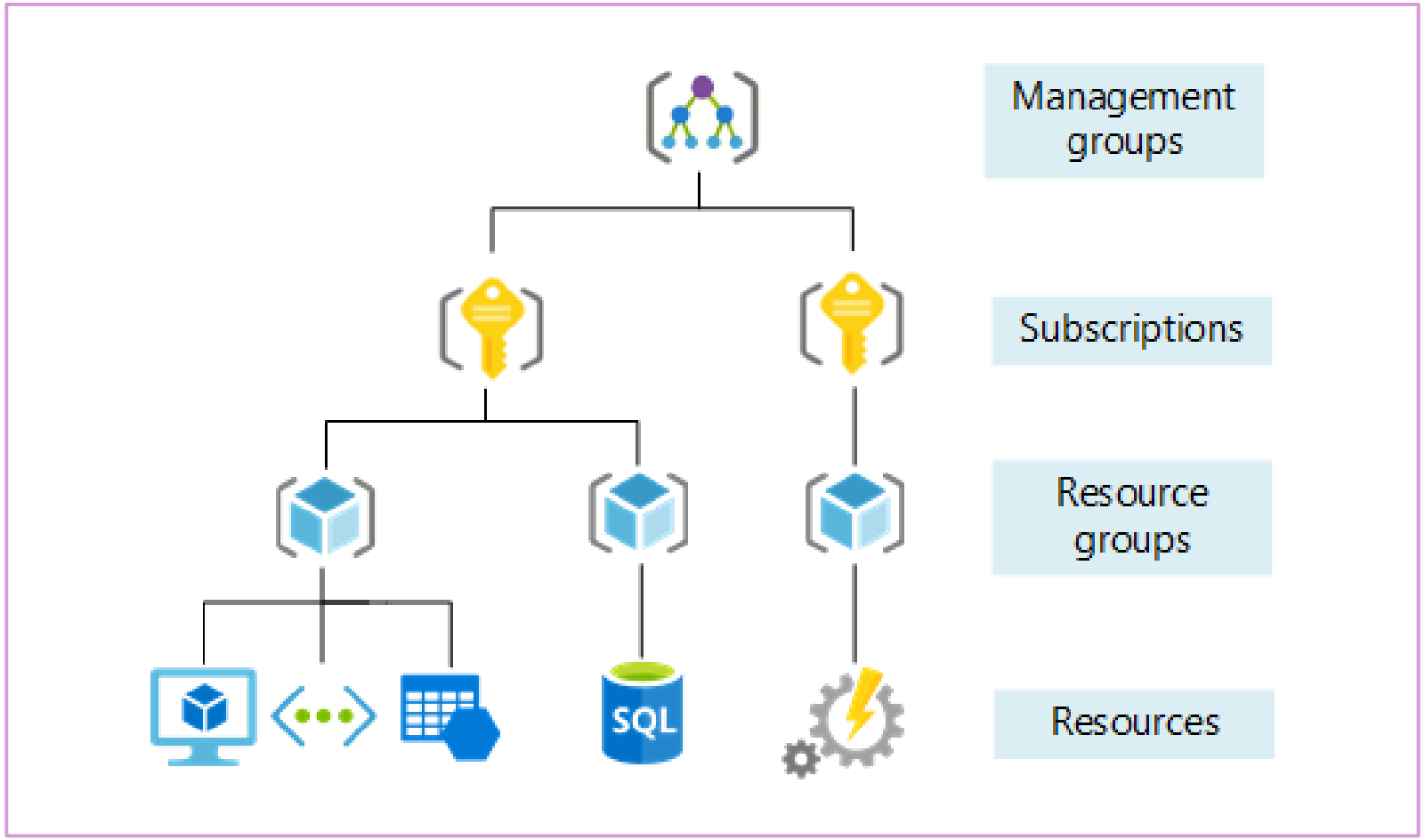
An Azure subscription provides you with authenticated and authorized access to Azure accounts.

- **Billing boundary:** Generate separate billing reports and invoices for each subscription.
- **Access control boundary:** Manage and control access to the resources that users can provision with specific subscriptions.



Management groups

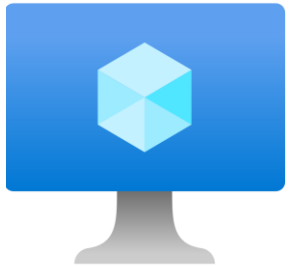
- Management groups can include multiple Azure subscriptions.
- Subscriptions inherit conditions applied to the management group.
- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth.



Compute and networking

Azure compute services

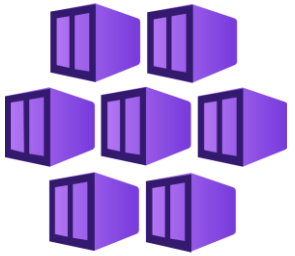
Azure **compute** is an on-demand service that provides computing resources such as disks, processors, memory, networking, and operating systems.



Virtual Machines

App Services

Container Instances



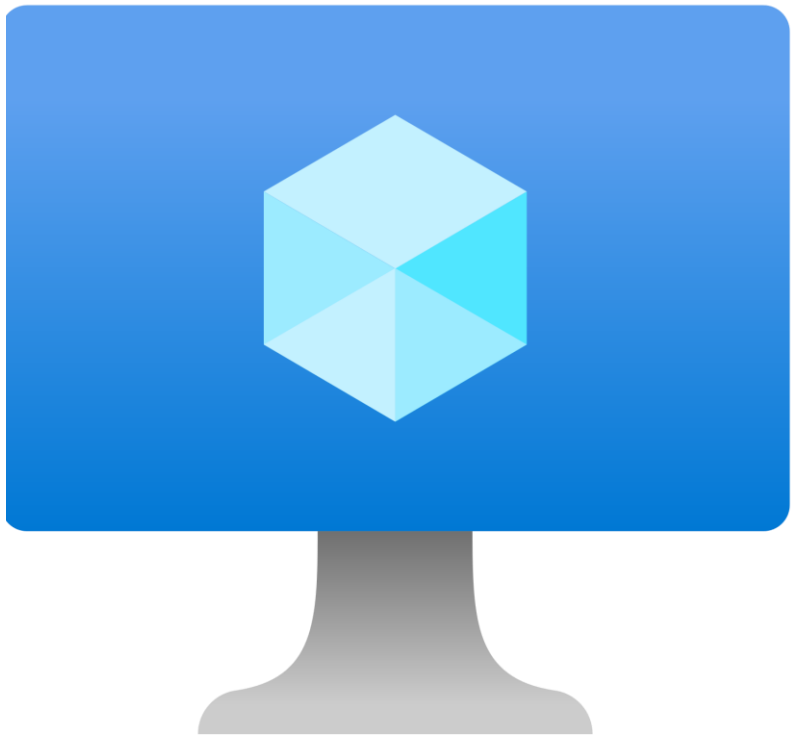
Azure Kubernetes Services (AKS)

Azure Virtual Desktop

Azure virtual machines

Azure **virtual machines (VMs)** are software emulations of physical computers.

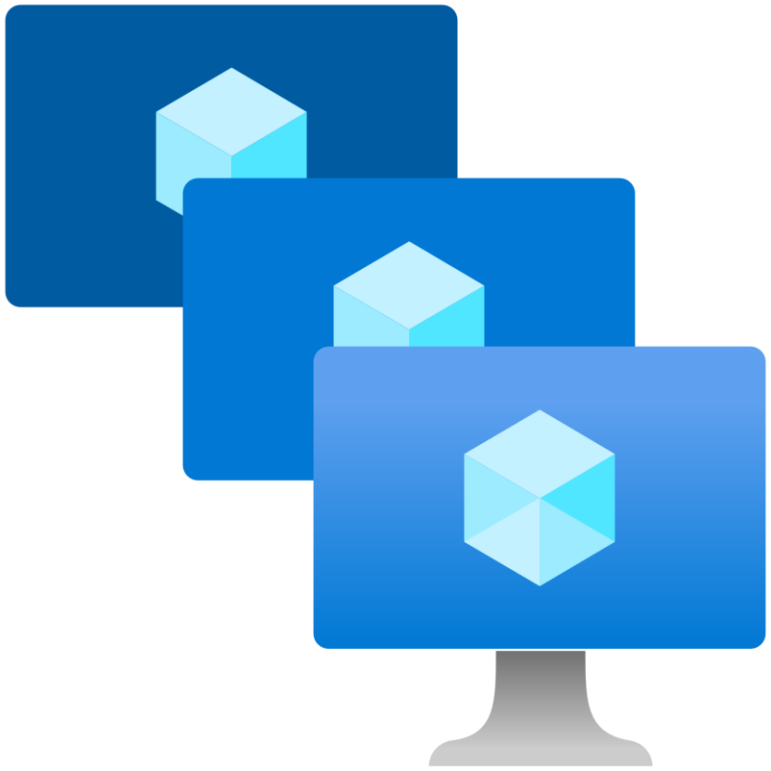
- Includes virtual processor, memory, storage, and networking.
- IaaS offering that provides total control and customization.



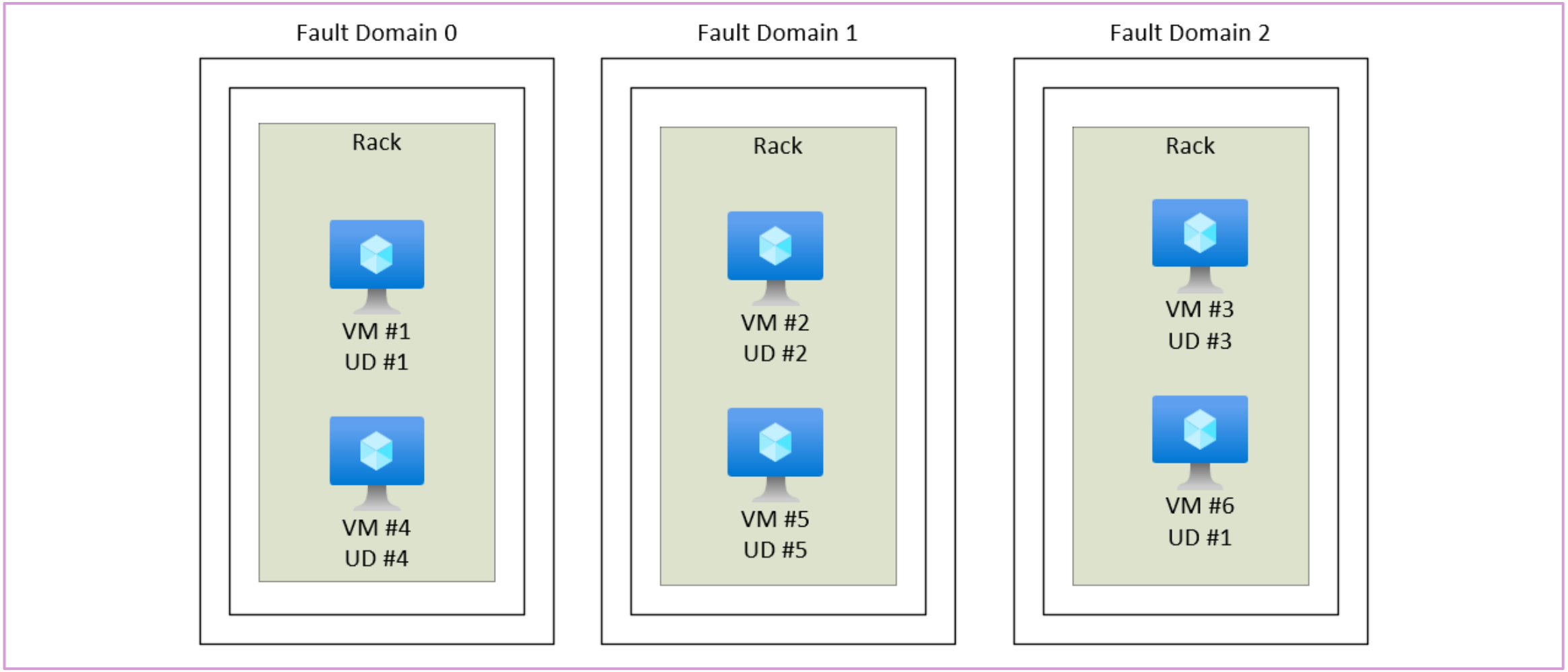
VM scale sets

Scale sets provide a load-balanced opportunity to automatically scale resources.

- Scale out when resource needs increase.
- Scale in when resource needs are lower.



VM availability sets



Azure Virtual Desktop

Azure Virtual Desktop is a desktop and app virtualization that runs in the cloud.

- Create a full desktop virtualization environment without having to run additional gateway servers.
- Reduce risk of resource being left behind.
- True multisession deployments.

Azure container services

Azure **containers** provide a lightweight, virtualized environment that does not require operating system management, and can respond to changes on demand.

Azure Container Instances: A PaaS offering that runs a container or pod of containers in Azure.

Azure Container Apps: A PaaS offering, like container instances, that can load balance and scale.

Azure Kubernetes Service: An orchestration service for containers with distributed architectures and large volumes of containers.

Azure Functions

Azure Functions: A PaaS offering that supports serverless compute operations. Event-based code runs when called without requiring server infrastructure during inactive periods.

Comparing Azure compute options

Virtual machines

- Cloud-based server that supports either Windows or Linux environments.
- Useful for lift-and-shift migrations to the cloud.
- Complete operating system package, including the host operating system.

Virtual Desktop

- Provides a cloud-based personal computer Windows desktop experience.
- Dedicated applications to connect and use, or accessible from any modern browser.
- Multiclient login allows multiple users to log into the same machine at the same time.

Containers

- Lightweight, miniature environment well suited for running microservices.
- Designed for scalability and resiliency through orchestration.
- Applications and services are packaged in a container that sits on top of the host operating system. Multiple containers can sit on one host OS.

Azure App Services

Azure **App Services** is a fully managed platform to build, deploy, and scale web apps and APIs quickly.

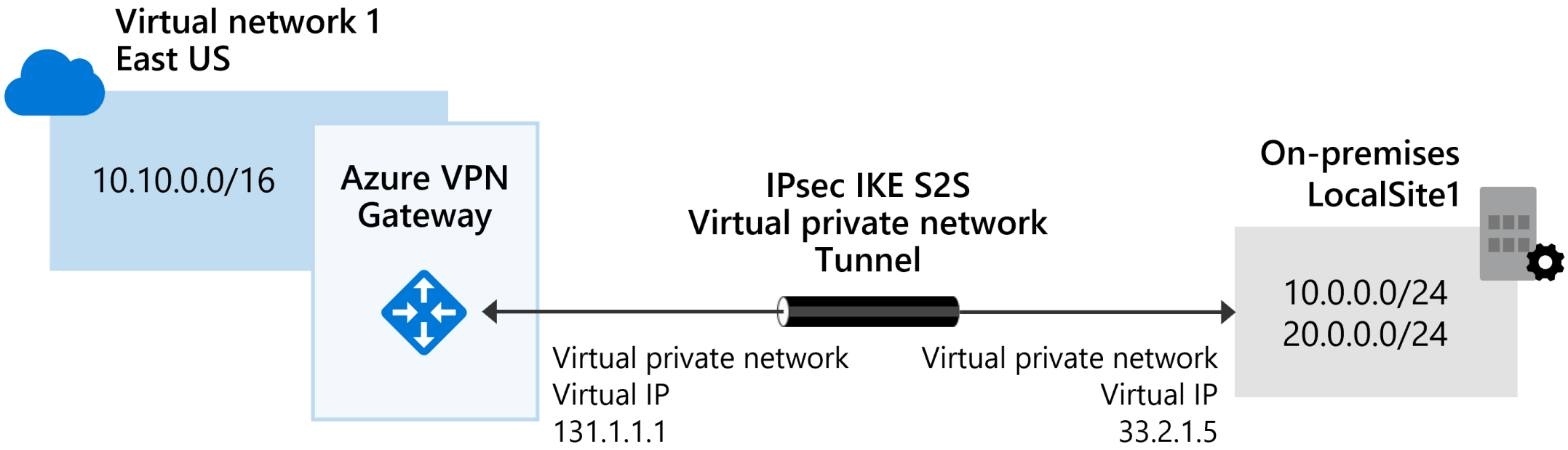
- Works with .NET, .NET Core, Node.js, Java, Python, or php.
- PaaS offering with enterprise-grade performance, security, and compliance requirements.

Azure networking services

Azure Virtual Network (VNet) enables Azure resources to communicate with each other, the internet, and on-premises networks.

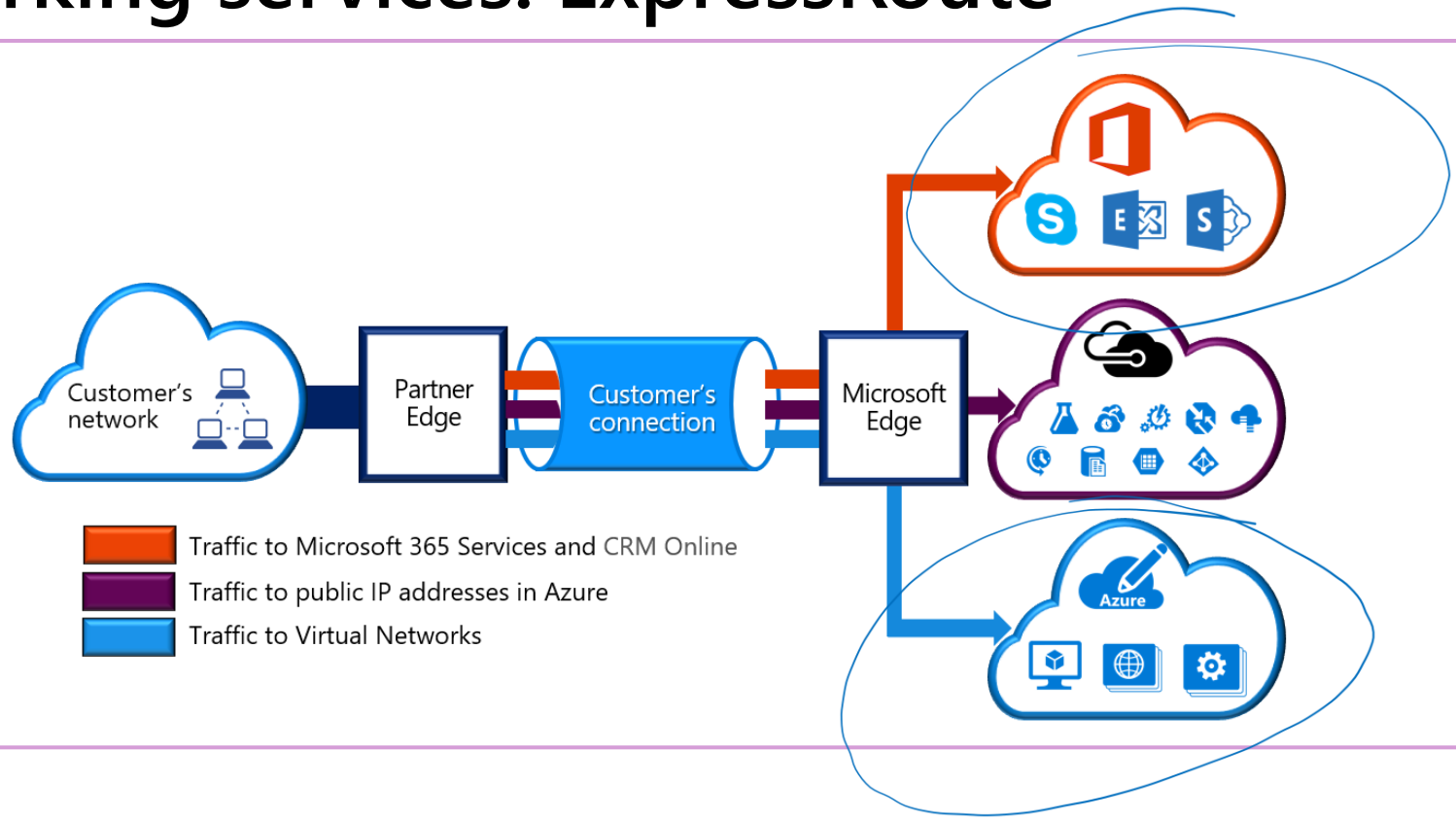
- Public endpoints, accessible from anywhere on the internet.
- Private endpoints, accessible only from within your network.
- Virtual subnets segment your network to suit your needs.
- Network peering connects your private networks directly together.

Azure networking services: VPN Gateway



VPN Gateway is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet.

Azure networking services: ExpressRoute



ExpressRoute extends on-premises networks into Azure over a private connection that is facilitated by a connectivity provider.

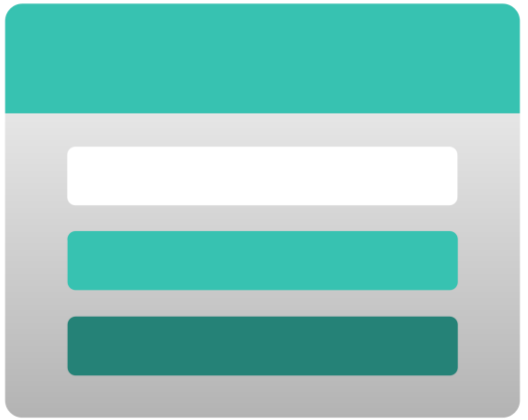
Azure DNS

- Reliability and performance by leveraging a global network of DNS name servers using Anycast networking.
- Azure DNS security is based on Azure resource manager, enabling role-based access control and monitoring and logging.
- Ease of use for managing your Azure and external resources with a single DNS service.
- Customizable virtual networks allow you to use private, fully customized domain names in your private virtual networks.
- Alias records support alias record sets to point directly to an Azure resource.

Storage

Storage accounts

- Must have a globally unique name.
- Provide over-the-internet access worldwide.
- Determine storage services and redundancy options.



Storage redundancy

Redundancy configuration	Deployment	Durability
Locally redundant storage (LRS)	Single datacenter in the primary region	11 nines
Zone-redundant storage (ZRS)	Three availability zones in the primary region	12 nines
Geo-redundant storage (GRS)	Single datacenter in the primary and secondary region	16 nines
Geo-zone-redundant-storage (GZRS)	Three availability zones in the primary region and a single datacenter in the secondary region	16 nines

Azure storage services

Azure Blob: Optimized for storing massive amounts of unstructured data, such as text or binary data.

Azure Disk: Provides disks for virtual machines, applications, and other services to access and use.

Azure Queue: Message storage service that provides storage and retrieval for large amounts of messages, each up to 64 KB.

Azure Files: Sets up a highly available network file share that can be accessed by using the Server Message Block protocol.

Azure Tables: Provides a key/attribute option for structured nonrelational data storage with a schema-less design.

Storage service public endpoints

Storage service	Public endpoint
Blob Storage	https://<storage-account-name>.blob.core.windows.net
Data Lake Storage Gen2	https://<storage-account-name>.dfs.core.windows.net
Azure Files	https://<storage-account-name>.file.core.windows.net
Queue Storage	https://<storage-account-name>.queue.core.windows.net
Table Storage	https://<storage-account-name>.table.core.windows.net

Azure storage access tiers

Hot	Cool	Cold	Archive
Optimized for storing data that is accessed frequently.	Optimized for storing data that is infrequently accessed and stored for at least 30 days.	Optimized for storing data that is infrequently accessed and stored for at least 90 days.	Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements.

Azure Migrate

- Unified migration platform.
- Range of integrated and standalone tools.
- Assessment and migration.

Azure Data Box

- Store up to 80 terabytes of data.
- Move your disaster recovery backups to Azure.
- Protect your data in a rugged case during transit.
- Migrate data out of Azure for compliance or regulatory needs.
- Migrate data to Azure from remote locations with limited or no connectivity.

File management options

AzCopy

- Command-line utility.
- Copy blobs or files to or from your storage account.
- One-direction synchronization.

Azure Storage Explorer

- Graphical user interface (similar to Windows Explorer).
- Compatible with Windows, MacOS, and Linux.
- Uses AzCopy to handle file operations.

Azure File Sync

- Synchronizes Azure and on-premises files in a bidirectional manner.
- Cloud tiering keeps frequently accessed files local, while freeing up space.
- Rapid reprovisioning of failed local server (install and resync).

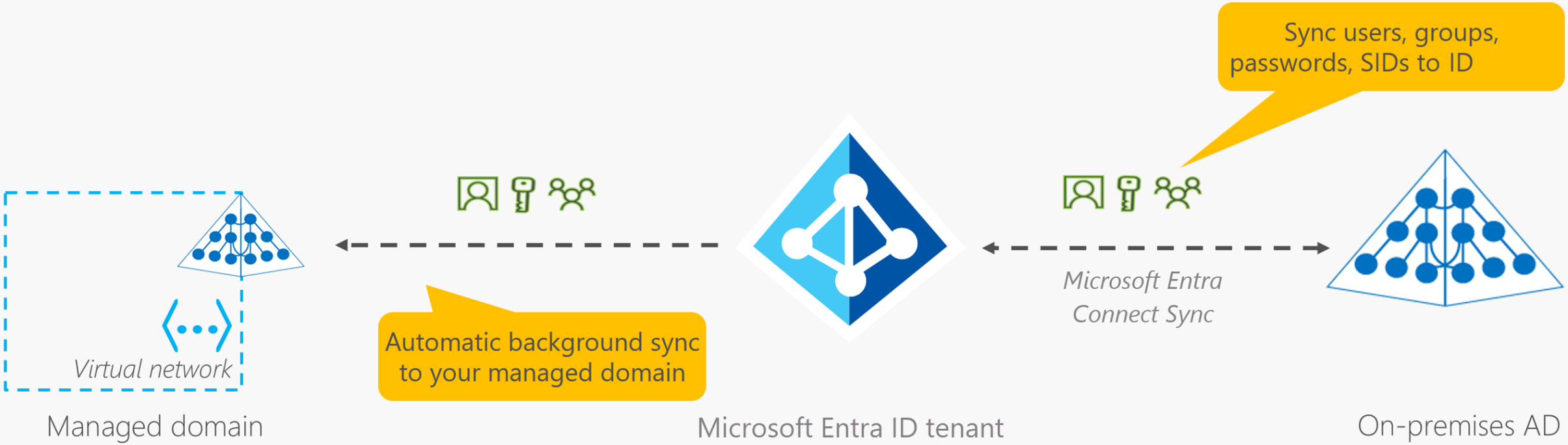
Identity, access, and security

Microsoft Entra ID

Microsoft Entra ID is Microsoft Azure's cloud-based identity and access management service.

- Authentication (employees sign in to access resources).
- Single sign-on (SSO).
- Application management.
- Business to Business (B2B).
- Device management.

Microsoft Entra Domain Services



- Gain the benefit of cloud-based domain services without managing domain controllers.
- Run legacy applications (that can't use modern auth standards) in the cloud.
- Automatically sync from Microsoft Entra ID.

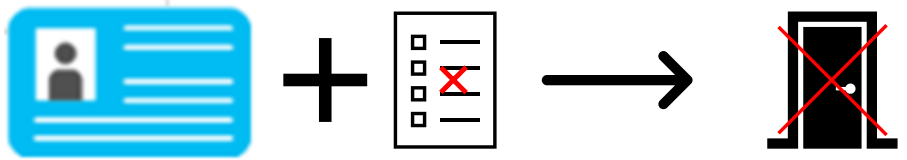
Compare authentication and authorization

Authentication

- Identifies the person or service seeking access to a resource.
- Requests legitimate access credentials.
- Basis for creating secure identity and access control principles.

Authorization

- Determines an authenticated person's or service's level of access.
- Defines which data they can access, and what they can do with it.

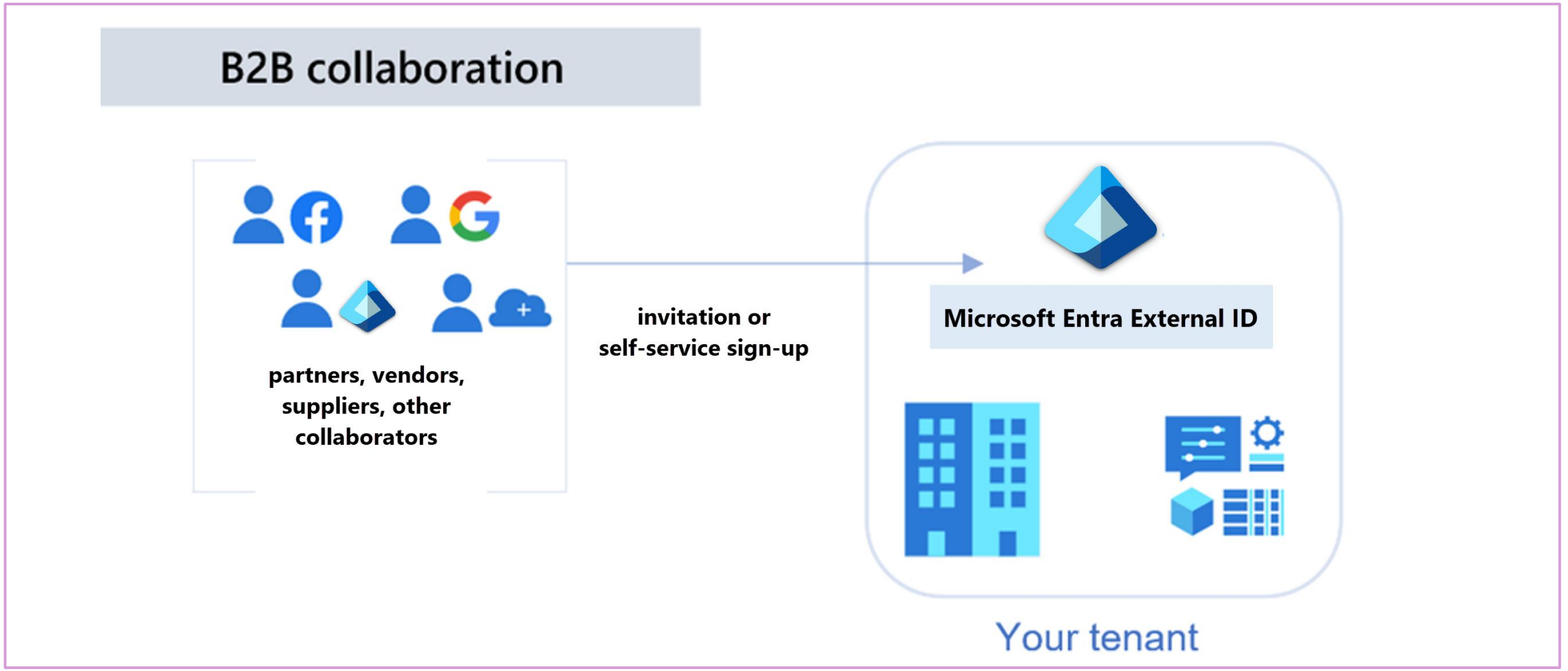


Multifactor authentication

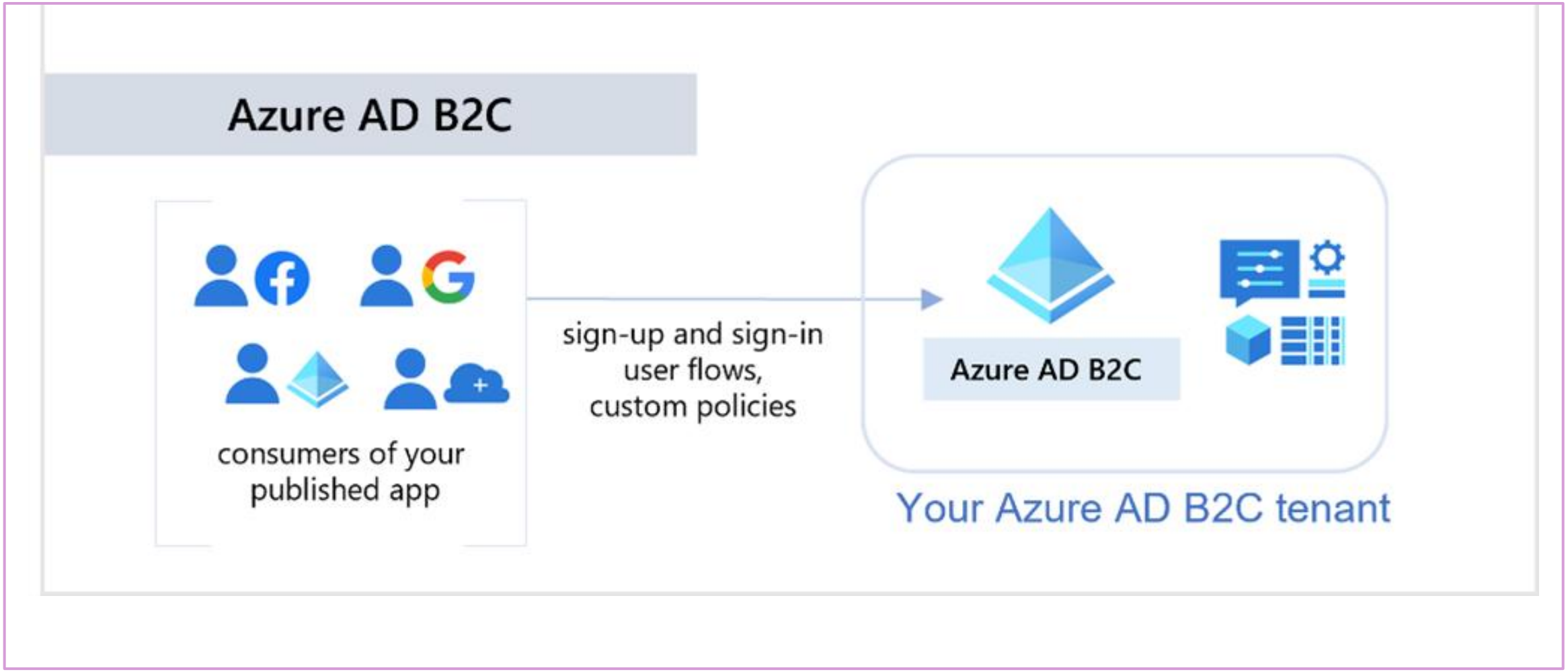
Provides additional security for your identities by requiring two or more elements for full authentication.

- Something you know ←→ Something you possess ←→ Something you are

Microsoft Entra External ID B2B



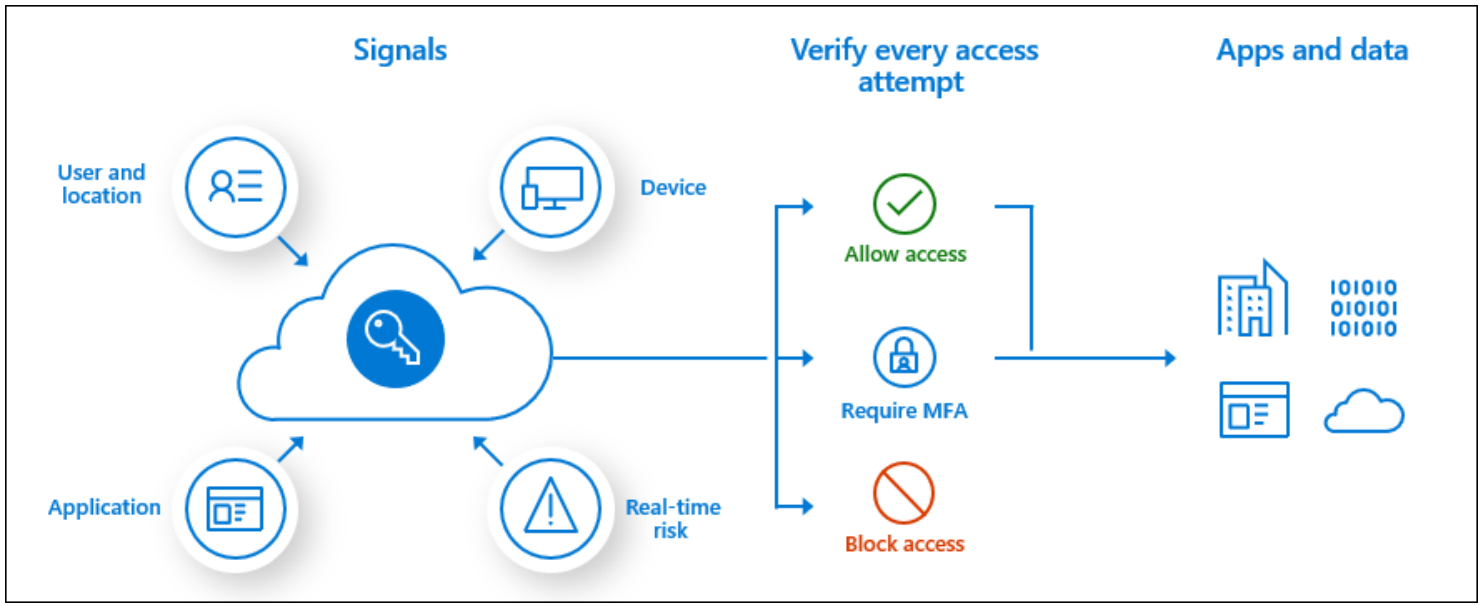
Azure AD External Identities B2C



Conditional Access

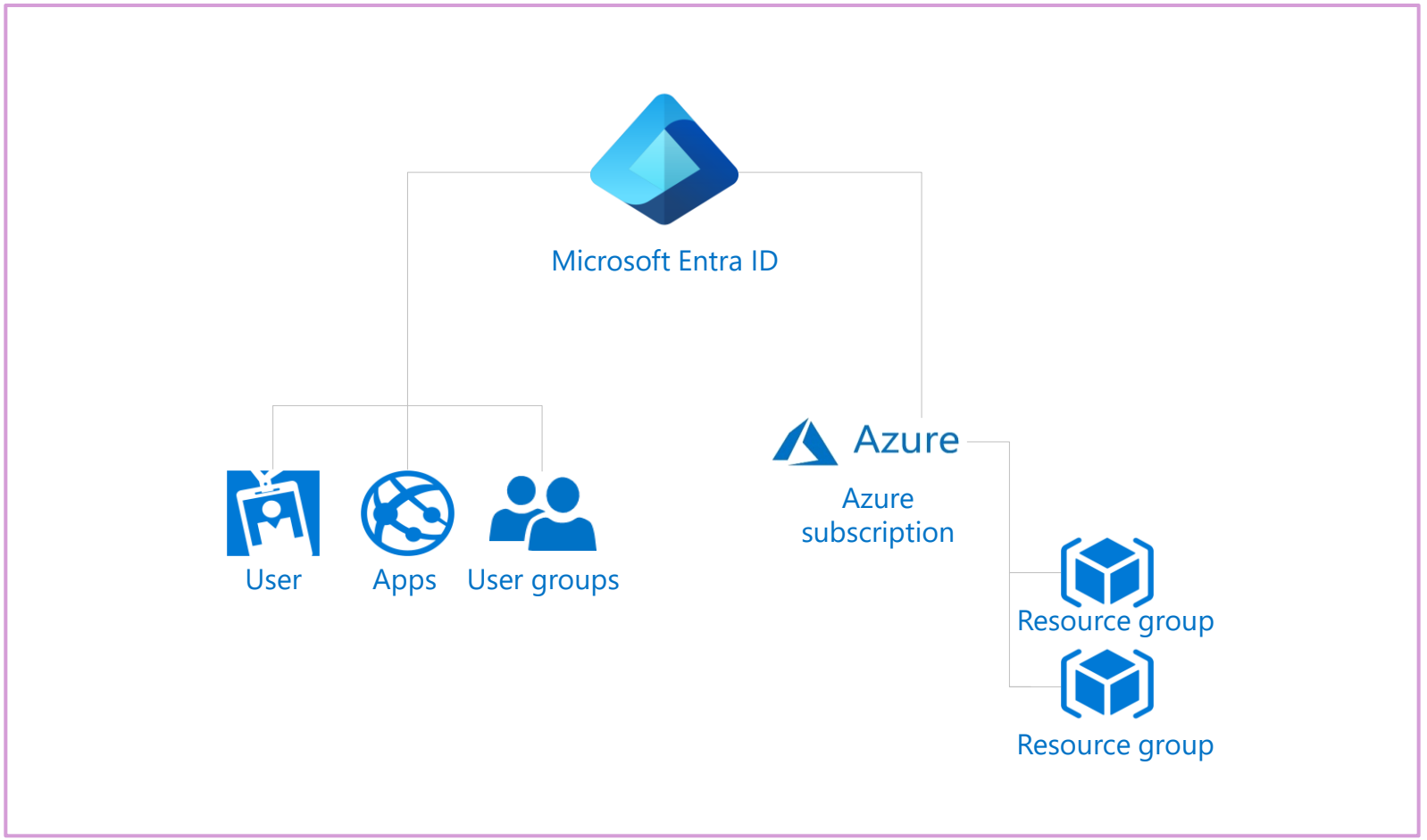
Conditional Access is used to bring signals together, to make decisions, and enforce organizational policies.

- User or group membership
- IP location
- Device
- Application
- Risk detection

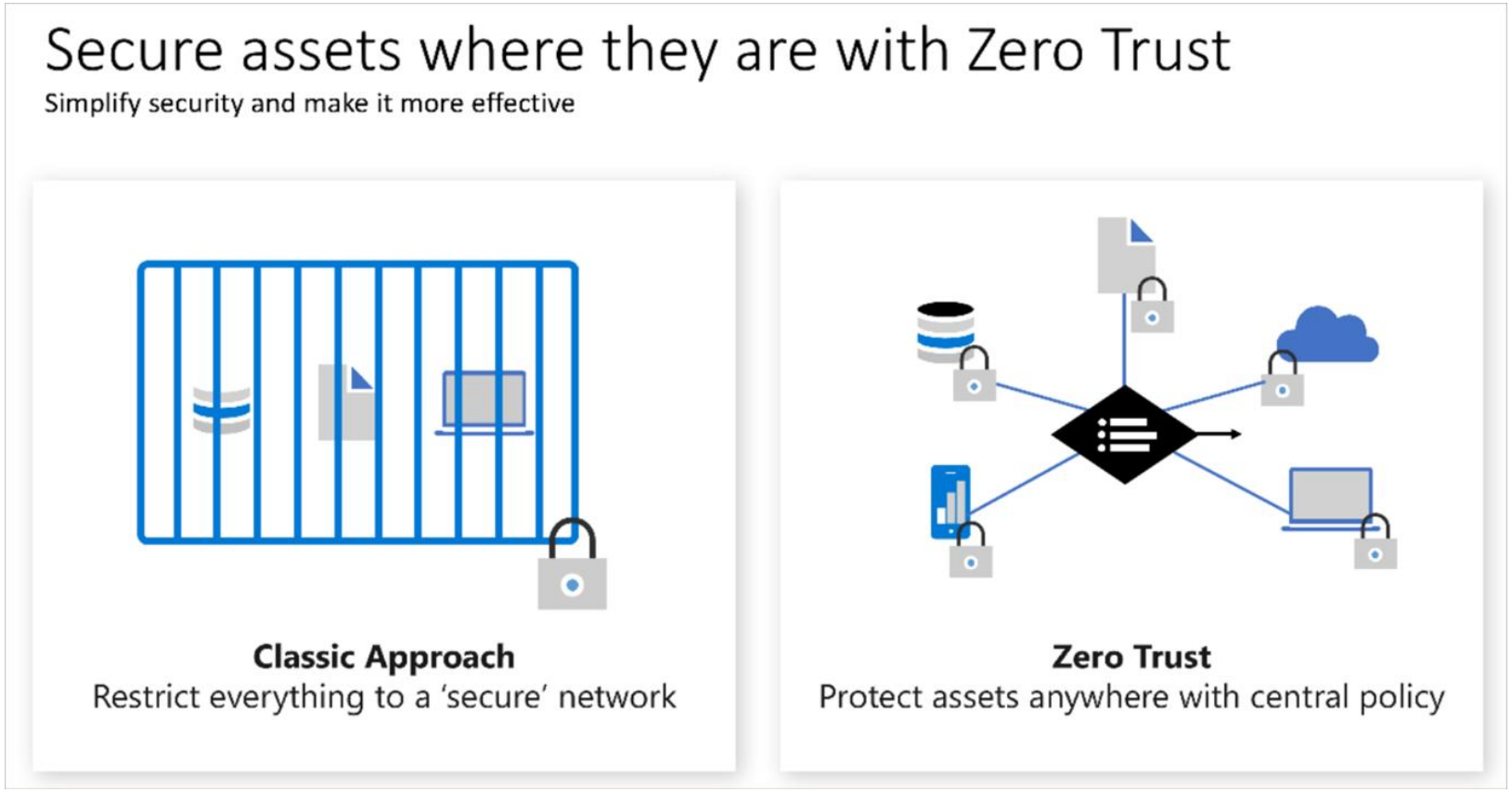


Role-based access control

- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
- Enables access to the Azure portal and controlling access to resources.

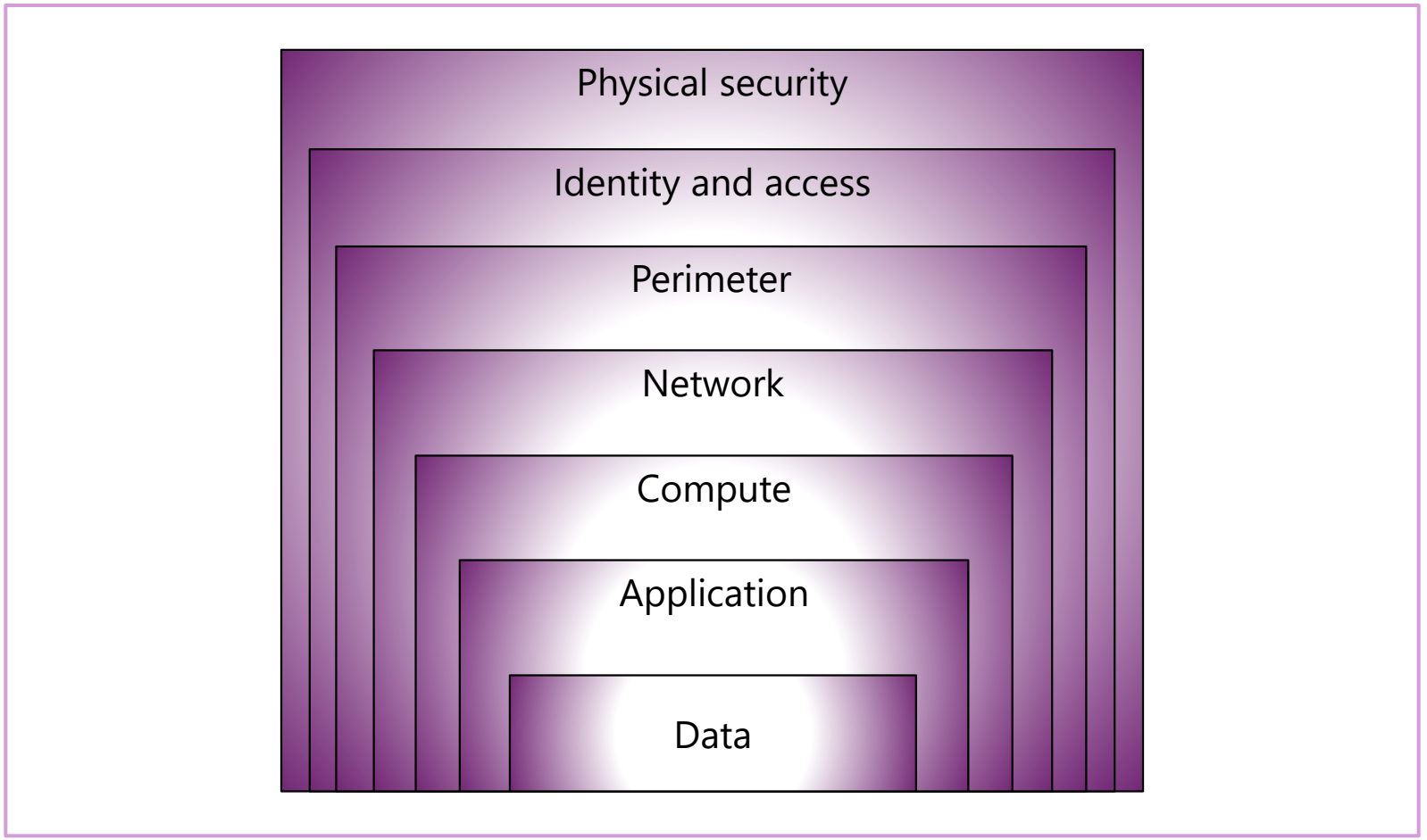


Zero Trust



Defense in depth

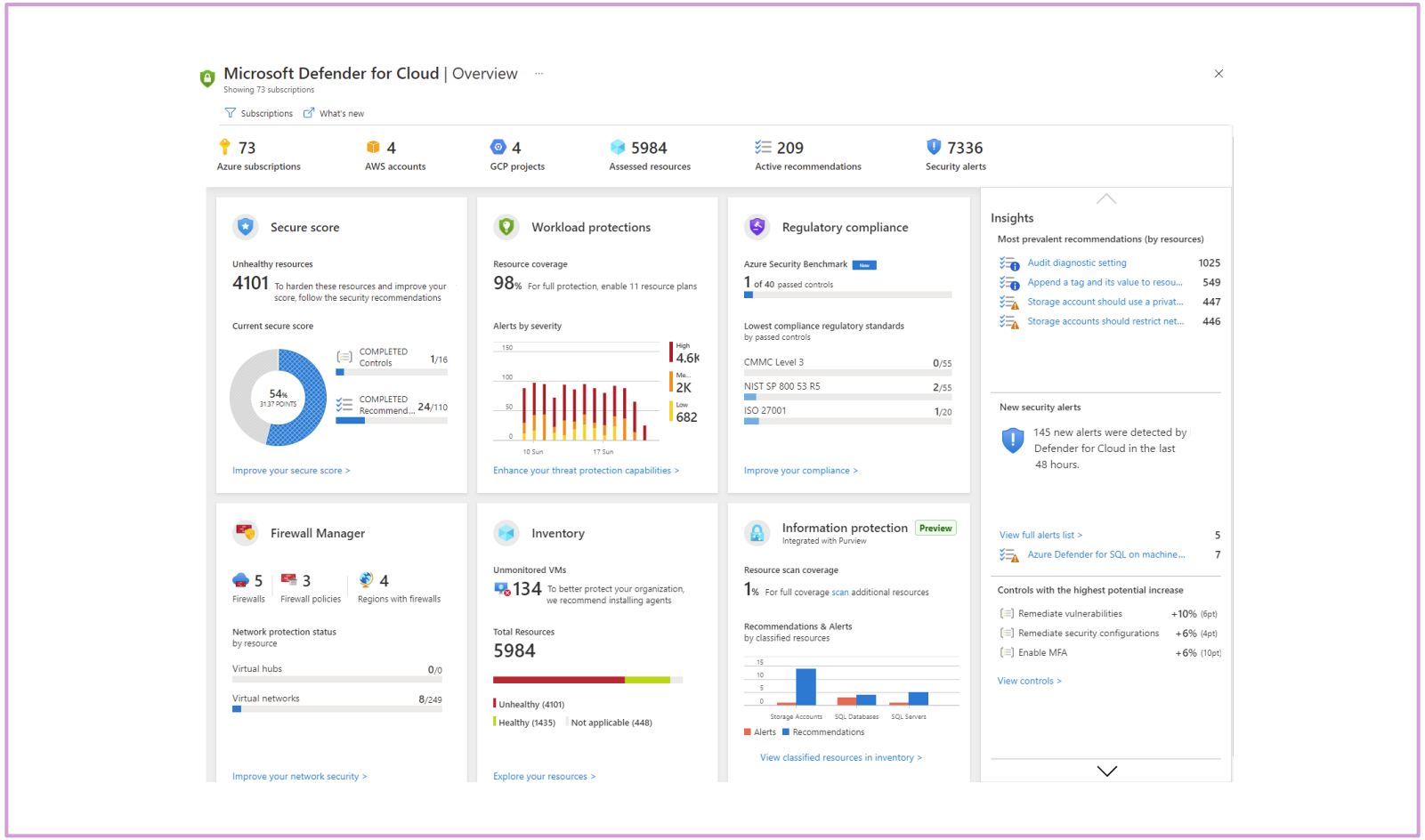
- A layered approach to securing computer systems.
- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



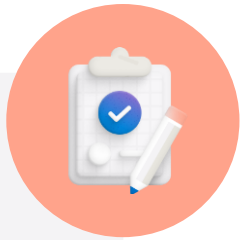
Microsoft Defender for Cloud

Microsoft Defender for Cloud is a monitoring service that provides threat protection across both Azure and on-premises datacenters.

- Provides security recommendations.
- Detect and block malware.
- Analyze and identify potential attacks.
- Just-in-time access control for ports.



Learning path 02 review



Microsoft Learn Modules (learn.microsoft.com/training)

- Physical and management infrastructure of Microsoft Azure
- Compute and networking services
- Storage services
- Identity, access, and security