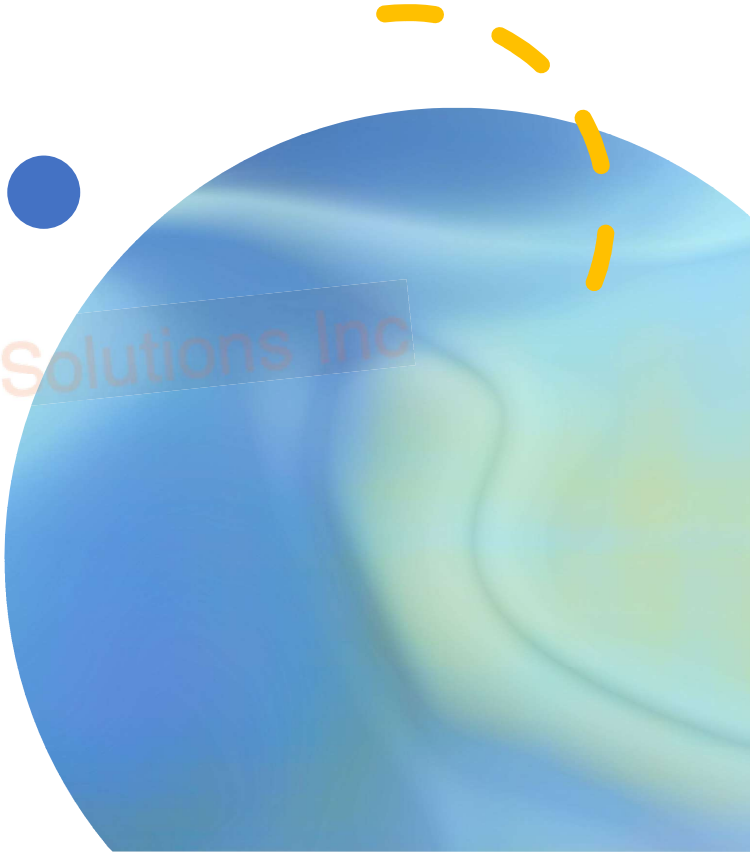
Azure ExpressRoute

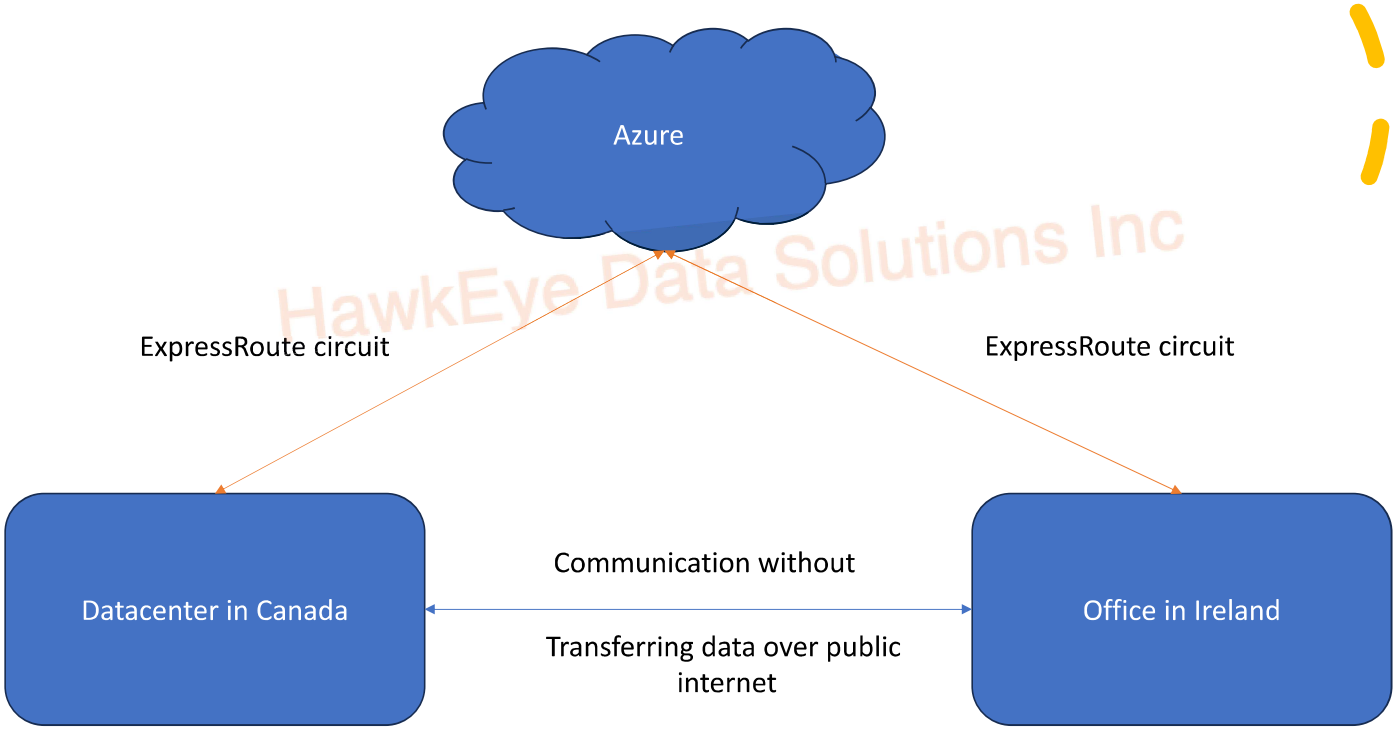
Like a dedicated, private highway between your on-premises data center or network and Microsoft Azure's cloud infrastructure. It provides a fast, reliable, and secure connection **that bypasses the public internet.**

With Azure ExpressRoute, you can establish a private and direct link to Azure's data centers, ensuring low-latency, consistent performance, and enhanced security for your data and applications.

It's like having a private road to Microsoft Azure, allowing your organization to extend its network into the cloud with reliability and minimal exposure to the internet's potential risks.



Azure ExpressRoute

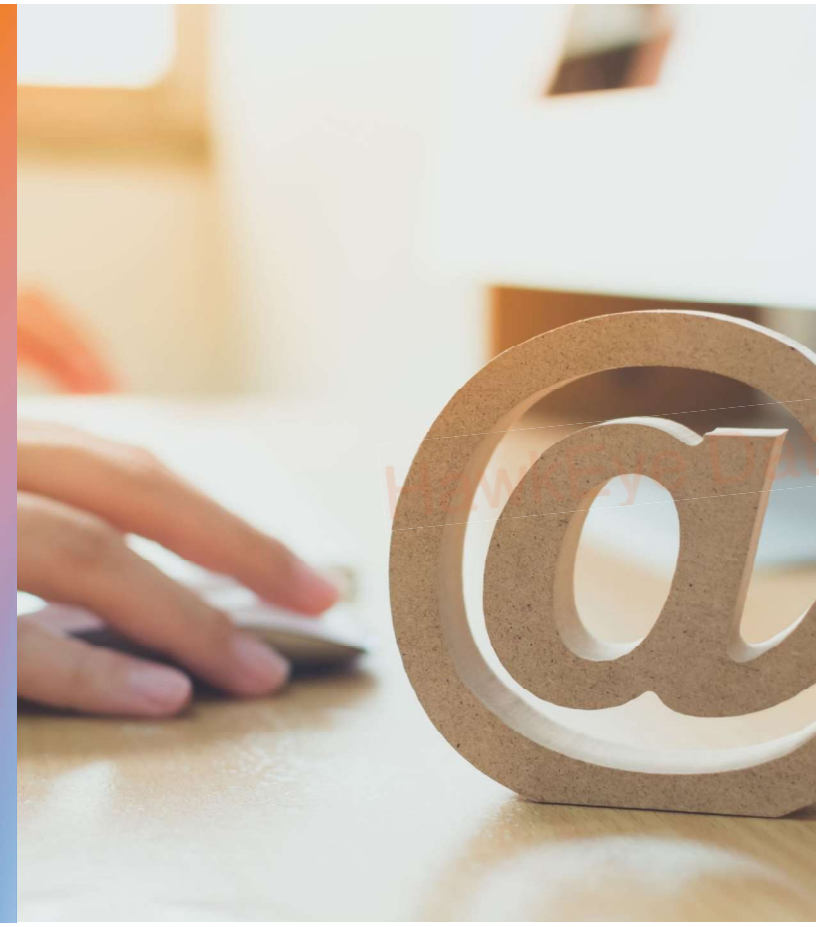


Filter Network Traffic

- ✓ **Network Security Groups (NSGs) -** Like a virtual wall that you can place around your Azure resources. It acts as a protective shield, allowing you to define rules that control inbound and outbound traffic to and from those resources. Think of it as a security guard that decides who can enter and exit your building.

- ✓ With NSGs, you can specify which network traffic is allowed or denied, based on factors like source and destination IP addresses, ports, and protocols.

- ✓ **Network Virtual Appliances (NVAs) –** Specialized VMs that behave/act as hardened network appliances. Eg – WAN optimization, running a firewall etc.



Azure DNS

- ✓ Like a big, magical address book for the internet. Instead of people's names and phone numbers, it's filled with website and service names and their "phone numbers" (IP addresses).
- ✓ Every domain will translate to an IP Address. Eg. www.hawkeyedata.ca -> Some IP Address.
- ✓ Instead of remembering long strings of numbers (IP addresses), you can use easy-to-recall website names like www.azure.com. It is dynamic, real-time and global!
- ✓ Easily manage domain name records for your Azure Services + Provide DNS for your external resources as well!
- ✓ Uses anycast networking - Every DNS query is answered by the closest available DNS server. Fast performance + Scalability.
- ✓ **CAN'T** use Azure DNS to buy a domain name. Can do it using a 3rd Party Registrar or App Service for an annual fee.

Azure Storage Accounts

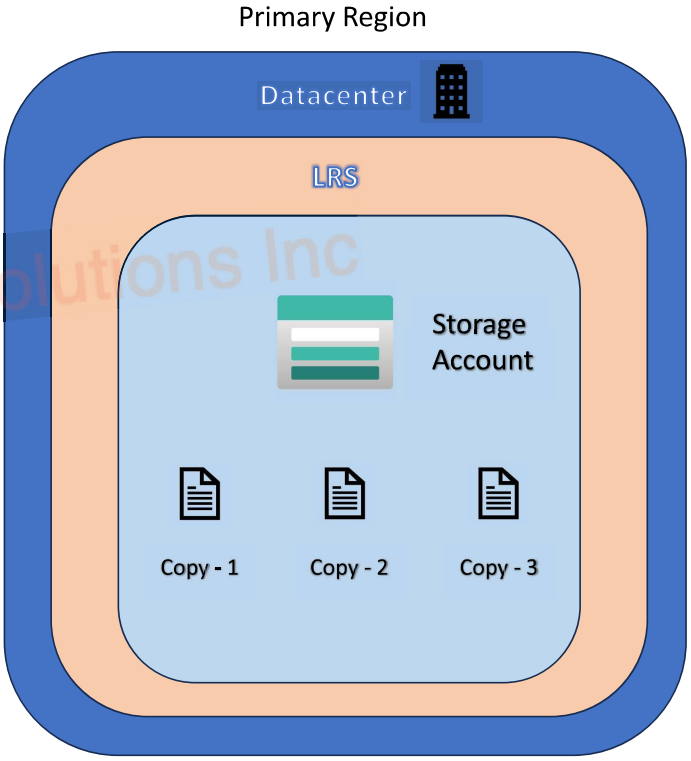
- ✓ Like digital warehouses where you can store and manage various types of data in Microsoft Azure.
- ✓ Can store various types of data, including files, databases, backups, and unstructured data like documents and images.
- ✓ Provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS.
- ✓ Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only.
- ✓ E.g. - https://<storage-accountname>.blob.core.windows.net

Azure Storage Redundancy

- ✓ Multiple copies of the data is stored.
- ✓ Unplanned events like natural disasters, hardware failure, power outages etc. can happen at any time – HA & FT.
- ✓ Can have a **Primary Region** (MUST) & a **Secondary Region** (Optional).
- ✓ Data in the Primary Region is always replicated 3 times - does not matter which option we choose – HOW it is stored is the key difference.
- ✓ Options –
  - Locally Redundant Storage (LRS)
  - Zone Redundant Storage (ZRS)
  - Geo-Redundant Storage (GRS)
  - Geo-Zone Redundant Storage (GZRS)

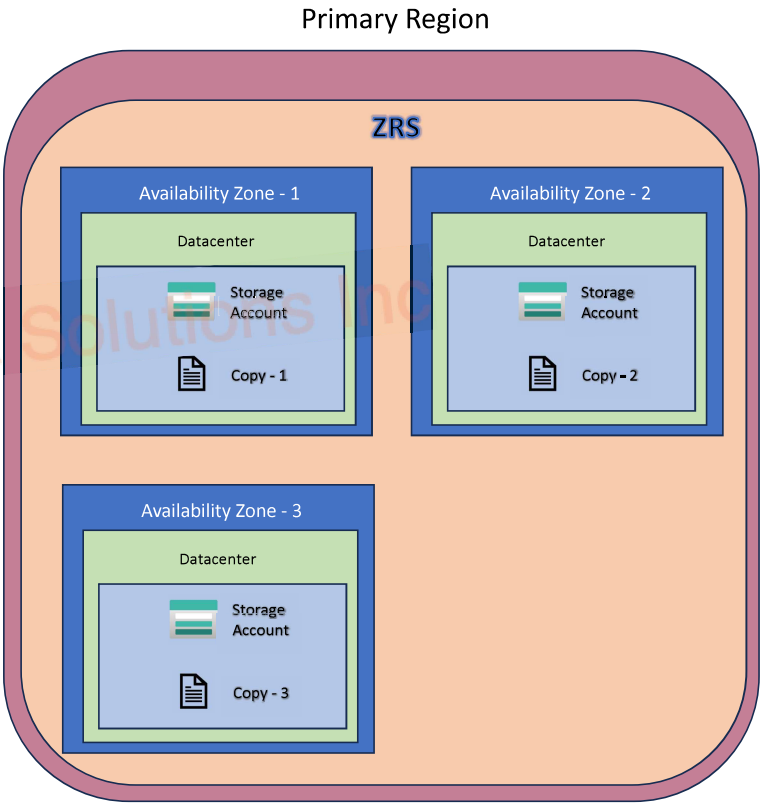
Locally Redundant Storage (LRS)

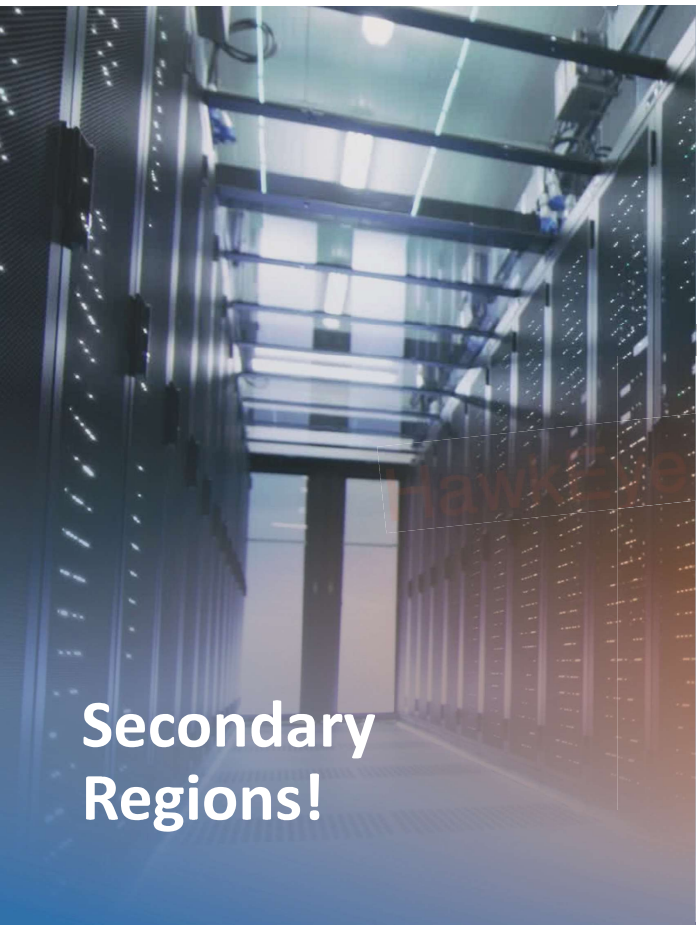
- ✓ Replicates your data 3 times in a **SINGLE** datacenter in the primary region, no secondary region.
- ✓ Provides at least 11 nines of durability (99.999999999%) of objects over a year.
- ✓ Cheapest redundancy option & least durable out of all the options.
- ✓ Can protect against drive or server rack failures.
- ✓ Think of a scenario where this 1 datacenter goes down or is destroyed – data may be unrecoverable.
- ✓ Microsoft highly recommends ZRS, GRS, GZRS (the other 3 options).



Zone Redundant Storage (ZRS)

- ✓ Replicates your data synchronously across 3 Availability Zones in the Primary Region, still no secondary region.
- ✓ Provides at least **12** nines of durability (99.9999999999%) of objects over a year.
- ✓ Costlier than LRS but much more durable!
- ✓ Data still available for read & write if a zone becomes unavailable – Azure will take care of DNS repointing, other networking tasks.
- ✓ Might be needed to meet data governance requirements – data still in same country.



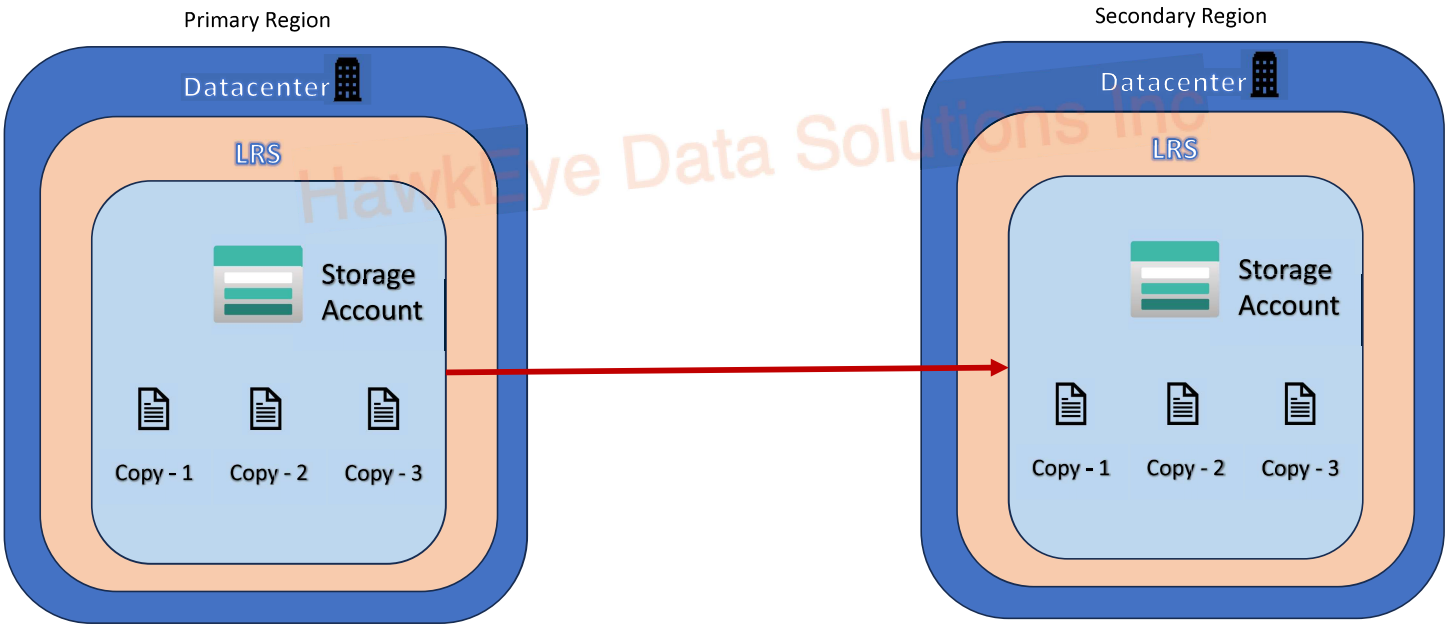


Secondary Regions!

- ✓ For apps needing high durability – replicate the data in the storage account to a secondary region (100's of miles away)
- ✓ Create a storage account – select the primary region. Paired secondary region is based on Azure Region Pairs!
- ✓ By default, data in secondary region isn't available for R/W unless Primary Region fails (can enable it : RA-GRS / RA-GZRS).
- ✓ After Primary Region fails, the secondary becomes your new primary!
- ✓ RPO (Recovery Point Objective) – Point in time to which data can be recovered : Difference between the most recent write to the primary region & the last write to the secondary region.

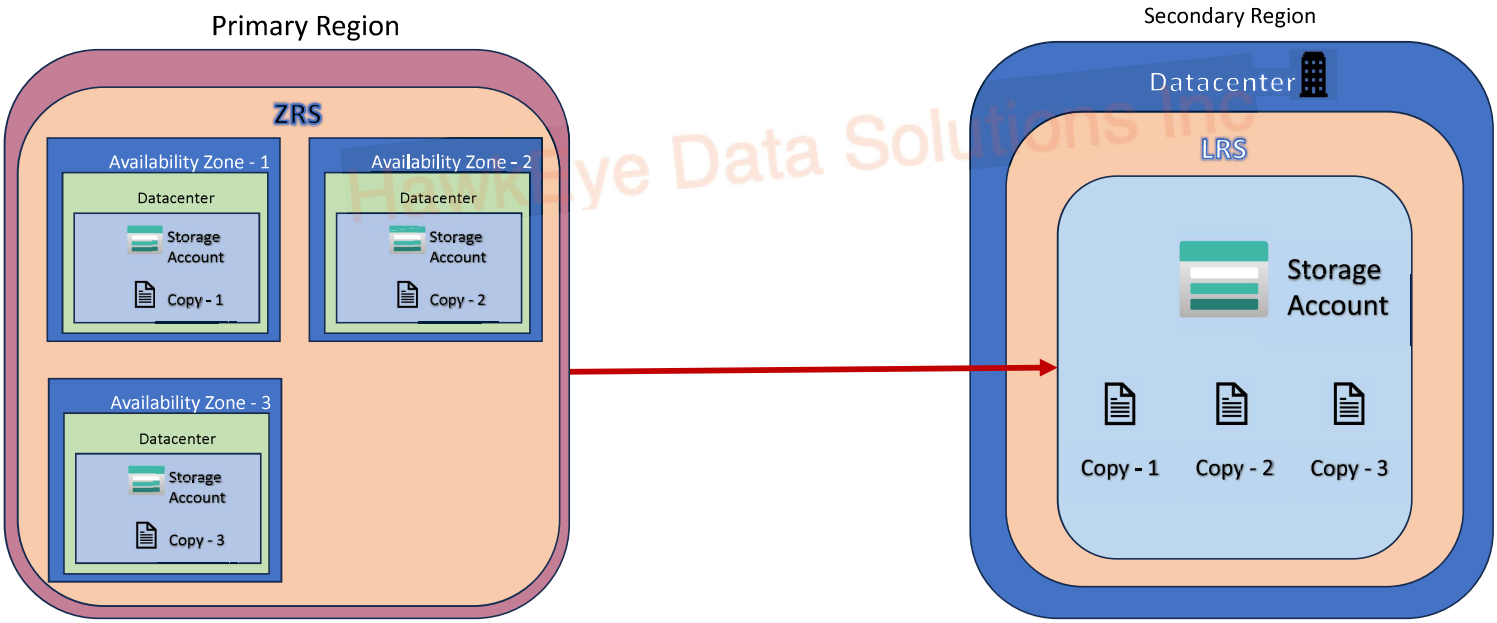
Geo Redundant Storage (GRS)

- ✓ Like running LRS in **two** different regions.
- ✓ Copies the data synchronously in a single physical location in the primary region using LRS. Then asynchronously to a single physical location in the secondary region – region pair.
- ✓ Durability of 16 nines over a given year! (99.99999999999999%) over a given year.
- ✓ Think of it as LRS + LRS!



Geo-Zone-Redundant Storage (GZRS)

- ✓ Copies the data across 3 availability zones in the primary region (ZRS). Then to a secondary region using LRS.
- ✓ Durability of **16 nines** over a given year! (99.99999999999999%) over a given year.
- ✓ Think of it as ZRS + LRS!
- ✓ Provides the maximum durability!



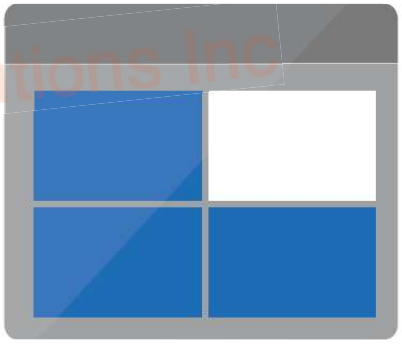
Storage Services - Azure Blobs

Cloud-Based Object Storage offered by Azure – designed to store and manage unstructured data.

Data is stored in the form of objects / blobs – can be a file, image, video, audio, logs, binary data etc.

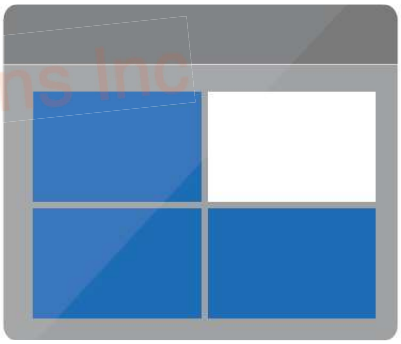
Upload data as blobs, let Azure take care of the physical storage - incredible scalable!

Can be accessed simply by using HTTP/HTTPS and multiple programming languages are supported.



Azure Blob Storage Tiers

- High level idea is to manage costs based on frequency of access & retention period.
- **Hot Access Tier –** Optimized for storing data that's accessed frequently & low-latency is needed (Your Profile Picture)
- **Cool Access Tier –** Optimized for storing data that's accessed infrequently and stored for at least 30 days (Historical data / compliance data)
- **Cold Access Tier –** Optimized for storing data that's access infrequently and stored for at least 90 days!
- **Archive Access Tier –** Best for data that's rarely accessed for at least 180 days with flexible latency needs. Costs the lowest but has the highest costs to rehydrate the data and then access it.



Azure Files

Fully managed file-shares in the cloud accessible via Server Message Block (SMB) or Network File System (NFS) protocols.

Accessible from Windows, MacOS, or Linux clients.

Caching on Windows Servers with Azure File Sync near customers for lower latency is also possible!

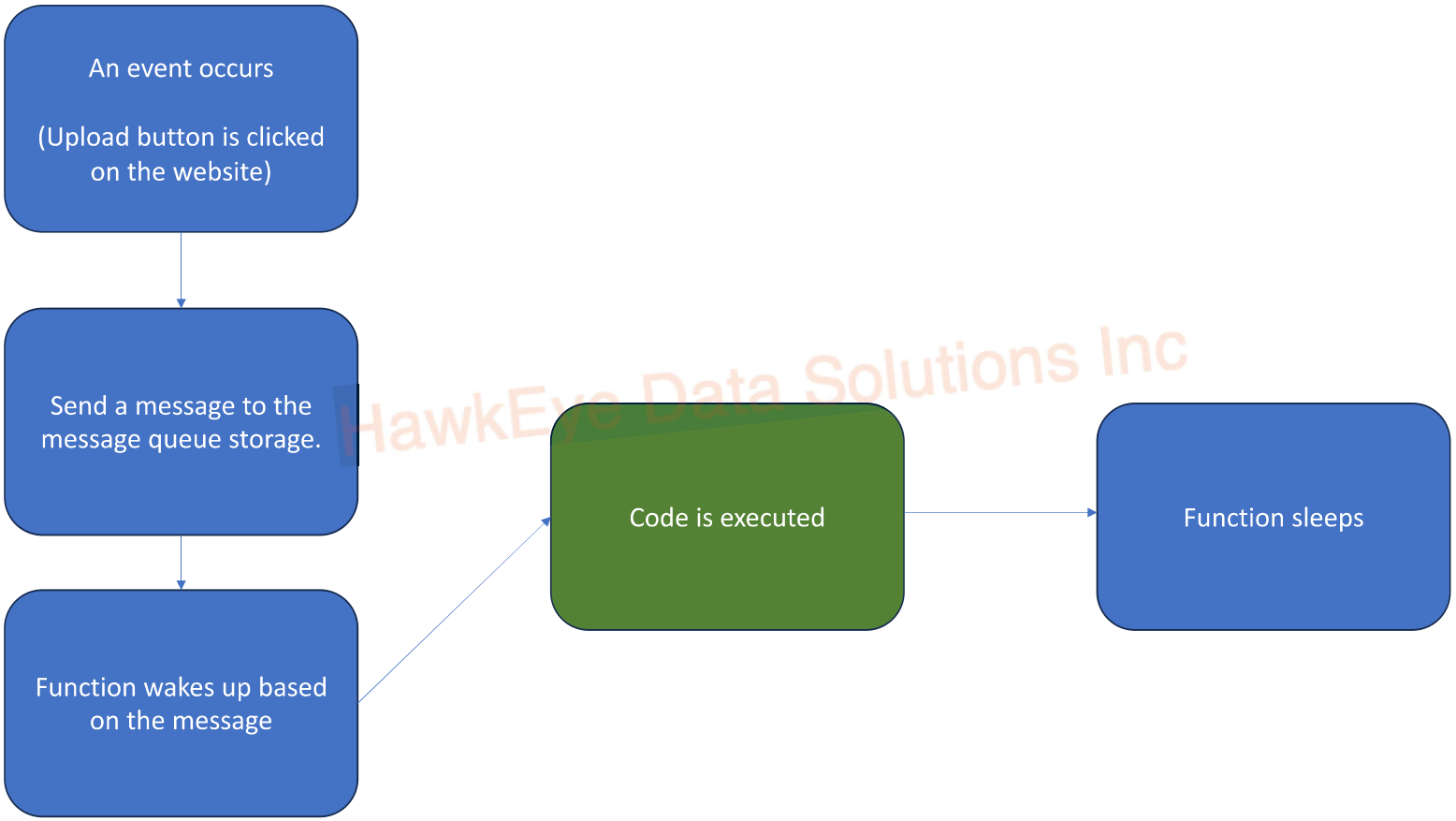
Can be mounted as Network Drives on Windows or Directories on Linux and MacOS to seamlessly access data.

Microsoft will take care of infrastructure, high availability and backups!

Excellent for lift and shift scenarios – can move both app & data to the cloud (classic scenario) or just the data (hybrid scenario)

Azure Queues

- A messaging service that enables async communication & storing large number of messages (backlog).
- Each message can be upto 64KB in sizes, and millions of messages can be stored.
- Messages are stored in the queues until they are processed by the receiving component.
- Helps to decouple different parts of an application, making it more resilient to failures.
- Uses HTTP/HTTPS as the protocols for communication.
- Ability to set Time-To-Live (TTL) for messages – how long a message should remain in queue.

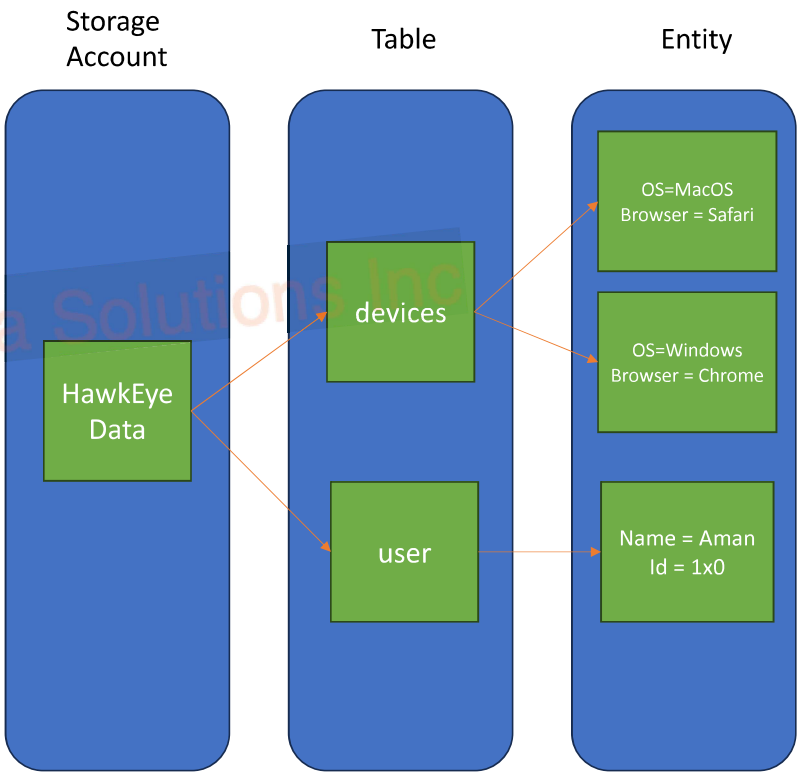


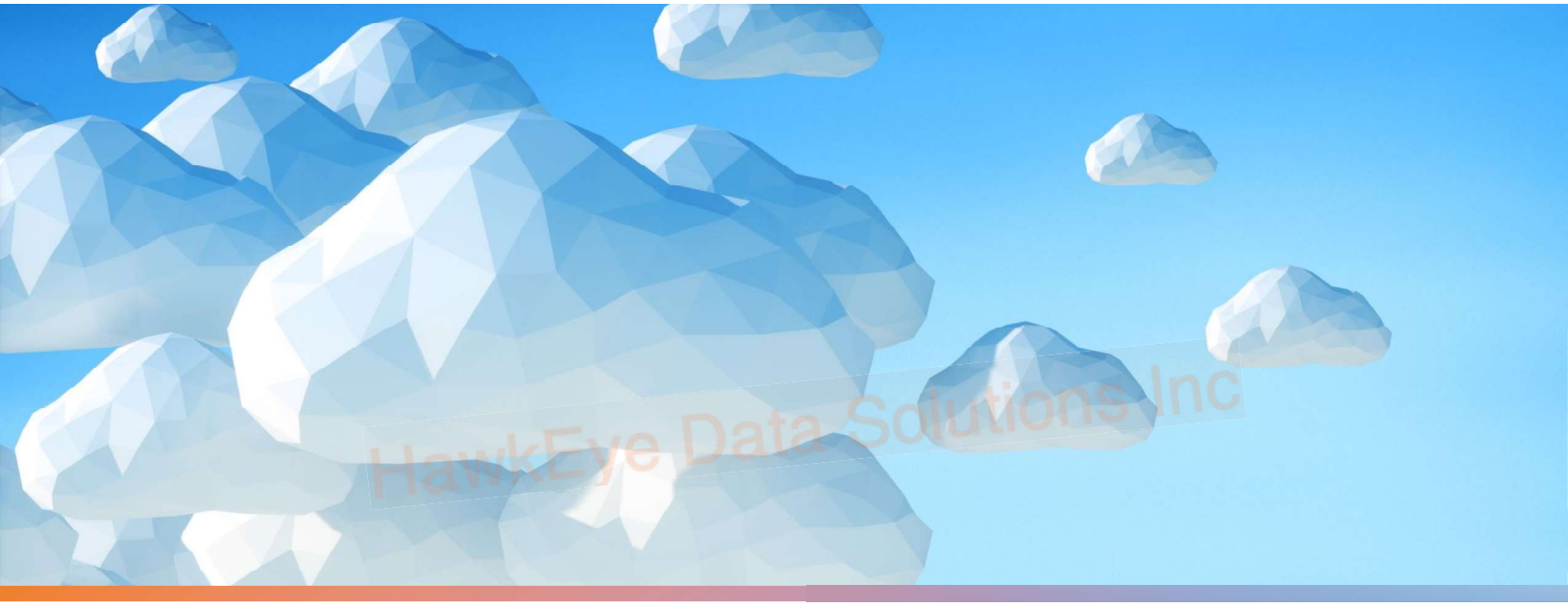
Azure Disks

- The primary means of persistent storage for VMs running on Azure.
- These disks provide the storage capacity needed to store the OS, data, applications etc.
- Wide range of disk sizes to suit storage needs.
- Managed disks are also available that handle storage for you, including replications, backups and availability!

Azure Tables

- Part of the NoSQL family – suitable for storing large amounts of structured & semi-structured data without the need of a fixed schema.
- This is great for quickly changing data requirements & is extremely scalable.
- Data is stored as Key-Value pairs.
- Typically, cheaper than traditional SQL for similar volumes of data.
- Good for storing TBs of structured data that don't need complex joins, fast access etc.
- E.g. – Device data, metadata, user data etc.



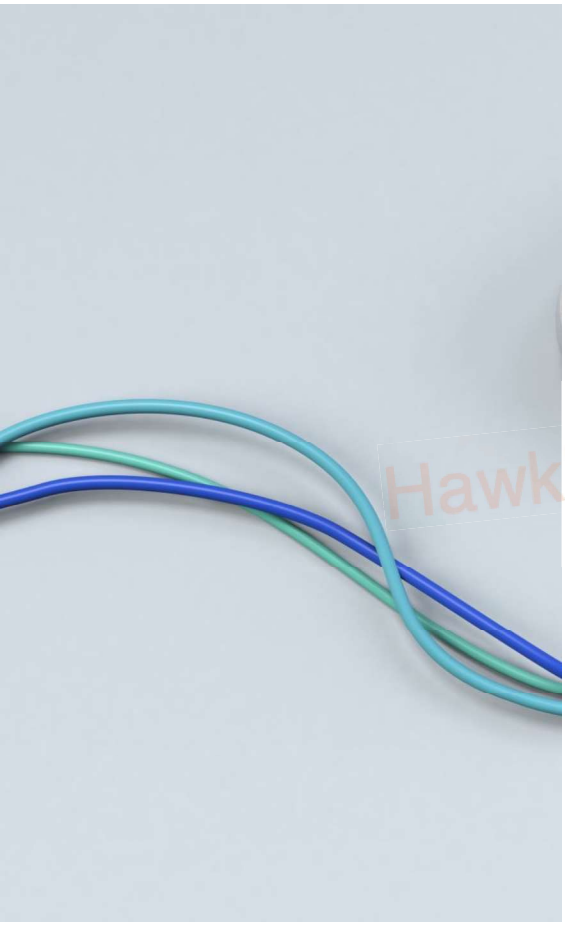


Migration

Process of moving resources & deployments to the cloud

Azure Migrate

- Managed service that helps to migrate from on-prem env. to the cloud – one portal to do it all.
- Range of tools to assess, analyze & then perform the migration.
- **Dependency Mapping** - It provides dependency maps, showing which servers or components are dependent on each other.
- **Right Sizing** - Azure Migrate suggests appropriate Azure VM sizes based on the performance and resource requirements of your on-premises workloads.
- **Compatibility Analysis** - It evaluates the compatibility of your on-premises workloads with Azure, identifying any dependencies, and providing recommendations for migration.

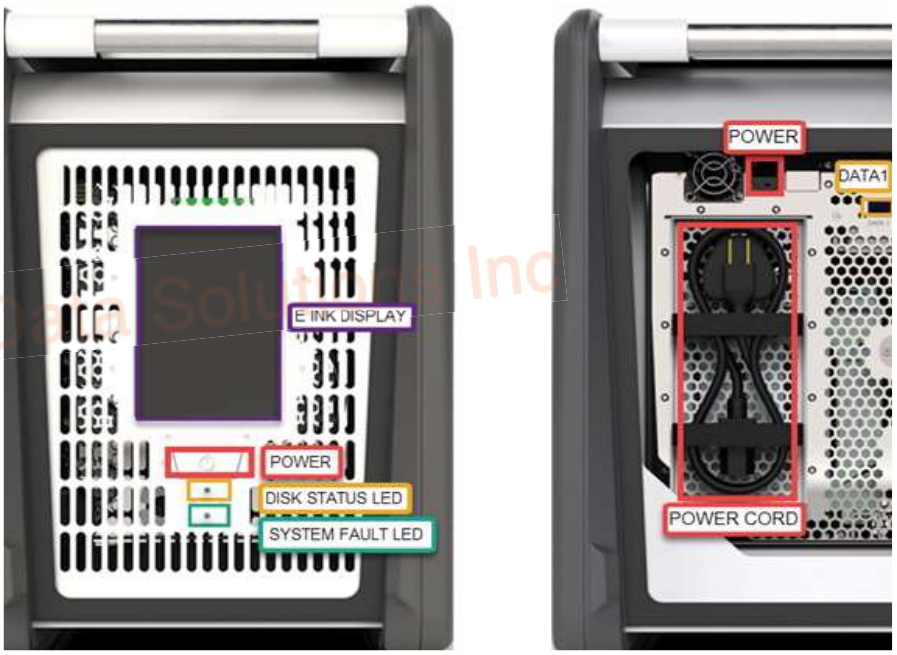


Azure Migrate – Integrated Tools

- Azure Migrate: Discovery & Assessment – Tool to discover and assess on-prem servers running on Hyper-V, VMware before migration.
- Azure Migrate: Server Migration – Tool to migrate servers running on Hyper-V, VMWare and other physical servers to Azure.
- Data Migration Assistant – Tool to assess SQL servers & identify problems beforehand that can affect migration, new features & if anything is unsupported.
- Azure Database Migration Assistant – Tool to migrate on-prem databases to Azure SQL, or VMs running SQL.
- Azure Web App Migration

Azure Data Box!

- Proprietary storage solution to ship data in and out of Azure (~<50lbs)
- Capacity of 80TB & shipped to your datacenter.
- Can be used to copy data into it, or from it in an inexpensive and reliable fashion.
- Addresses challenges related to transferring large amounts of data over the internet, which can be slow and costly.
- Great for one-time migrations (ideally >=40TB), disaster recovery (periodic backups), multi-cloud scenarios!
- Data on Azure Data Box devices is encrypted, ensuring data security during transit.



Source: https://learn.microsoft.com/en-us/azure/databox/media/data-box-overview/data-box-combined.png

AzCopy

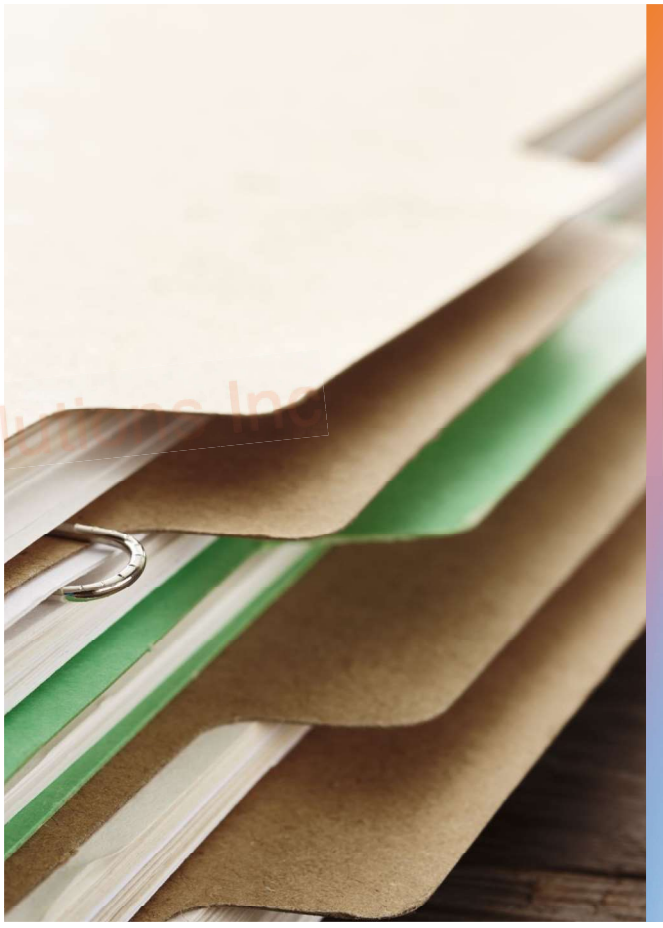
- Command-line tool provided by Microsoft for efficiently copying and transferring data to and from Azure Blob Storage, Azure Files, and Azure Data Lake Storage & even sync data.
- Can be used to move data to and from other cloud providers too!
- Syncs are uni-directional. Specify source & destination & let it sync.
- CLI tool - Suitable for scripting, automation, and integration with other applications and workflows.

Azure Storage Explorer

- Offers a Graphical User Interface (GUI) that simplifies the management of Azure Blob Storage, Azure Queue Storage, Azure Table Storage, Azure Files, and Azure Data Lake Storage.
- Upload to Azure , download from Azure, move data between accounts.
- Available on multiple OS – MacOS, Windows, Linux
- Uses AzCopy behind the scenes!
- Supports connecting to multiple Azure subscriptions and storage accounts simultaneously, streamlining management for organizations with multiple accounts.

Azure File Sync

- Offers a convenient way to centralize files shares in Azure while keeping the benefits of a Windows File Share!
- Windows Server can create a local cache.
- Azure File Sync supports multi-site synchronization, making it suitable for organizations with distributed offices or branch locations.
- Setup FileSync on Windows Server -> bi-directionally synced with files.
- Configure Cloud Tiering – replicated more imp. files locally & less imp. sit in Azure.
- Multiple protocols – SMB, NFS, FTPS

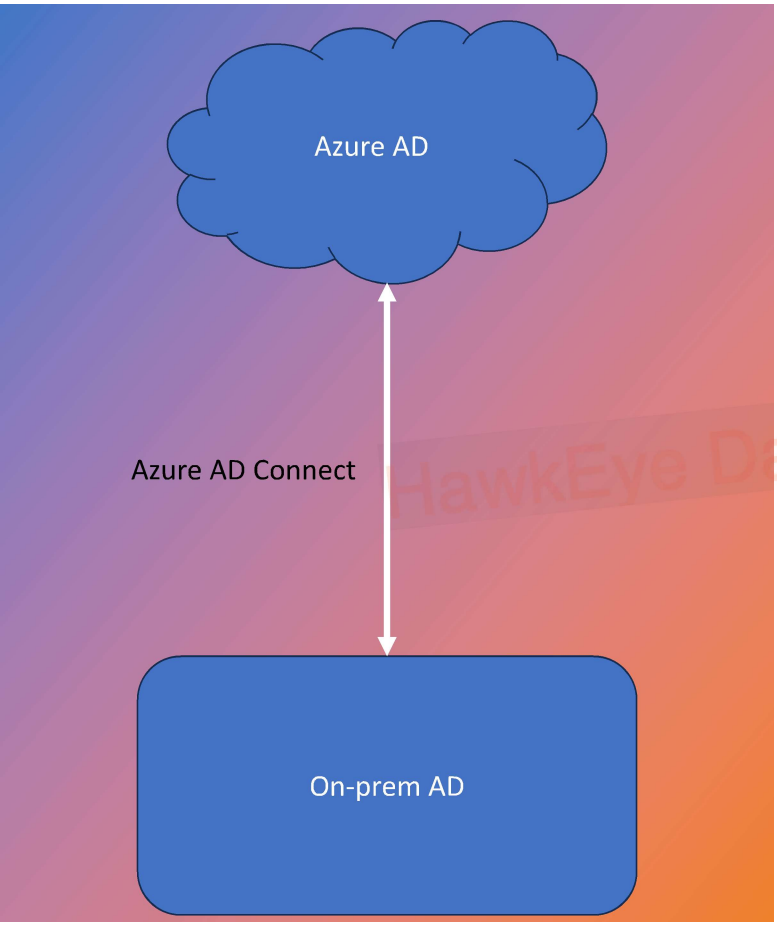


Azure Active Directory (AD)

- ✓ Cloud-based identity and access management service. Like having your very own digital passport office in the cloud. It's the place where you get your digital identity documents and access to all your online services.
- ✓ Serves as the foundation for secure authentication, authorization, and management of users, devices, and applications in the Microsoft Azure cloud environment.
- ✓ All about managing who has access to what in your organization's digital environment, including users, devices, and applications.

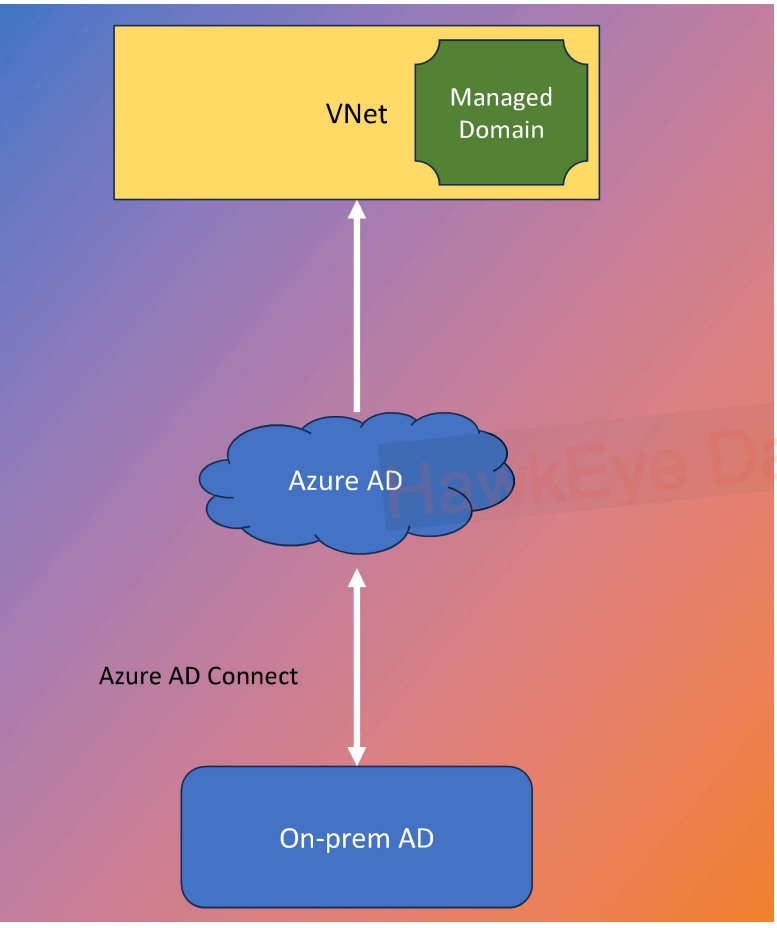
Azure Active Directory (AD) – Key Points

- ✓ **Single Sign-On (SSO)** - Azure AD enables users to sign in once with their credentials and then access multiple applications and resources without needing to sign in separately for each one. Delete 1 identity upon quitting!
- ✓ **Cloud Identity and Hybrid Scenarios** - Azure AD supports cloud-only identities, but it also seamlessly integrates with on-premises Active Directory in hybrid setups, allowing you to leverage existing infrastructure.
- ✓ **User Authentication** - It provides secure authentication methods, including username and password, multi-factor authentication (MFA), and device-based authentication.
- ✓ **Device Management** - Azure AD helps manage and secure devices used by your organization, whether they are corporate-owned or employee-owned (BYOD) – Microsoft Intune + device-based conditional access.
- ✓ **Application Access Control** - You can use Azure AD to control who can access specific applications and services, ensuring that only authorized users can use them.
- ✓ **Role-Based Access Control (RBAC)** - It enables assigning roles and permissions to users and groups, controlling what they can do within Azure and other integrated services.
- ✓ **Application Integration** - You can integrate Azure AD with thousands of third-party applications for secure and streamlined access.



Azure Active Directory + Active Directory (On-Prem)

- ✓ Yes, connecting the two is possible.
- ✓ Without this separate identity sets would need to be maintained but now we can sync the two.
- ✓ Use Azure AD Connect.
- ✓ Use MFA, SSO with both deployments!



Azure Active Directory Domain Service (DS)

1. **Same Key, New Places**: With Azure AD DS, you can use your office key (your username and password) to unlock doors on the internet. So, you don't need a new key for online stuff.

2. **Office Rules Apply**: The same rules and settings that keep your computer safe at the office also apply online. It's like having the same lock on your office door and your internet accounts.

3. **Easy Connections**: You can connect your work computer to the internet (like a cloud computer) and still use your office key to access files and apps, just like you do at the office.

4. **Extra Security**: It makes sure your key works safely online by using special codes and protections.

5. **No New Keys**: You don't need to remember new usernames and passwords for internet stuff. Your office key works everywhere.

6. Simply use AD without supporting the infrastructure it needs.

7. Great for moving legacy apps to the cloud that need modern authentication but can't support it!

8. Supports LDAP, group policies, Kerberos authentication.

Azure Authentication Services

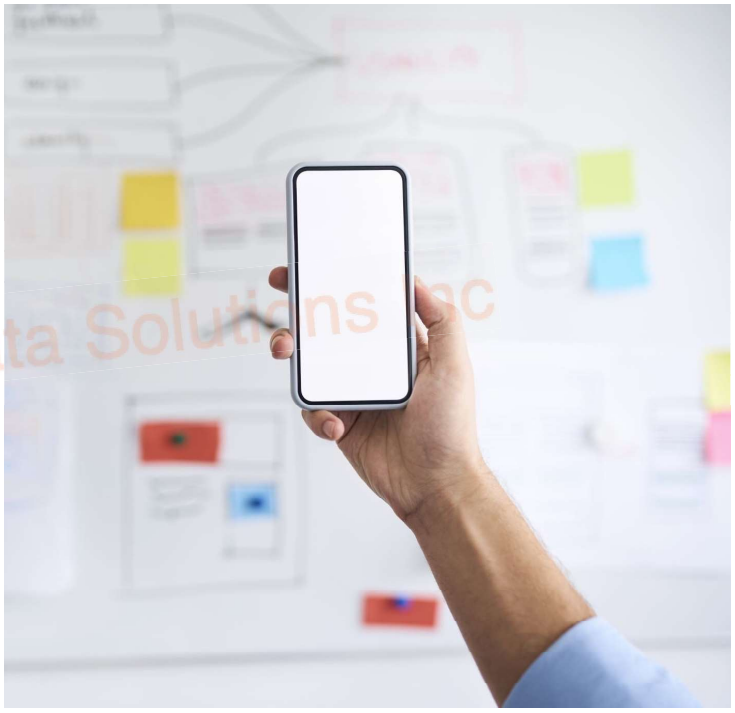
1. Process of establishing the identity of a device, person or service.
2. Proving who you say you are.
3. Passwordless, MFA, SSO.
4. Trade-off between security & convenience for the longest time.

Single-Sign On (SSO)

- ✓ Service offered by Microsoft Azure that simplifies and streamlines the process of signing in to multiple applications and services
- ✓ One set of credentials to access multiple services/applications.
- ✓ These apps and services must trust the initial authenticator.
- ✓ Increased productivity as users can access multiple applications seamlessly without the hassle of repeated sign-ins.
- ✓ Improves the user experience by reducing the number of credentials users need to remember, leading to fewer password-related issues.
- ✓ User leaves -> delete all credentials (tracking is hard). Similarly, granting access by mistake or extra privilege is common.

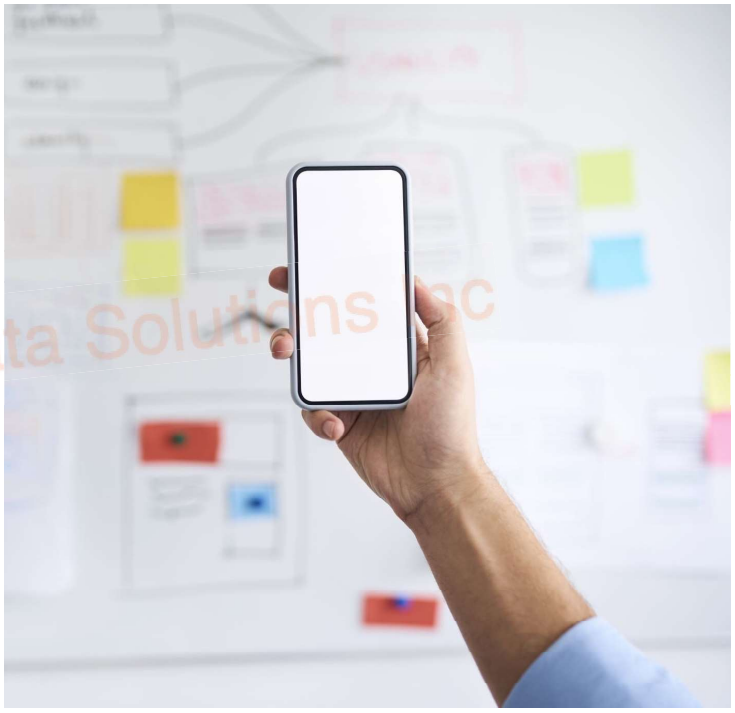
Multi-Factor Authentication (MFA)

- ✓ What if password gets leaked? Single point of failure.
- ✓ Adds an extra layer of defence – OTP (One time passcode) is an example.
- ✓ 3 categories :
  - Something you know – OTP, passphrase, security key, security question
  - Something you have.- Mobile Phone, Security Key
  - Something you are – Biometrics like facial scan, fingerprint etc.
- ✓ Malicious users would need password + one of the three above to get authorised.



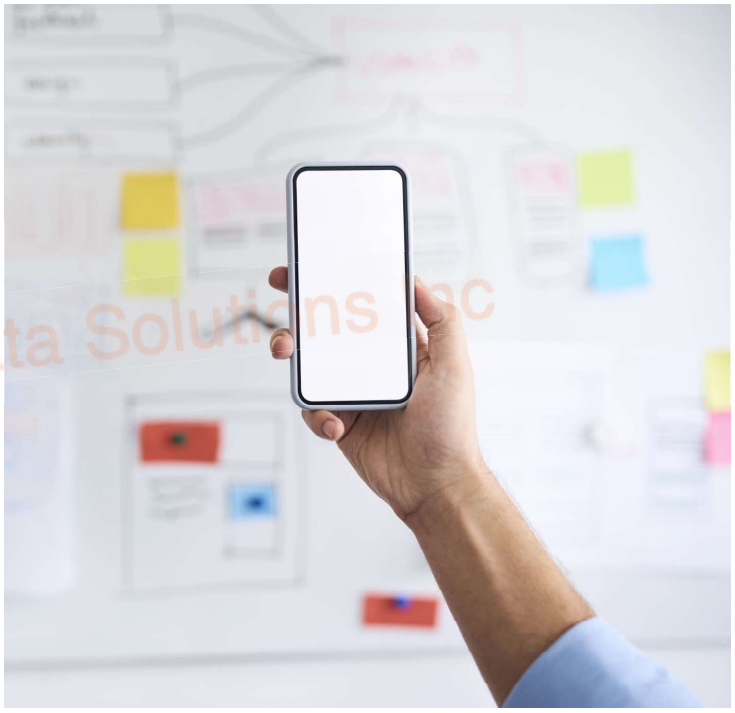
Azure Passwordless

- ✓ Alternative to traditional password + MFA combo – can get frustrating.
- ✓ Needs to be setup on a device for it to be used.
- ✓ E.g. – Enroll your mobile phone -> Azure knows who you are -> Authenticate with FaceID / Fingerprint -> Good to go!
- ✓ 3 options!



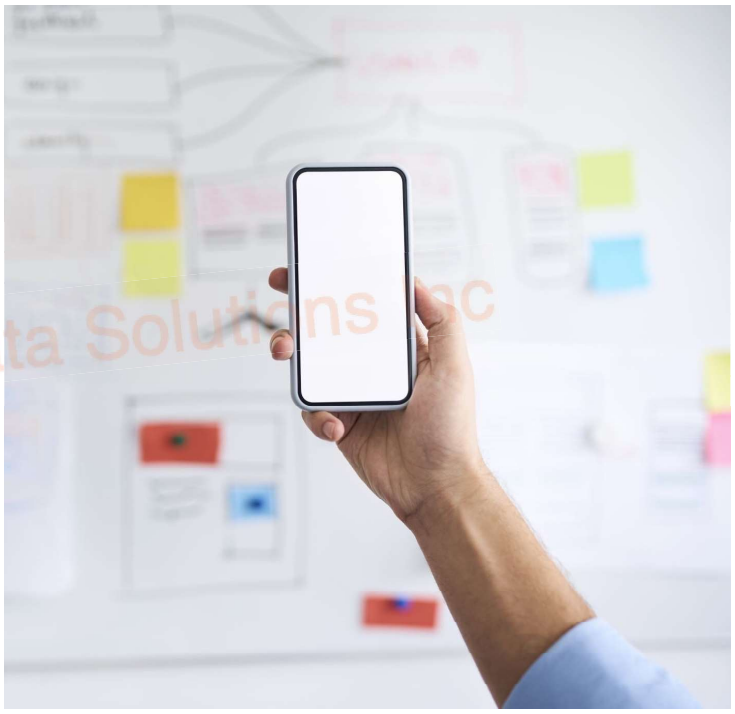
Windows Hello!

- ✓ Great if you have a company issued PC.
- ✓ Azure knows who you are using that PC.
- ✓ Authenticate using a pin, face recognition -> good to go!
- ✓ In-built SSO support!



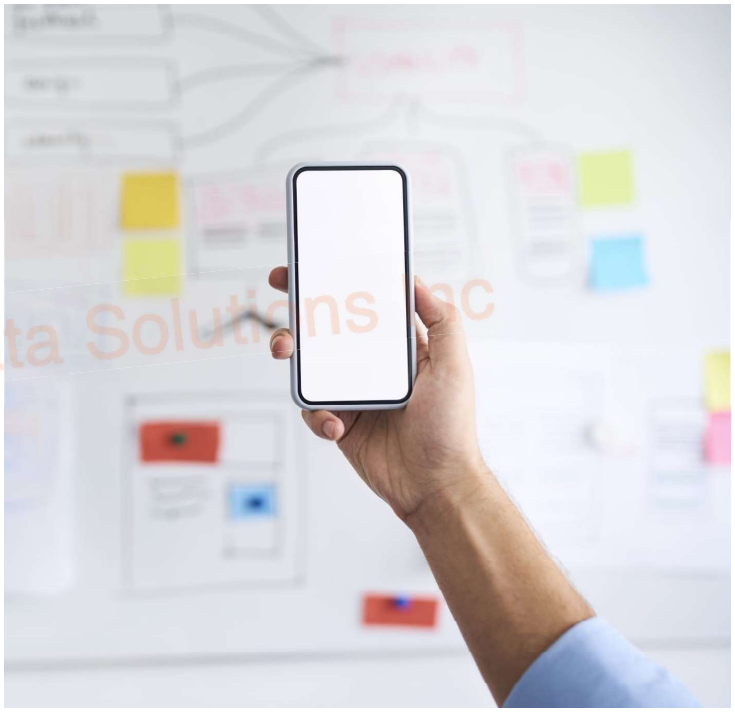
Microsoft Authenticator App

- ✓ Very common option especially for BYOD enrolled mobiles!
- ✓ ‘Approve login request’ & choose a number.
- ✓ FaceID / Biometric like fingerprint to login!
- ✓ No chances of password leaks!



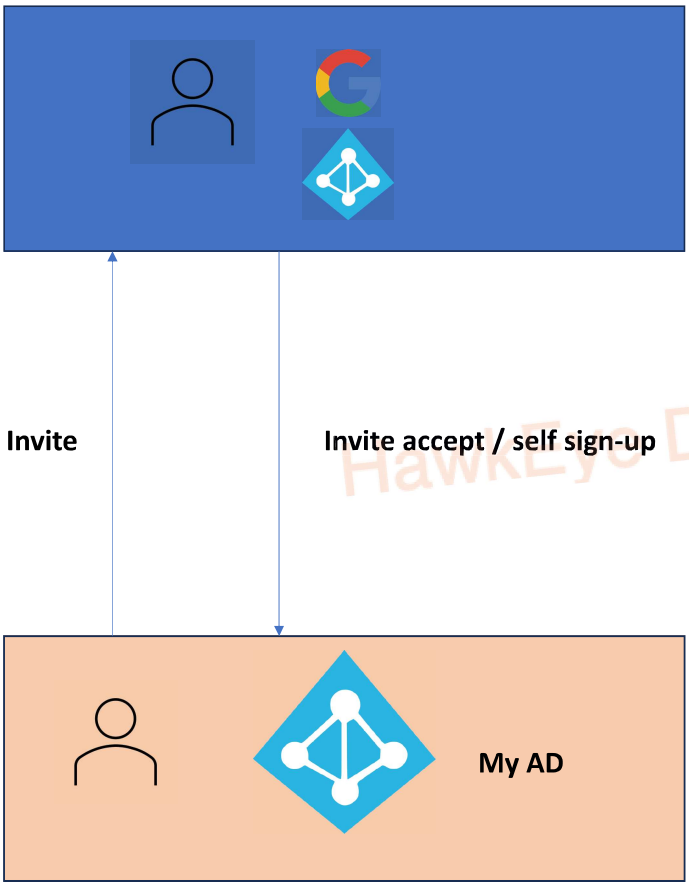
FIDO2 (Fast Identity Online)

- ✓ Incorporates the Web Authentication standard (WebAuthn).
- ✓ Use security key baked into a device.
- ✓ Mostly USB but NFC, Bluetooth also very common.
- ✓ Again no password that can be leaked!



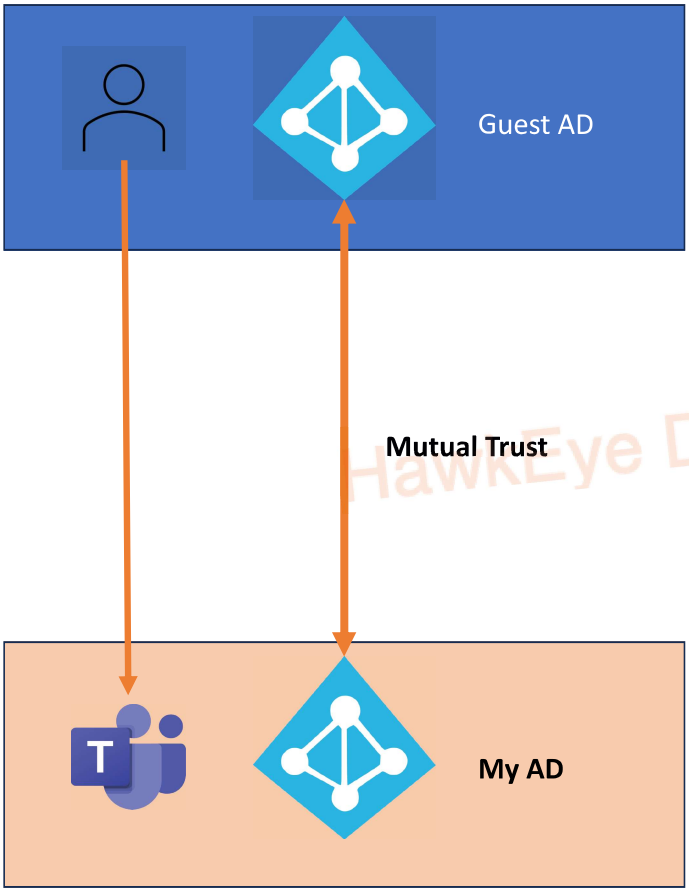
External Identities & Guests in Azure

- ✓ Concept of allowing users who are not part of your organization's primary Azure Active Directory (Azure AD) to access and collaborate on your Azure resources and applications.
- ✓ Essential for scenarios where you need to include partners, vendors, customers, or external collaborators in your Azure environment.
- ✓ Secured restricted access to resources!



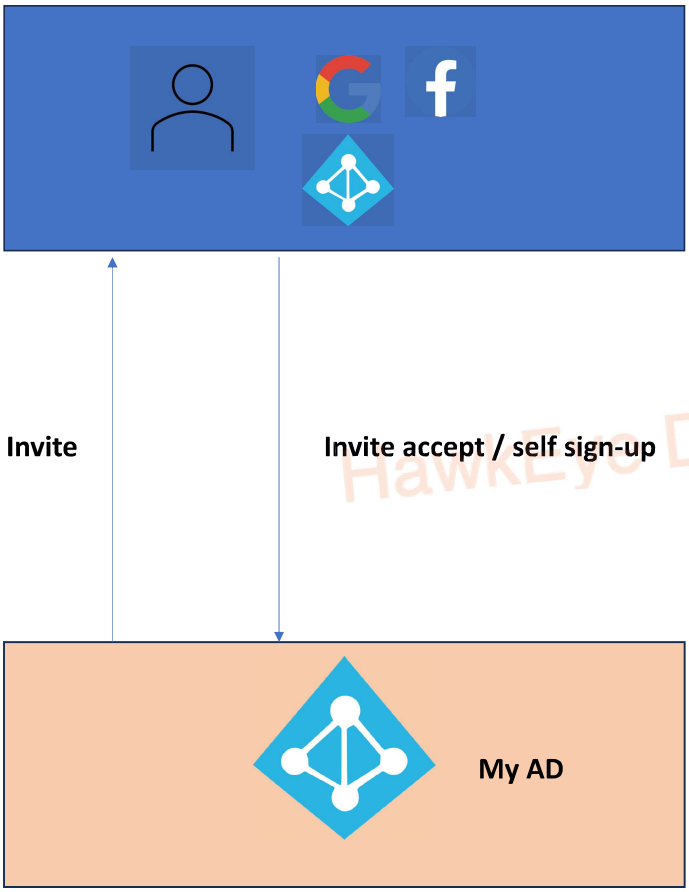
Business 2 Business (B2B)

- ✓Partners can use their own credentials to access your Azure resources.
- ✓Can be invitation based or self-service sign up!
- ✓Users appear as guests users in your directory.



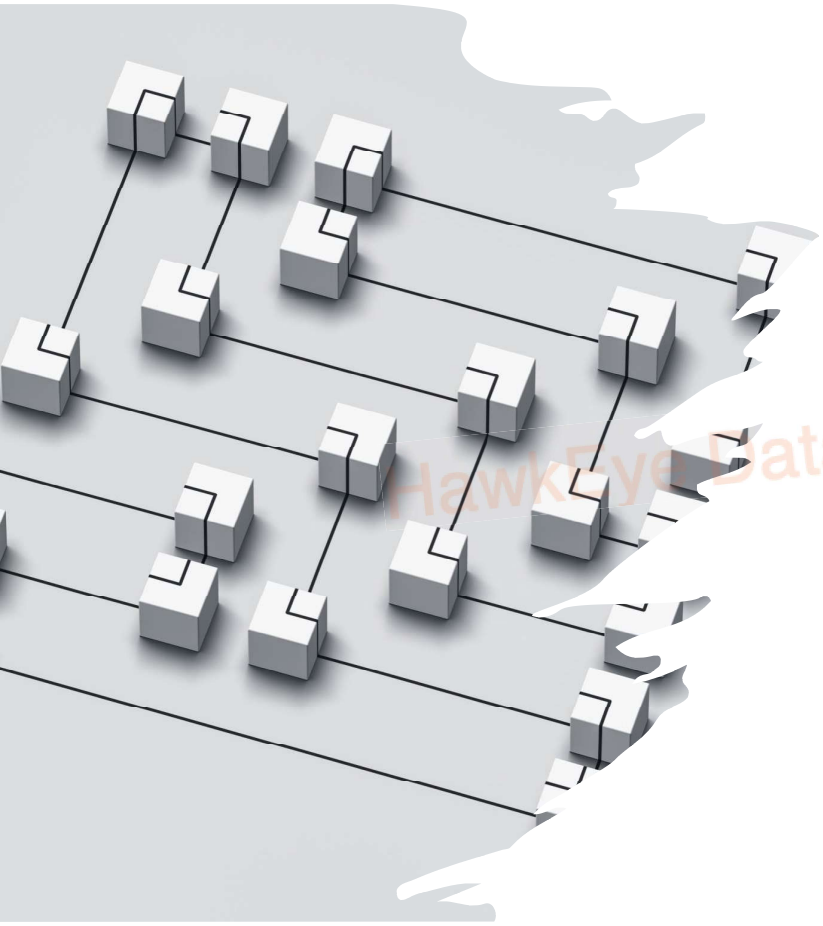
Business 2 Business (B2B) Direct Connect

- ✓Mutual Trust Relationship with another Azure AD organization.
- ✓Presently works with MS Teams shared channels.
- ✓Access shared Teams instance from home credentials itself!
- ✓Users not represented as guests but can view them in this shared Teams channel.



Business 2 Consumer (B2C)

- ✓ Designed for customer-facing applications, where you need to manage and authenticate many external users or customers. Designed for customer identity and access management.
- ✓ Allows customizing the sign-in and registration experience.
- ✓ Supports identity providers like social media logins (e.g., Facebook, Google).
- ✓ Ideal for scenarios involving e-commerce, online services, or applications with a broad customer base.
- ✓ Provides features like self-service password reset and multi-factor authentication for consumer accounts.



Conditional Access

- ✓ Like having a security gatekeeper in the cloud who's also your tech-savvy friend - helps keep your digital world safe while making sure you have easy and secure access
- ✓ Enhances security – ensures that the right users have the right level of access to Azure resources and applications, while also considering factors like device health and location.
- ✓ Policies can be based on various signals - user identity, device status, location, application sensitivity etc. E.g., enforce multi-factor authentication (MFA) only for users accessing sensitive applications from outside the corporate network / block requests from unusual locations.
- ✓ Conditional Access allows you to define access controls, such as requiring multi-factor authentication, blocking access, granting access with limited access rights, or requiring password changes.
- ✓ One of the most common use cases is enforcing MFA, which adds an extra layer of security by requiring users to provide two or more forms of verification during sign-in.
- ✓ You can set policies to ensure that devices meet specific security and compliance standards before granting access. This is especially important for BYOD (Bring Your Own Device) scenarios.

Azure RBAC

- RBAC (Role-Based Access Control) is like giving people different keys to open different doors in a building. Each key (role) has a specific set of permissions.
- For example, some keys can open any door (Owner), while others can only open certain rooms (Contributor), and some can only look through the windows without opening any doors (Reader).
- RBAC helps you control who can do what with your Azure resources, making sure people have the right access to do their job, but nothing more (least privilege).
- Fundamental component of Azure's identity and access management system. It allows organizations to manage and control access to Azure resources by assigning specific roles and permissions to users, groups, and applications. Enforced through Resource Manager (CLI, Portal etc.)