Introduction to IaaS best practices

IaaS Best Practice Checklist

RUDRA PRODUCTS & SERVICES

01. VM Access

Control network access using firewall or NSG.
Implement RBAC controls for user access to VM

02. Protection against malware

You should install antimalware protection to help identify and remove viruses, spyware, and other malicious software.

03. Periodic updates

Use the Update Management solution in Azure Automation to manage operating system updates for your Windows and Linux computers

04. Monitor VM's security

Security Center can actively monitor for threats, and potential threats are exposed in security alerts.

05. Encrypt VM's disk

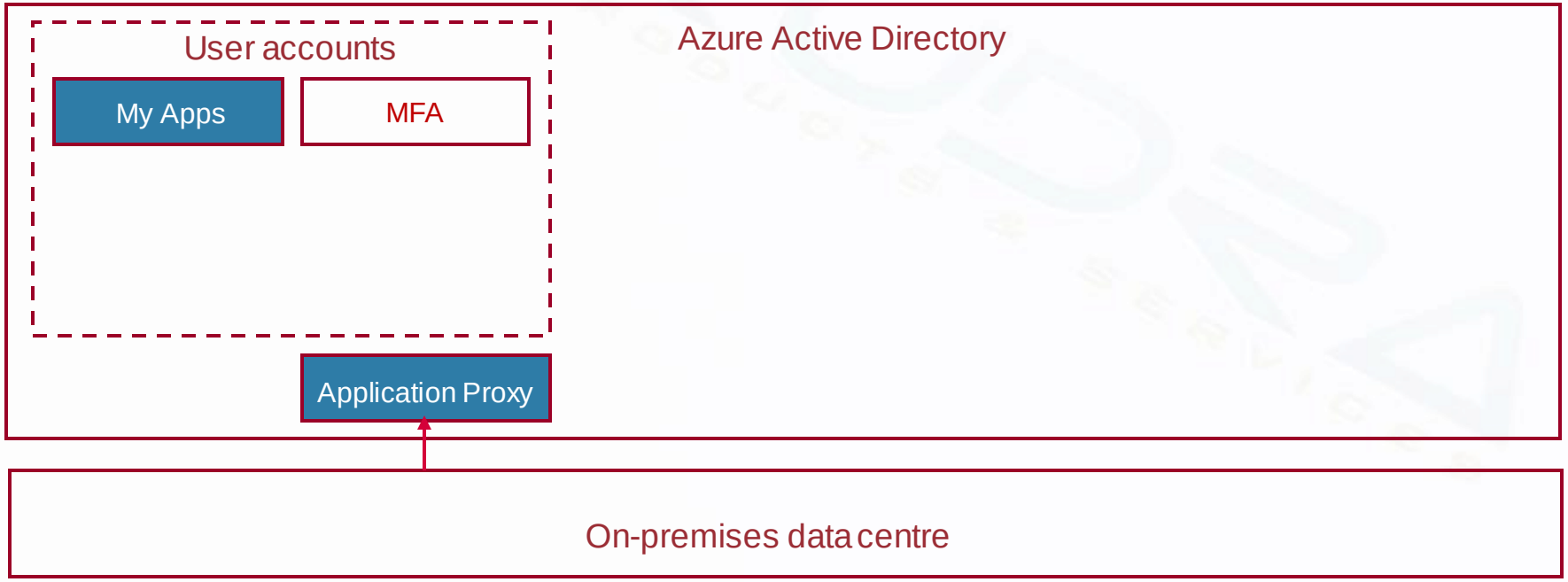
Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks.

Step by step implementation of Azure Security Controls

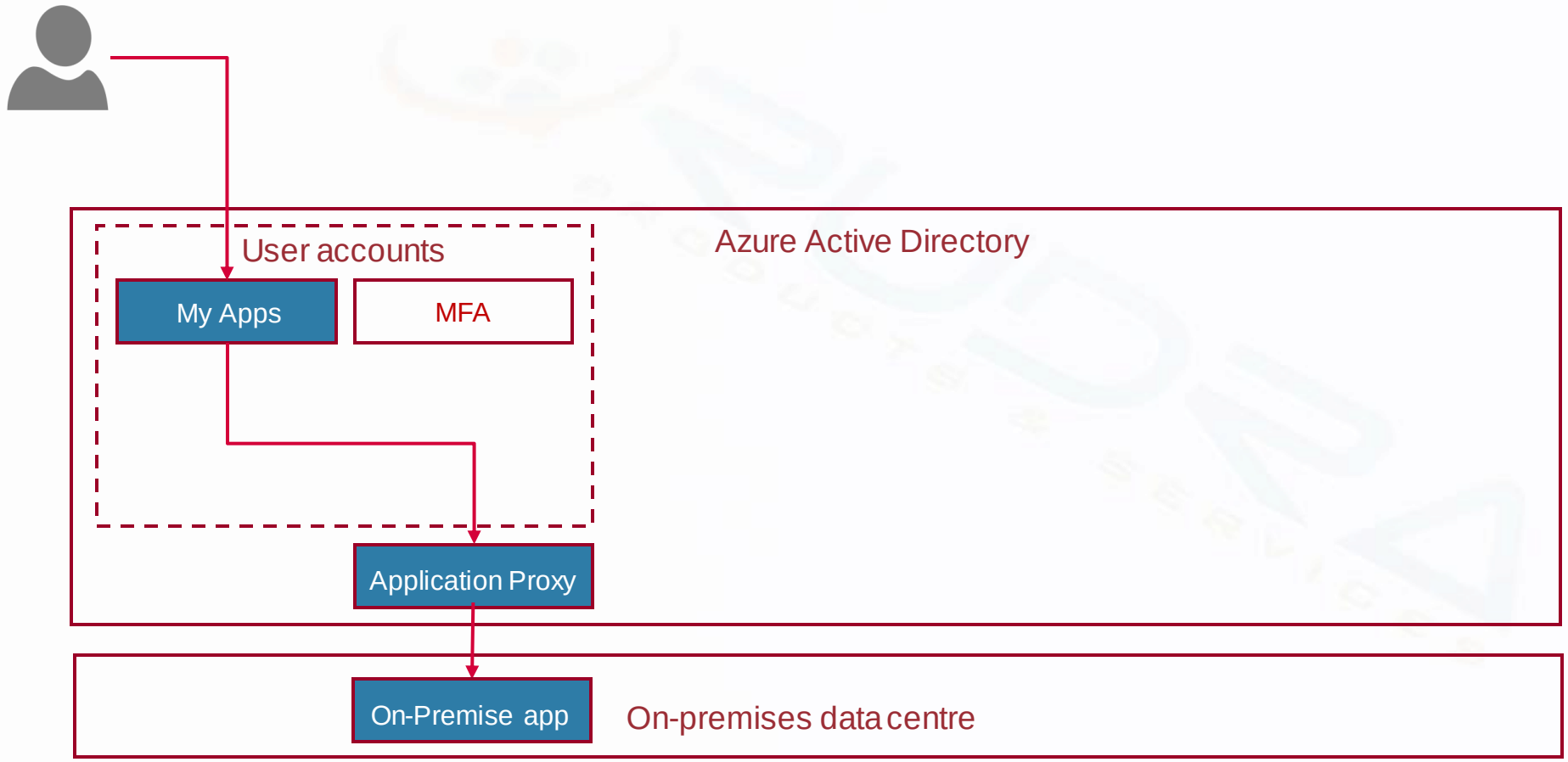
Step 1 – Manage user accounts

Step 2 – My Apps portal password reset, MFA and groups configuration

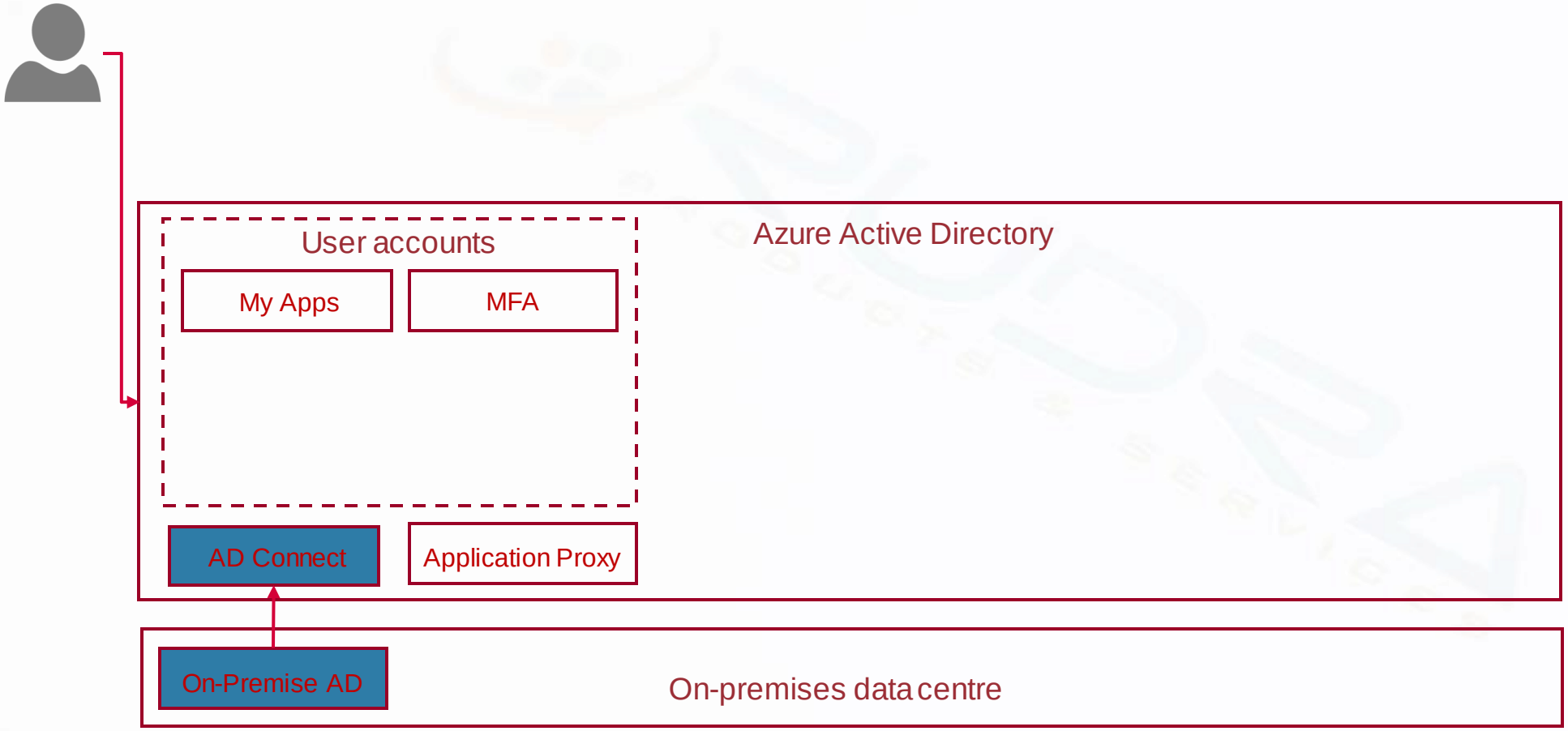
Step 3 – Publish an On-premise app into MyApps portal



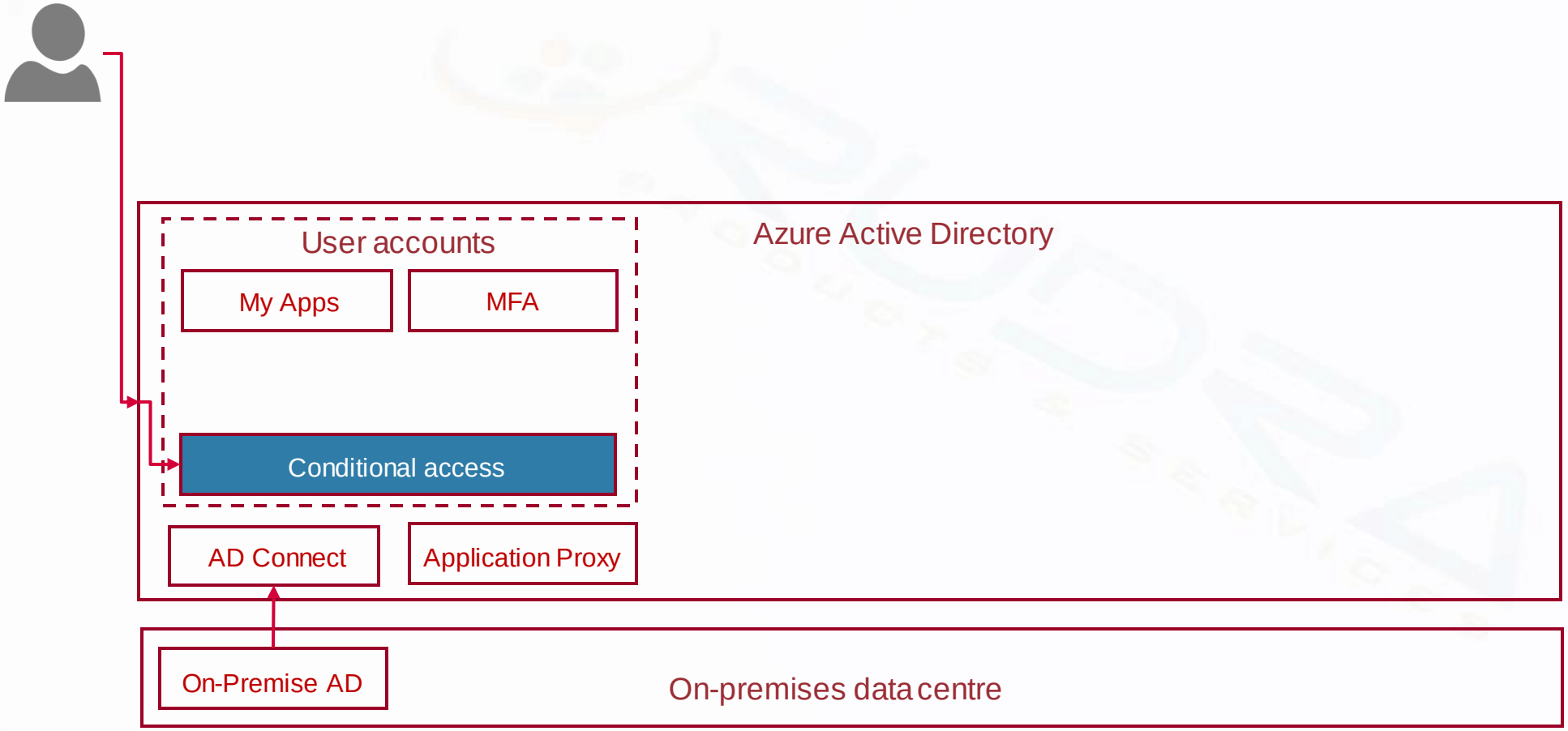
Step 4 – Enable Password based SSO for an on-premise app



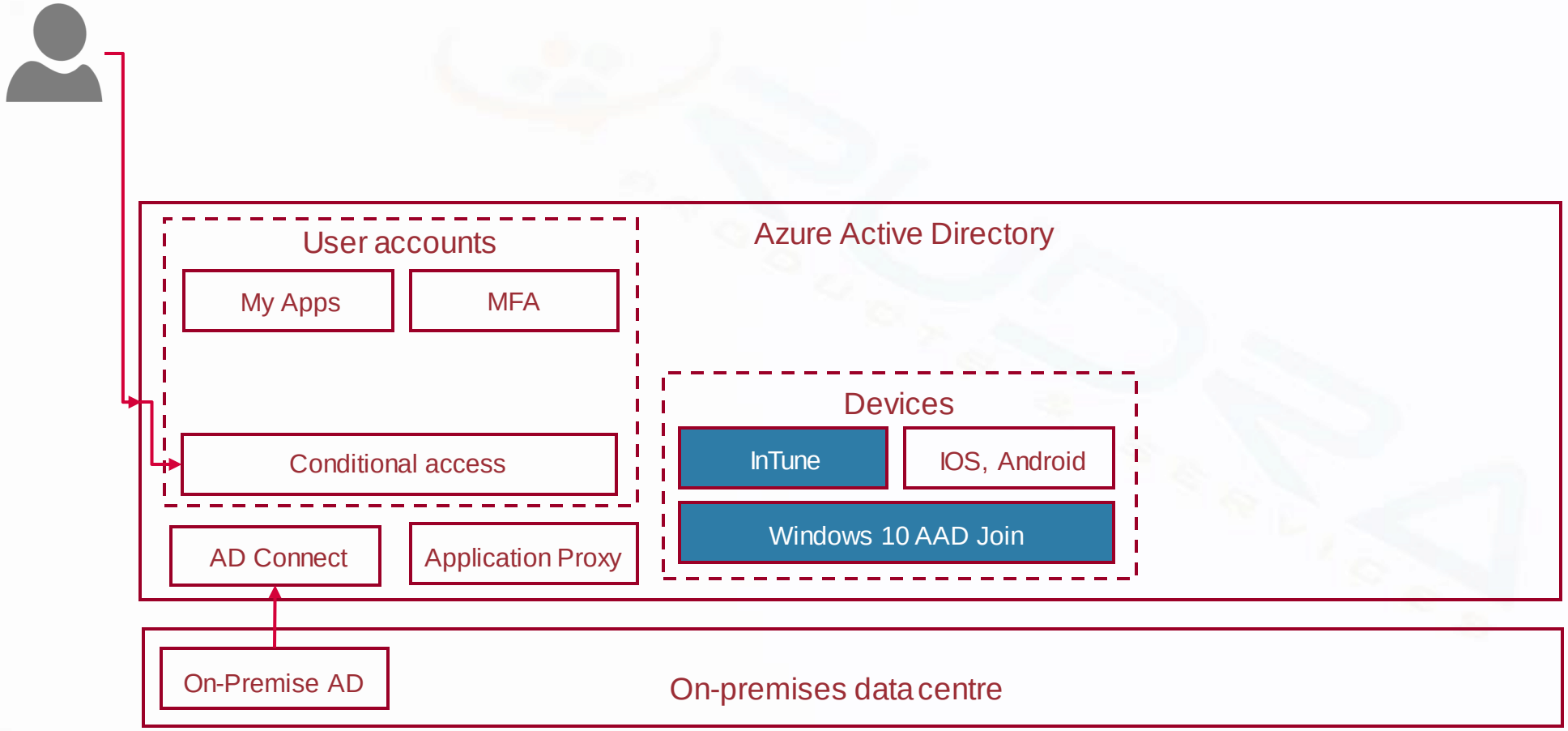
Step 5 – Synchronise users from On-premise AD into AAD



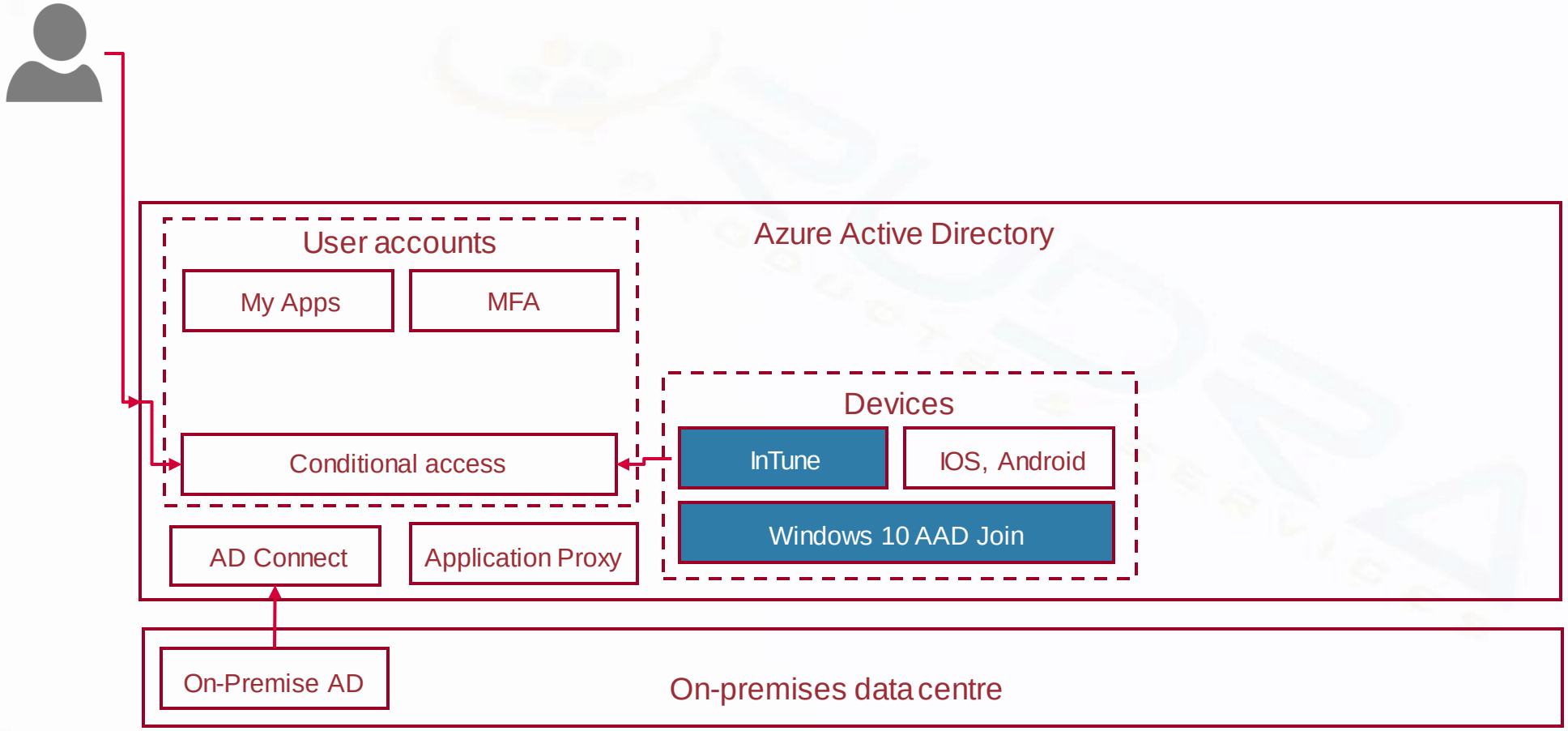
Step 6 – Implement location based conditional access policy



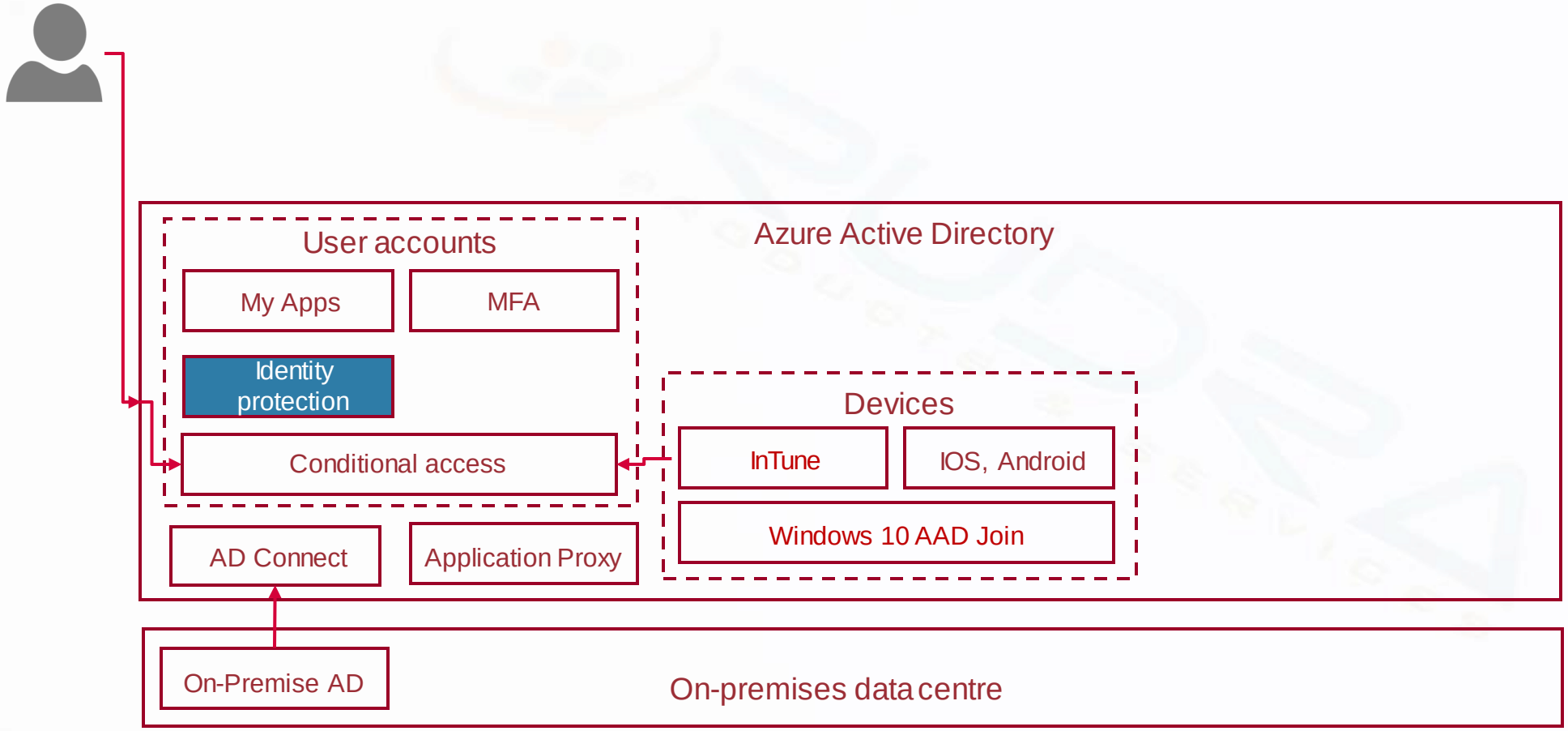
Step 7 – AAD join a Windows 10 device and enrol into Intune



Step 8 – Implement device based conditional access



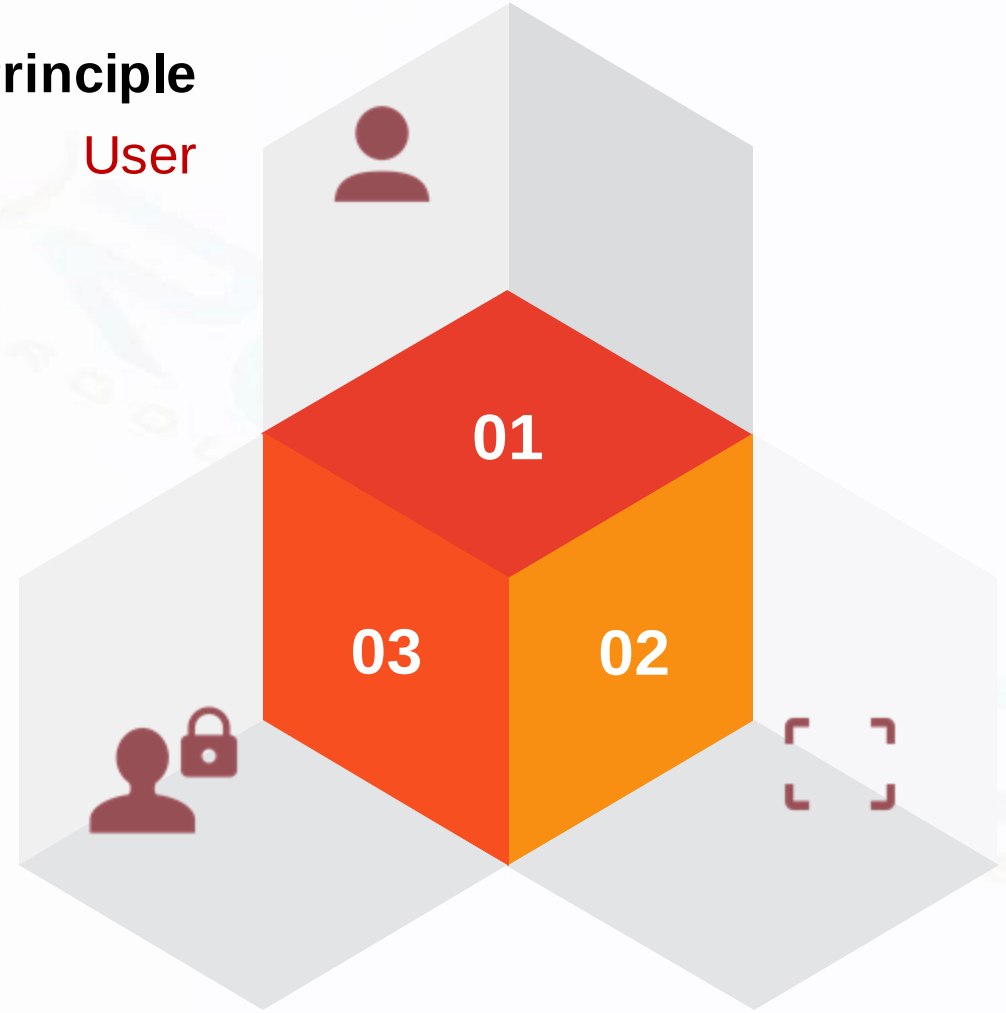
Step 8a – Implement AAD Identity protection



Step 9 – Built in roles, Role assignment and Creation of custom role

Security Principle

User



Role definition

Built in Role
Custom Role

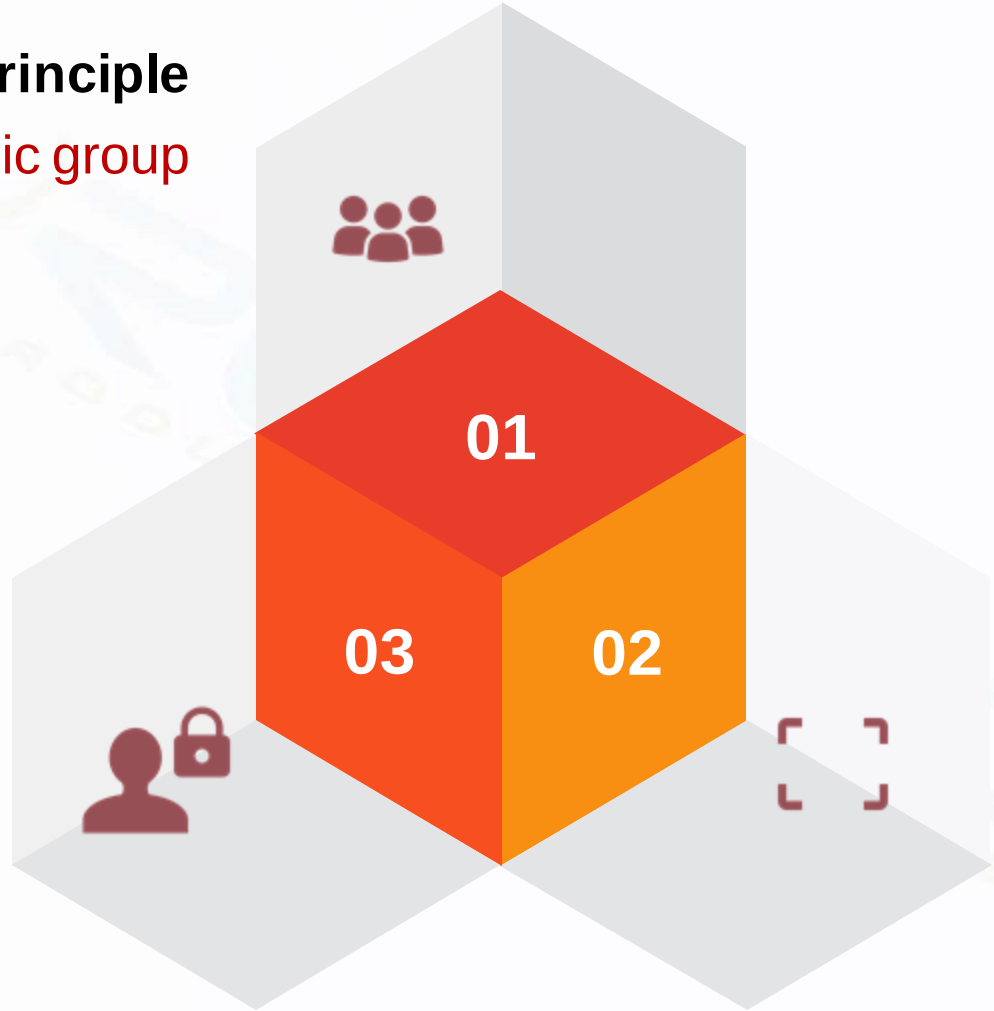
Scope

Subscription
Storage account

Step 10 – Dynamic group creation and role assignment

Security Principle

Dynamic group



Role definition

Built in Role

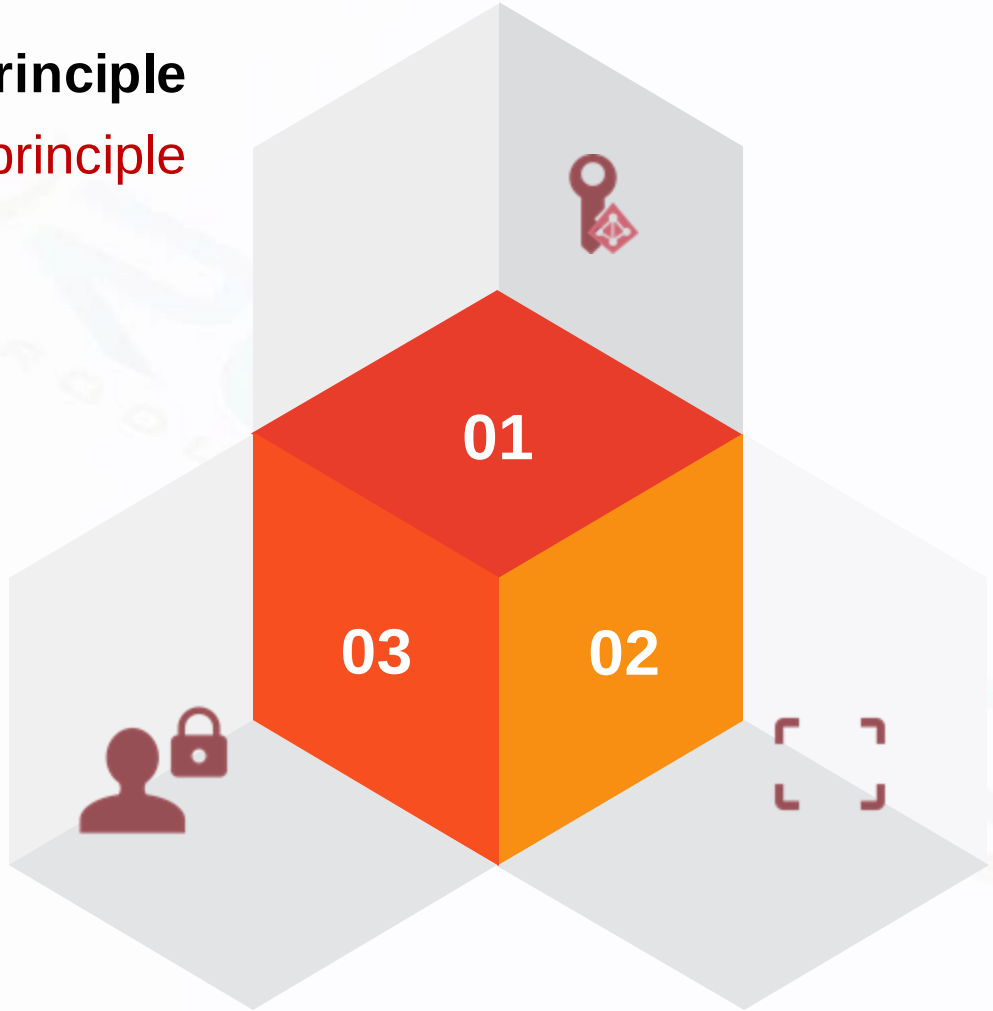
Scope

Storage account

Step 11 – Service principle creation and role assignment

Security Principle

Service principle



Role definition

Built in Role

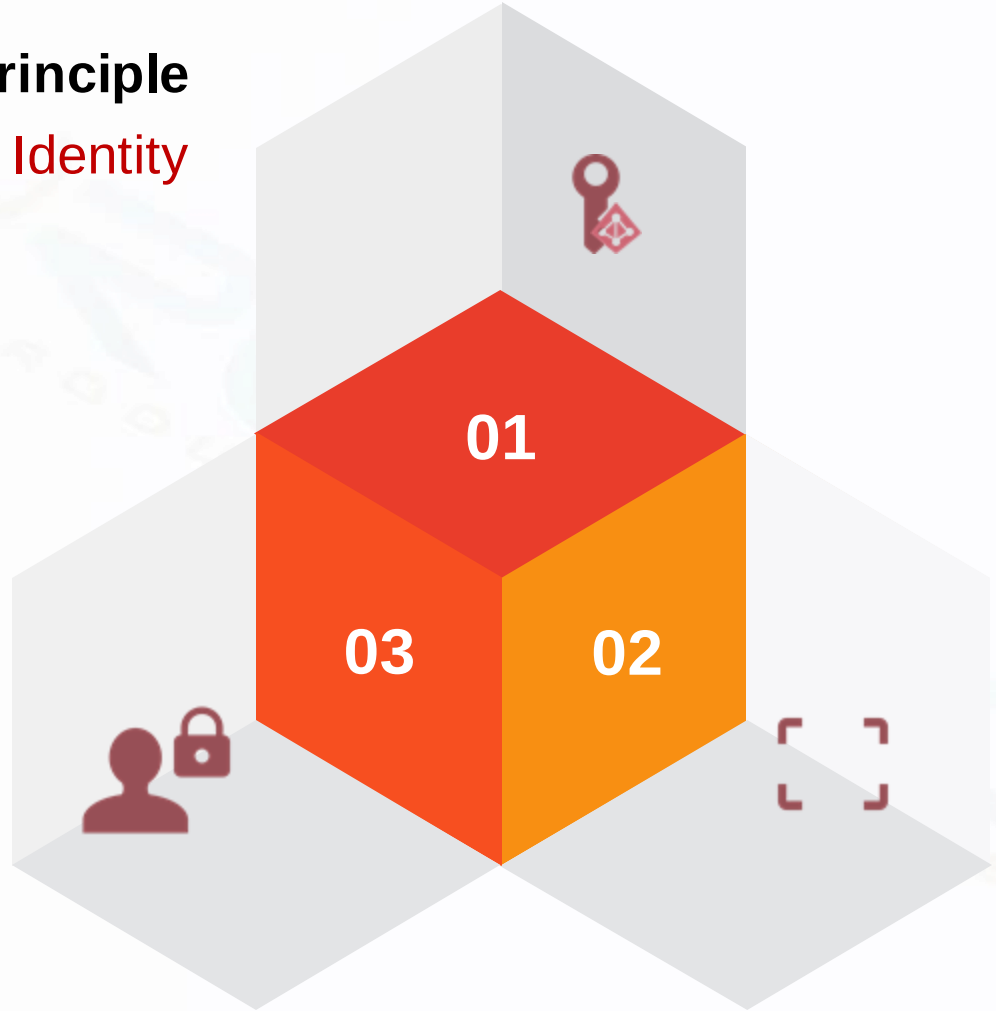
Scope

Storage account

Step 12 – Managed identity creation and role assignment

Security Principle

Managed Identity



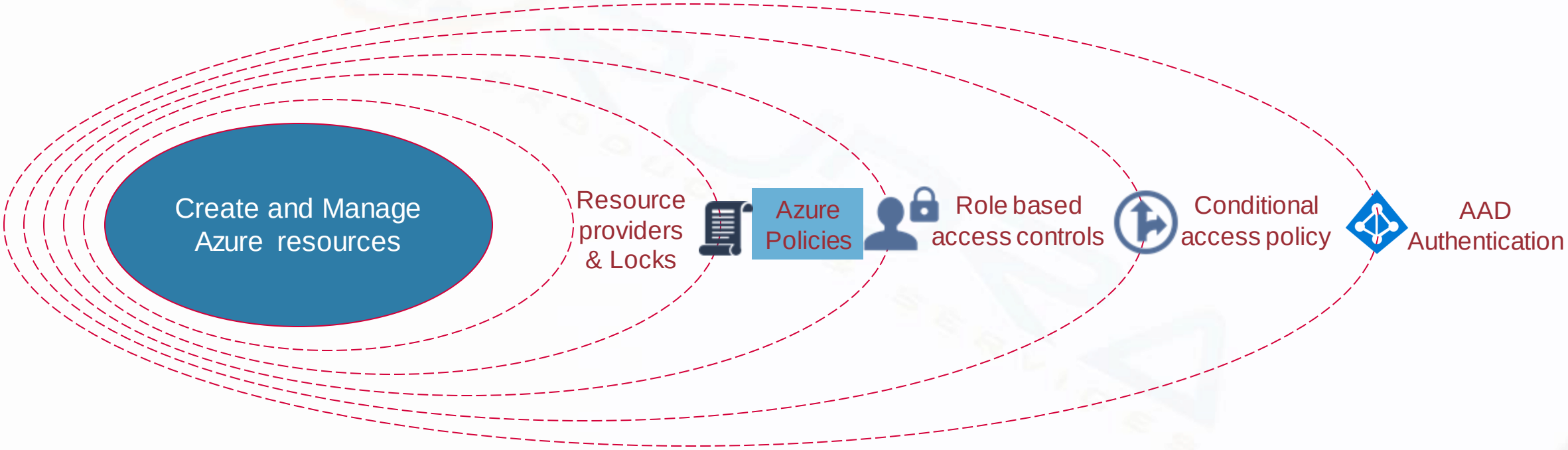
Role definition

Built in Role

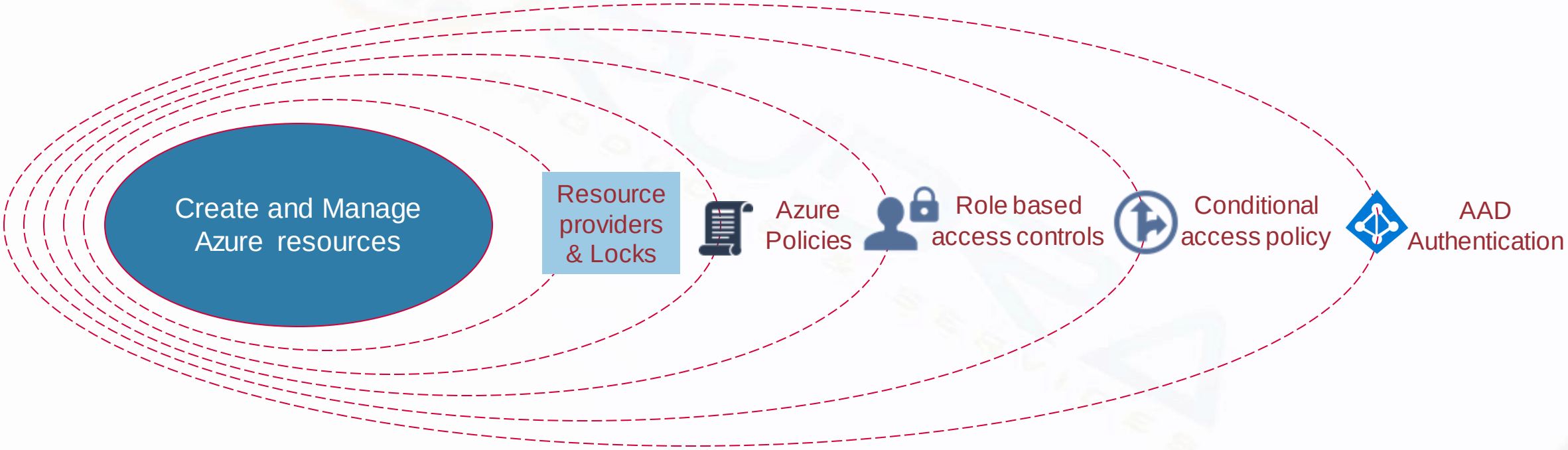
Scope

Storage account

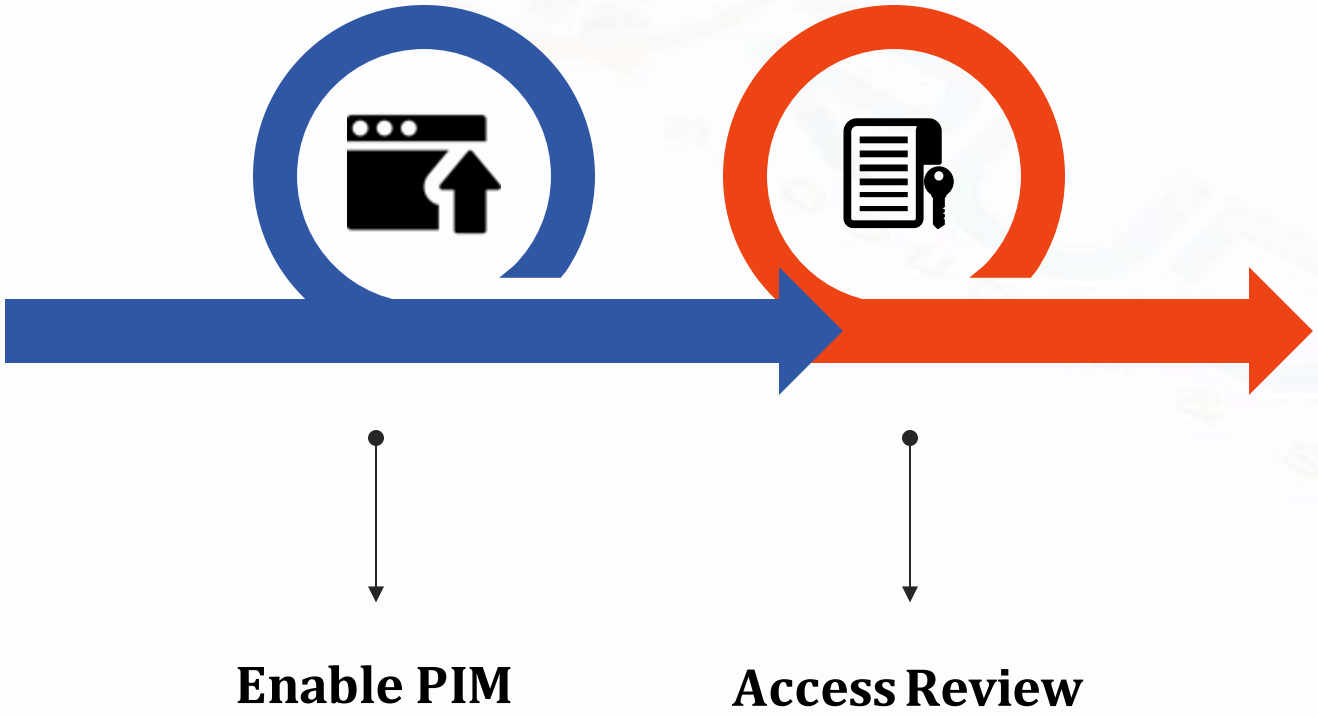
Step 13 – Implement Azure policies



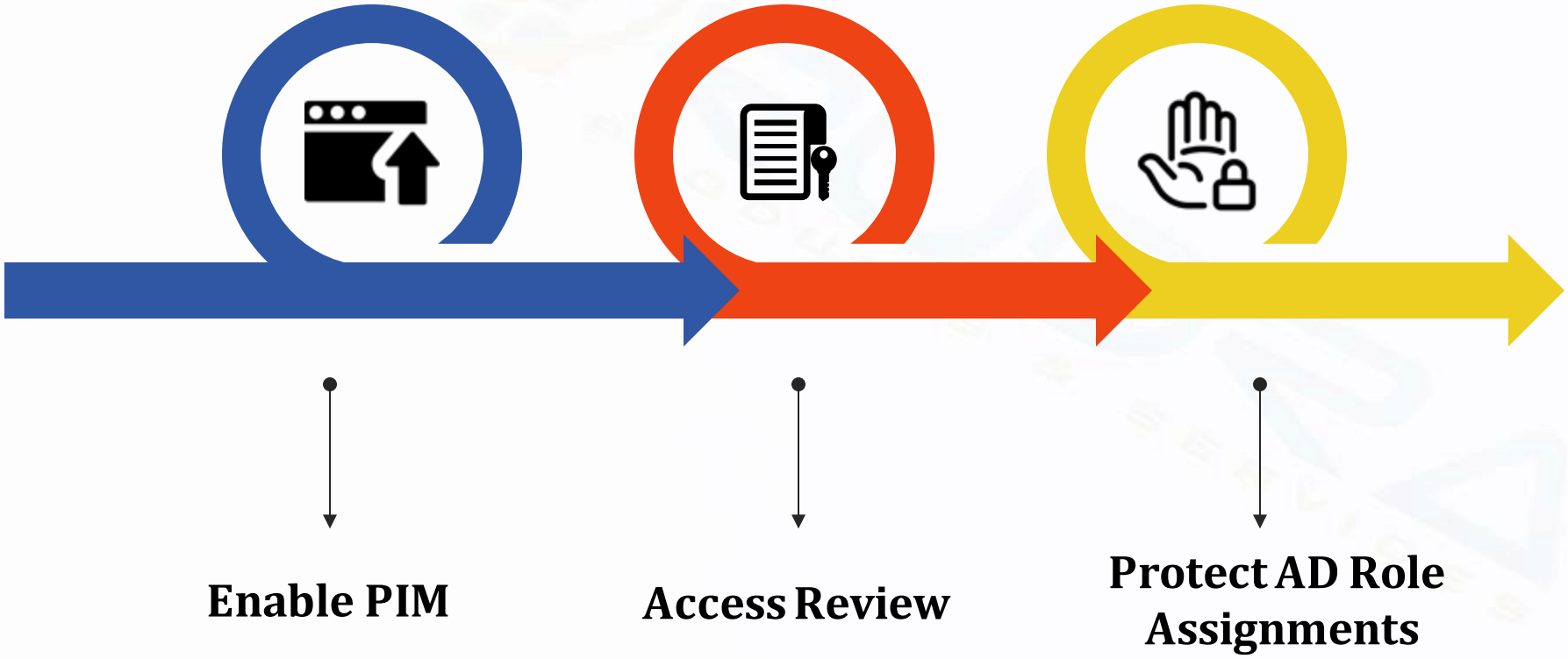
Step 14 – Resource providers & locks



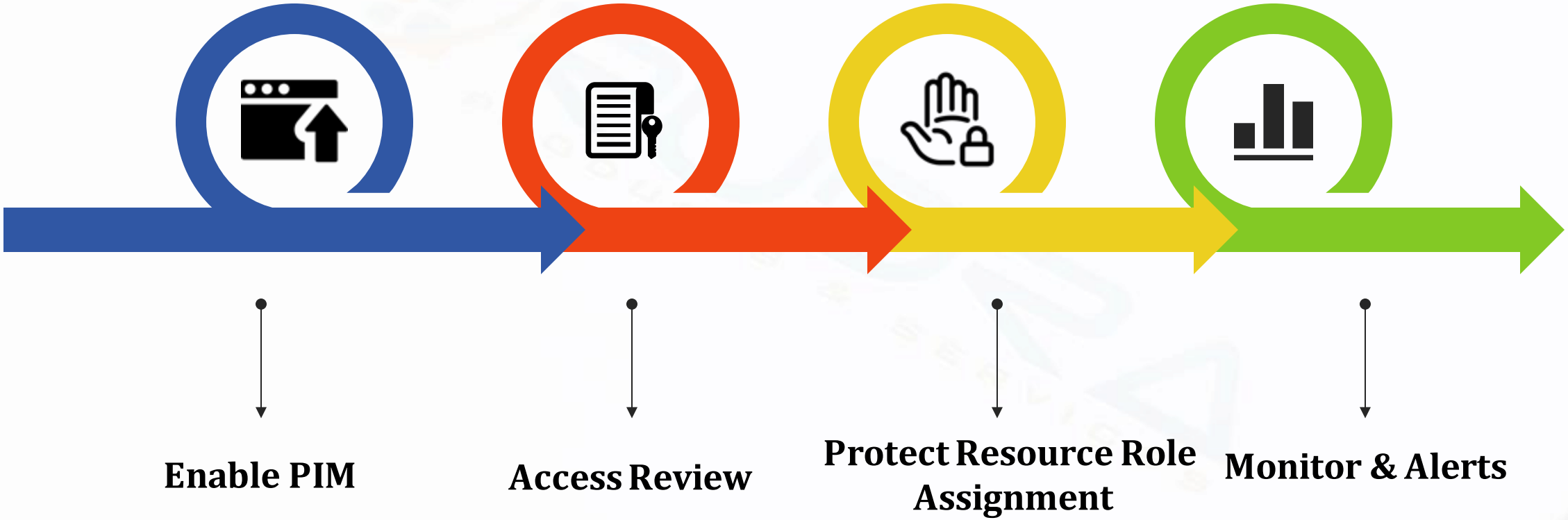
Step 15 – Initiate PIM and conduct access review



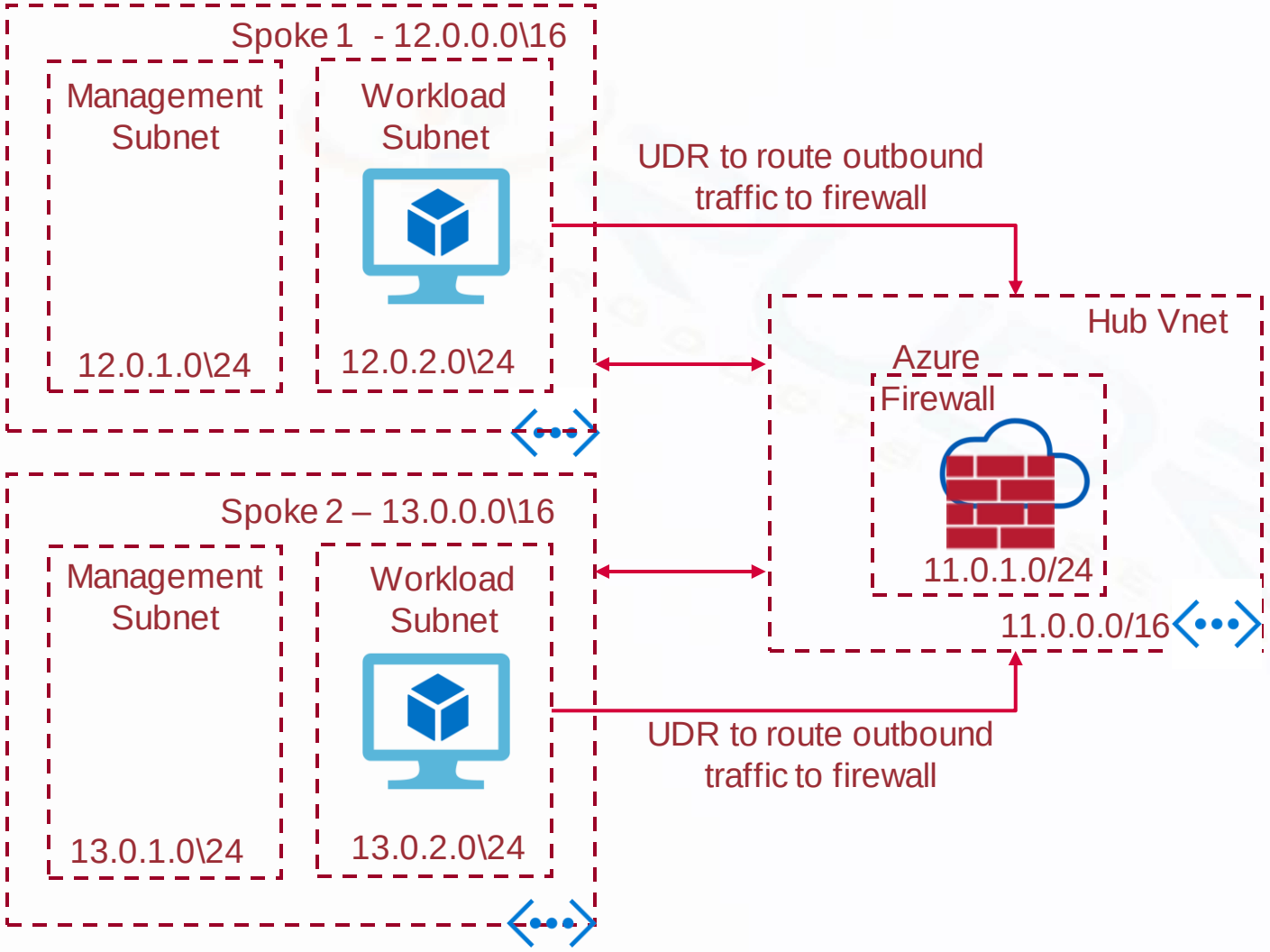
Step 16 – Protect AD role assignments using PIM



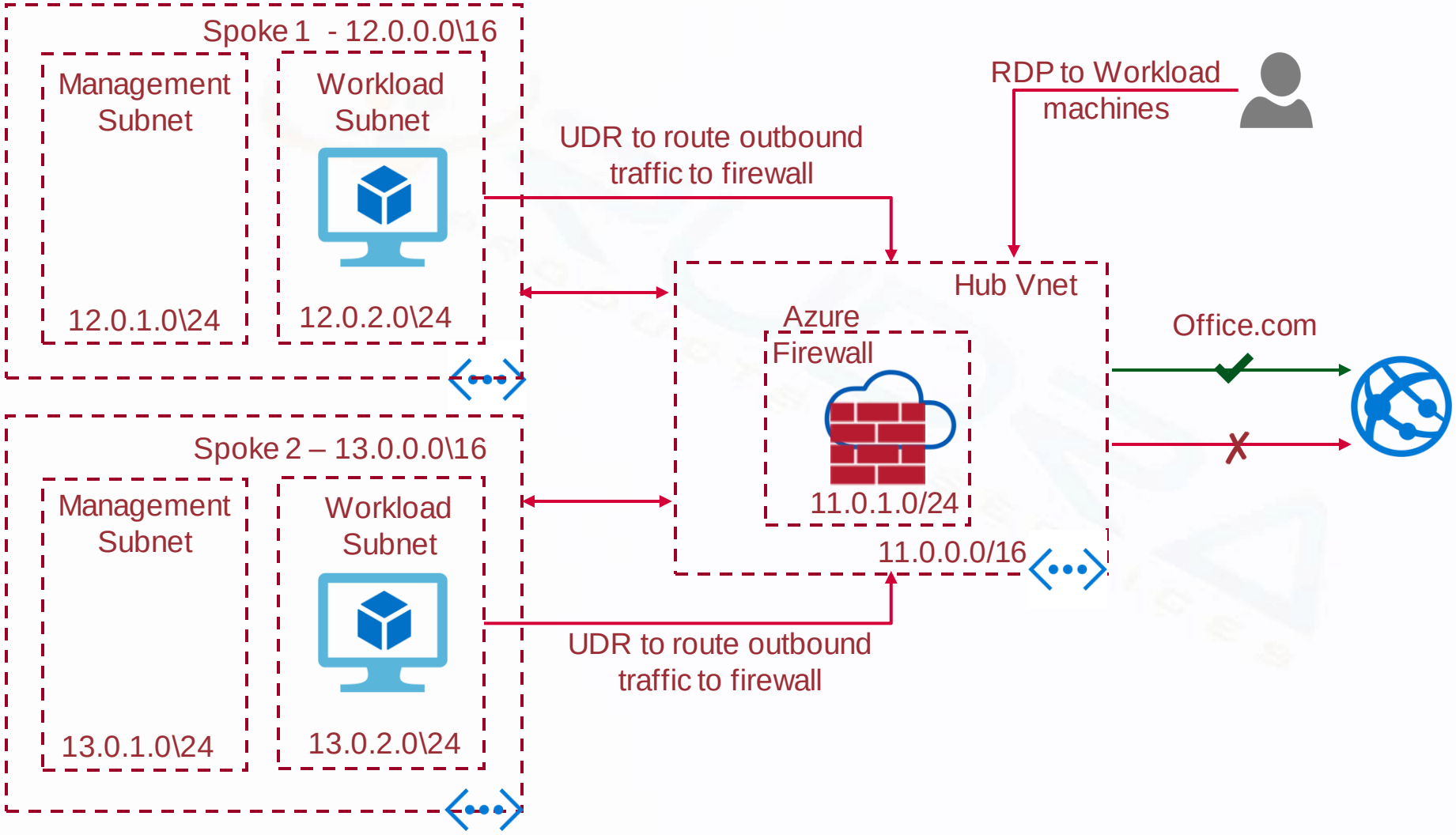
Step 17 – Protect resource role assignment and monitor PIM



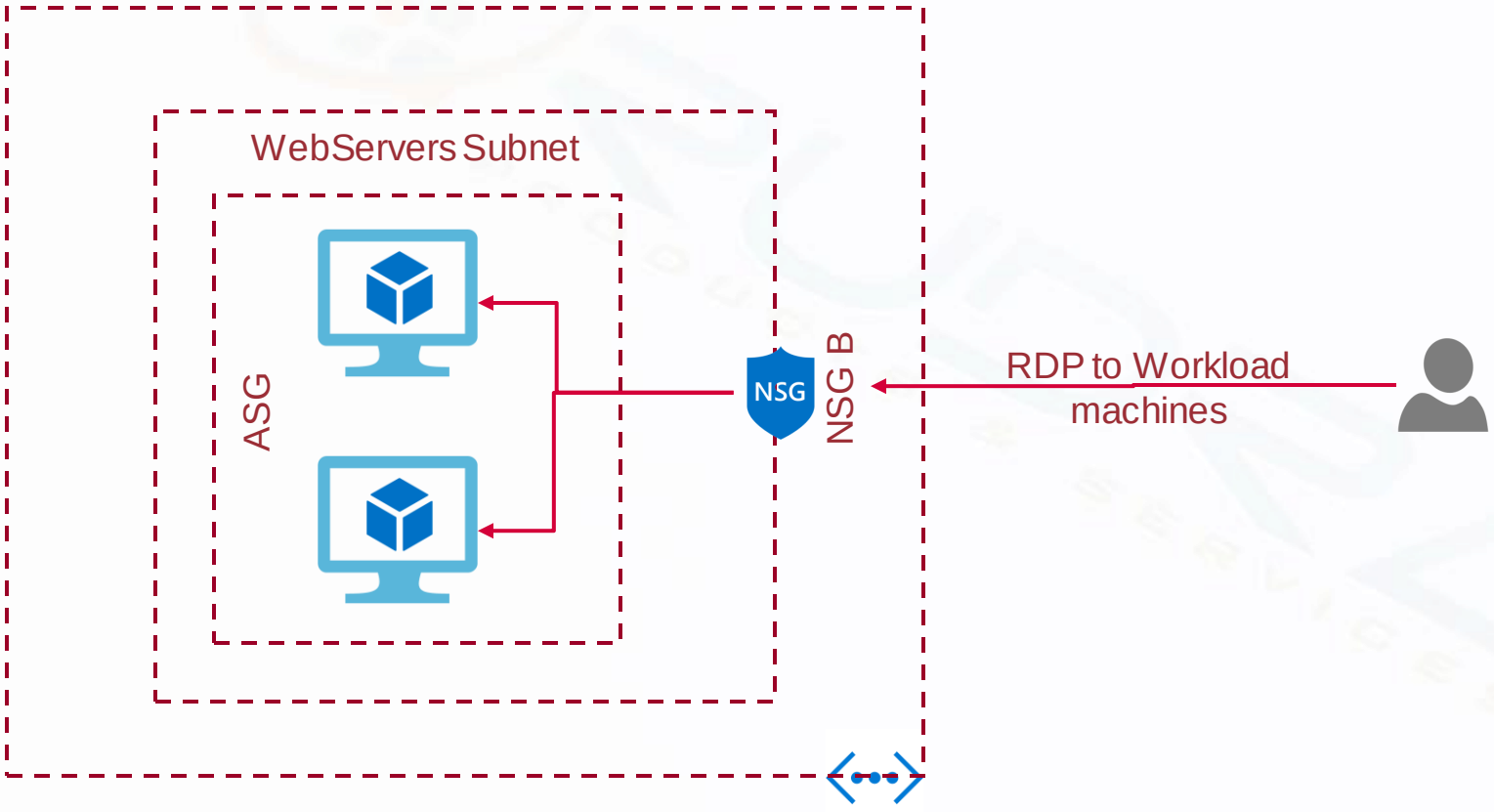
Step 18a – Deploy Azure Firewall in Hub and Spoke model



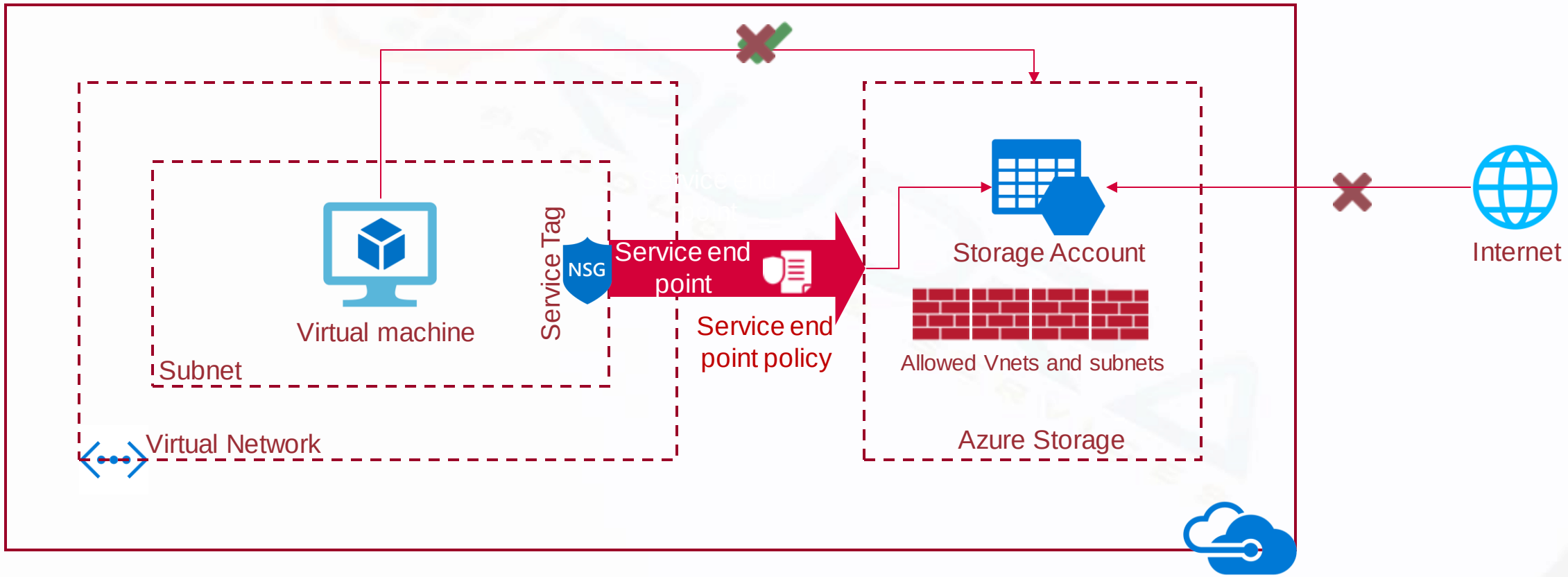
Step 18b – Configure Azure Firewall to allow RDP and control outbound traffic



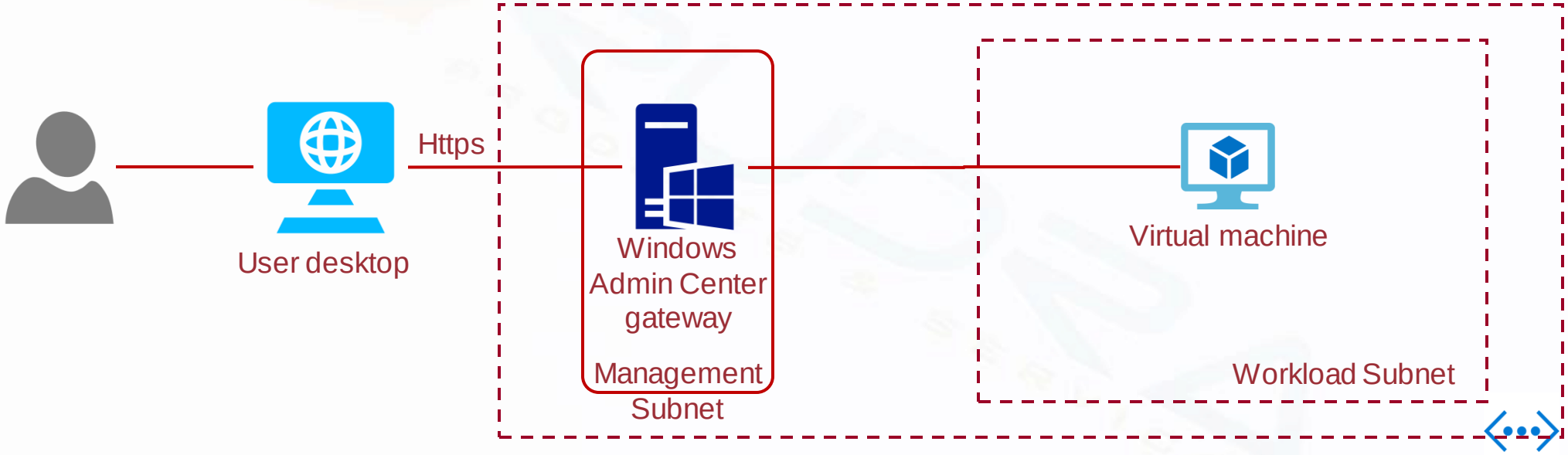
Step 19 – Configure NSG & ASG to control inbound RDP traffic



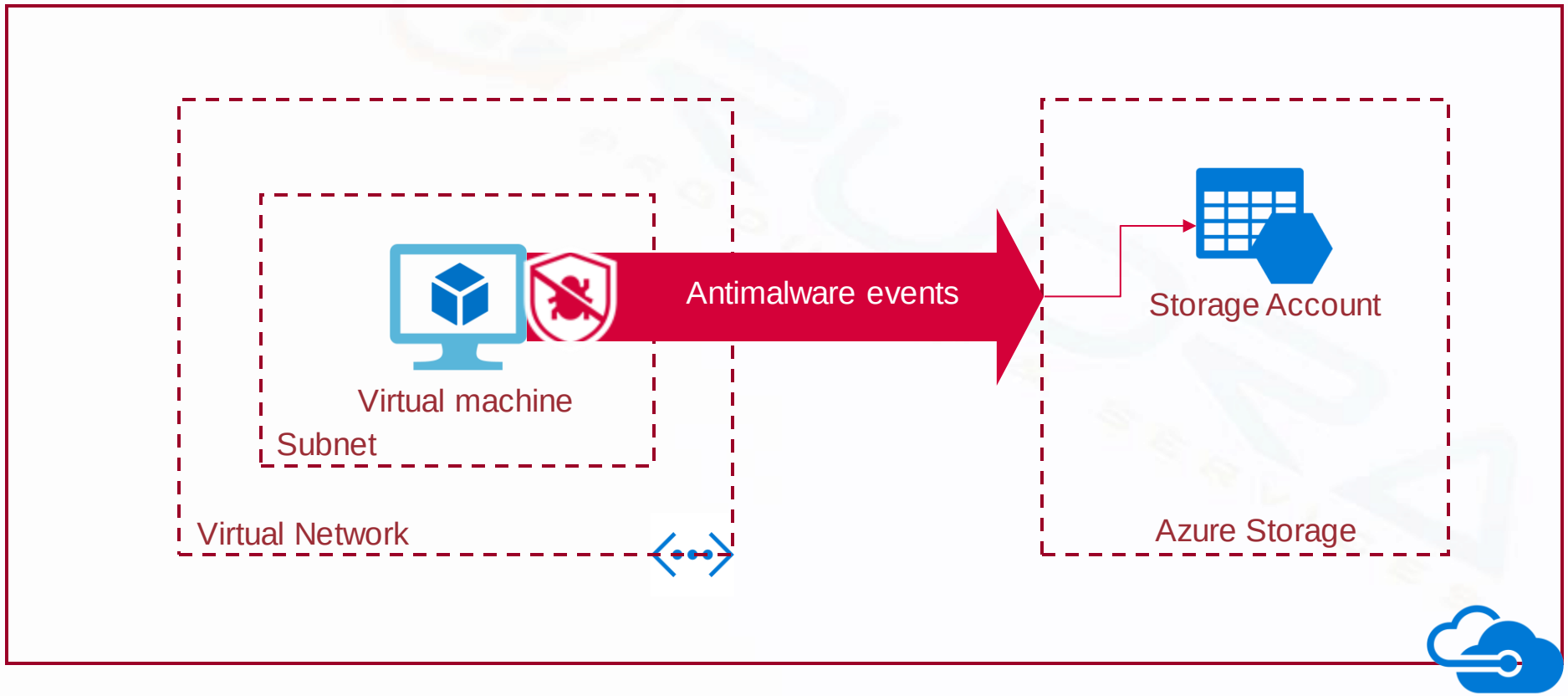
Step 20 – Configure service endpoint and policy



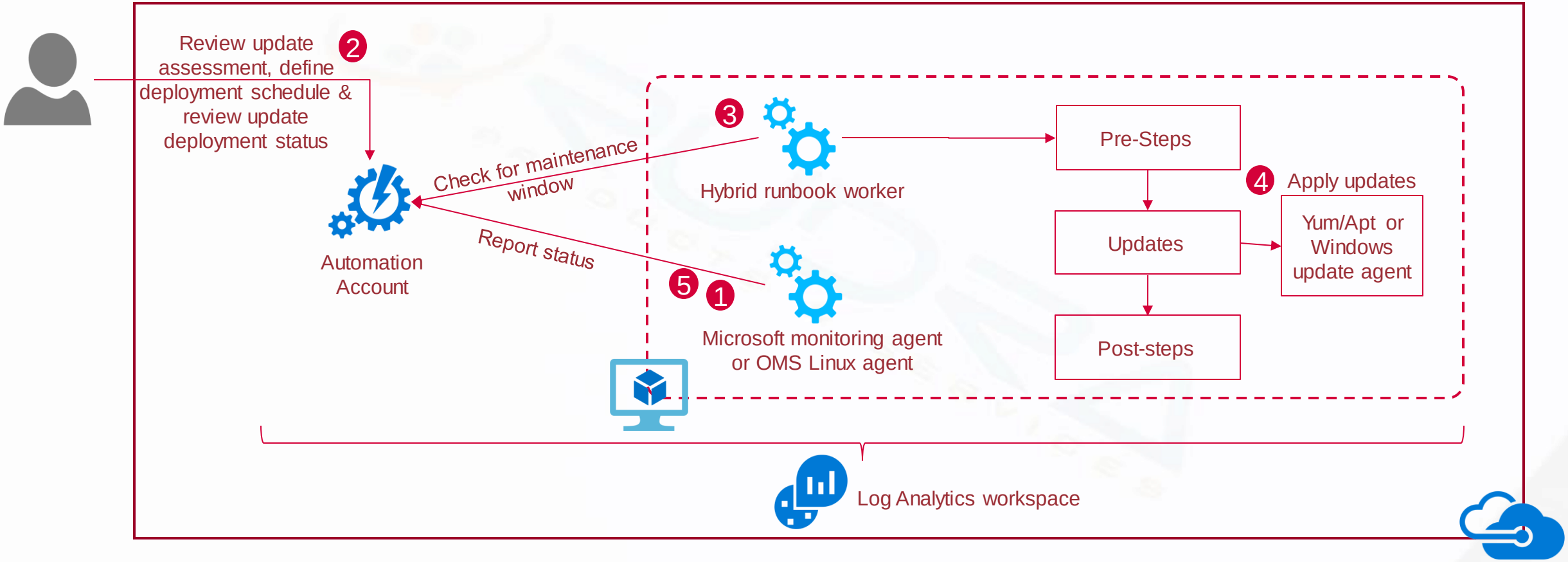
Step 21 – Remote access Azure VM using Windows Admin Centre



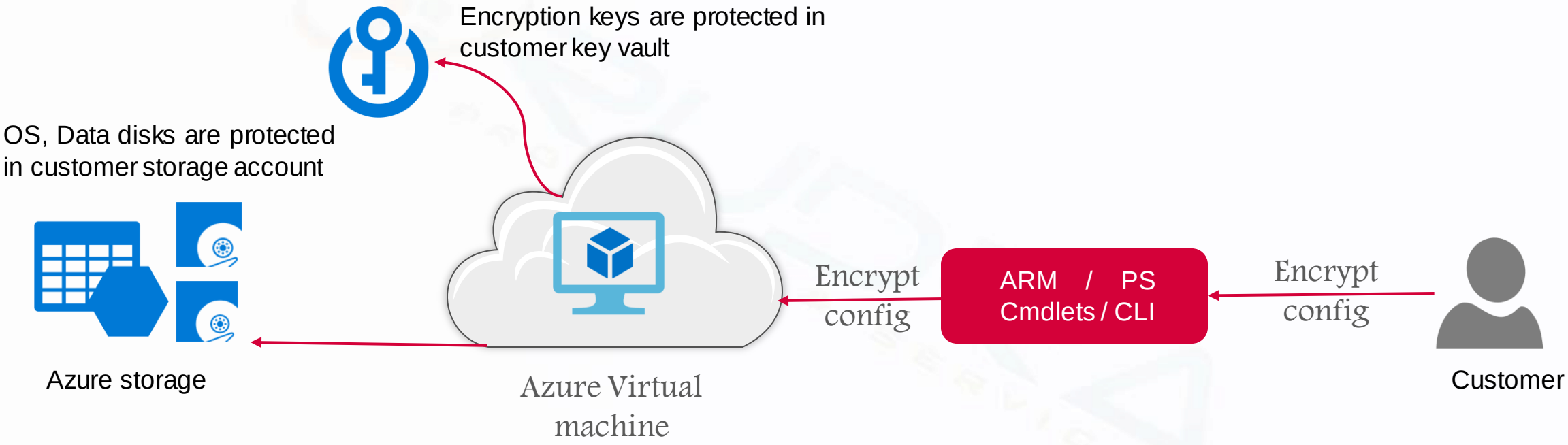
Step 22 – IaaS security – Endpoint protection



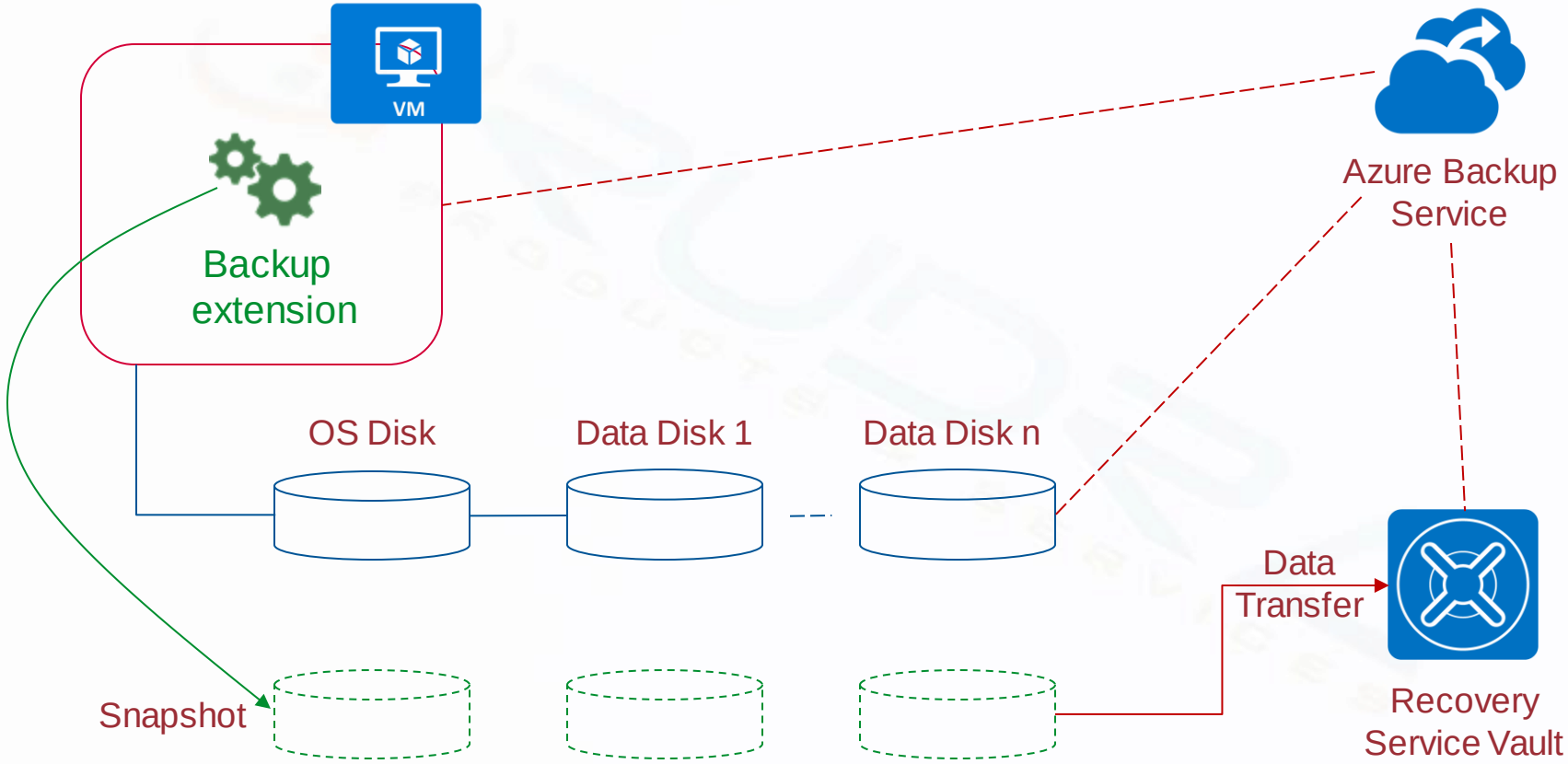
Step 23 – IaaS Security – Update management



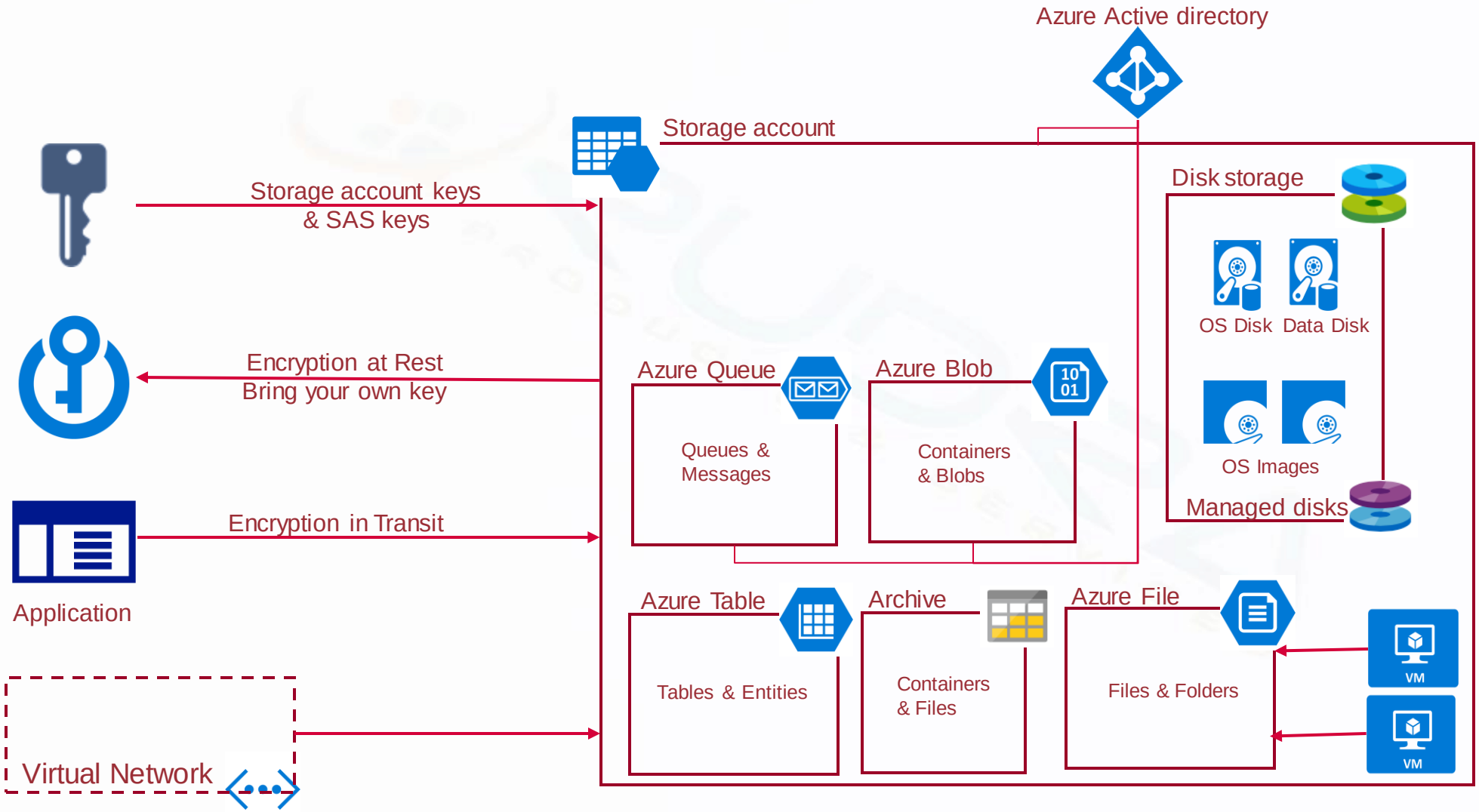
Step 24 – IaaS Security – Disk encryption



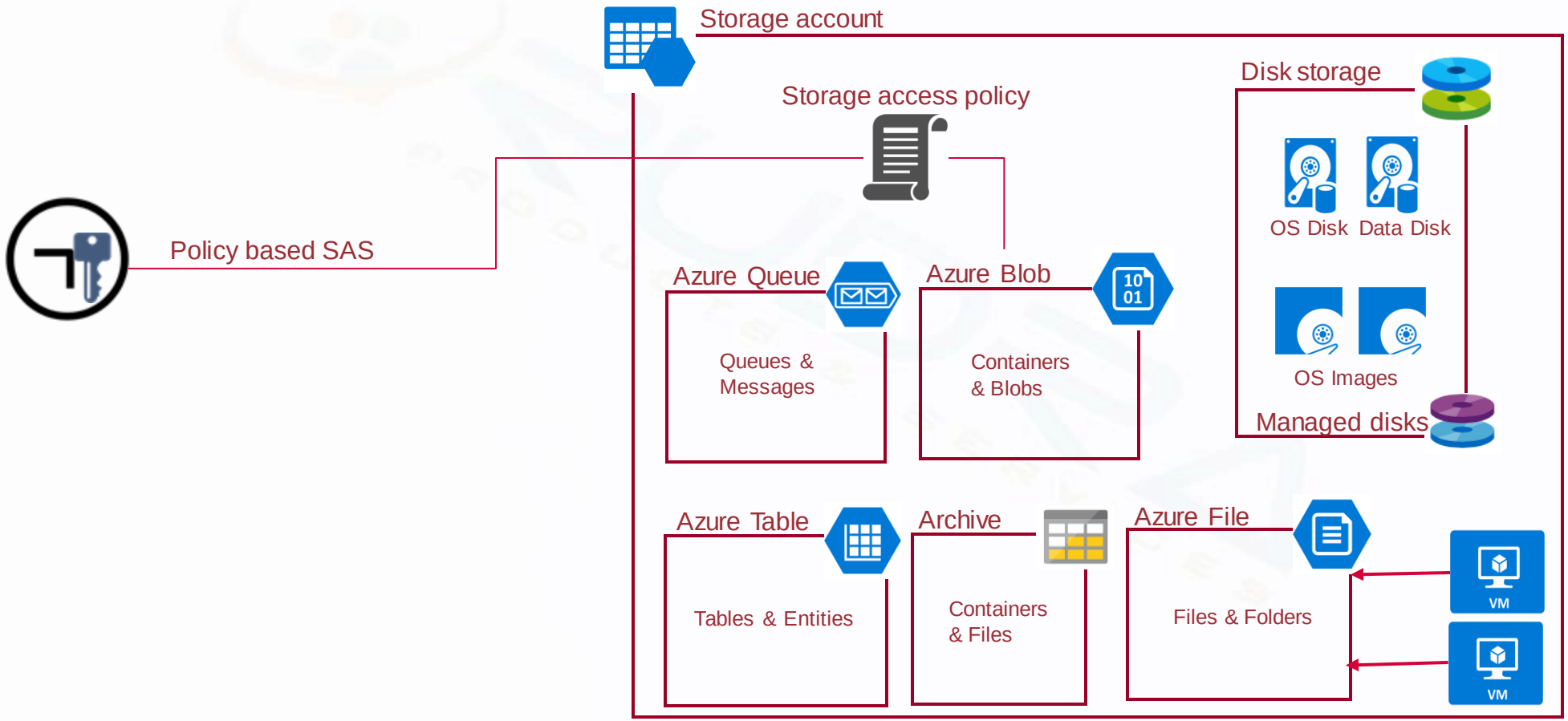
Step 25 - IaaS Security – Backup encryption



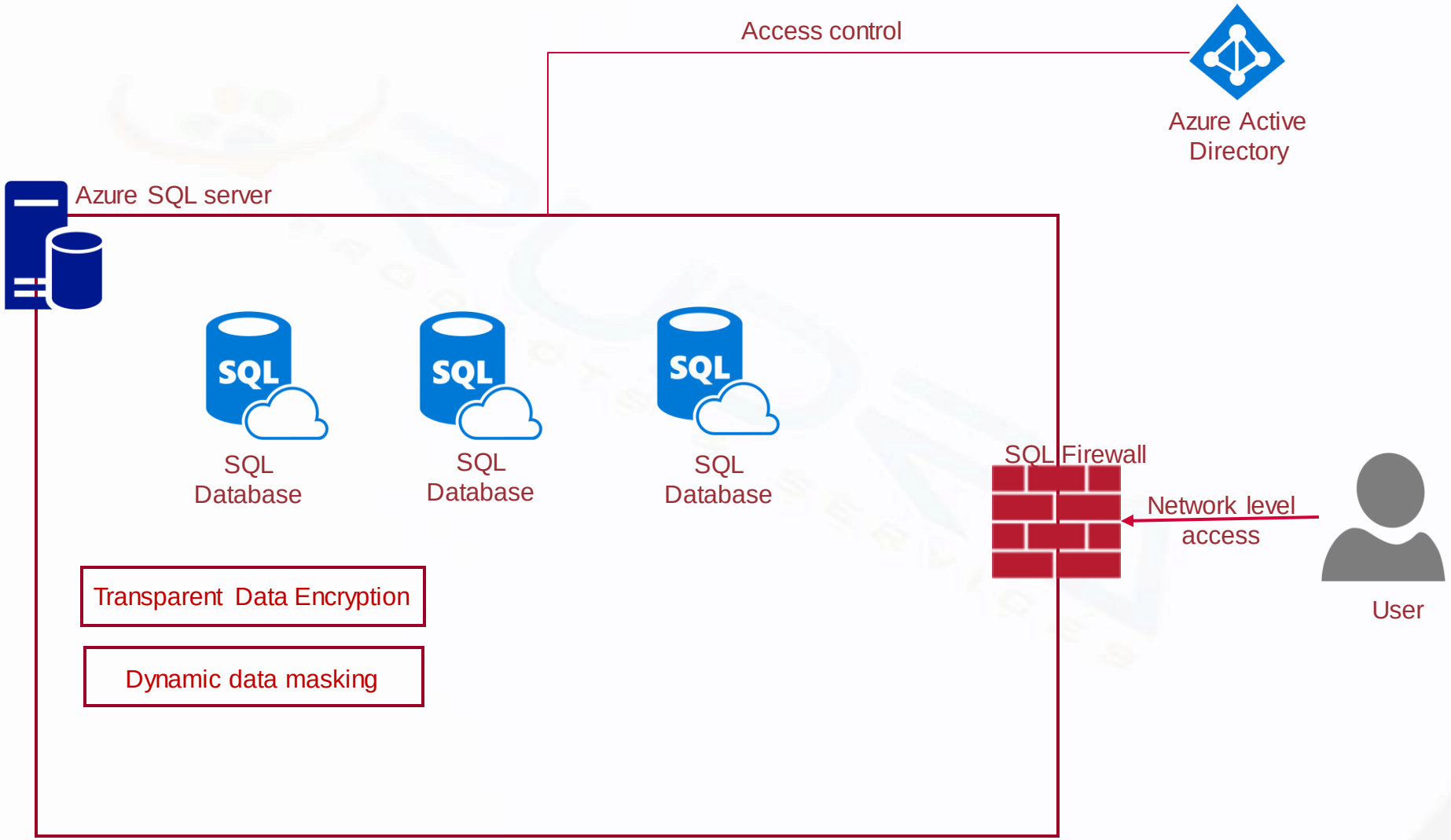
Step 26 – Walkthrough of Azure storage security features



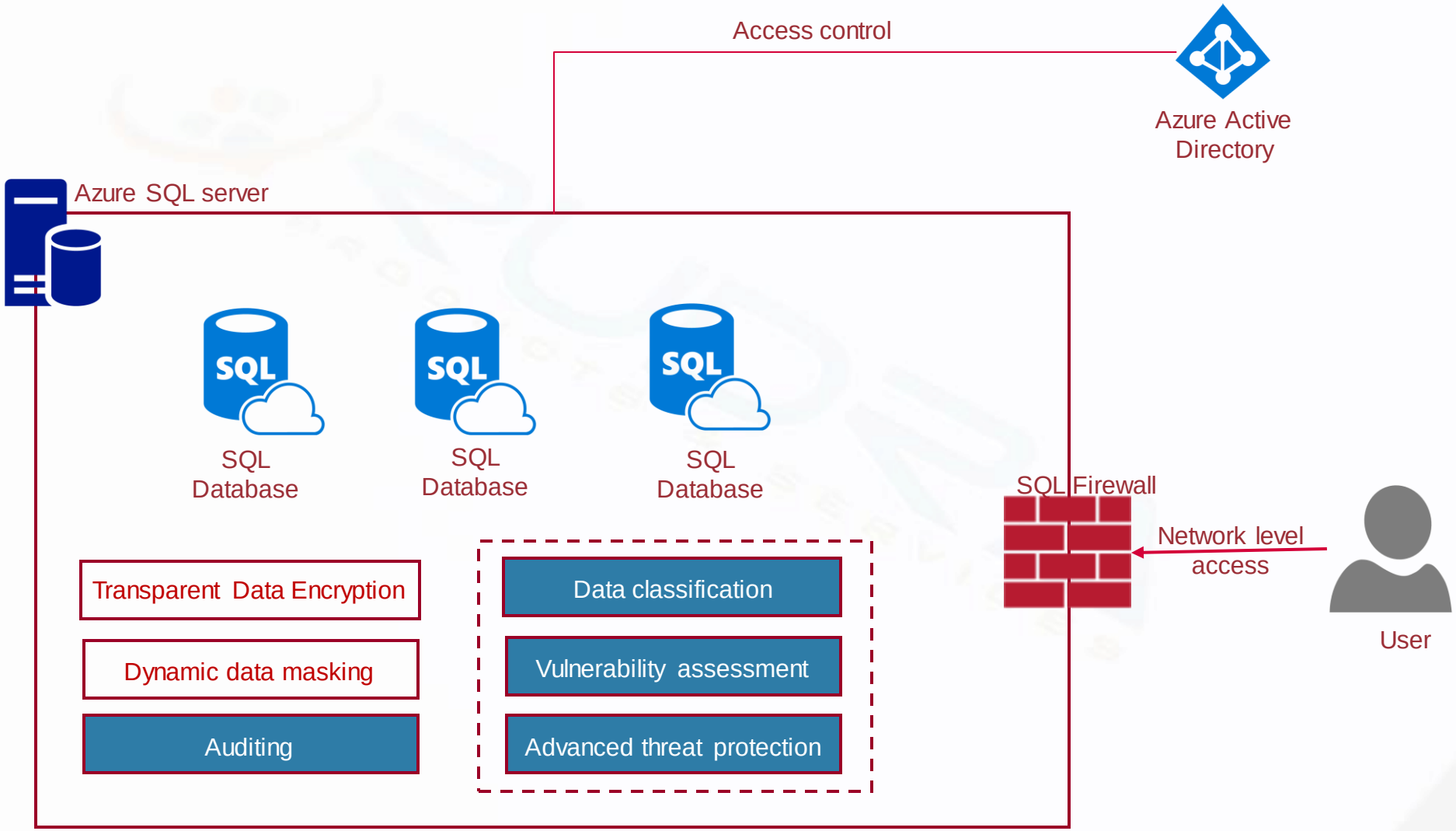
Step 27 - Create and use SAS Keys based on Storage access policies



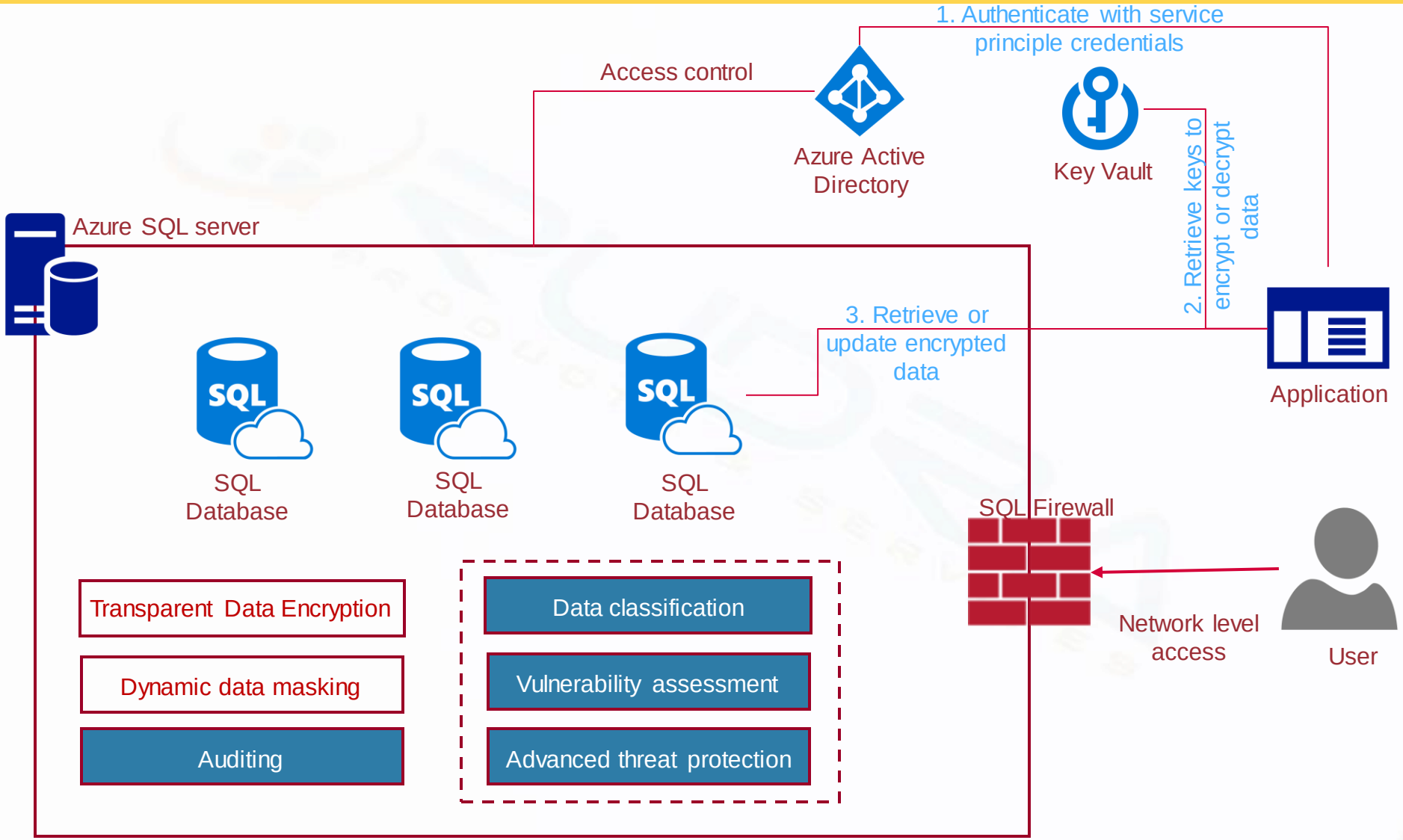
Step 28 – Implement access control, Firewall rules, TDE and dynamic data masking



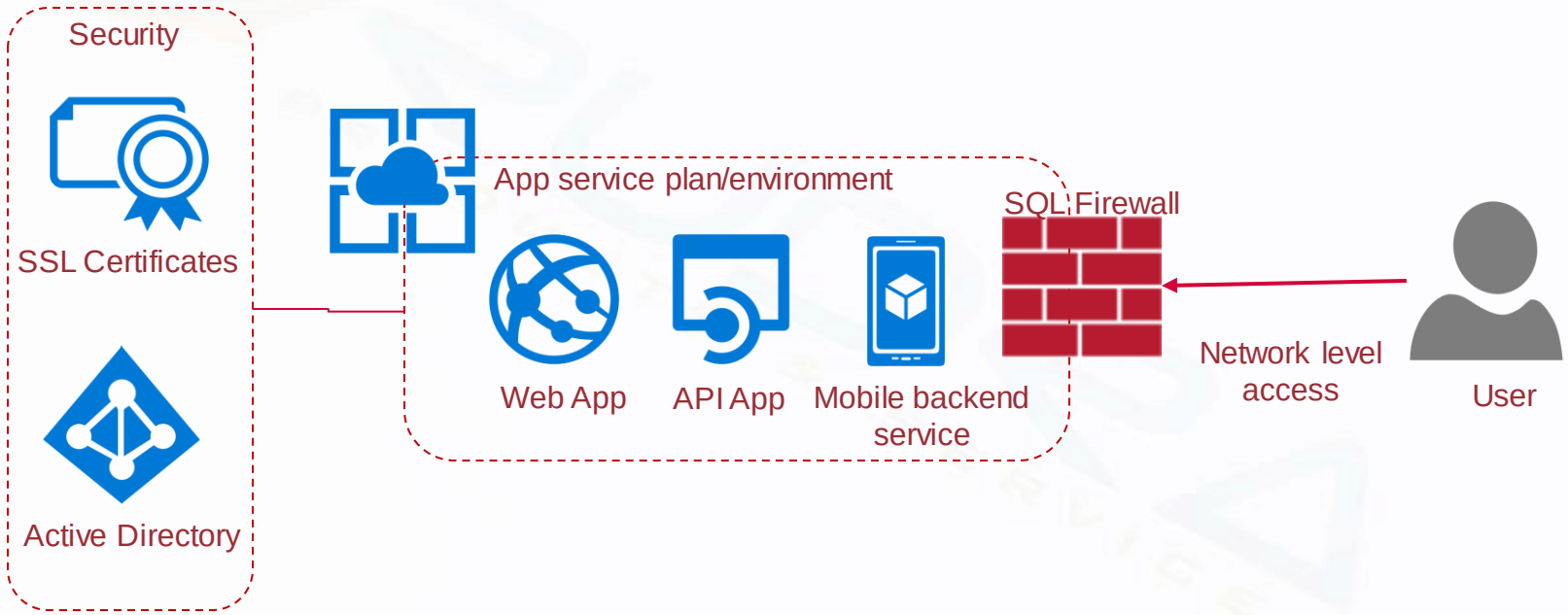
Step 29 – Implement Advanced Data Security and Auditing



Step 30 - Implement Always encrypted in Azure SQL database

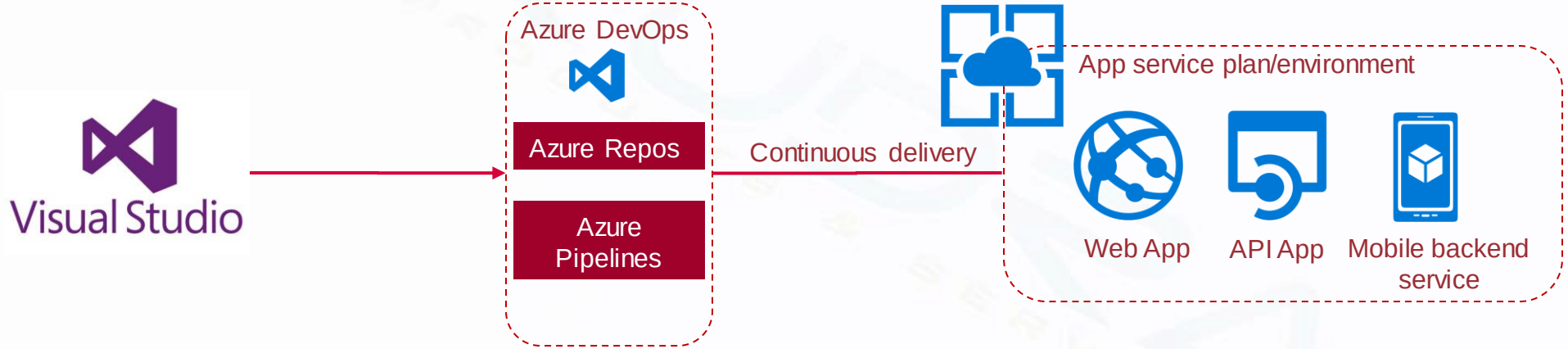


Step 31 - Authentication with AAD and configure SSL for Azure App service

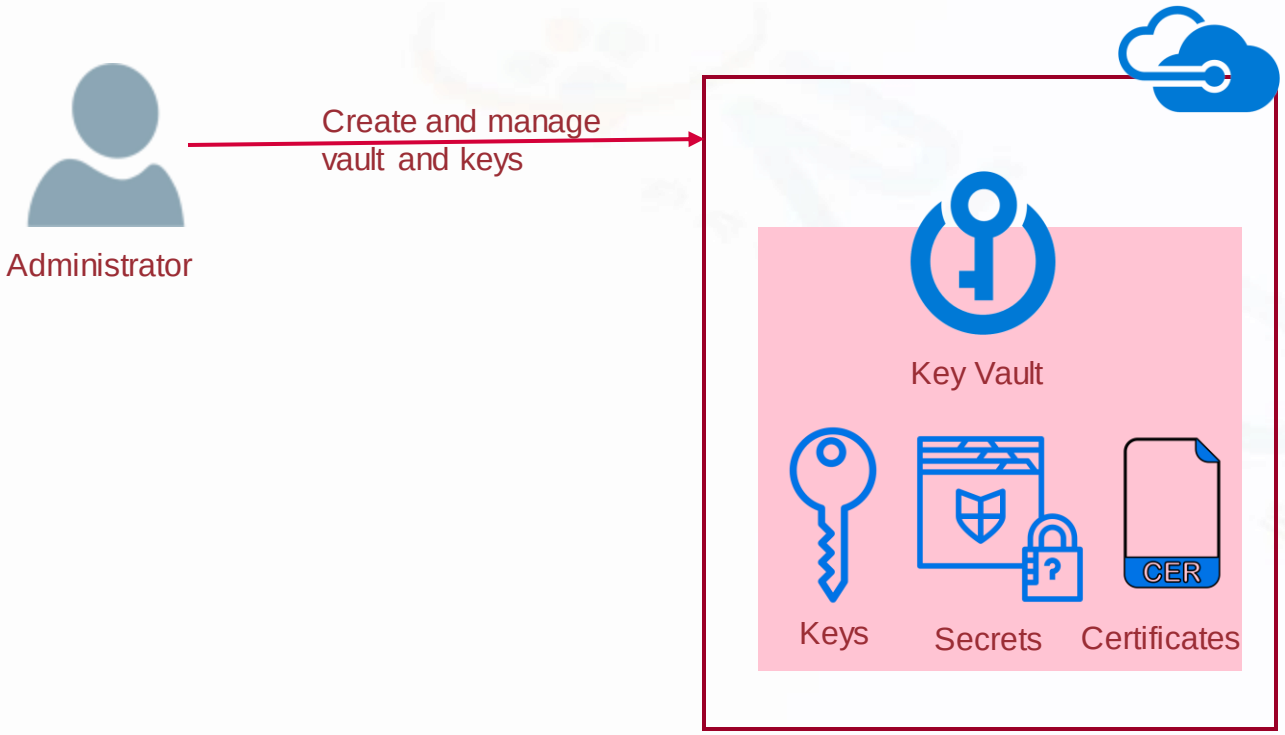


Step 32a – Securely deploying code using Azure Devops

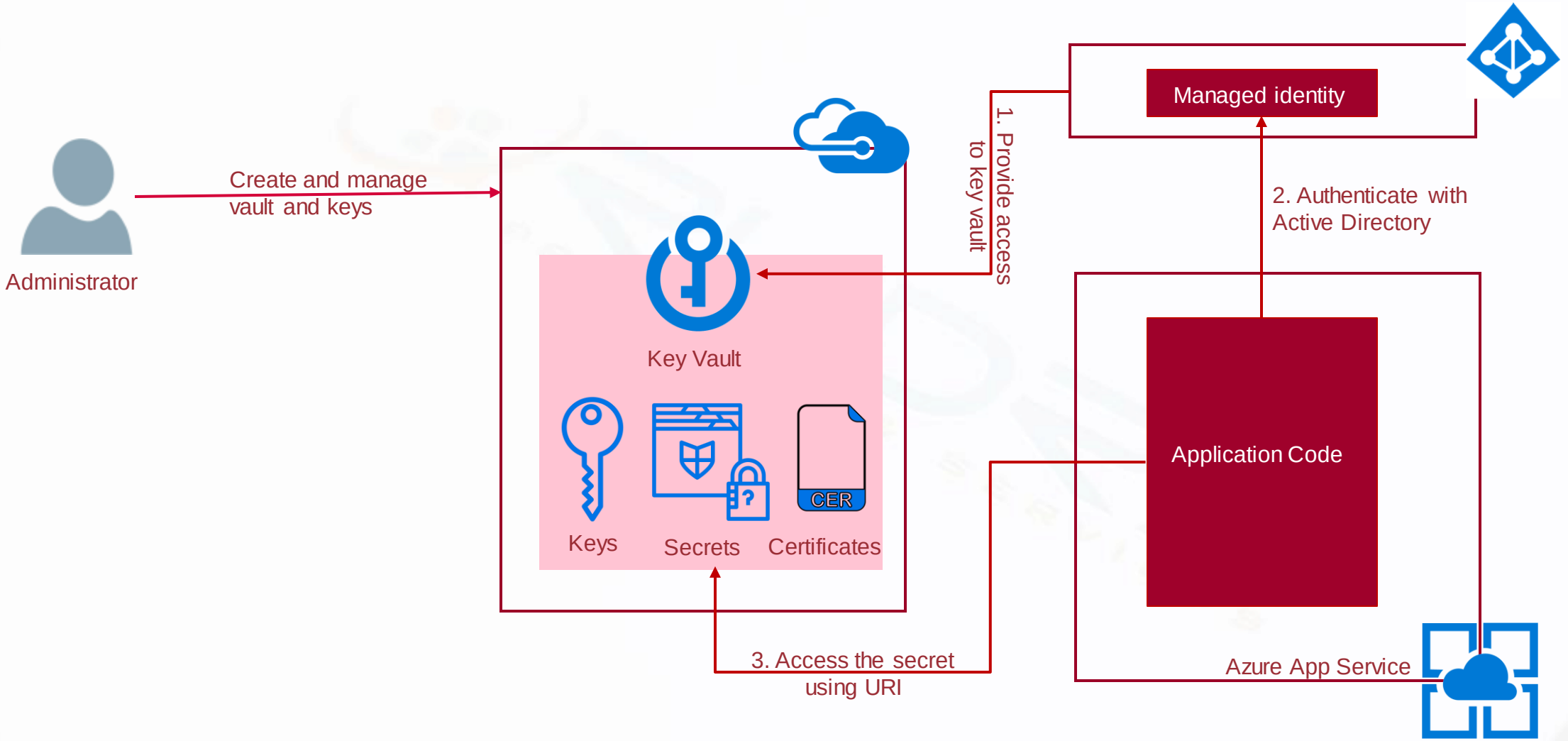
Step 32b – Securely deploying code using Azure Devops



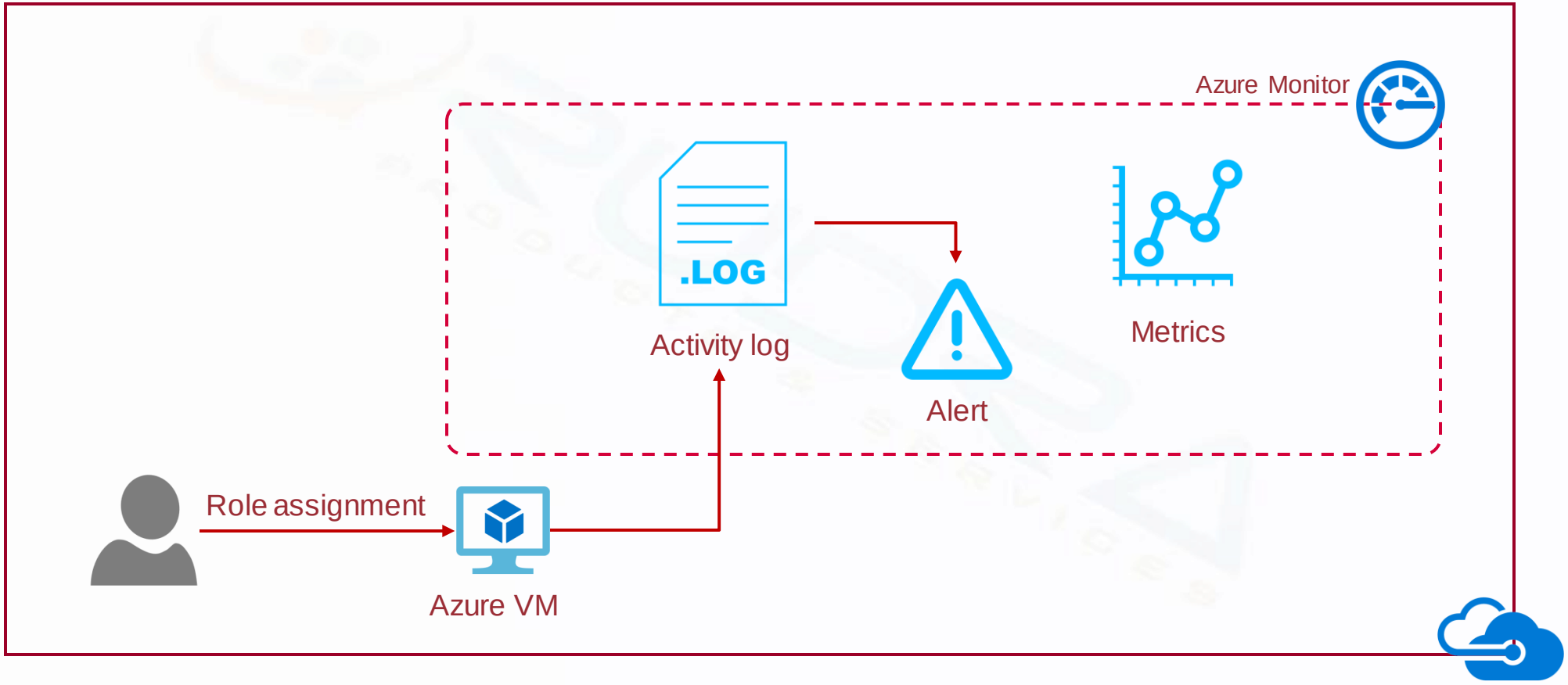
Step 33 – Create and manage Key Vault using Azure portal



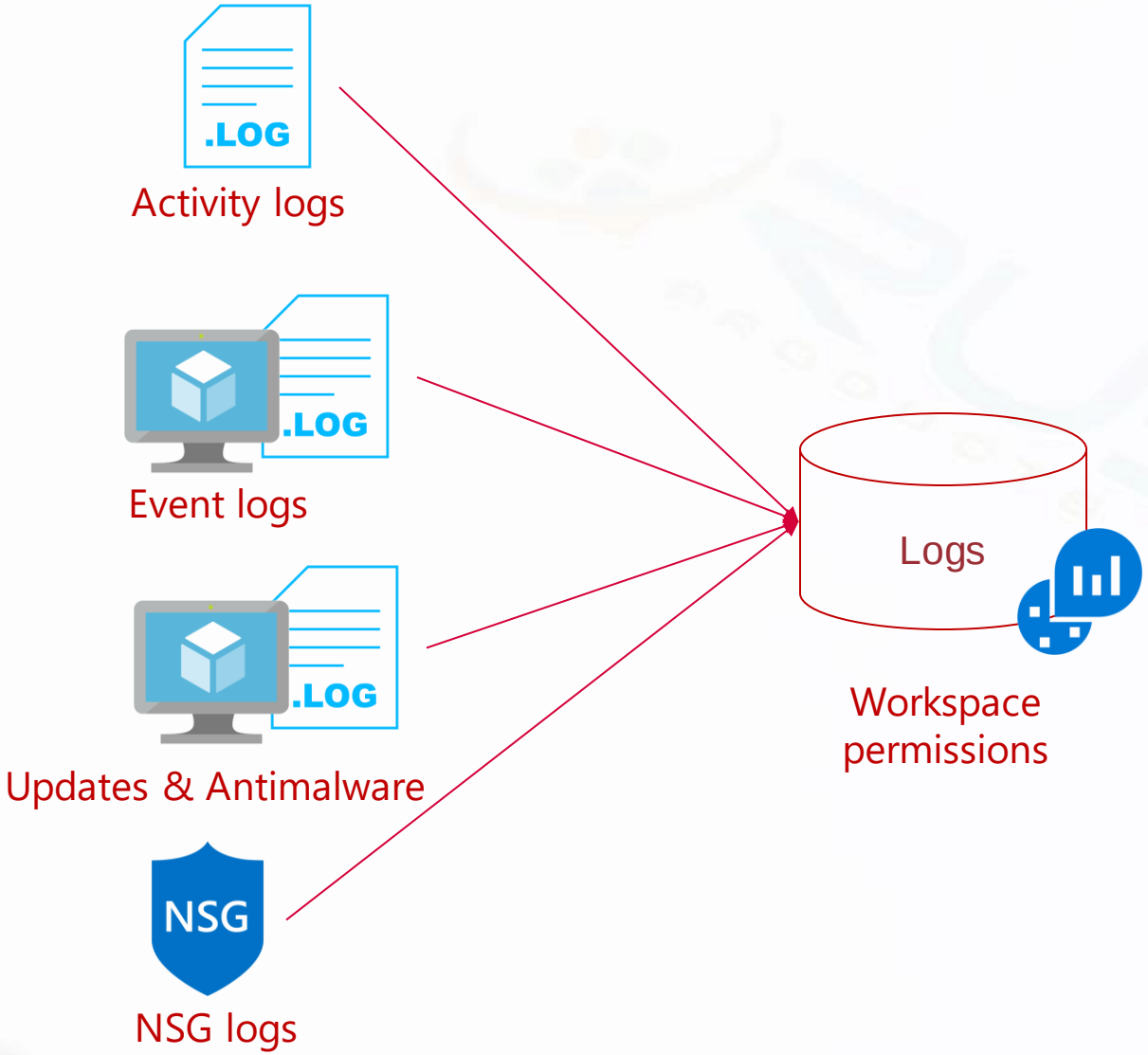
Step 34 – Access secret in Key Vault from Azure web app



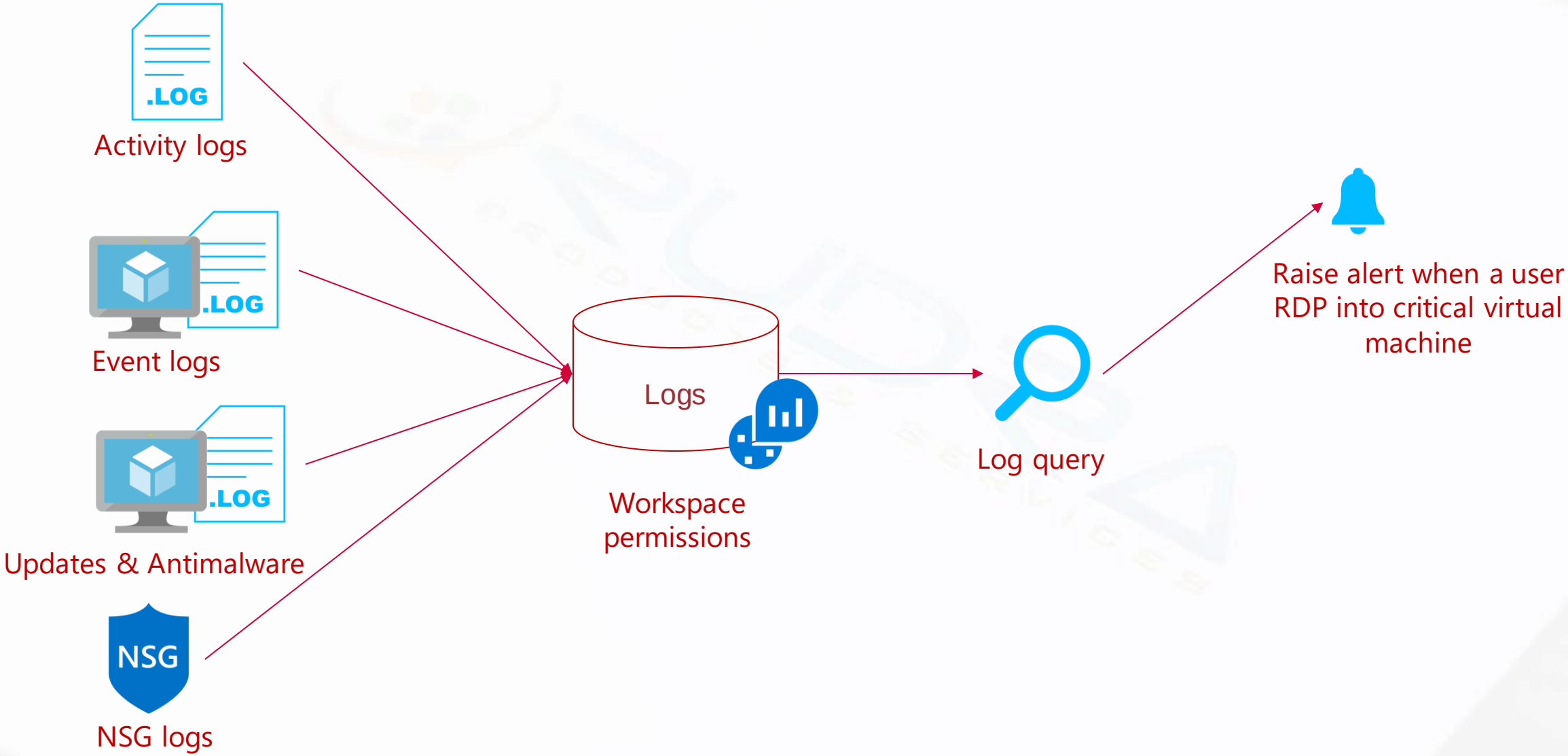
Step 35 – Monitoring – Metrics, Activity logs and Alerts



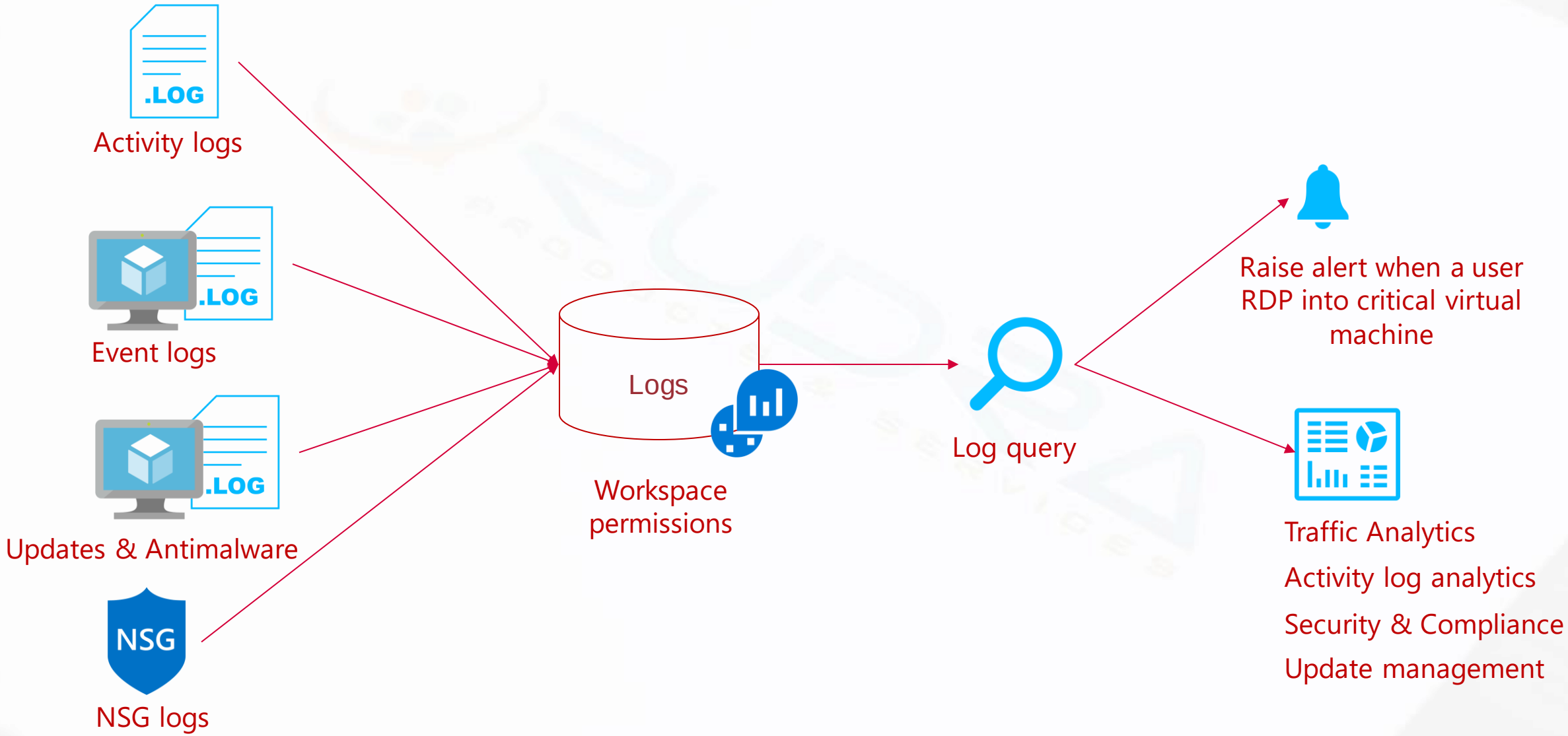
Step 36a – Monitoring – Azure monitor logs



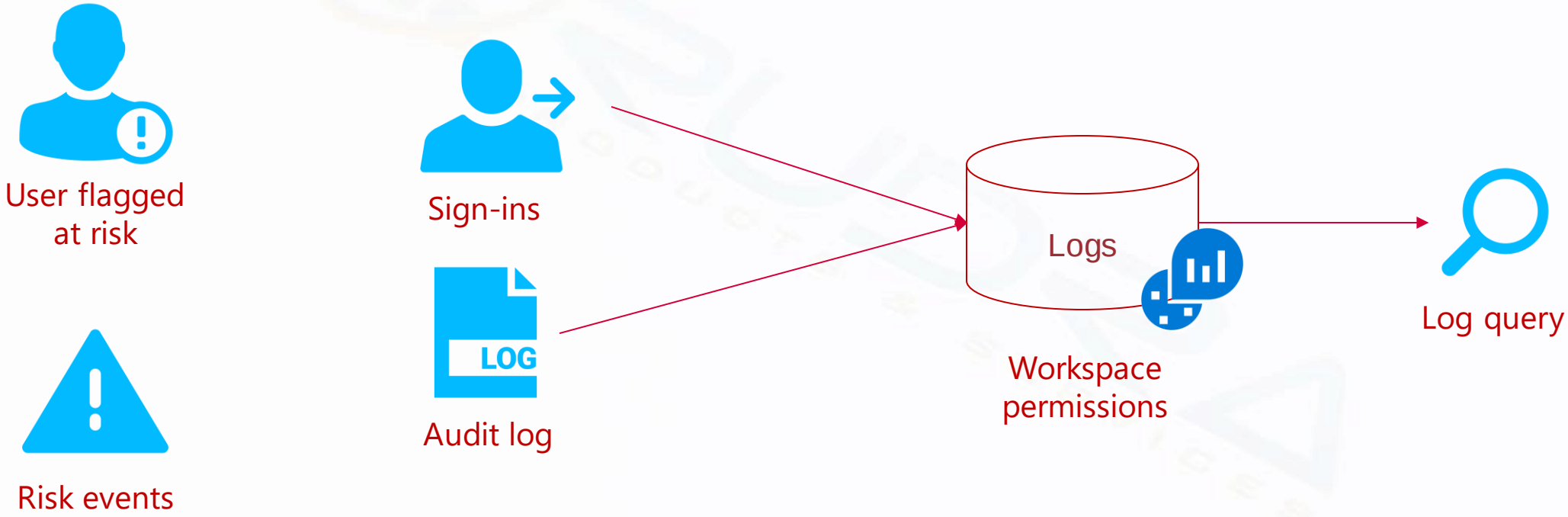
Step 36b – Monitoring – Azure monitor logs



Step 36c – Monitoring – Azure monitor logs



Step 37 – Monitoring – Azure Active Directory monitoring



Step 38 – Security center – Preventive monitoring and remediation

RUDRA PRODUCTS & SERVICES

Scope

Bring the subscriptions and management groups under the coverage of Security center

Policies & Configurations

Azure Security Center automatically assigns its built-in security policies on each subscription that is onboarded. You can configure them in Azure Policy.

Implement advanced cloud defences

Advanced cloud defenses such as Just In Time access, Adaptive application controls etc.

Implement the recommendations

When Security Center identifies potential security vulnerabilities, it creates recommendations. Remediate them to harden security posture of your solution.

Improve the overall secure score

Improve your overall secure score by implementing recommendations and monitor score continuously.

Step 39 – Security center – Implement Just In Time Access

RUDRA PRODUCTS & SERVICES

Scope

Bring the subscriptions and management groups under the coverage of Security center

Policies & Configurations

Azure Security Center automatically assigns its built-in security policies on each subscription that is onboarded. You can configure them in Azure Policy.

Implement advanced cloud defences

*Advanced cloud defenses such as **Just In Time access**, Adaptive application controls etc.*

Implement the recommendations

When Security Center identifies potential security vulnerabilities, it creates recommendations. Remediate them to harden security posture of your solution.

Improve the overall secure score

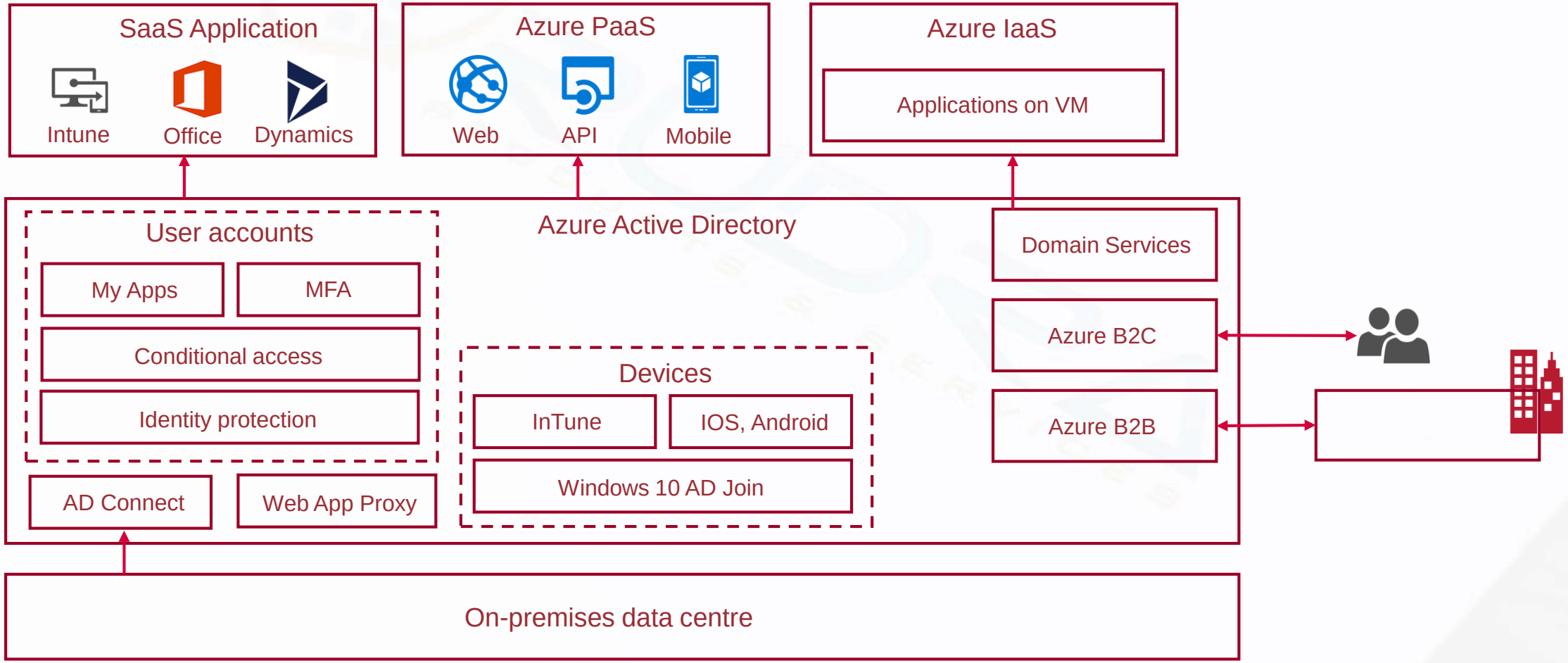
Improve your overall secure score by implementing recommendations and monitor score continuously.

Step 40 – Security center – Security alerts

Azure Active Directory Overview

Azure Active Directory overview

Azure AD is a leading provider of cloud-based Identity as a Service (IDaaS) and provides a broad range of capabilities for enterprise organizations.



AD Identities

An Identity in Azure Active directory can be

- User – Individual who can be given access to apps, app resources based on your business requirements
- Managed identity
  - System assigned managed identity
  - User assigned managed identity
- Devices
  - Device based conditional access
- Group

Groups

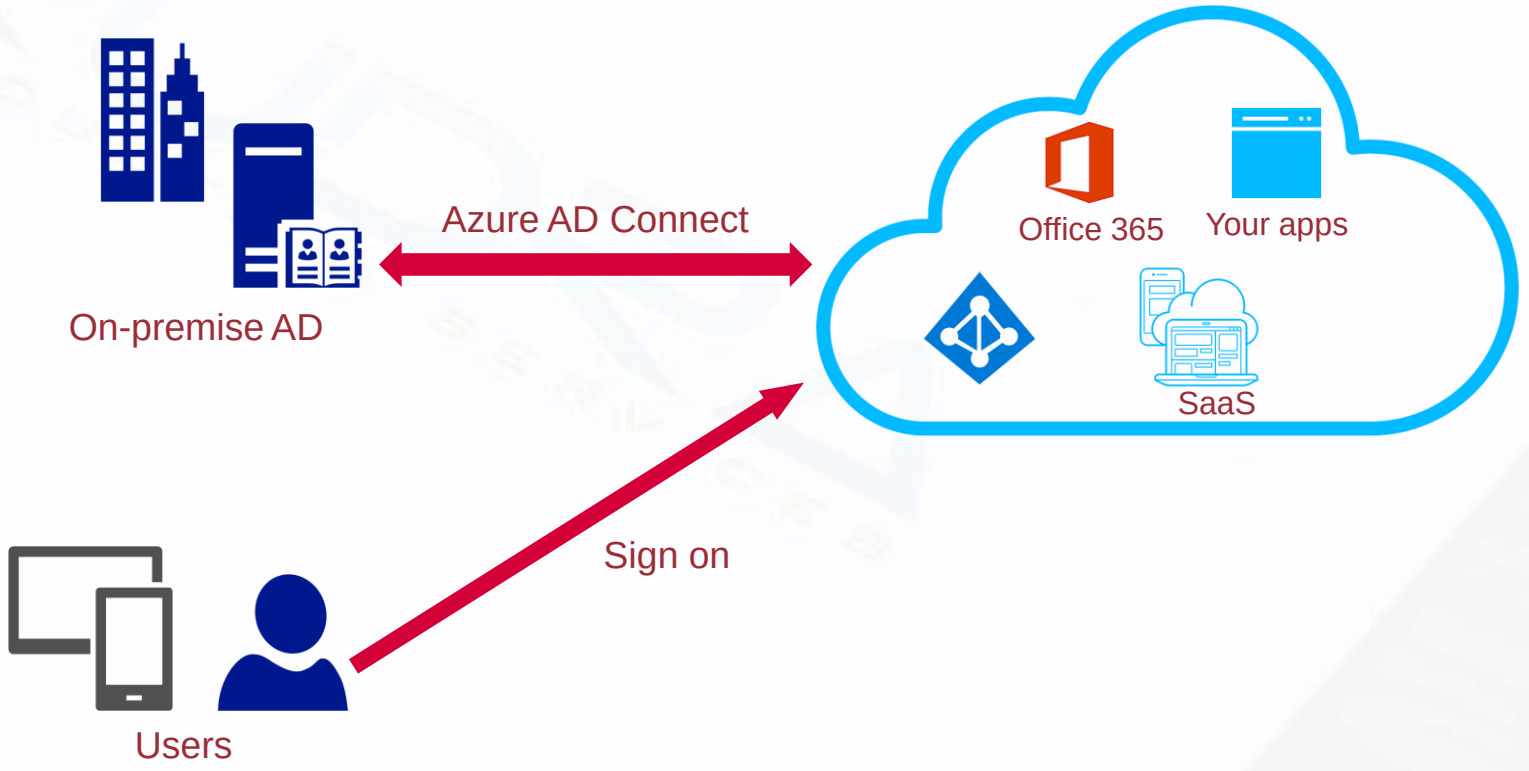
Azure AD helps you give access to your organization's resources by providing access rights to an entire Azure AD group. Using groups lets the resource owner (or Azure AD directory owner), assign a set of access permissions to all the members of the group, instead of having to provide the rights one-by-one. Four ways to assign resource access rights to user..

- **Direct assignment** - The resource owner directly assigns the user to the resource
- **Group assignment** - The resource owner assigns an Azure AD group to the resource, which automatically gives all of the group members access to the resource.
- **Rule-based assignment** - The resource owner creates a group and uses a rule to define which users are assigned to a specific resource. The rule is based on attributes that are assigned to individual users
- **External authority assignment** - Access comes from an external source, such as an on-premises directory or a SaaS app

Hybrid identities & Azure AD connect

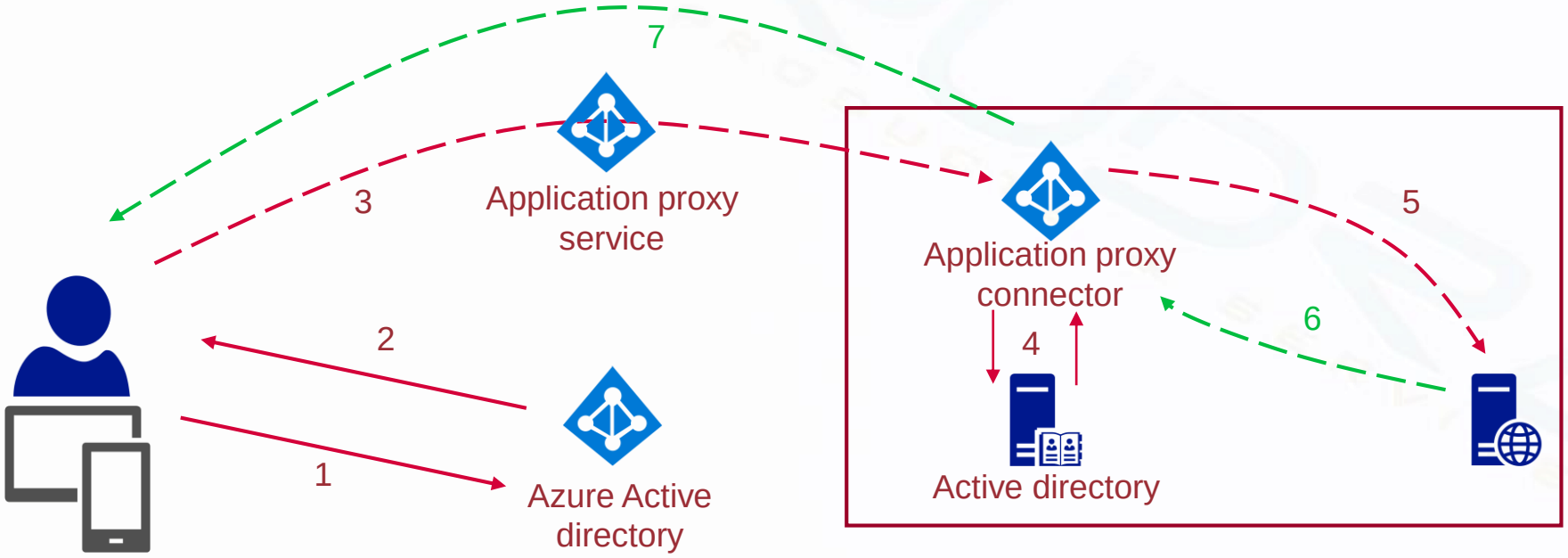
Hybrid identity is a common identity for authentication and authorization to all resources regardless location

- Password hash synchronisation
- Pass through authentication
- Federation integration
- Synchronisation
- Health Monitoring



Web app proxy

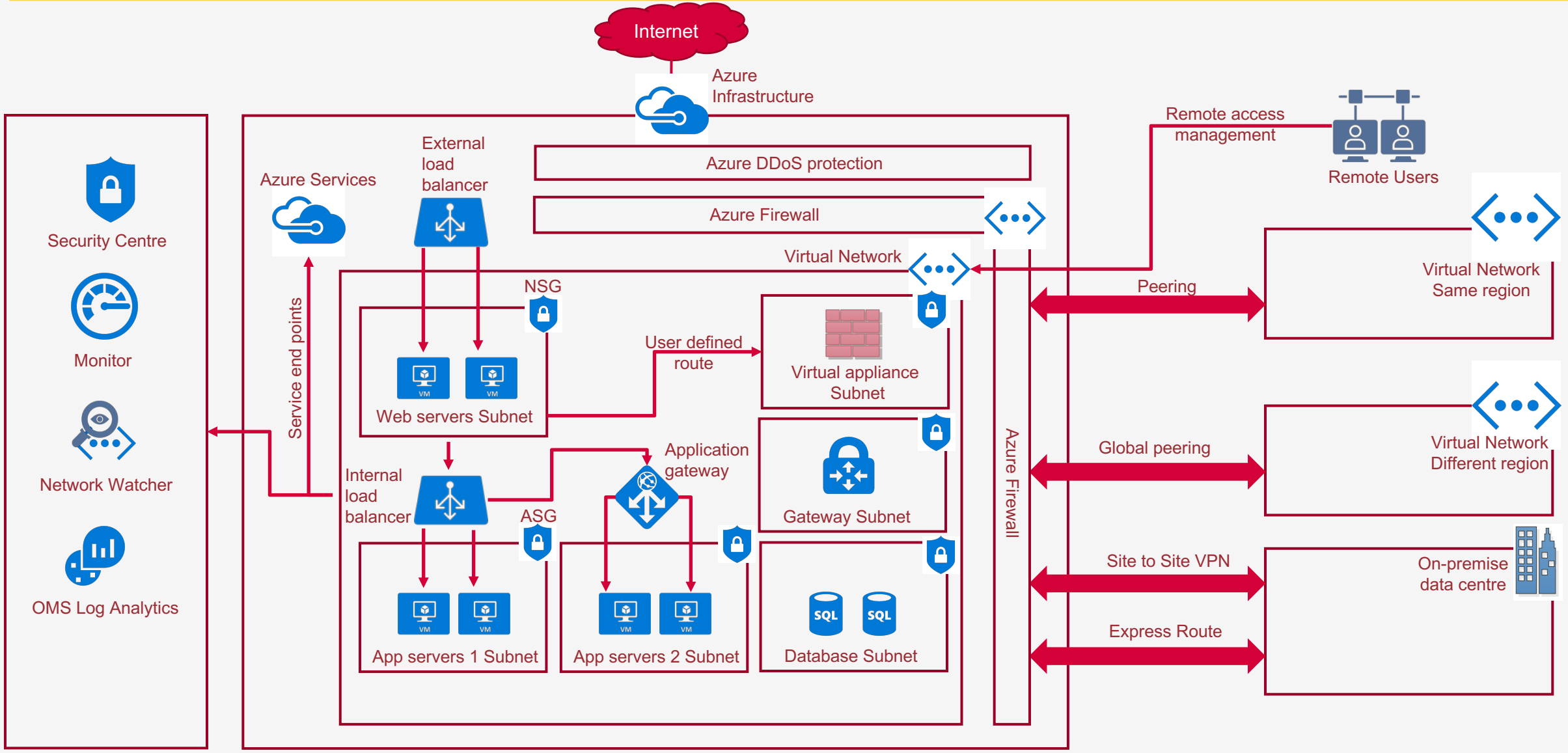
Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.



1. After the user has accessed the application through an endpoint, the user is directed to the Azure AD sign-in page.
2. After a successful sign-in, Azure AD sends a token to the user's client device.
3. The client sends the token to the Application Proxy service, which retrieves the user principal name (UPN) and security principal name (SPN) from the token. Application Proxy then sends the request to the Application Proxy connector.
4. If you have configured single sign-on, the connector performs any additional authentication required on behalf of the user.
5. The connector sends the request to the on-premises application.
6. The response is sent through the connector and Application Proxy service to the user.

Introduction to Azure Network Security Controls

Network Architecture – Security controls overview



Azure Security Monitoring Overview

Azure Security monitoring overview

RUDRA PRODUCTS & SERVICES

Management solutions

Use different management solutions in Azure monitor and start monitoring security posture of your workloads in Azure.

AM Insights

Monitor users logins and accesses in web applications using Application Insights

AM logs

Stream security information along with other data into AM logs and troubleshoot the issues

Azure Monitor (AM)

Use Azure metrics and activity logs to monitor security related activities and events

Security center

Monitor & protect your Azure IaaS and PaaS service centrally and implement recommendations & preventive actions.

Alerts

Configure alerts to proactively notify you when important conditions are found in your monitoring data.

Integration

Trigger logic apps, runbooks and webhook functions to initiate remediation processes.

Secure monitored data

Secure monitoring data both in transit and at rest. Keep data in right location to meet local compliance laws

Introduction to DDoS protection and Azure Firewall

DDoS protection

A Distributed denial of service (DDoS) attack attempts to exhaust an application's resource making the application unavailable to legitimate users. Azure DDoS protection provides the following tiers.

Basic

- Automatically enabled as part of the Azure platform.
- Always-on traffic monitoring, and real-time mitigation of common network-level attacks, provide the same defenses utilized by Microsoft's online services.
- Protection is provided for IPv4 and IPv6 Azure public IP addresses.

Standard

- Provides additional mitigation capabilities over the Basic service tier that are tuned specifically to Azure Virtual Network resources
- Provide protection against volumetric attacks, Protocol attacks, Resource layer attacks.
- Provides different metrics, alerts and mitigation reports

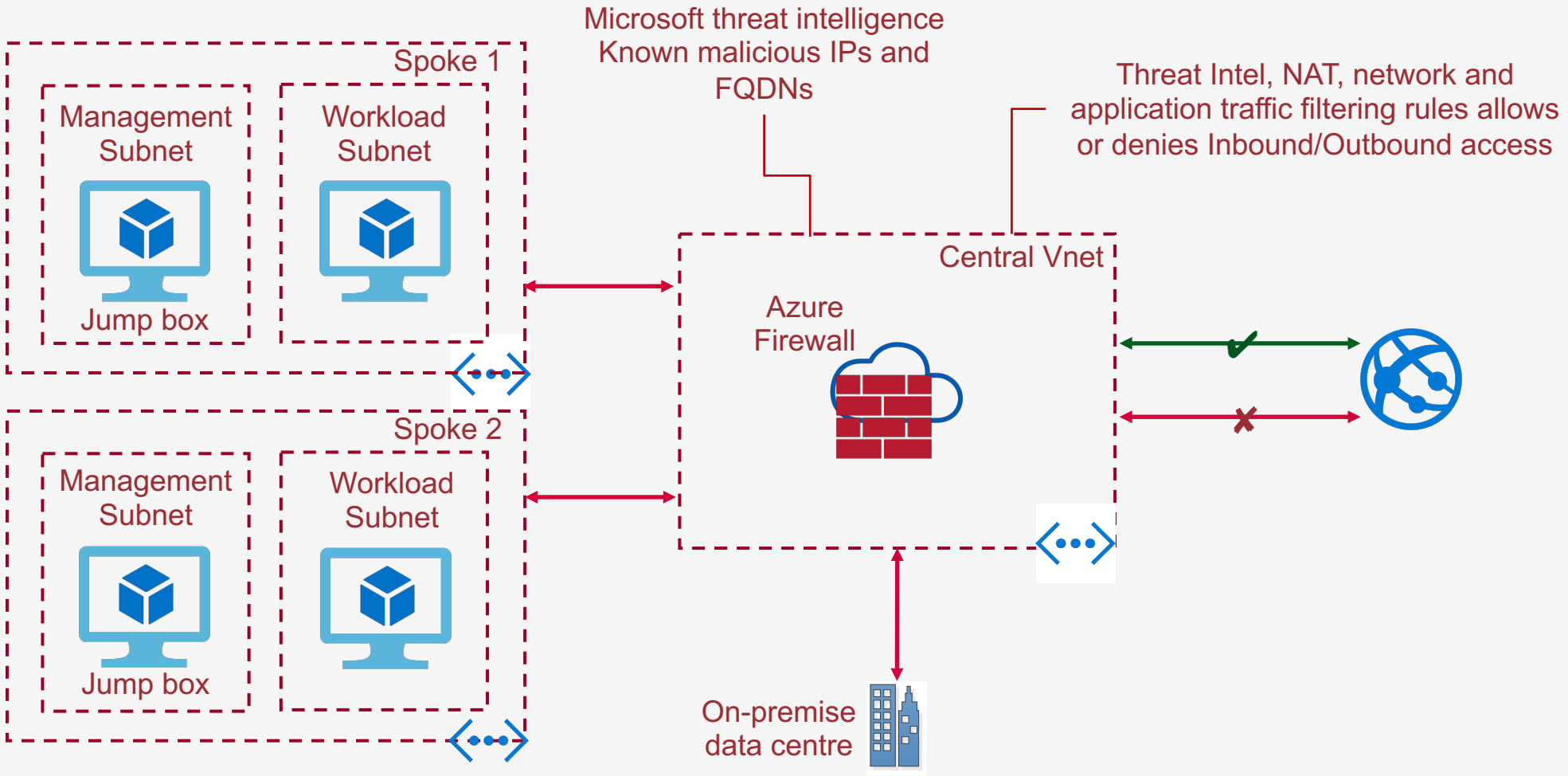
Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

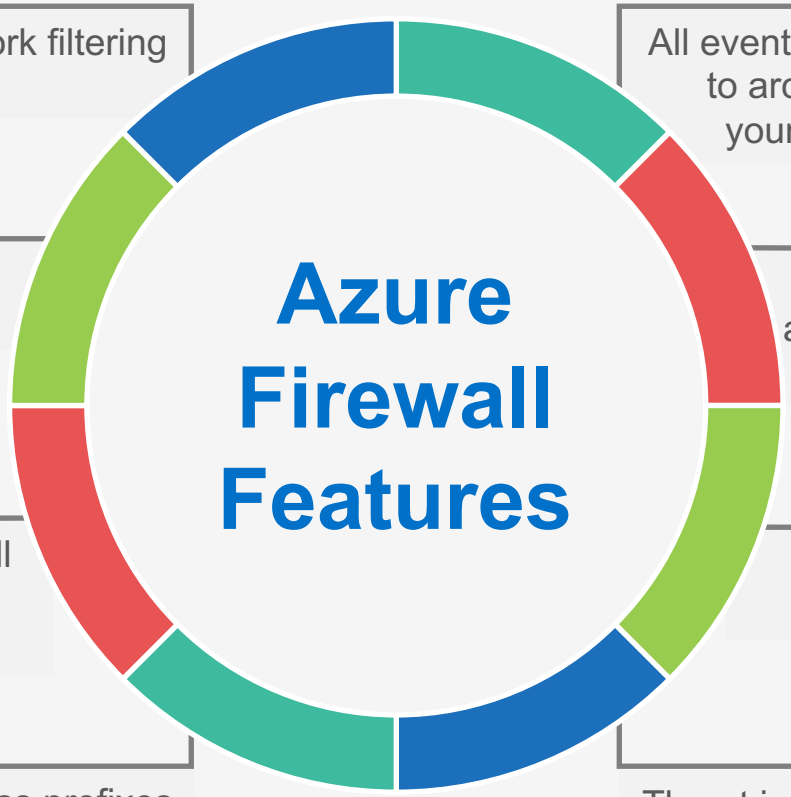
Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network

Network architecture with Azure Firewall



Features of Azure Firewall

RUDRA PRODUCTS & SERVICES



Network traffic filtering rules

You can centrally create allow or deny network filtering rules

Application FQDN filtering rules

You can limit outbound HTTP/S traffic to a specified list of FQDN's including wild cards

FQDN tags

FQDN tags make it easy for you to allow well known Azure service network traffic through your firewall

Service tags

A service tag represents a group of IP address prefixes to help minimize complexity for security rule creation.

Azure Monitor logging

All events are integrated with Azure Monitor, allowing you to archive logs to a storage account, stream events to your Event Hub, or send them to Azure Monitor logs.

Inbound DNAT support

Inbound network traffic to your firewall public IP address is translated and filtered to the private IP addresses on your virtual networks.

Outbound SNAT support

All outbound virtual network traffic IP addresses are translated to the Azure Firewall public IP

Threat intelligence

Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains

Introduction to Azure AD Privileged Identity Management (PIM)

Introduction

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Using PIM, you can manage both AD roles and Resource roles



Using PIM

- Manage risk - Secure your organization by enforcing the principle of least privilege access and just-in-time access.
- Address compliance and governance - Deploying PIM creates an environment for on-going identity governance.
- Reduce costs - Reduce costs by eliminating inefficiencies, human error, and security issues by deploying PIM correctly.

Features of Privileged Identity Management

RUDRA PRODUCTS & SERVICES

Just-in-time

Provide just-in-time privileged access to Azure AD and Azure resources.

Time bound

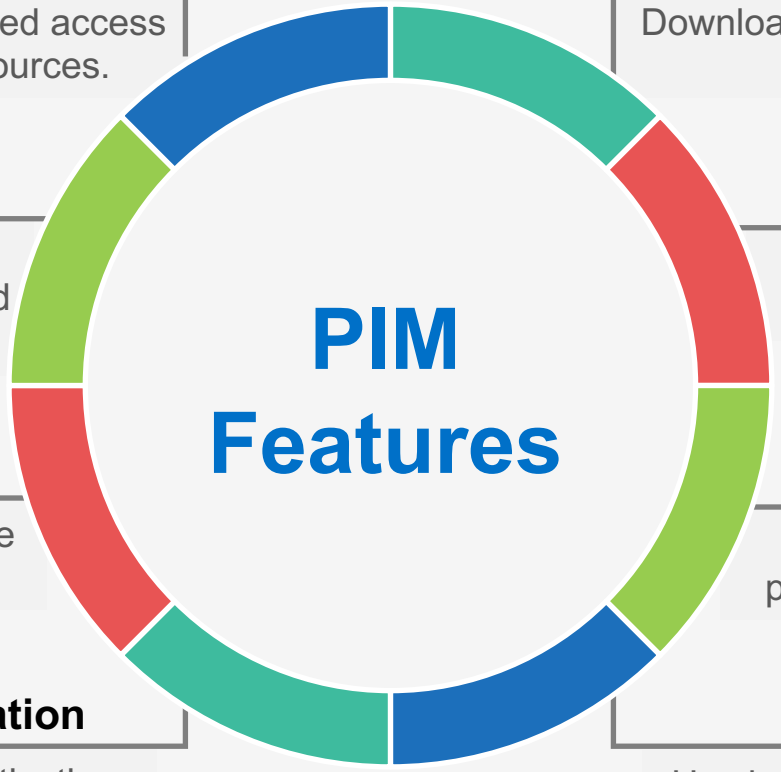
Assign time-bound access to resources using start and end dates

Approval

Require approval to activate privileged roles

Multi factor authentication

Enforce multi-factor authentication to activate any role



Audit history

Download audit history for internal or external audit.

Access reviews

Conduct access reviews to ensure users still need roles

Notifications

Get notifications when privileged roles are activated.

Justification

Use justification to understand why users activate

Implementation steps of PIM

Enable PIM

To enable PIM, you first need to provide consent. First person to enable PIM will be automatically assigned with Security Administrator and Privileged role Administrator.

Access Review

Role assignments become "stale" when users have privileged access that they don't need anymore. In order to reduce the risk, carry out frequent access reviews

Protect Role Assignment

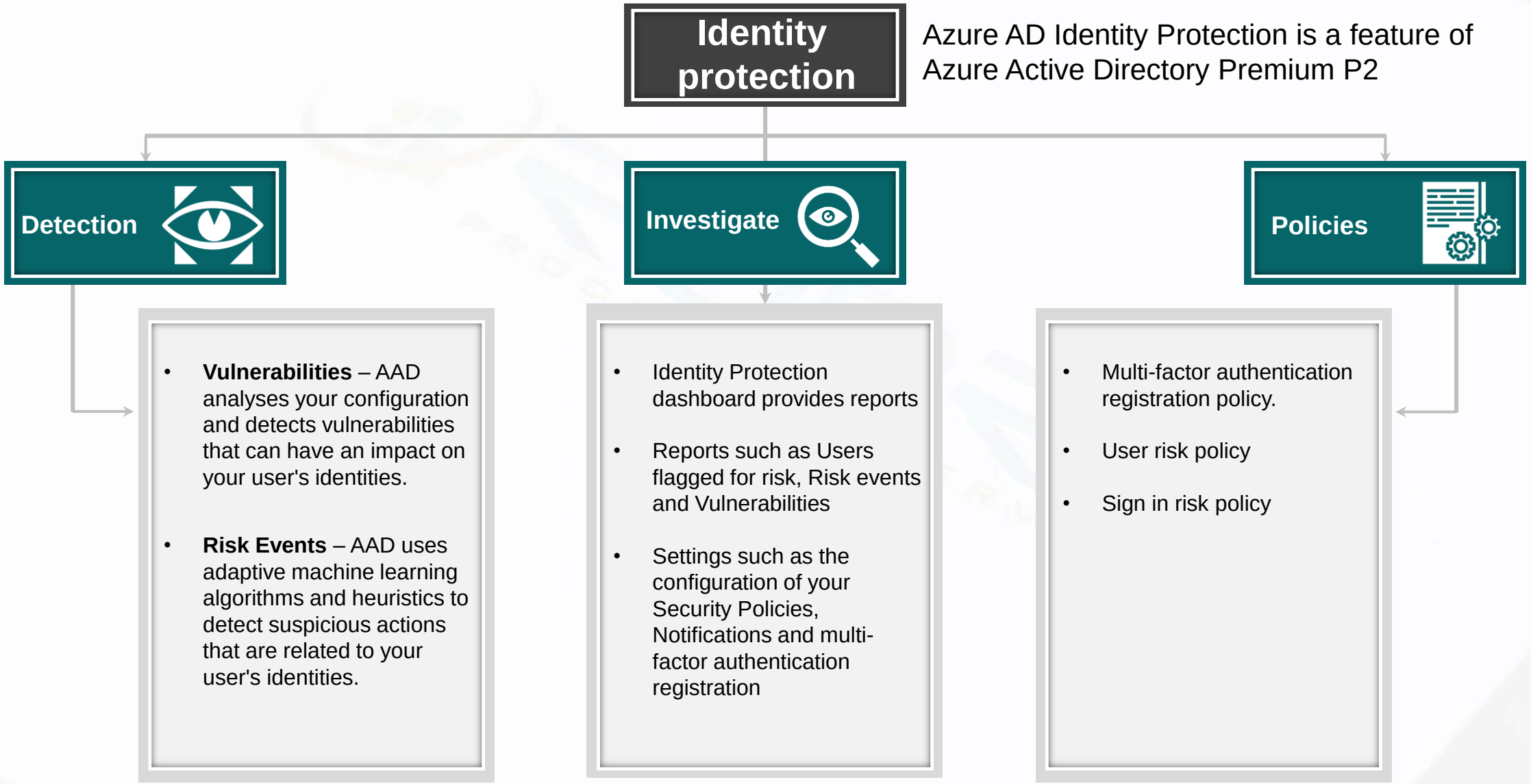
Eligible users assigned to PIM must elevate to use the privileges granted by the role.

Monitor & Alerts

Utilize PIM's built-in alerting functionality to better safeguard your tenant. Set up recurring access reviews to regularly audit you organisation's privileges identities

Introduction to Azure AD Identity Protection

Identity Protection capabilities



Types of risks

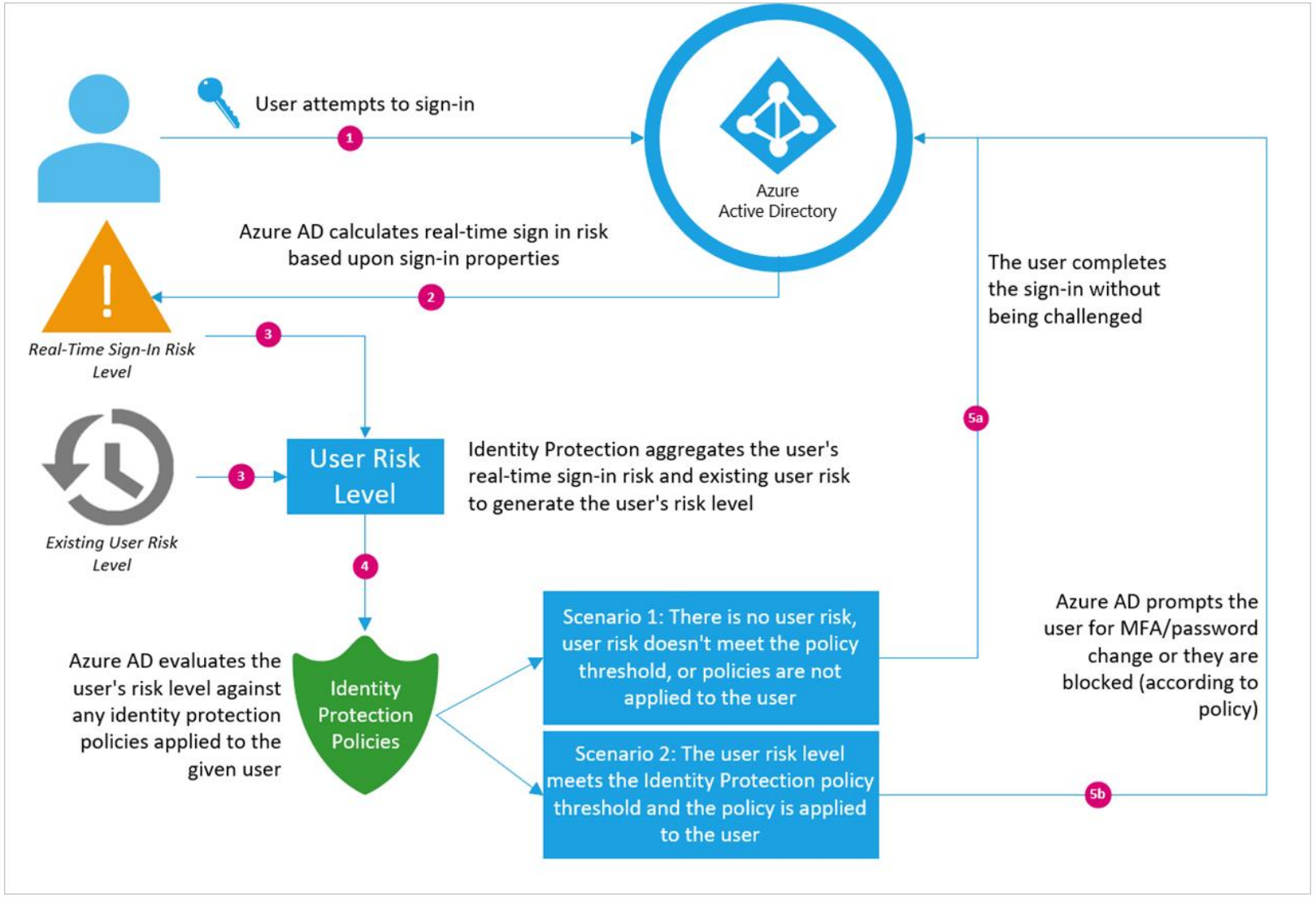
Sign in risk

- A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.
- **Sign-in risk real time** (such as sign-ins from anonymous IP addresses)
- **Sign-in risk aggregate** - Total sign-in risk is the aggregate of detected real-time sign-in risks as well as any subsequent non-real-time risk events associated with the user's sign ins

User risk

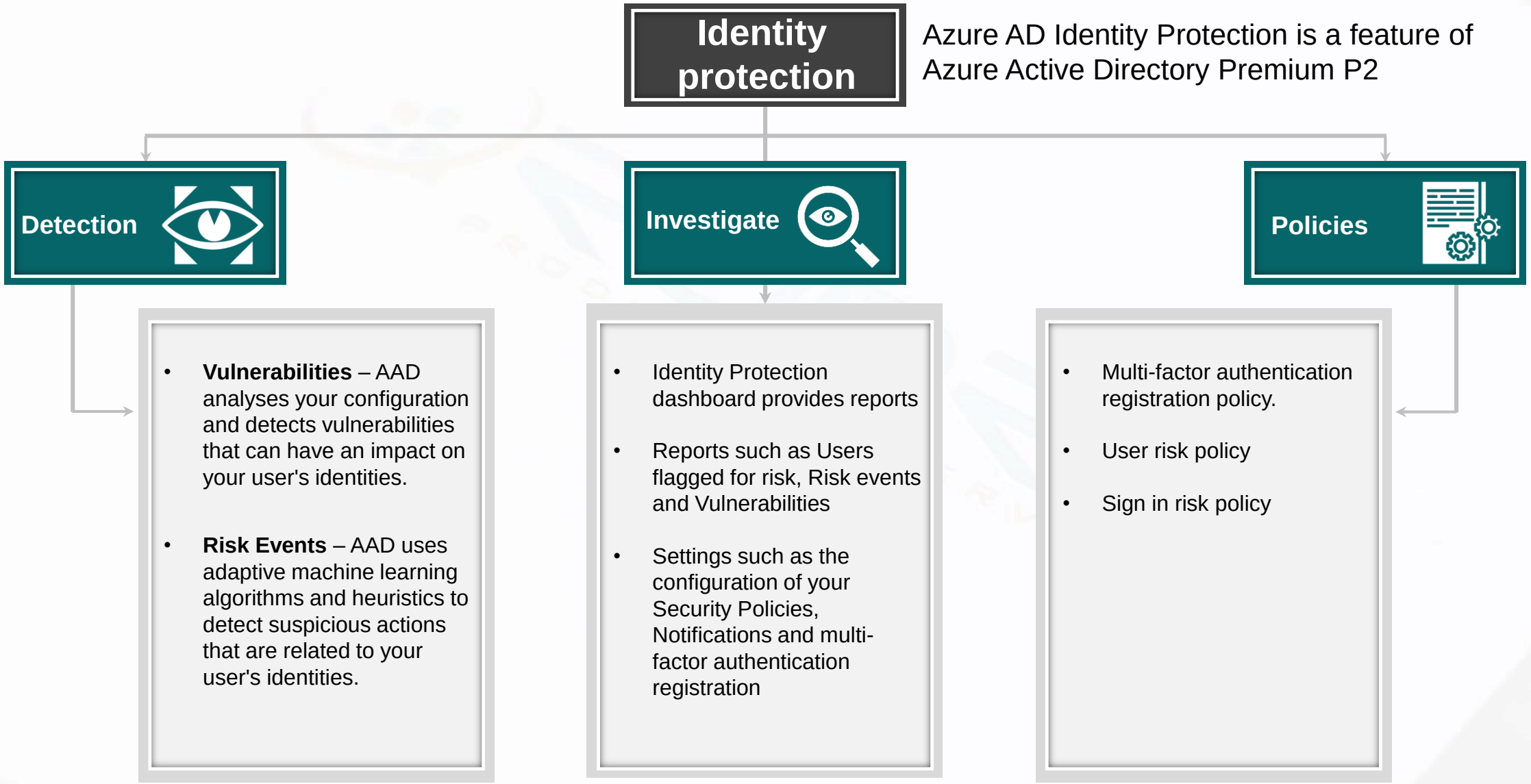
- User risk reflects the overall likelihood that a bad actor has compromised a given identity. User risk contains all the risk activities for a given user, including:
  - Real-time sign-in risk
  - Subsequent sign-in risk
  - Risky user detections.

Identity protection risk detection flow



Introduction to Azure AD Identity Protection

Identity Protection capabilities



Types of risks

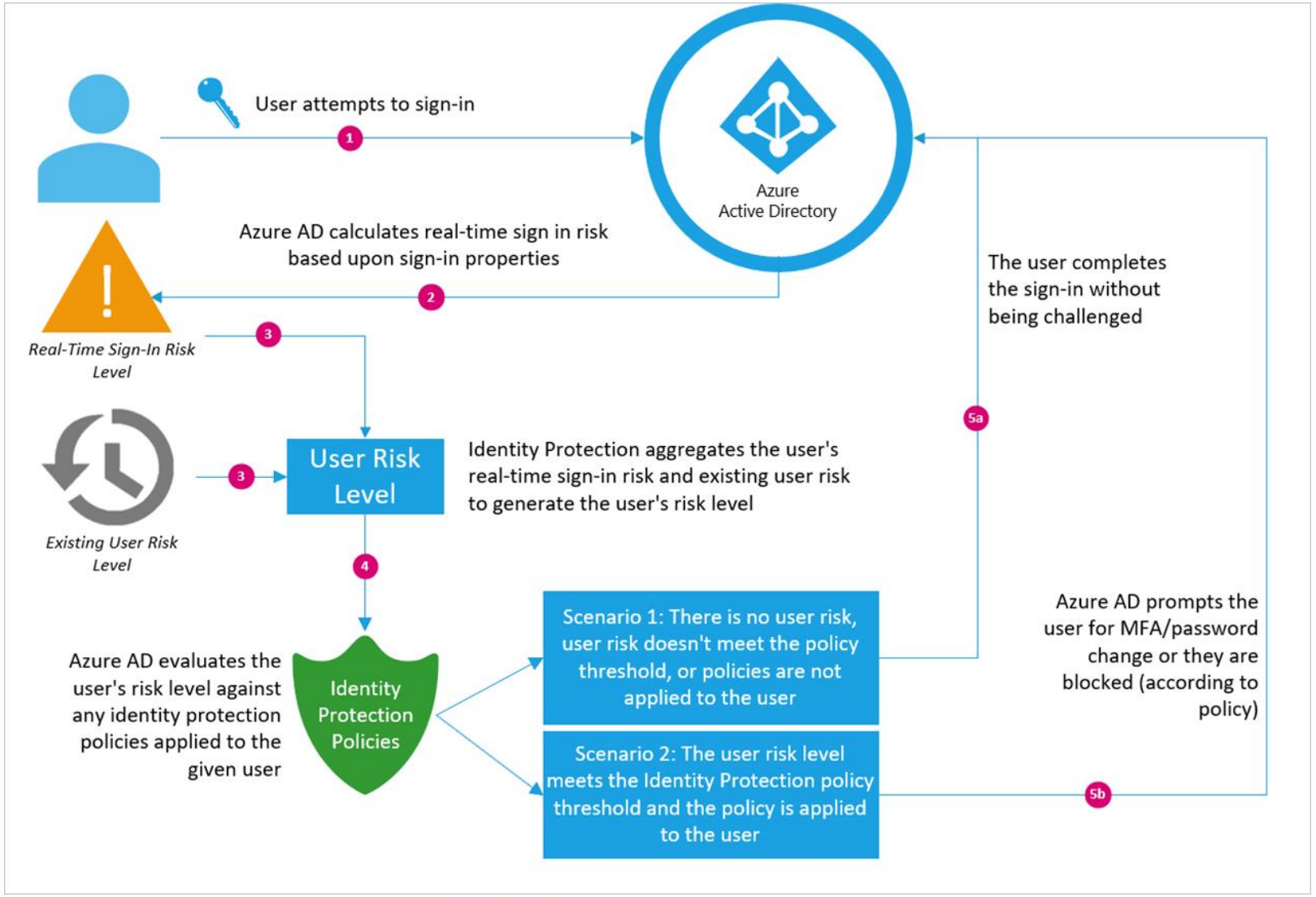
Sign in risk

- A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.
- **Sign-in risk real time** (such as sign-ins from anonymous IP addresses)
- **Sign-in risk aggregate** - Total sign-in risk is the aggregate of detected real-time sign-in risks as well as any subsequent non-real-time risk events associated with the user's sign ins

User risk

- User risk reflects the overall likelihood that a bad actor has compromised a given identity. User risk contains all the risk activities for a given user, including:
  - Real-time sign-in risk
  - Subsequent sign-in risk
  - Risky user detections.

Identity protection risk detection flow



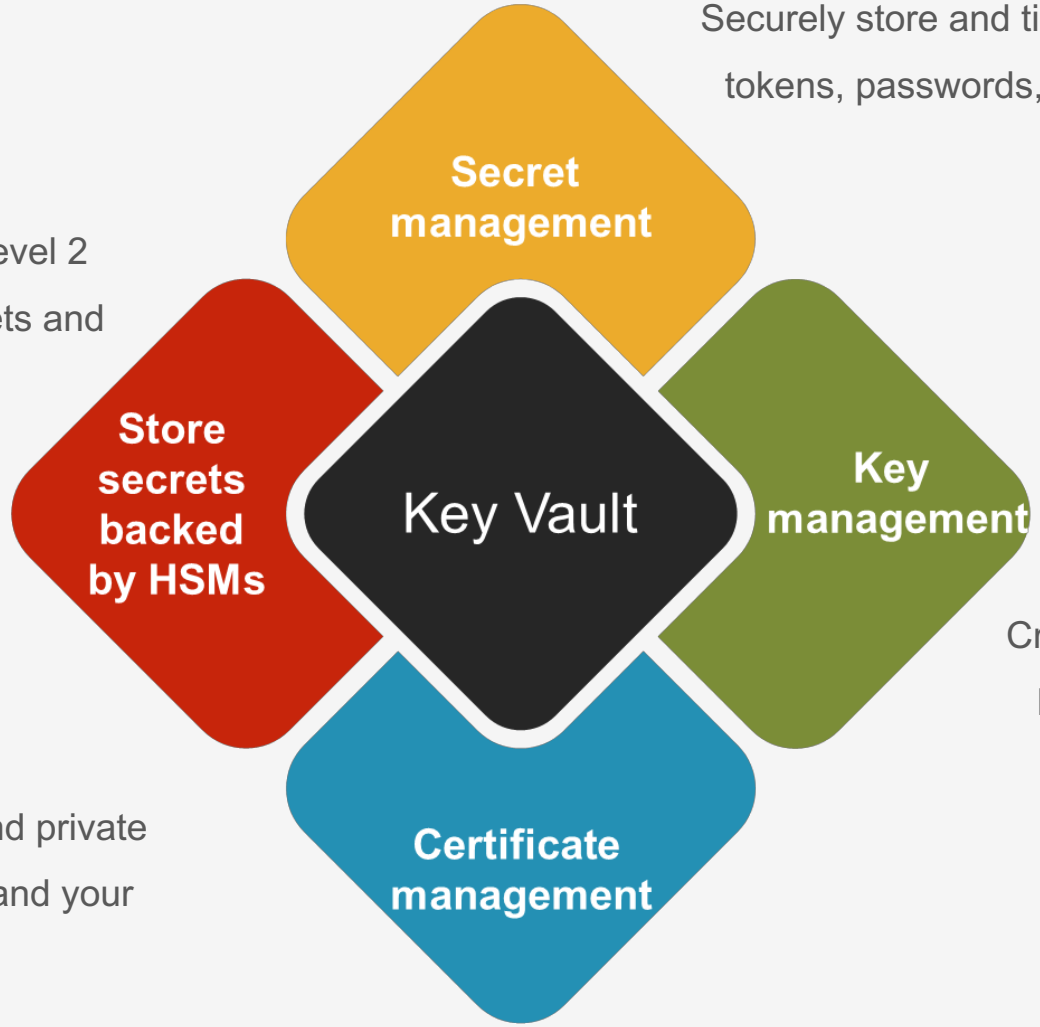
Introduction to Azure Key Vault

Azure Key Vault overview

Azure Key Vault is a service for securely managing Keys, secrets, certificates and any other critical confidential information.

Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets..

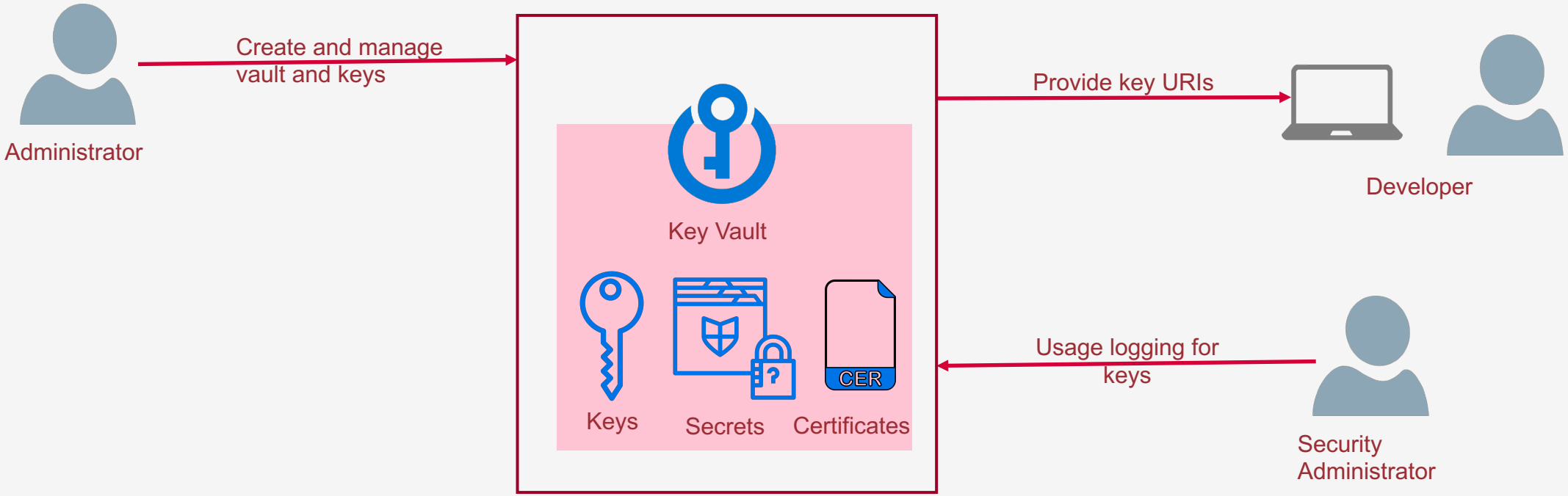
Use either software or FIPS 140-2 Level 2 validated HSMs to help protect secrets and keys.



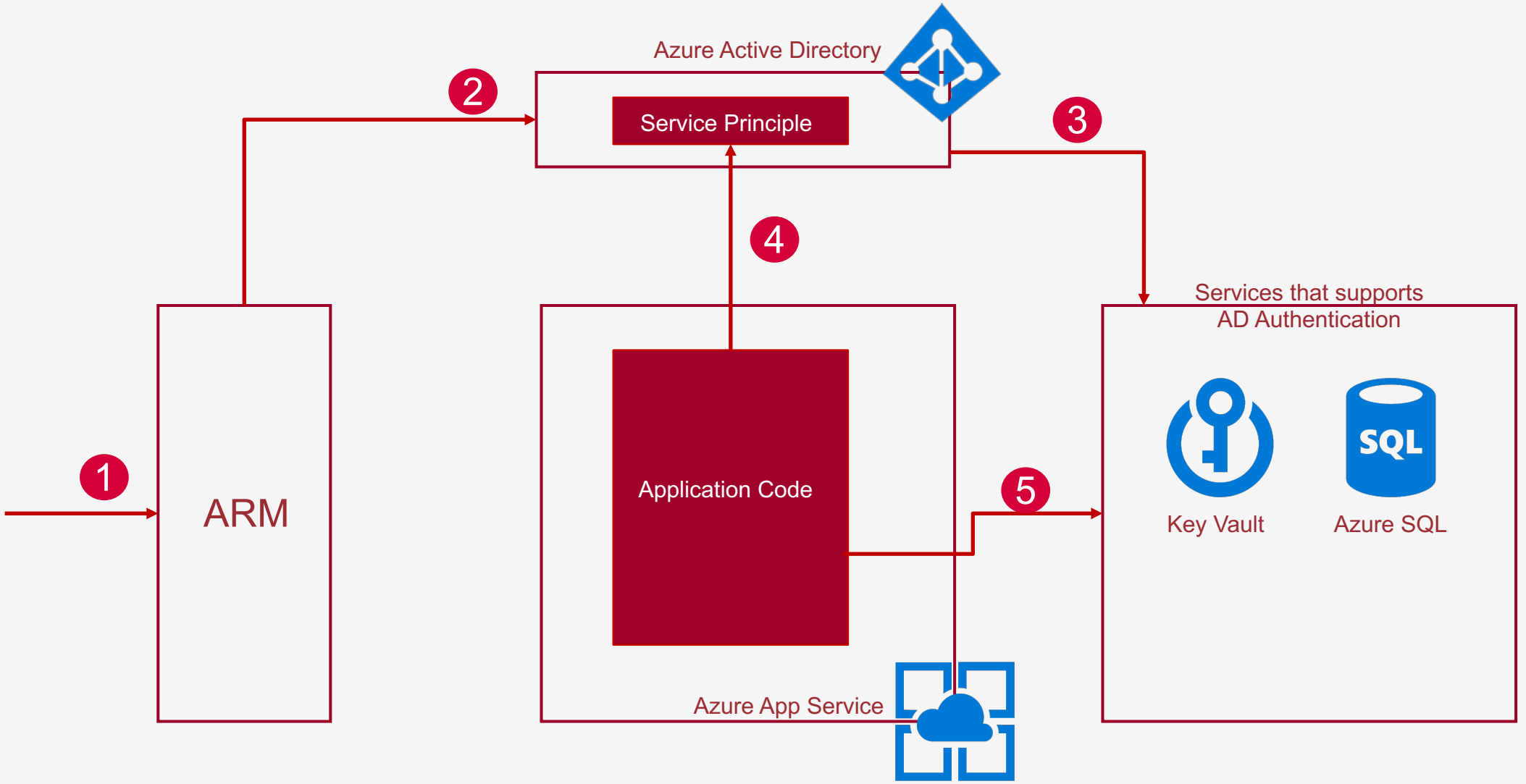
Create and control encryption keys that encrypt your data.

Provision, manage, and deploy public and private SSL/TLS certificates for use with Azure and your internal connected resources.

Key vault usage approach



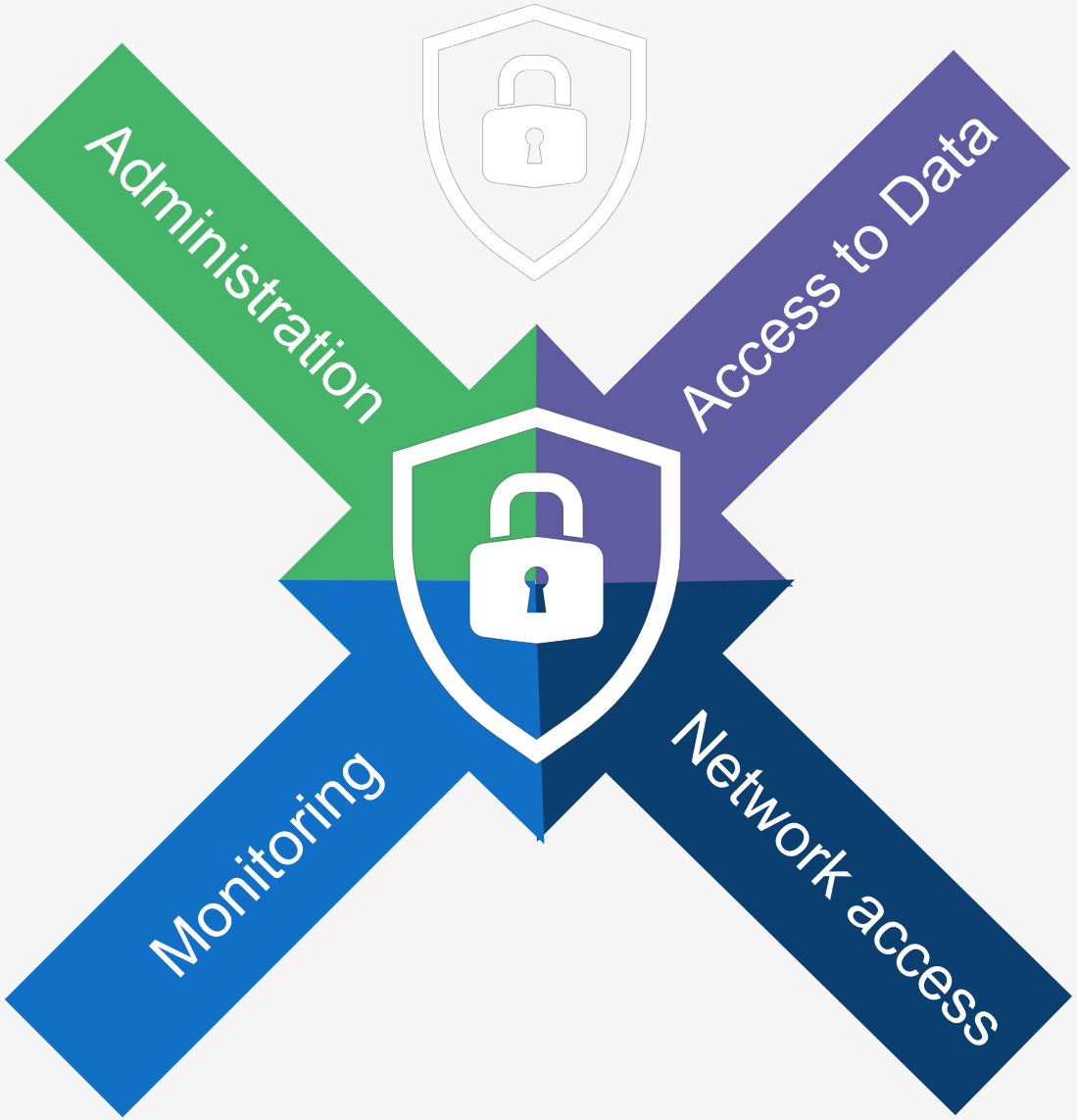
Azure Key Vault usage best practice



Key vault security

01

The management plane is where you manage Key Vault itself and it is the interface used to create and delete vaults. You can also read key vault properties and manage access policies.



02

Key Vault access policies grant permissions separately to keys, secrets, or certificate. Access permissions for keys, secrets, and certificates are managed at the vault level.

04

Key Vault logging saves information about the activities performed on your vault. Logging information can be accessed within 10 minutes after the key vault operation

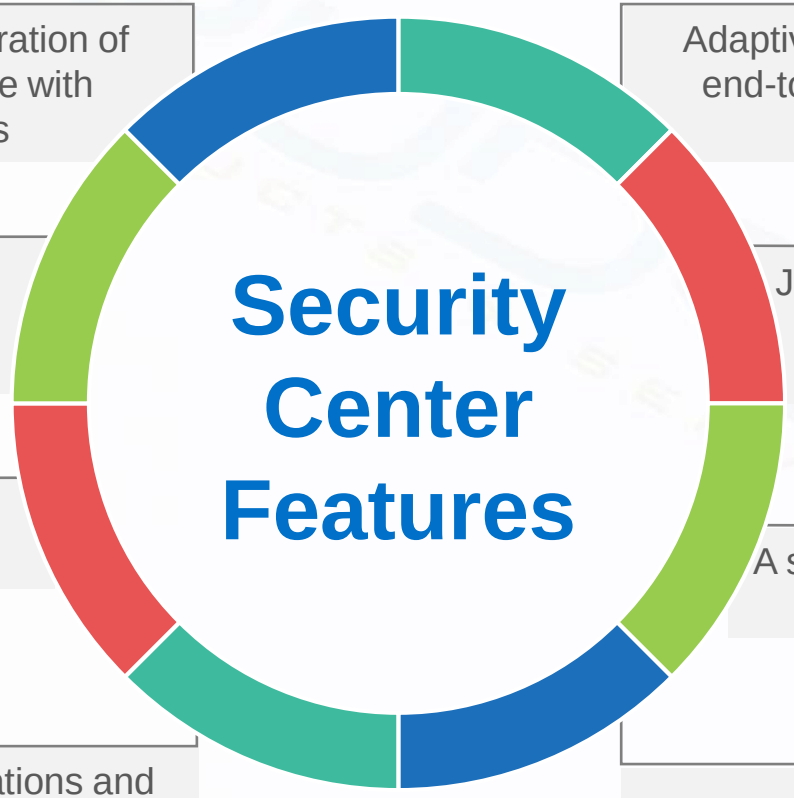
03

You can reduce the exposure of your vaults by specifying which IP addresses have access to them. The virtual network service endpoints for Azure Key Vault allow you to restrict access to a specified virtual network.

Introduction to Azure Security Center

Security Center overview

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud and as well as on premises.



Manage security policy and compliance

A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements

Continuous assessments

Continuously discovers new resources and assesses whether they are configured according to security best practices.

Recommendations

Creates recommendations based on the controls set in the security policy.

Secure score

Constantly reviews your active recommendations and calculates your secure score based on them

Adaptive Application Controls

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center.

Manage Just In Time Access

JIT VM access can be used to lock down inbound traffic to Azure VMs while providing easy access to connect to VMs when needed.

Incidents

A security incident is an aggregation of all alerts for a resource that align with kill chain patterns.

Security Alerts

Detected threats will be raised as security alerts

Preventive monitoring and remediation

RUDRA PRODUCTS & SERVICES

Scope

Bring the subscriptions and management groups under the coverage of Security center

Policies & Configurations

Azure Security Center automatically assigns its built-in security policies on each subscription that is onboarded. You can configure them in Azure Policy.

Implement advanced cloud defences

Advanced cloud defenses such as Just In Time access, Adaptive application controls etc.

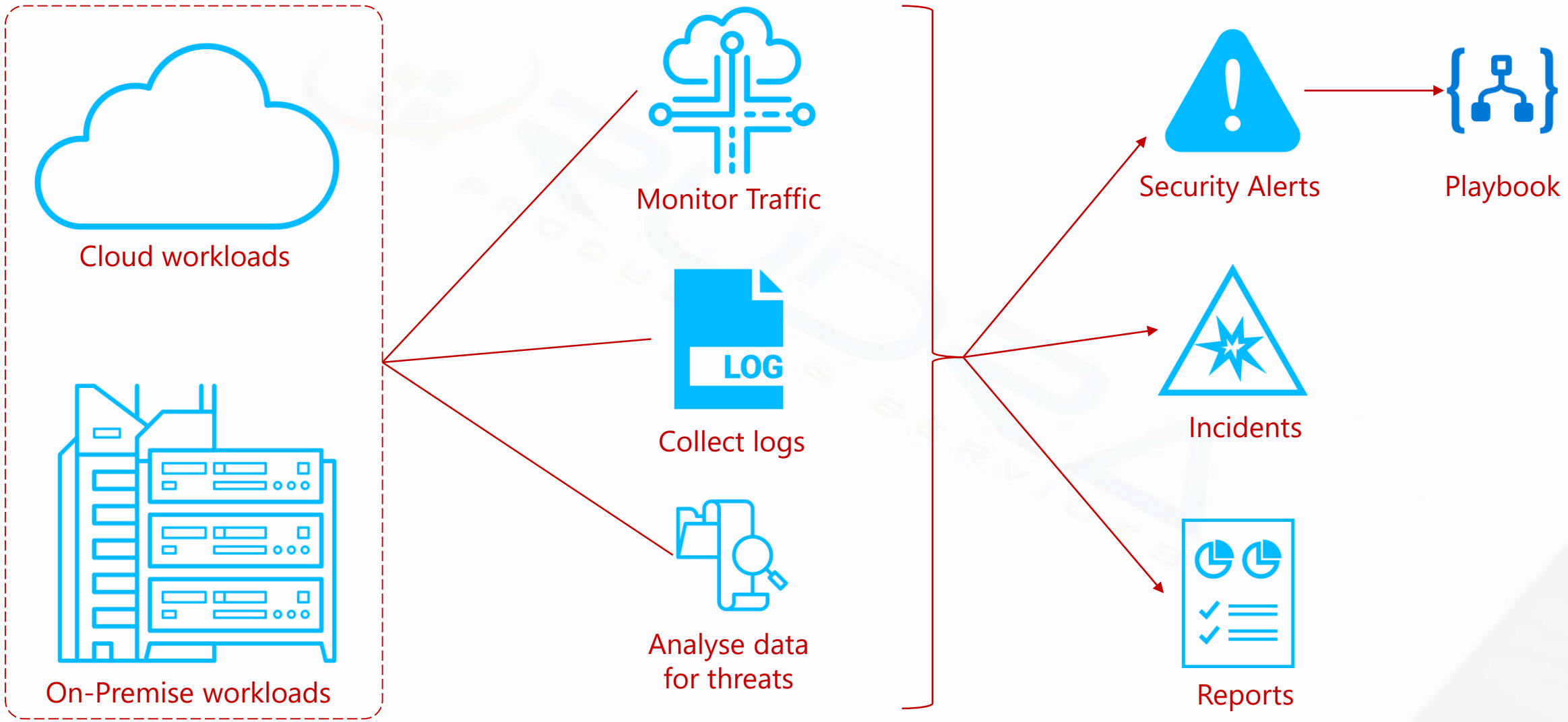
Implement the recommendations

When Security Center identifies potential security vulnerabilities, it creates recommendations. Remediate them to harden security posture of your solution.

Improve the overall secure score

Improve your overall secure score by implementing recommendations and monitor score continuously.

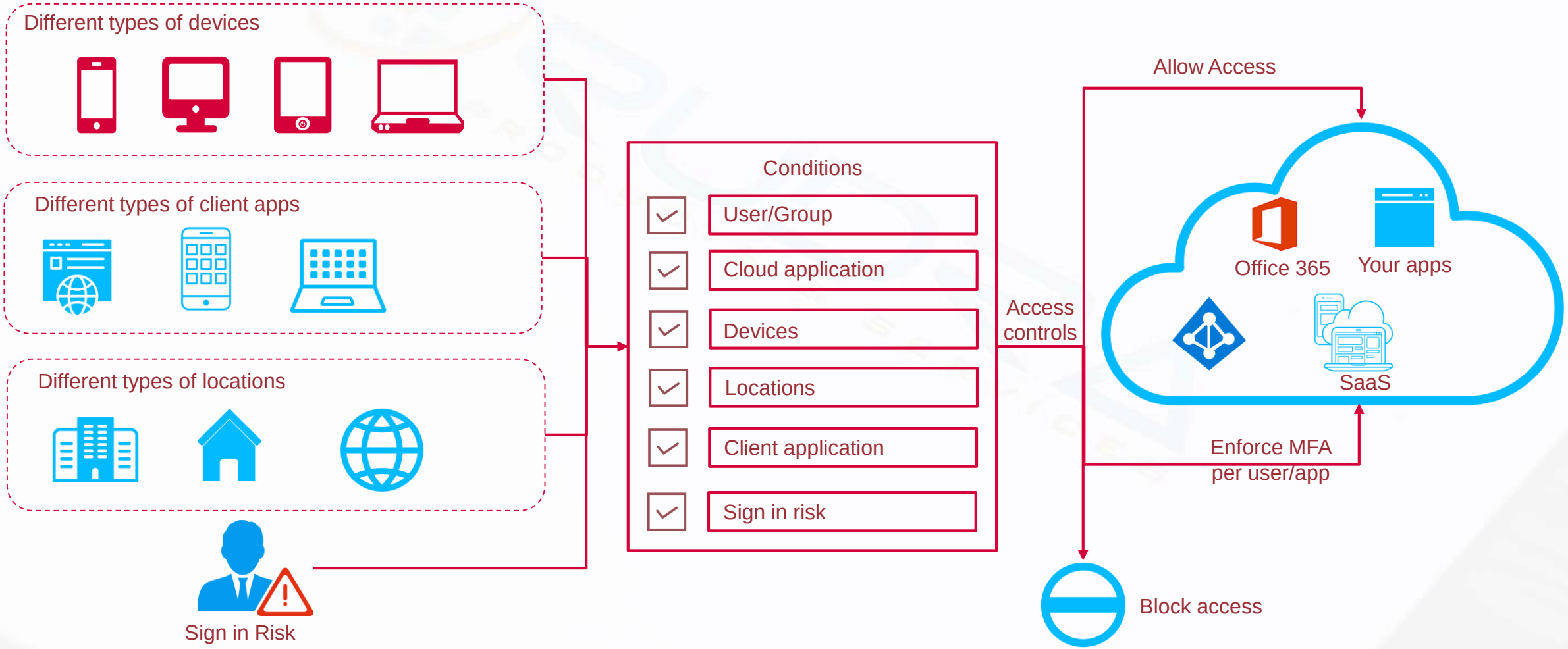
Reactive monitoring and remediation



Introduction to Conditional access

What is Conditional access?

Conditional access is a capability of Azure Active Directory using which you can implement automated access control decisions for accessing your cloud apps that are based on conditions.



Conditional access key points

How conditional access policies applied?

- All policies are enforced in two phases:
  - In the first phase, all policies are evaluated and all access controls that aren't satisfied are collected.
  - In the second phase, you are prompted to satisfy the requirements you haven't met. If one of the policies blocks access, you are blocked and not prompted to satisfy other policy controls.

What you should be careful about?

- For all users, all cloud apps:
  - Block access
  - Require compliant device
  - Require domain join

Plan your conditional access deployment

- **Draft policies**
  - With a conditional access policy, you define a response (**do this**) to an access condition (**when this happens**). Define every conditional access policy you want to implement using this planning model.
- **Plan polices**
  - What outcomes you want to achieve?
  - Block access, Require MFA, Require managed access, Require approved client apps
- **Test policies**
  - You should evaluate your policy using the What if tool
  - Apply a policy to a small set of users and verify it behaves as expected.
  - Apply a policy to all users only if necessary.

Introduction to Azure VM endpoint protection

Microsoft Antimalware

Microsoft Antimalware for Azure is a free real-time protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems.

Real time protection

Monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution

Scheduled scanning

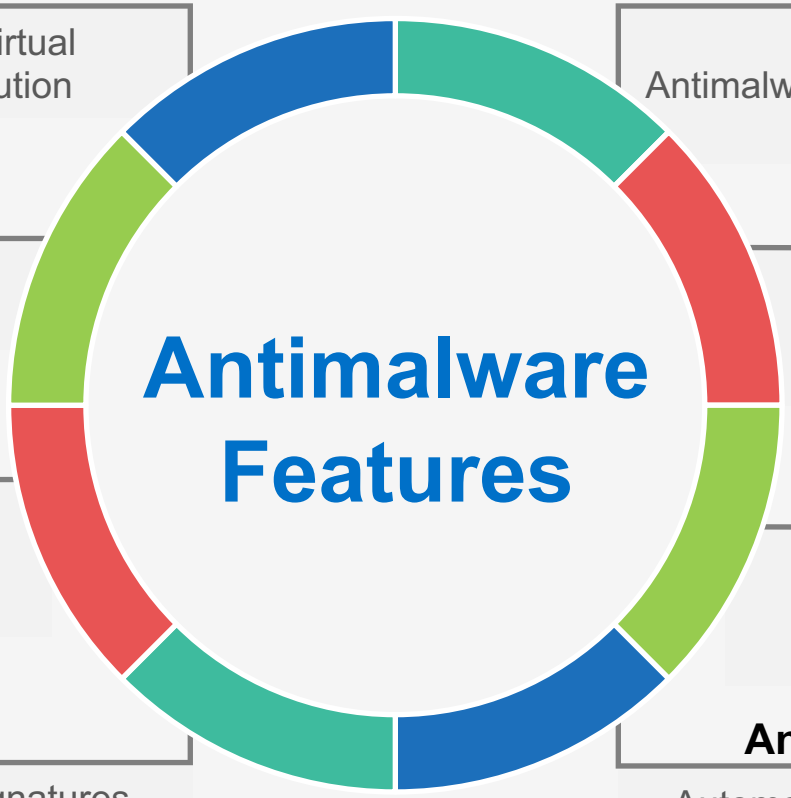
Scans periodically to detect malware, including actively running programs.

Malware remediation

Automatically takes action on detected malware, such as deleting or quarantining malicious files.

Signature updates

Automatically installs the latest protection signatures



Samples reporting

Provides and reports samples to the Microsoft Antimalware service to help refine the service and enable troubleshooting.

Antimalware event collection

Records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log

Exclusions

Allows application and service administrators to configure exclusions for files, processes, and drives

Antimalware engine and platform updates

Automatically updates Antimalware engine and platform

Antimalware customisation

RUDRA PRODUCTS & SERVICES

Exclude extensions

List of file extensions to exclude from scanning

Exclude paths

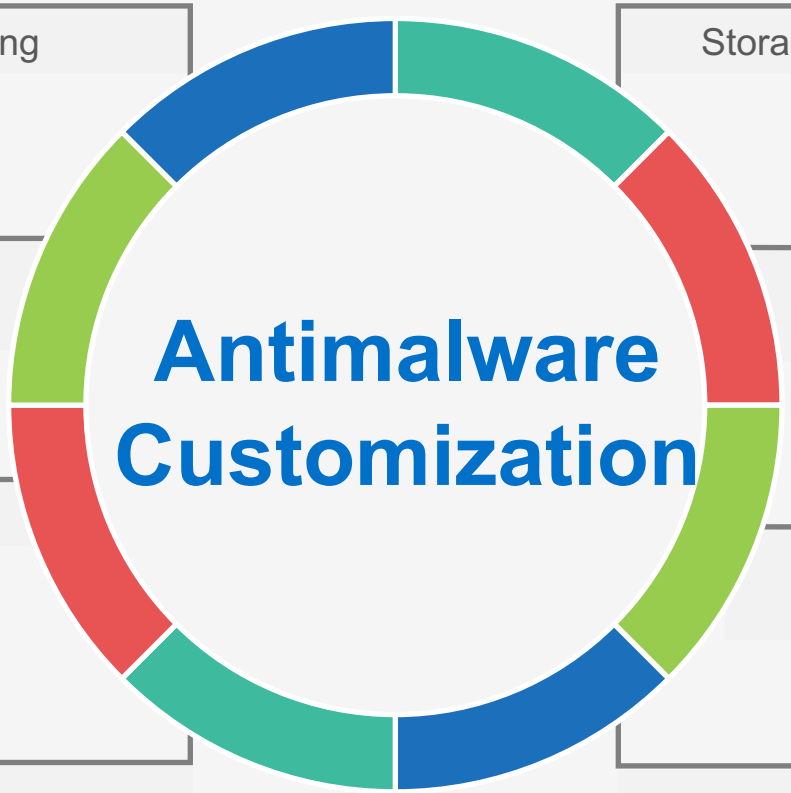
List of files and folders to exclude from scanning

Exclude processes

List of process exclusions

RealtimeProtectionEnabled

Enable or Disable Realtime protection



StorageAccountName

Storage account where collected events will be stored

Monitoring

Enable Antimalware event collection to user subscription storage

Scheduled scan enable

Enables or disables a periodic scan for active malware on the system

Scheduled scan settings

Customize day, time & scan type

Deployment scenarios

RUDRA PRODUCTS & SERVICES

Virtual machines & Scale sets

The Microsoft Antimalware Client and Service is not installed by default in the Virtual Machines platform

For virtual machines, install as an extension using Azure portal, Visual studio and Cmdlets

Cloud services

The Microsoft Antimalware Client and Service is installed by default in a disabled state in all supported Azure guest operating system families in the Cloud Services platform

For cloud service, use AntiMalware PowerShell Cmdlets

App services

When using Azure App Service, the underlying service that hosts the web app has Microsoft Antimalware enabled on it.

Events written to System OS events log under the “Microsoft Antimalware”

Azure Storage

Azure Storage security

Azure storage security overview

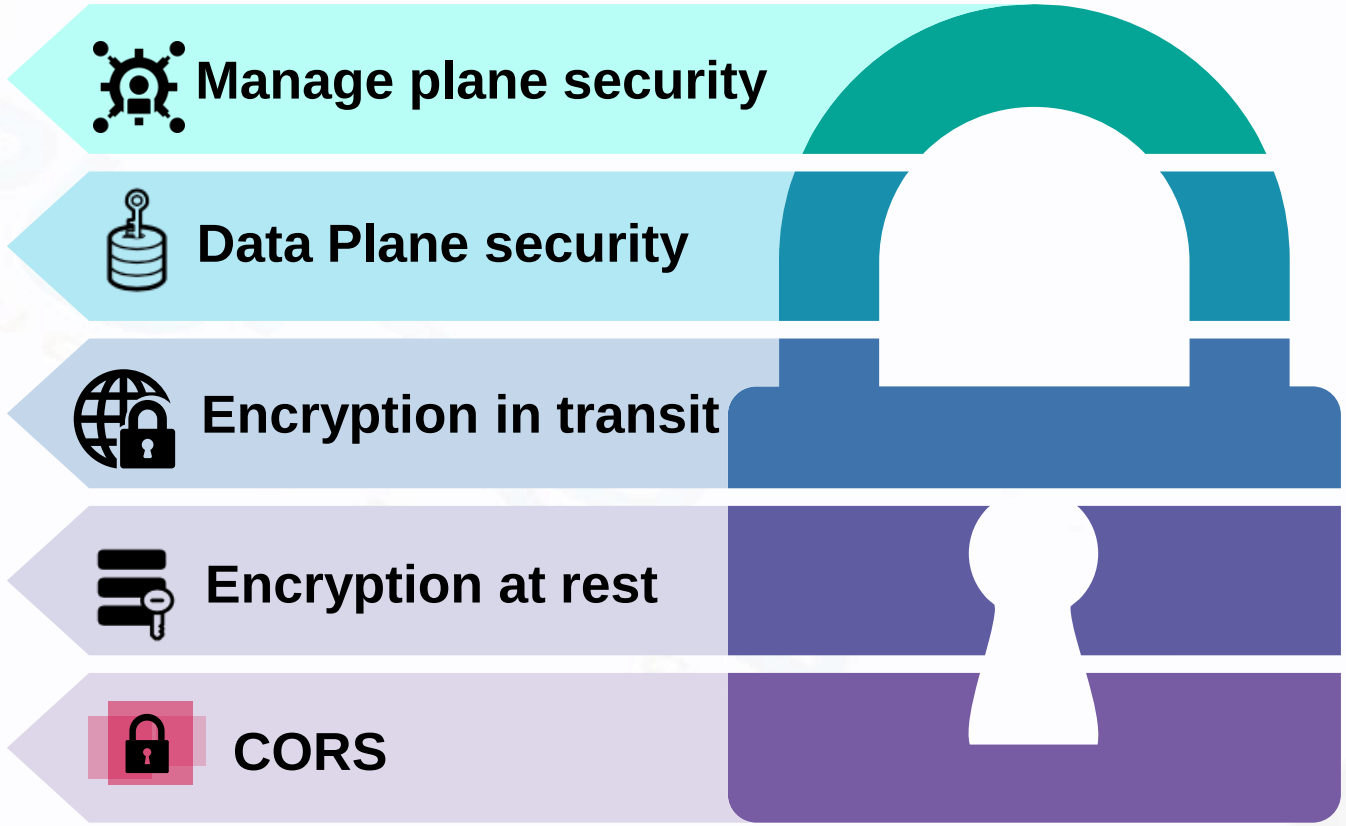
Securing your storage account

Securing access to your data

Encryption in transit

Encryption at rest

Cross Origin Resource Sharing



Management plane security

- Management plane refers to the operations that effect the storage account itself.

- Role Based Access Control
  - Each Azure subscription has an Azure Active Directory. Users, groups and applications from that directory can be granted access to manage resources in the Azure subscription. This is referred as Role Based Access Control.
  - Access is granted by assigning the appropriate RBAC role to users, groups, and applications at the right level. This level can be subscription, resources group and resources.

- Key points to remember
  - When you assign a role, You can control access to operations used to manage the storage account and data objects in the account..
  - Each role has a list of Actions & Not Actions.
  - There are some standard management roles available. For e.g. Owner, Reader, Contributor etc.
  - Data operations roles include Storage blob data reader role etc.

Data plane security

- Data plane security refers to the methods used to secure data objects (blobs, queues, tables and files) within the storage account.

- Three methods for controlling access to data objects

    - Using Azure AD to authorize access to containers and queues (Preview). Azure AD provides advantages over other approaches to authorization, including removing the need to store secrets in your code.
    - Storage account keys
    - Shared Access Signatures

- You can allow public access to your blobs by setting the access level for the container that holds the blob accordingly.

- Storage firewall to restrict access only to known IP address ranges and virtual networks

Encryption in Transit

- Transport level Encryption using HTTPS
  - Always use HTTPS when using REST APIs or accessing objects in storage.
  - If you are using SAS, you can specify that only HTTPS should be used

- Using encryption in transit for Azure file shares
  - SMB2.1 do not support encryption so connections are only allowed within the same region.
  - SMB3.0 supports encryption and cross region access is allowed

- Client side encryption
  - Encrypt the data before being transferred to Azure storage
  - When retrieving the data from Azure, data is decrypted after it is received on the client side.

Encryption at rest

- Client side encryption
  - Encrypt the data before being transferred to Azure storage
  - When retrieving the data from Azure, data is decrypted after it is received on the client side

- Storage Service Encryption (SSE)
  - SSE is enabled for all storage accounts and cannot be disabled
  - SSE automatically encrypts data in all performance tiers (Standard and Premium), all deployment models (Azure Resource Manager and Classic), and all of the Azure Storage services (Blob, Queue, Table, and File).
  - You can use either Microsoft-managed keys or your own custom keys.

- Azure Disk Encryption
  - Encrypt the OS & data disks used by IaaS Virtual Machine
  - You can enable encryption on existing IaaS VMs
  - You can use customer provided encryption keys

Important note: Refer to the link in the resource section of this lecture for comparison between above three encryption types

Cross Origin Resource Sharing

- When a web browser running in one domain makes an HTTP request for a resource from a different domain, this is called a cross-origin HTTP request

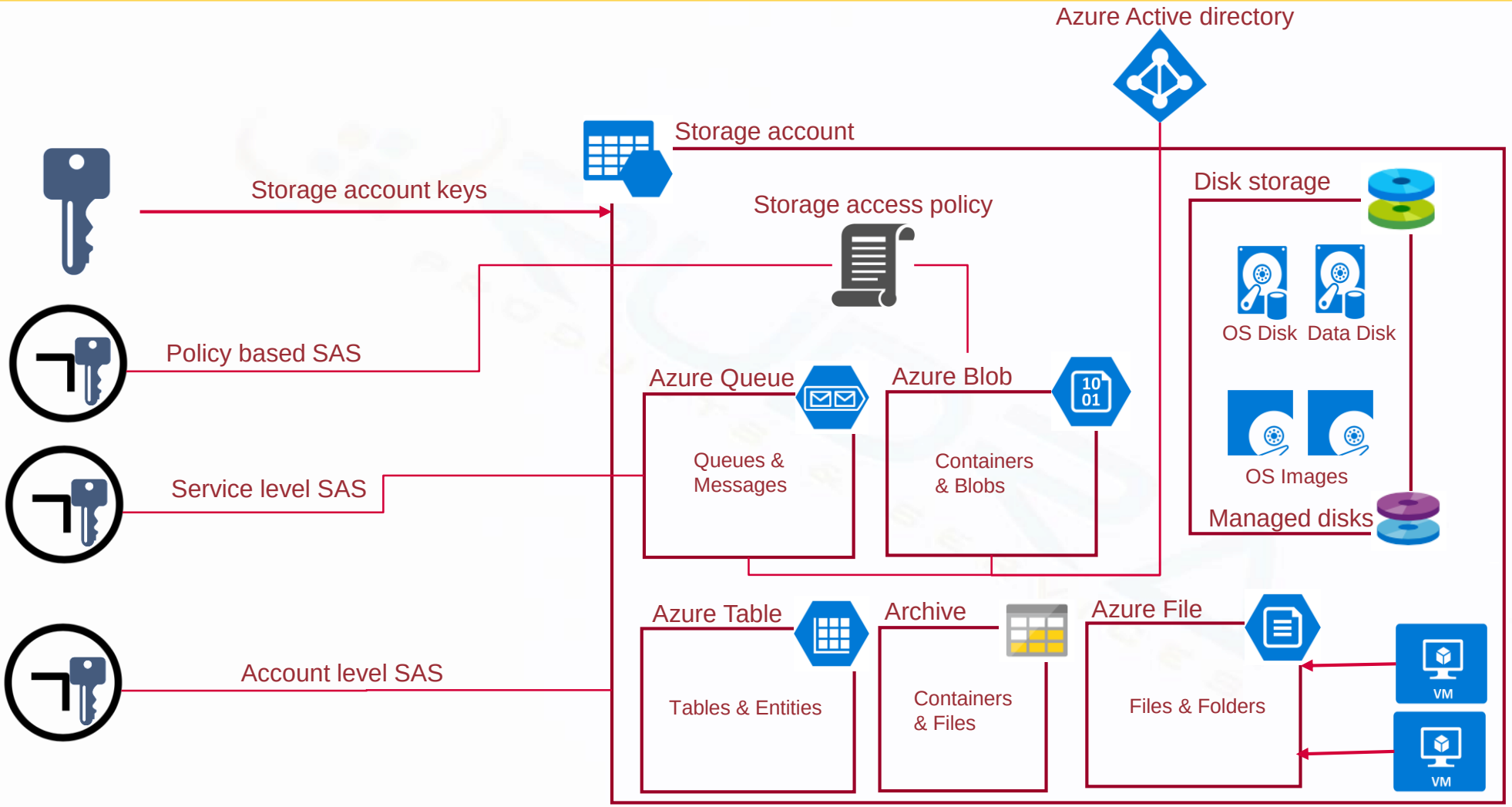
- Azure Storage allows you to enable CORS. For each storage account, you can specify domains that can access the resources in that storage account. For example, enable CORS on the mystorage.blob.core.windows.net storage account and configure it to allow access to mywebsite.com

- CORS allows access but does not provide authentication which means you still need to use SAS to access non-public storage resources.

- By default, CORS is disabled on all services.

Azure Storage services – Data plane security deep dive

Data plane security options



Storage account keys

- **Storage account keys** – These are 512-bit strings created by Azure, along with the storage account name, can be used to access the data objects stored in storage account.
- For example, you can read blobs, write to queues, create tables, and modify files.
- Access to the storage keys for a storage account using the Azure Resource Manager model can be controlled through Role-Based Access Control (RBAC).

Shared Access Signatures

- A **Shared Access Signature** is a string containing a security token that can be attached to a URI that allows you to delegate access to storage objects and specify constraints such as permissions and date/time range of access
  - With tables, you can actually grant permissions to access a range of entities in the table by specifying the partition and row key ranges that you want user to access.
  - For queues, you can grant permission to a web role to put the messages into queue and a worker role to read messages from the queues.
  - With blobs, you can give somebody to upload videos into the container and an web application to read the videos.

- **Why SAS**
  - Storage account keys gives complete access to data objects in storage account whereas with SAS you can be selective.
  - Give permissions for a limited amount of time
  - Restrict requests made using SAS to a certain IP address or range external to Azure
  - Restrict requests to be made using a specific protocol

Types of SAS

- A **service level SAS** can be used to access specific resources in the storage account. For e.g.
  - Retrieving list of blobs in a container
  - Add messages into a queue

- An **account-level SAS** can be used to grant permissions that are not permitted using a service level SAS. For e.g.
  - Permission to create containers, tables, queues and file shares.
  - Access to multiple services at once

Controlling a SAS with a stored access policy

A shared access signature can take one of two forms:

Adhoc SAS: When you create an adhoc SAS, the start time, expiry time, and permissions for the SAS are all specified in the SAS URI. This type of SAS can be created as an account SAS or a service SAS.

SAS with stored access policy: A stored access policy is defined on a resource container--a blob container, table, queue, or file share--and can be used to manage constraints for one or more shared access signatures. When you associate a SAS with a stored access policy, the SAS inherits the constraints--the start time, expiry time, and permissions--defined for the stored access policy.

Application management with Azure Active Directory

Introduction to Application management

Azure Active Directory (Azure AD) provides secure and seamless access to cloud and on-premises applications. Users can sign in once to access Office 365 and other business applications from Microsoft, software as a service (SaaS) applications, on-premises applications, and line of business (LOB) apps

Key advantages

- Manage risk with conditional access policies
- Improve productivity with single sign on
- Address governance and compliance
- Manage costs

Introduction to Single sign on

Single sign-on (SSO) adds security and convenience when users sign-on to applications in Azure Active Directory (Azure AD).

Advantages of Single sign on

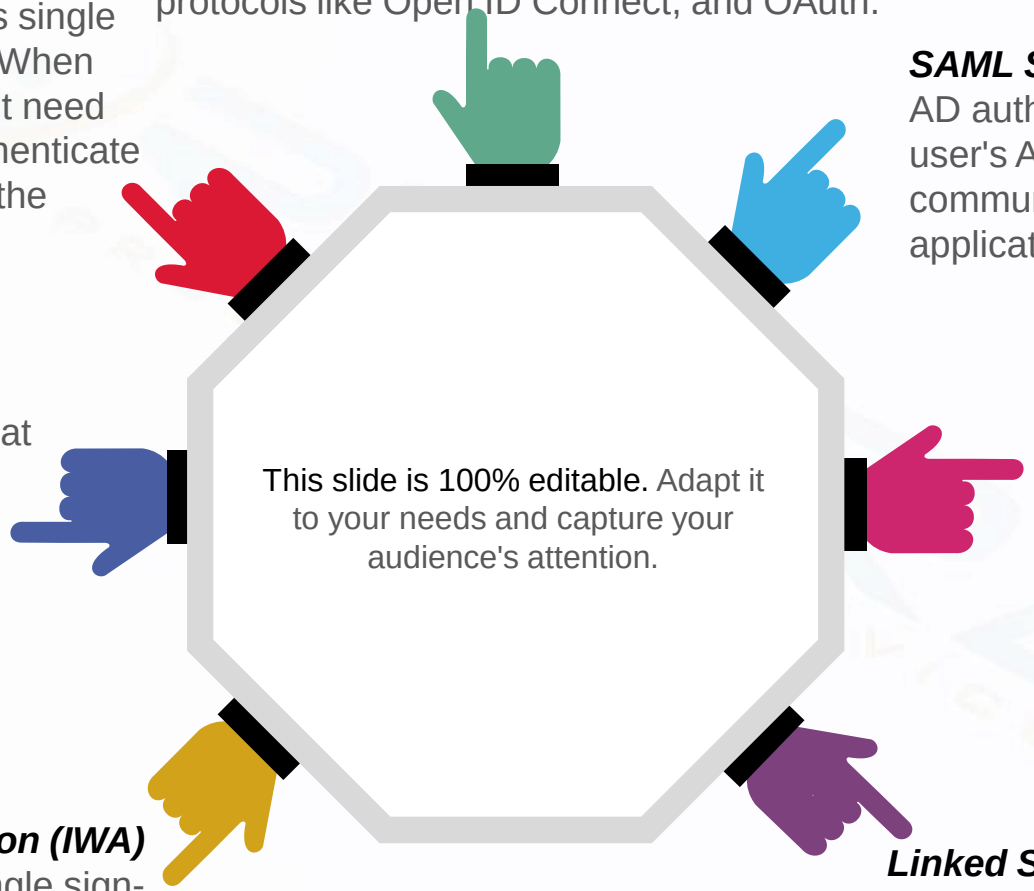
- One set of credentials to access domain joined devices, company resources, SaaS applications and web applications hosted on on-premise
- User can launch application from office 365 portal or Azure AD My apps panel
- Centralised user access management to applications based on group membership

Single sign on options

OpenID Connect and Oauth - When developing new applications, use modern protocols like Open ID Connect, and OAuth.

Disable SSO - Disabled mode means single sign-on isn't used for the application. When single sign-on is disabled, users might need to authenticate twice. First, users authenticate to Azure AD, and then they sign in to the application.

SAML SSO - With SAML single sign-on, Azure AD authenticates to the application by using the user's Azure AD account. Azure AD communicates the sign-on information to the application through a connection protocol



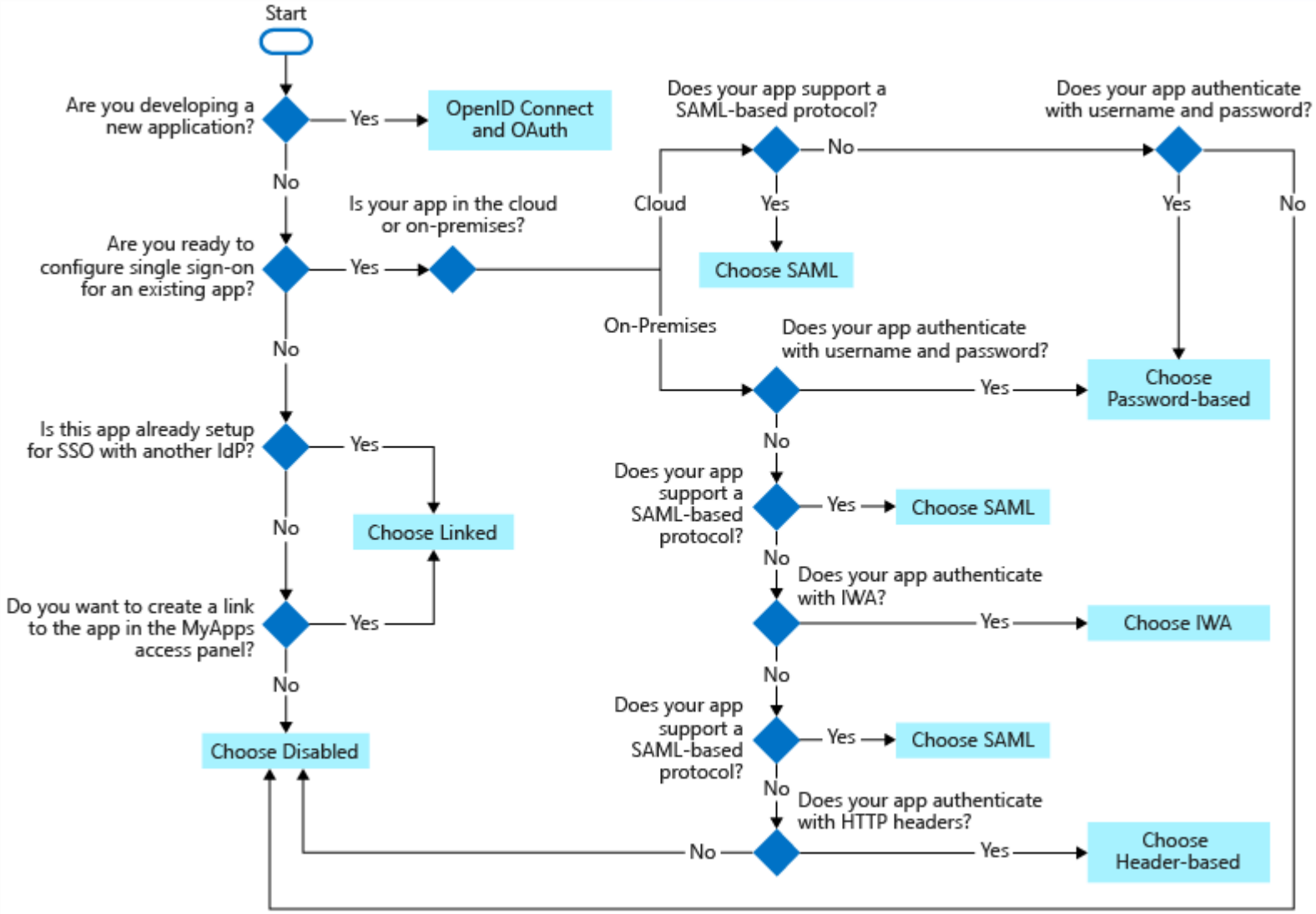
Header based SSO - Header-based single sign-on works for applications that use HTTP headers for authentication. This sign-on method uses a third-party authentication service called PingAccess. A user only needs to authenticate to Azure AD

Password based SSO - With password-based sign-on, users sign on to the application with a username and password the first time they access it. After the first sign-on, Azure AD supplies the username and password to the application.

Integrated Windows Authentication (IWA) SSO Application Proxy provides single sign-on (SSO) to applications that use Integrated Windows Authentication (IWA), or claims-aware applications

Linked SSO - Linked sign-on enables Azure AD to provide single sign-on to an application that is already configured for single sign-on in another service.

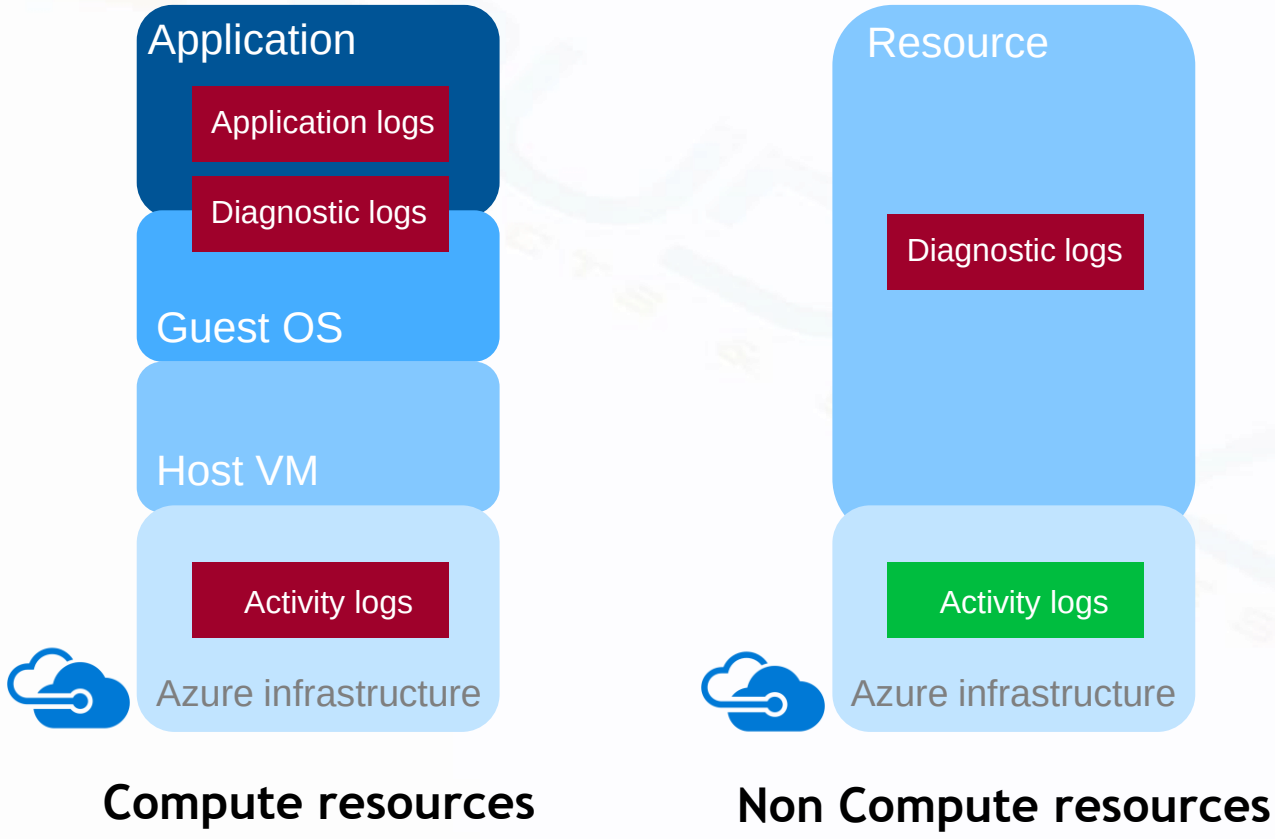
Decision tree for SSO option



Introduction to Azure Monitor Activity Logs, Metrics

Activity logs

The Azure Activity log is a subscription log that provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.



Activity log record categories

Alerts
This category contains the record of all activations of Azure alerts.

Autoscale
This category contains the record of any events related to the operation of the autoscale engine based on any autoscale settings you have defined in your subscription.

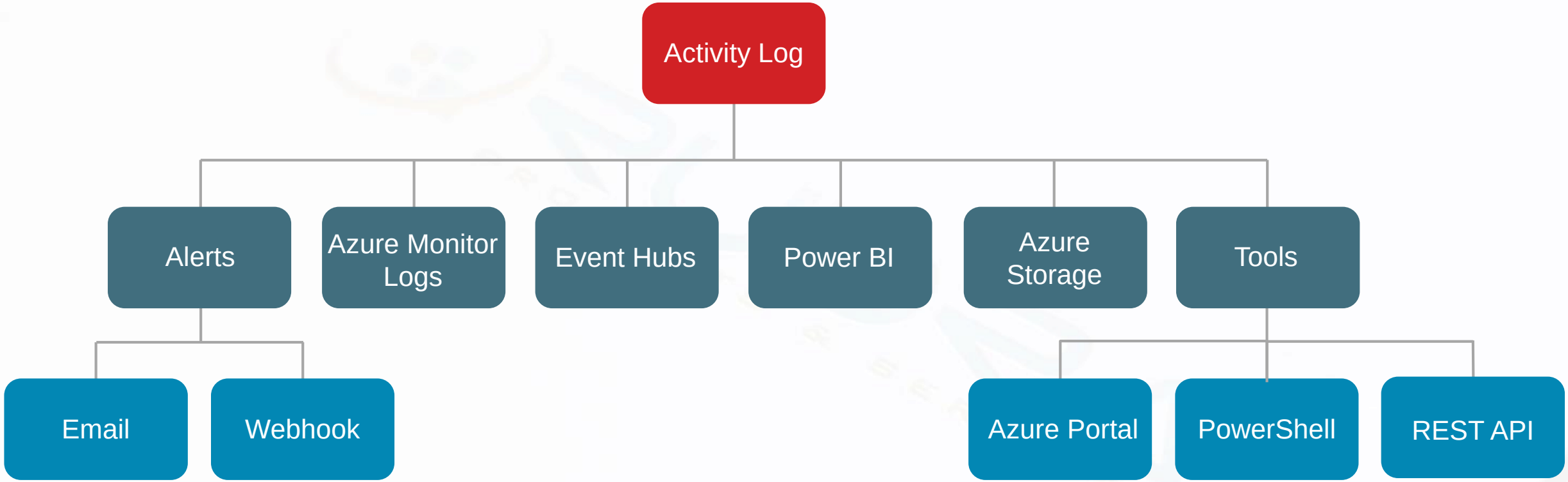
Service & Resource health
This category contains the record of any service health incidents and resource health events

Recommendations & Security
This category contains recommendation events from Azure Advisor and records of any security alerts from security centre

Administrative
This category contains the record of all create, update, delete, and action operations performed through Resource Manager

Policy
This category contains records of all effect action operations performed by Azure Policy.

Activity log – Things you can do



Metrics

Metrics are numerical values that describe some aspect of a system at a particular time. Metrics are collected at regular intervals and are useful for alerting because they can be sampled frequently, and an alert can be fired quickly with relatively simple logic.

01 ***Analyze & Visualize -*** *Use metrics explorer to analyze collected metrics on a chart and compare metrics from different resources.*

02 ***Alert -*** *Configure a metric alert rule that sends a notification or takes automated action when the metric value crosses a threshold..*

03 ***Automate -*** *Use Autoscale to increase or decrease resources based on a metric value crossing a threshold.*

04 ***Export -*** *Route Metrics to Logs to analyze data in Azure Monitor Metrics together with data in Azure*

05 ***Retrieve*** *- Access metric values from different tools*

Sources of Metrics

- **Platform metrics** are created by Azure resources and give you visibility into their health and performance. Platform metrics are collected from Azure resources at one-minute frequency unless specified otherwise in the metric's definition.

- **Guest OS metrics** are collected from the guest operating system of a virtual machine.

- **Application metrics** are created by Application Insights for your monitored applications and help you detect performance issues and track trends in how your application is being used.

- **Custom metrics** are metrics that you define in addition to the standard metrics that are automatically available.

Azure SQL database security overview

Azure SQL database storage security overview

RUDRA PRODUCTS & SERVICES

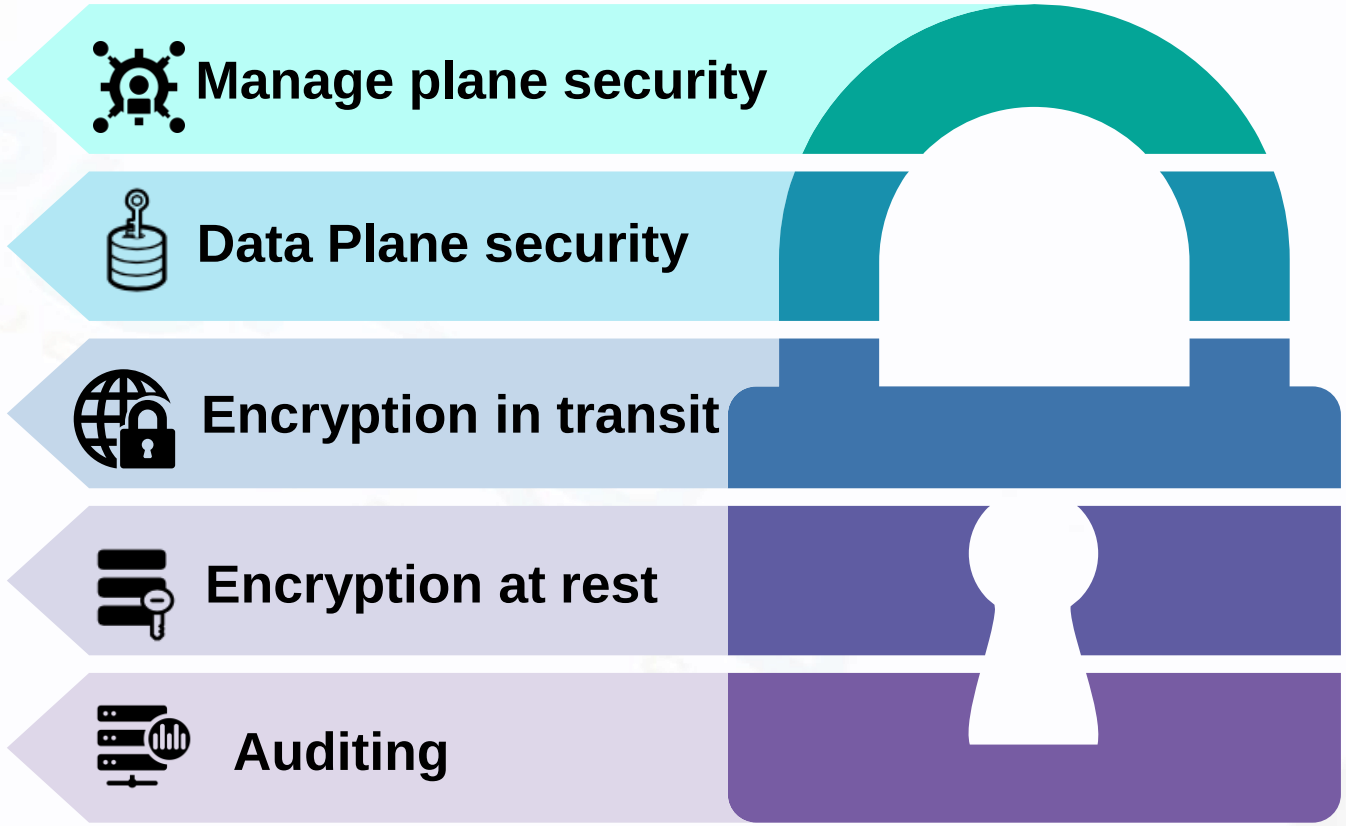
Securing your logical server and database configuration

Securing access to your data

Encryption in transit

Encryption at rest

Audit the changes to the data



Data plane security basics

- SQL Database supports two types of authentication, SQL Authentication and Azure Active Directory Authentication (Azure AD Authentication).

- **SQL Authentication** - With SQL Authentication, when you create a SQL Database, you also create a login that is the server-level principal account for your SQL Database server.

- **Azure AD authentication** uses identities managed by Azure Active Directory and is supported for managed and integrated domains. To use Azure AD authentication, you must create a second server-level principal account called “Azure AD Admin” to administer Azure AD users and groups. This admin can also perform all operations the regular (SQL) SA can.

- **Server- level roles** - While you can use the server-level principal account to manage server-level security, you also have the option to assign logins to other SQL Database security roles.

- **Database-level roles** - The built-in security roles at the database level are similar to on-premises SQL Server security roles. You can implement database-level security by using fixed database or custom roles for your application

Advanced data security

Advanced data security is a unified package for advanced SQL security capabilities.

	**Data discovery & Classification**	• *Discover, classify, label & protect the sensitive data in your database* • *Can be used to provide visibility into your database classification state, and to track the access to sensitive data within the database and beyond its borders..*
	**Vulnerability assessment**	• *Discover, track, and help you remediate potential database vulnerabilities* • *Provides visibility into your security state, and includes actionable steps to resolve security issues*
	**Advanced Threat Protection**	• *Continuously monitors your database for suspicious activities, and provides immediate security alerts on potential vulnerabilities, SQL injection attacks* • *Advanced Threat Protection alerts provide details of the suspicious activity and recommend actions*

Encryption at rest

- **Transparent Data Encryption** (TDE) has been an on-premises SQL Server option since SQL Server 2008, available exclusively for data at rest. That is, your data files and backups are encrypted, while data tables are not directly encrypted. Specifically, if a user has given permissions to a database with TDE enabled, the user can see all data.

- **Always Encrypted**, which introduces a set of client libraries to allow operations on encrypted data transparently inside of an application. The key is always under control of the client and application, and is never on the server. Neither server nor database administrators can recover data in plain text.

Encryption in transit

- SQL Database connections are encrypted using TLS/SSL for the Tabular Data Stream (TDS) transfer of data. For Azure SQL Database, Microsoft provides a valid certificate for the TLS connection.

- **Row-Level Security** (RLS) restricts access to rows, using a security predicate that is defined as an inline table-valued function (TVF). You create a security policy to enforce this function.

- **Dynamic data masking** - Dynamic Data Masking (DDM) is a feature that allows you to limit access to your sensitive data without making client or application changes, while also enabling visibility of a portion of the data. The underlying data in the database remains intact (data is obfuscated dynamically), and it is applied based on user privilege

Auditing

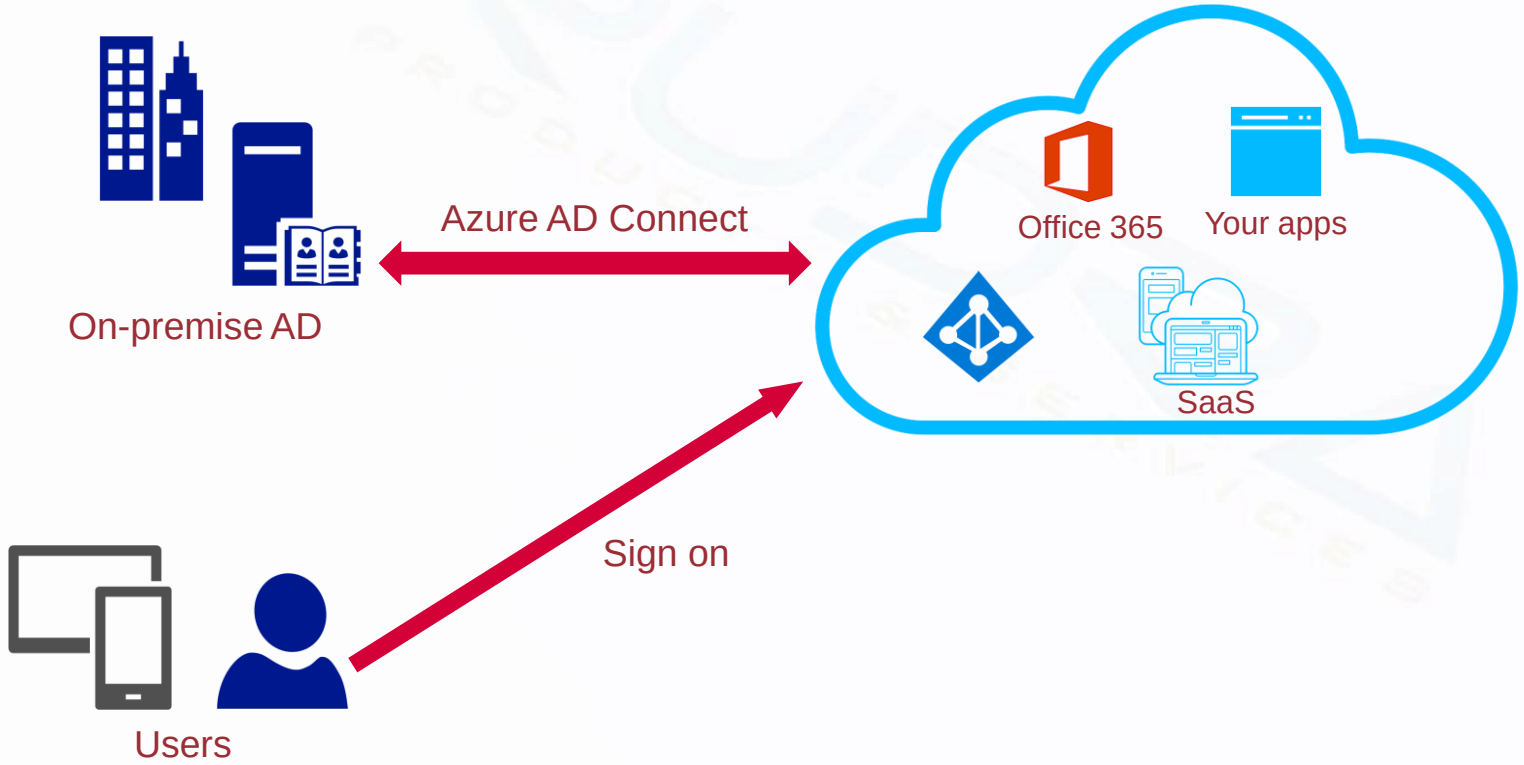
- SQL Database auditing is available in all service tiers. By implementing the auditing feature in SQL Database, you can retain your audit trail over time, as well as analyse reports showing database activity of success or failure conditions

- You can configure auditing at the server level. In that case, all databases inherit the same audit settings. As an alternative, you can configure audit policies for each SQL Database individually.

AD Connect, Authentication methods & topologies

Introduction to AD Connect

AD connect is a corner stone for delivering Azure Active Directory hybrid identity solution. Using AD connect you are able to synchronise identities between on-premise AD and Azure AAD and implement different authentication methods

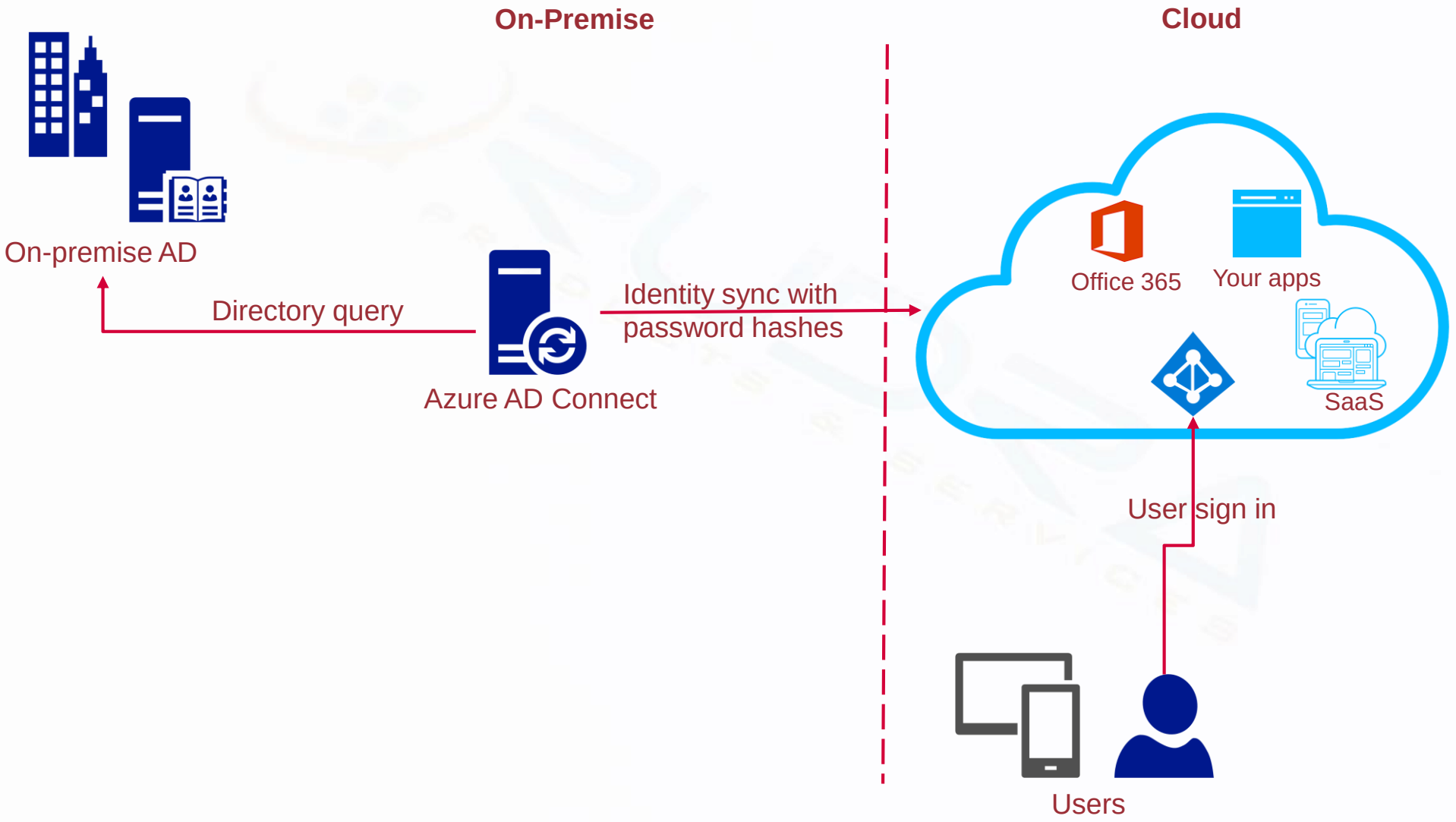


Authentication methods

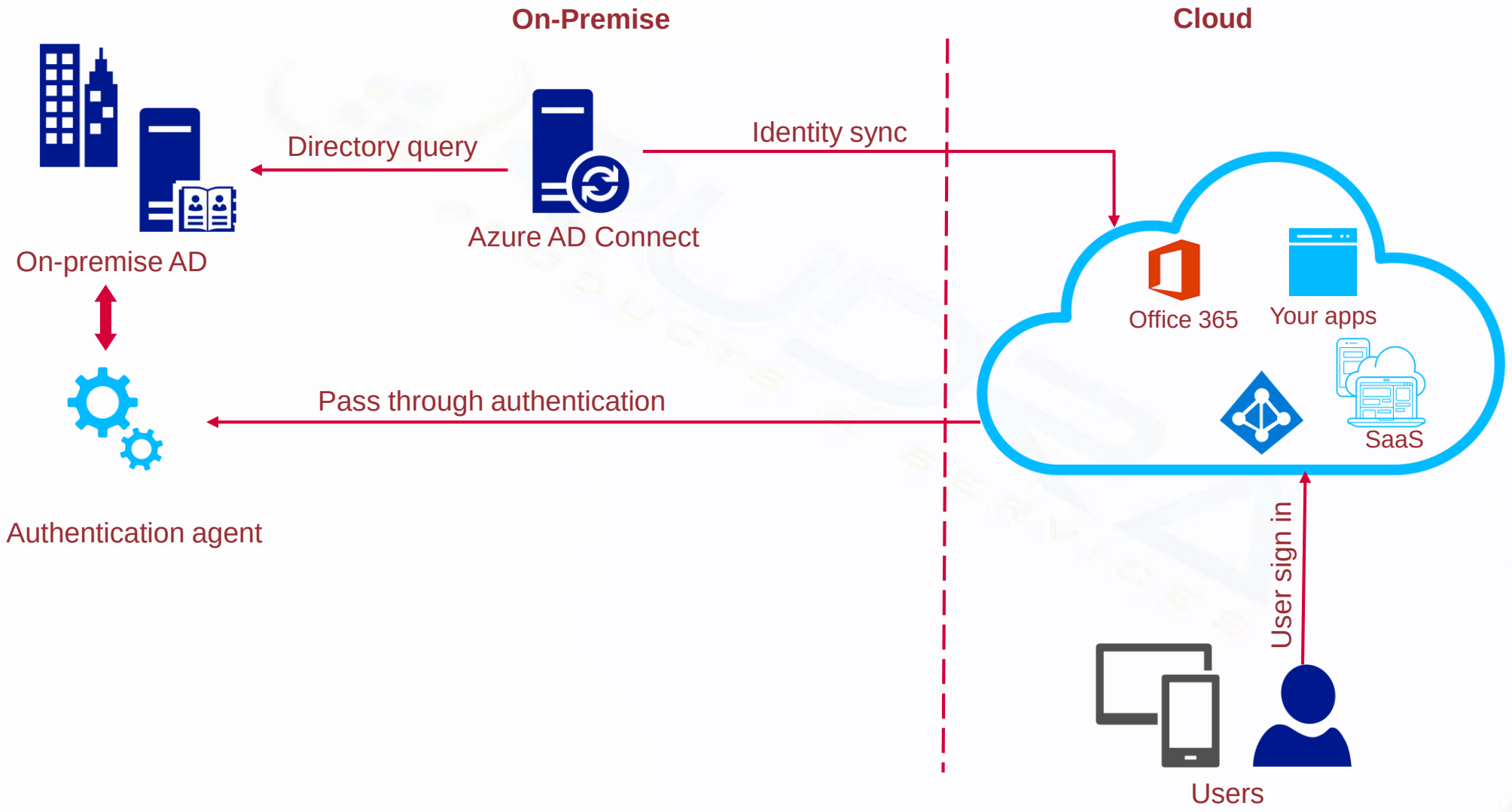
Choosing the correct authentication method is a crucial first decision in setting up an Azure AD hybrid identity solution. Implement the authentication method that is configured by using Azure AD Connect, which also provisions users in the cloud.

- **Cloud authentication**
    - **Azure AD password hash synchronization** - The simplest way to enable authentication for on-premises directory objects in Azure AD. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure.
    - **Azure AD Pass-through Authentication -** Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers.
- **Federated authentication -** When you choose this authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

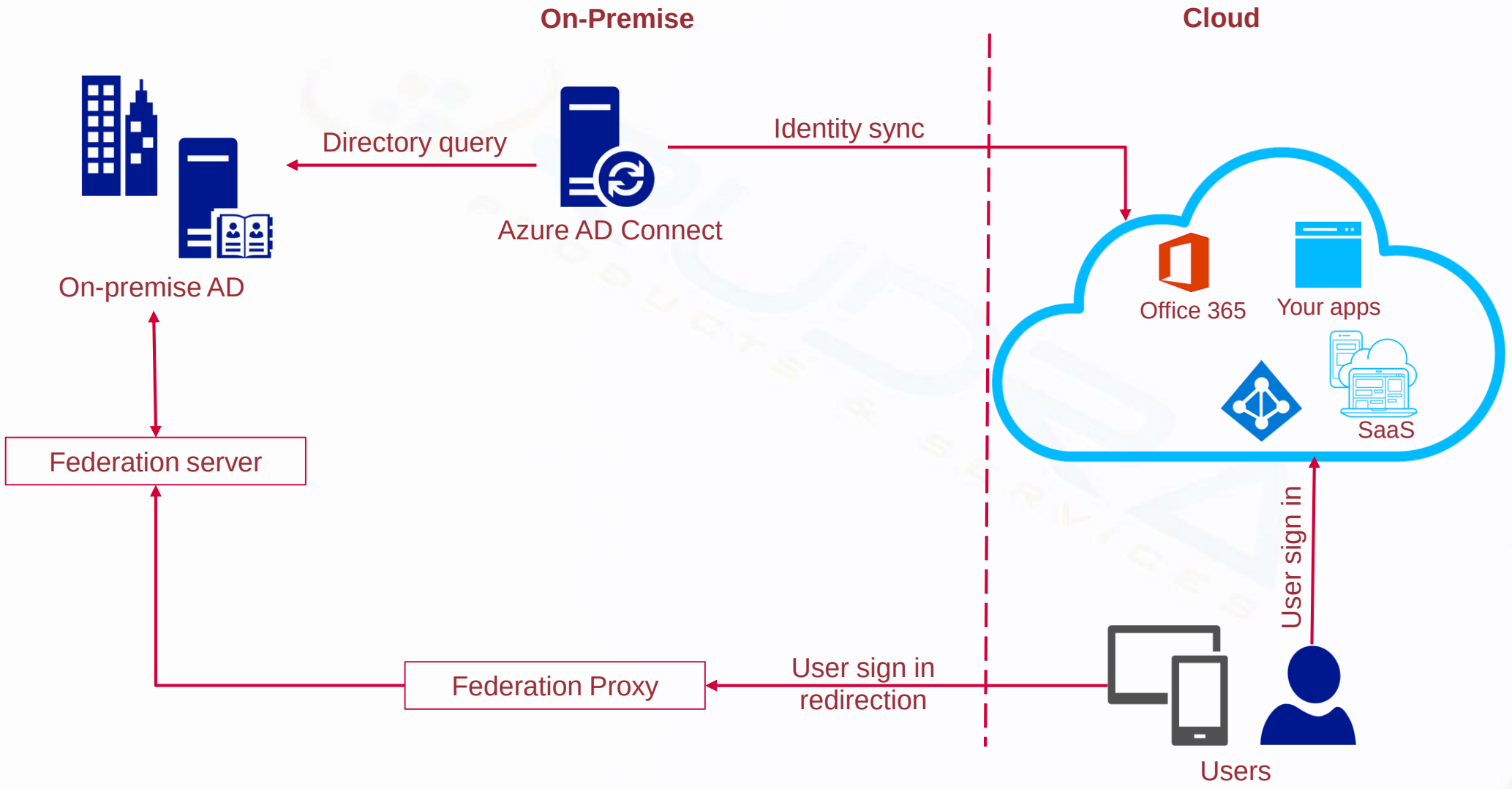
Password hash synchronisation architecture



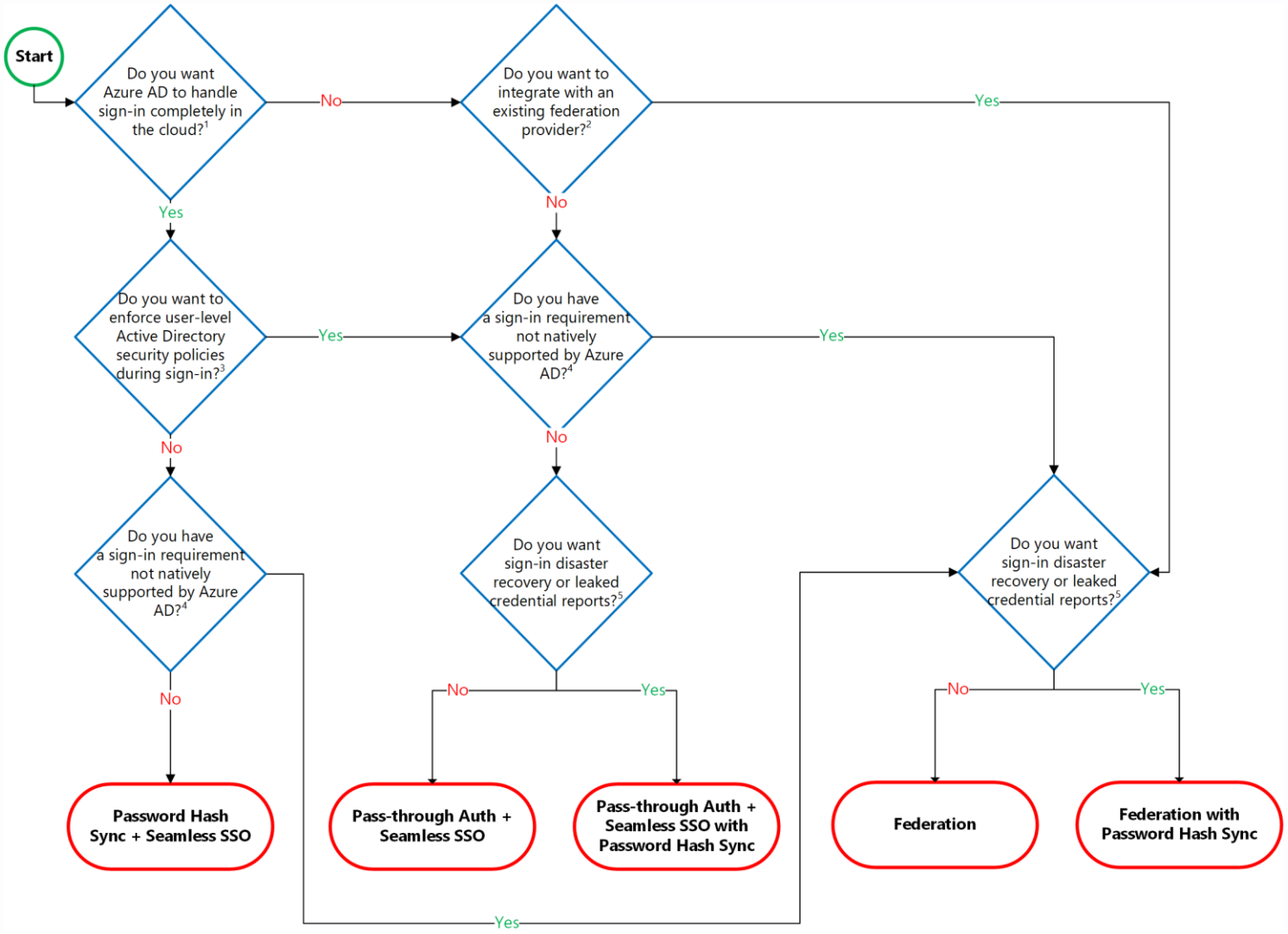
Pass through authentication architecture



Federation authentication architecture



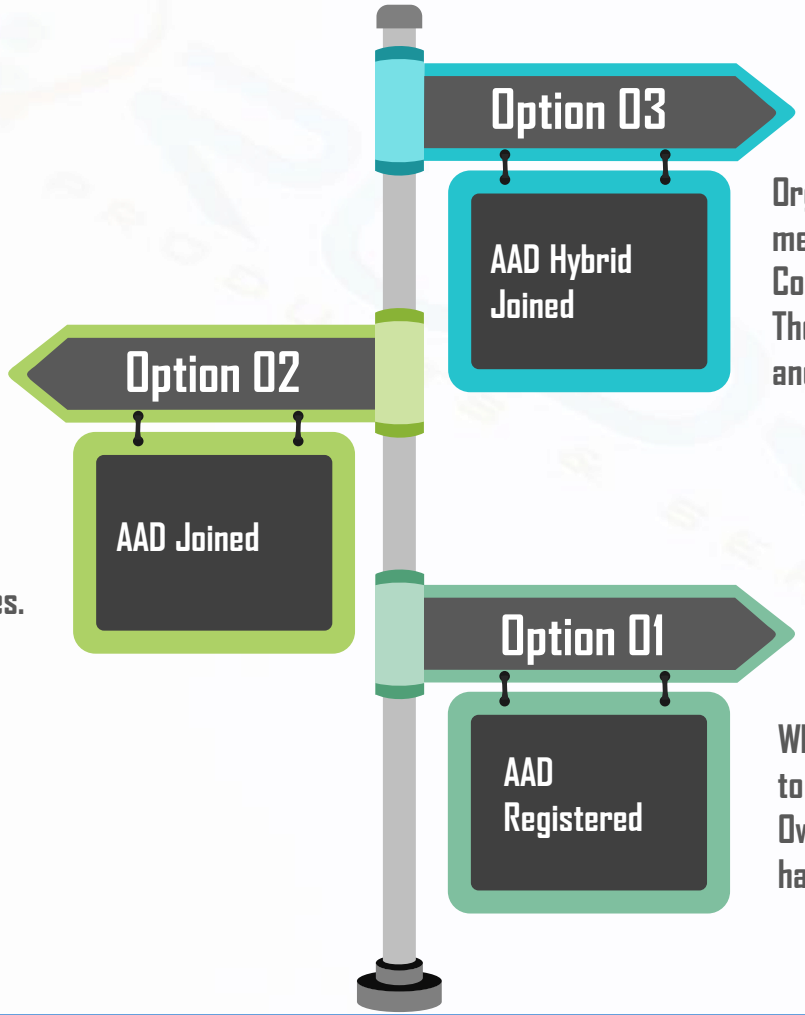
Decision tree for Authentication option



Introduction to Device Management

Device management in AAD

Device management is a foundation of Device based conditional access in AAD. With device-based conditional access, you can ensure that access to resources in your environment is only possible with managed devices.



Organizations with an on-premises footprint generally rely on imaging methods to provision devices, and they often use System Center Configuration Manager (SCCM) or group policy (GP) to manage them. Those devices will be domain joined to your on-premises Active Directory and registered with your Azure Active Directory.

Joining a device is an extension of registering. With Azure AD joined, you can implement SSO, Access to Windows store, restriction of apps only to complaint devices and seamless access to on-premise resources. Currently Windows 10 devices are suported

When device is registered, AAD will create an identity that can be used to authenticate the device. Goal is to provide support for Bring Your Own Device (BYOD) scenario. Access is based on a work account that has been entered on the device.

Device management options summary

AAD registered devices

- For personal devices
- To manually register devices with AD

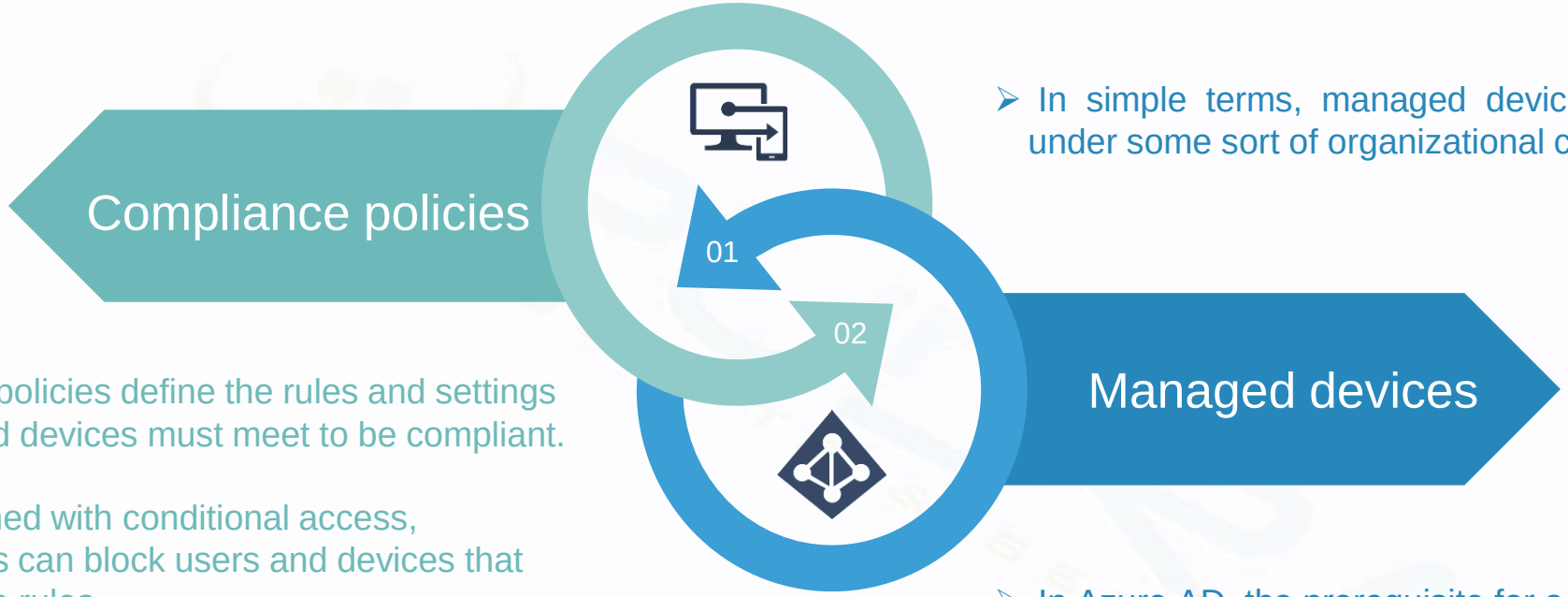
AAD joined devices

- For devices owned by the organization
- Devices that are not domain joined with On-premise AD
- Manually register devices with AAD
- To change the local state of the device

Hybrid AAD joined devices

- For devices owned by the organization
- Devices that are domain joined with On-premise AD
- Automatically register devices with AAD
- To change the local state of the device

Device based conditional access policies



- Compliance policies define the rules and settings that users and devices must meet to be compliant.
- When combined with conditional access, administrators can block users and devices that don't meet the rules.
- Compliance status is used by conditional access policies to block or allow access to e-mail and other corporate resources.

- In simple terms, managed devices are devices that are under some sort of organizational control.
- In Azure AD, the prerequisite for a managed device is that it has been registered with Azure AD.
- Registering a device creates an identity for the device in form of a device object. This object is used by Azure to track status information about a device.

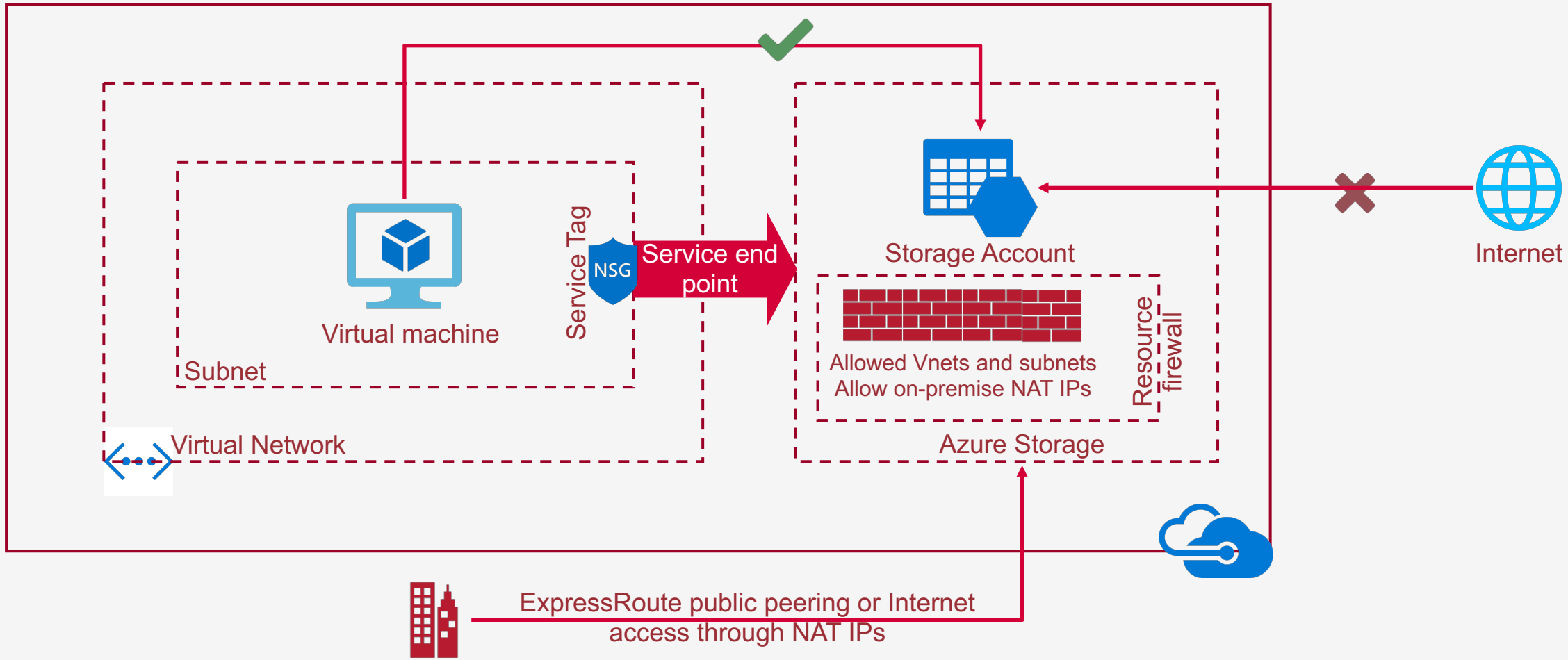
Enterprise state roaming

With Windows 10, Azure Active Directory (Azure AD) users gain the ability to securely synchronize their user settings and application settings data to the cloud. Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

- Separation of consumer and corporate data
- Enhanced security
- Better management and monitoring

Introduction to Service end points and policies

Introduction to VNet connectivity with Azure services



Introduction to Service endpoints

- VNet Service Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.

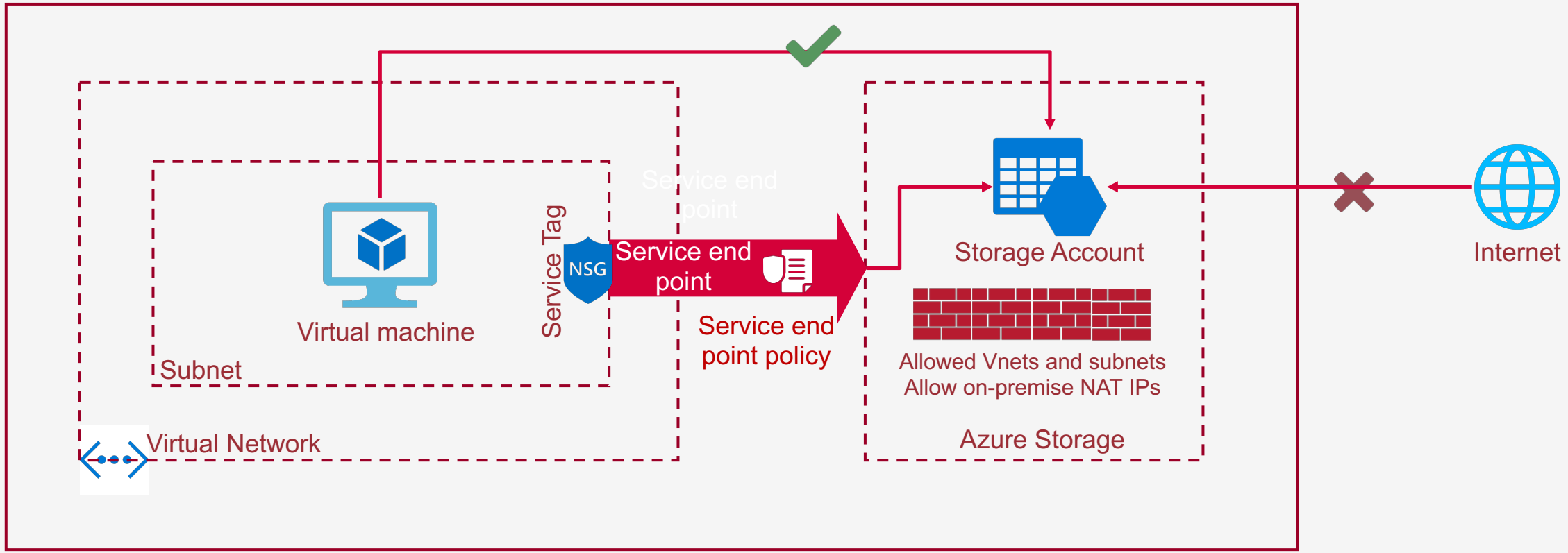
- Service endpoints are configured on a subnet in a virtual network. Endpoints work with any type of compute instances running within that subnet.

- You can configure multiple service endpoints for all supported Azure services (Azure Storage, or Azure SQL Database, for example) on a subnet.

- For Azure SQL Database, virtual networks must be in the same region as the Azure service resource. If using GRS and RA-GRS Azure Storage accounts, the primary account must be in the same region as the virtual network.

Virtual network service endpoint policies

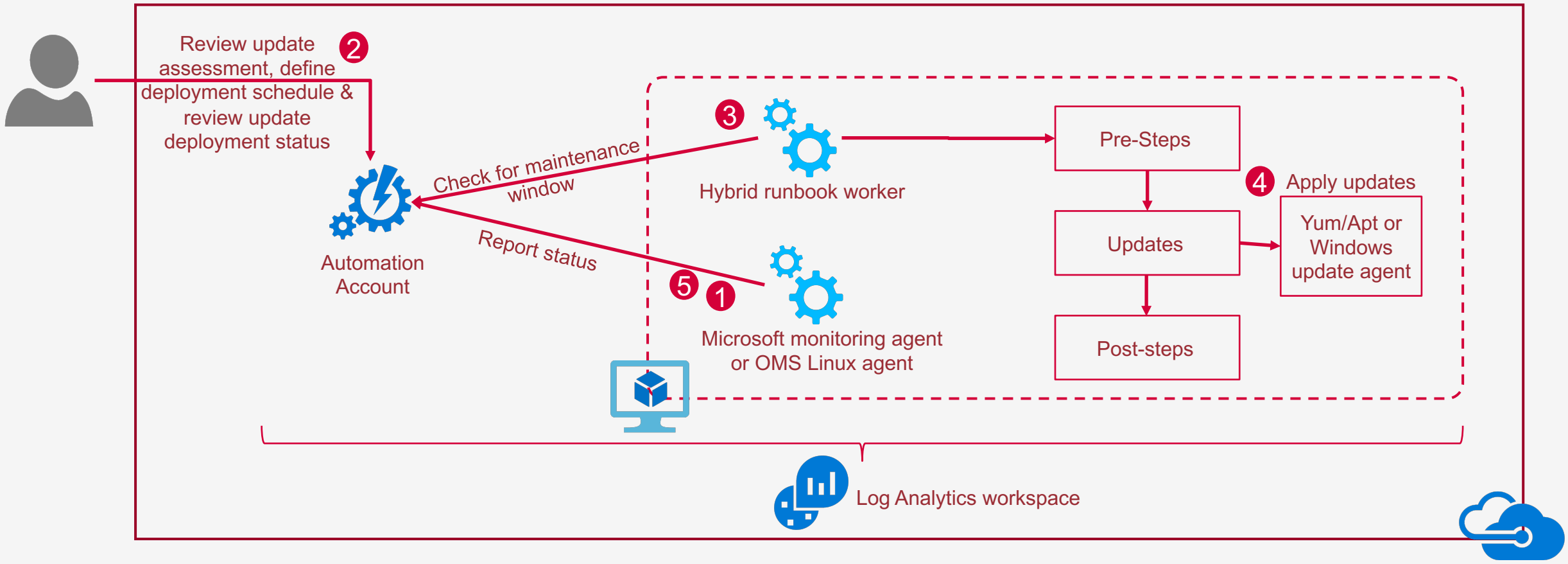
Virtual Network (VNet) service endpoint policies allow you to filter virtual network traffic to Azure services, allowing only specific Azure service resources, over service endpoints. Endpoint policies provide granular access control for virtual network traffic to Azure services.



Introduction to Update Management Solution in Azure

Update management solution overview

Update Management solution in Azure Automation can be used to manage operating system updates for your Windows and Linux computers in Azure, in on-premises environments, or in other cloud providers.

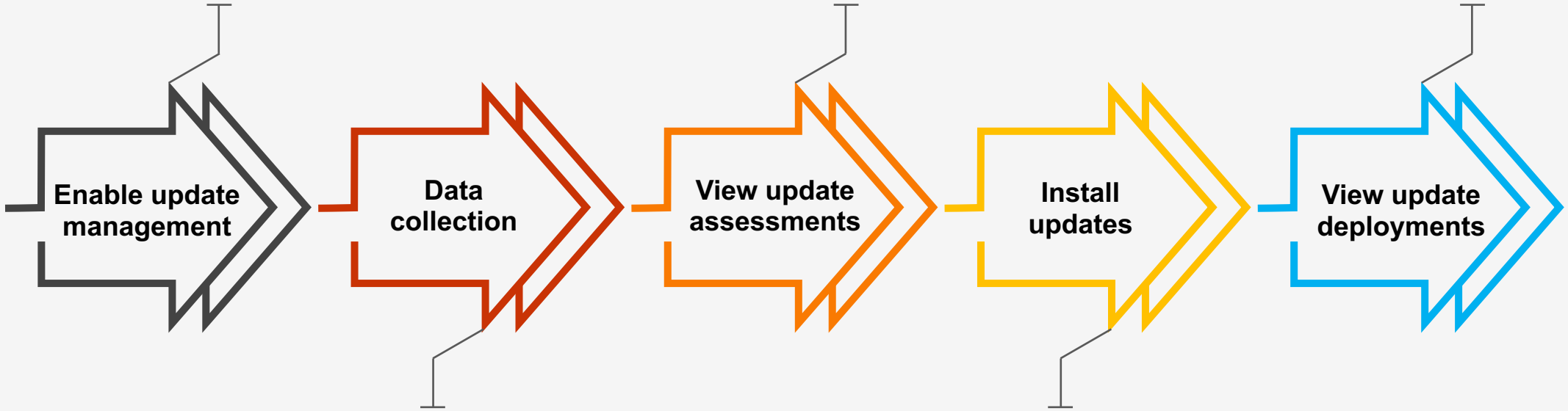


Update management solution steps

Onboard machines to update management. Supported ways include from individual VM or multiple VM's or Automation account

In your automation account, select update management to view status of the machine. Use log search to deep dive.

Select the Update Deployments tab to view the list of existing update deployments



By default data is collected every 12 hours for windows machine and every 3 hours for managed Linux computer

After updates are assessed for all the Linux and Windows computers in your workspace, you can install required updates by creating an update deployment

Update management solution key points

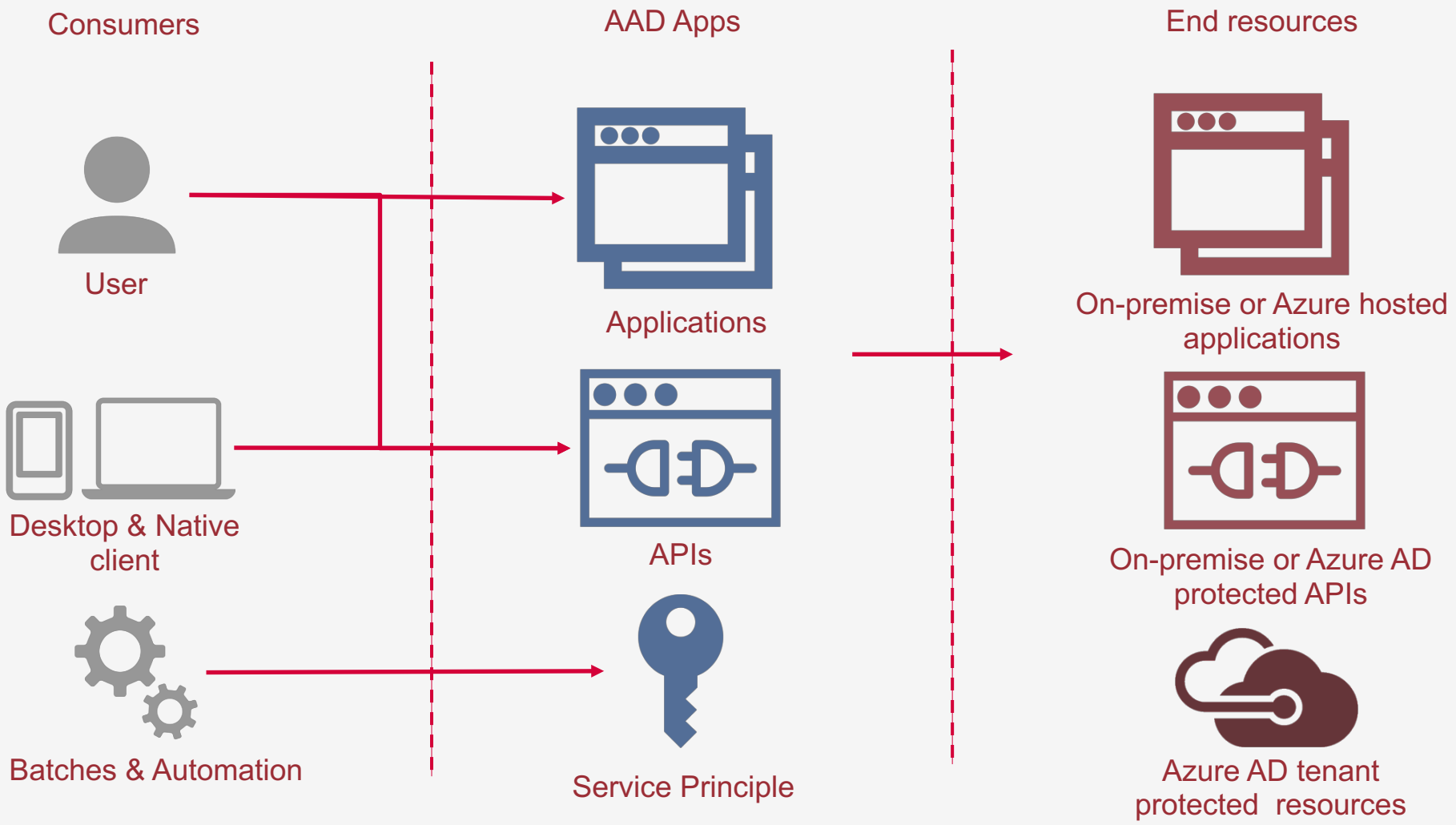
Advanced settings

- Pre download updates
- Disable automatic installation

- Open 443 to specific end points related to update management solution
- Use dynamic groups
- Integrate with System Center Configuration Manager

Introduction to Azure AD App Registrations

App registration types



Application scenarios supported by Azure AD

These are the five primary application scenarios supported by Azure AD

- **Single-page application (SPA) -** A user needs to sign in to a single-page application that is secured by Azure AD.
- **Web browser to web application -** A user needs to sign in to a web application that is secured by Azure AD.
- **Native application to web API -** A native application that runs on a phone, tablet, or PC needs to authenticate a user to get resources from a web API that is secured by Azure AD.
- **Web application to web API -** A web application needs to get resources from a web API secured by Azure AD.
- **Server application to web API -** A server application with no web user interface needs to get resources from a web API secured by Azure AD.

Application registration object types

When you register an Azure AD application in the Azure portal, two objects are created in your Azure AD tenant

- **Application object -** Application objects describe the application to Azure AD and can be considered as the definition of the application, allowing the service to know how to issue tokens to the application based on its settings. The application object will only exist in its home directory

- **Service principal object -** When an application is given permission to access resources in a tenant (upon registration or consent), a service principal object is created.

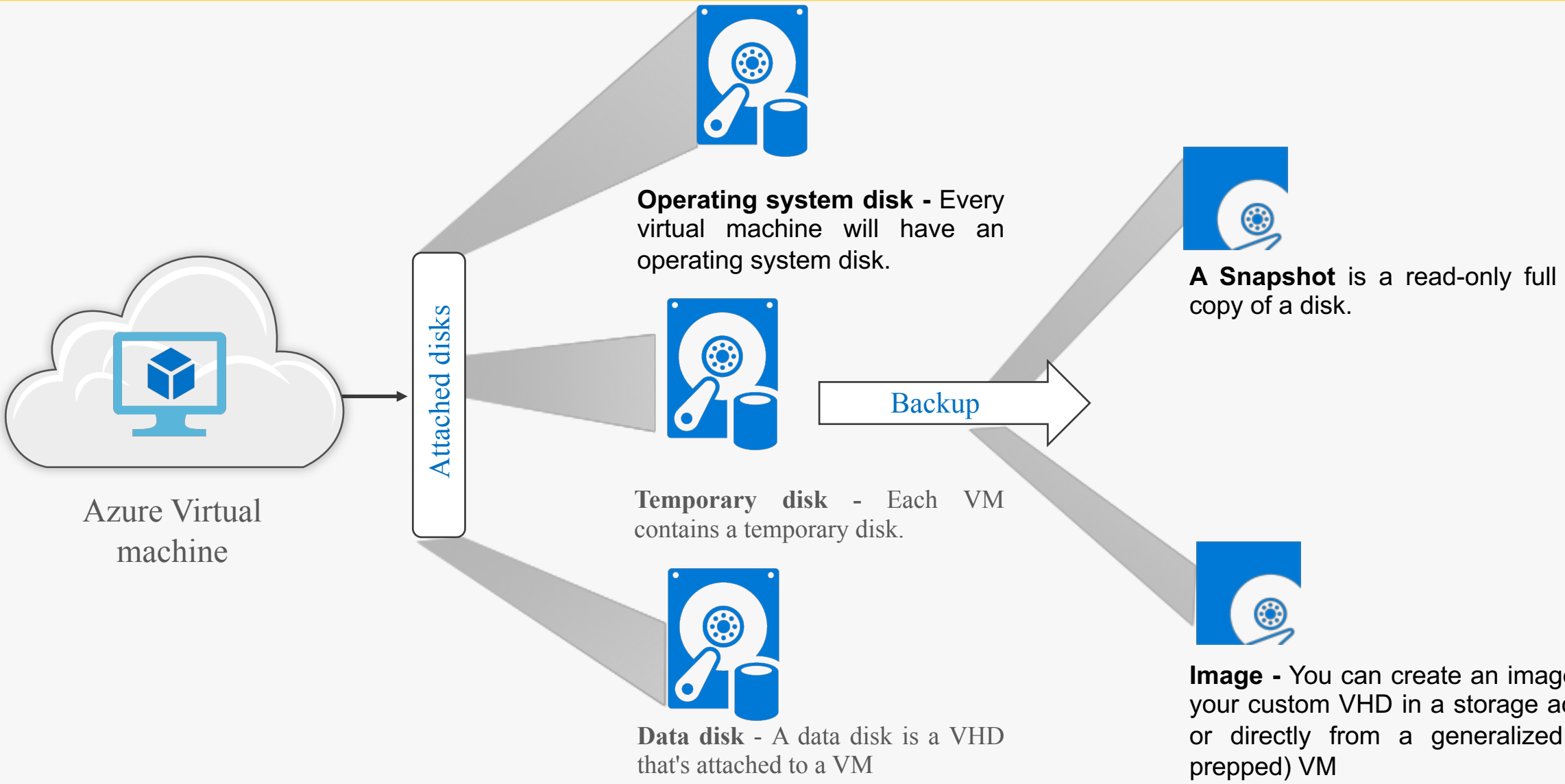
Types of permissions

- **Delegated permissions** - Are used by apps that have a signed-in user present. For these apps, either the user or an administrator consents to the permissions that the app requests and the app is delegated permission to act as the signed-in user when making calls to an API. Depending on the API, the user may not be able to consent to the API directly and would instead require an administrator to provide "admin consent".

- **Application permissions** - Are used by apps that run without a signed-in user present; for example, apps that run as background services or daemons. Application permissions can only be consented by an administrator because they are typically powerful and allow access to data across user-boundaries, or data that would otherwise be restricted to administrators.

Virtual machine storage encryption overview

VM Storage overview



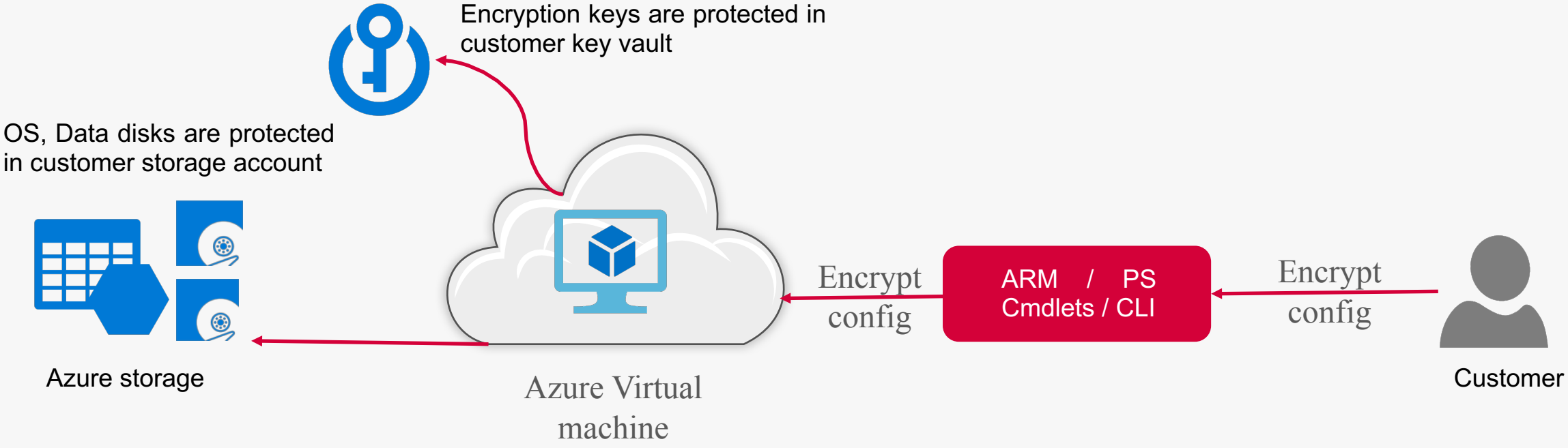
Azure Storage encryption

Azure Storage automatically encrypts your data when persisting it to the cloud. Encryption protects your data and to help you to meet your organizational security and compliance commitments. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant

Key management - You can rely on Microsoft-managed keys for the encryption of your storage account, or you can manage encryption with your own keys, together with Azure Key Vault.

Disk encryption

- Azure Disk Encryption allows you to encrypt the OS and Data disks used by an IaaS Virtual Machine
- For Windows, the drives are encrypted using industry-standard BitLocker encryption technology
- For Linux, the disks are encrypted using the DM-Crypt technology



Remote access management

Remote Access Management options

RDP rule

Configure an NSG rule to allow RDP traffic

Azure Firewall or NVA

Allow RDP traffic to end VMs via Azure Firewall or NVA

Azure Firewall and Jump box

Create a Jump box and allow RDP traffic to Jump box via Azure Firewall and user will RDP into end server from jump box

Point to Site VPN

Users can establish P2S VPN and remote desktop into Azure VMs using their private IP addresses

Remote Desktop Services

Use remote desktop web access to provide access to Azure VMs.

Security Centre Just In Time access

Grant RDP access to users using Security center Just In Time access.

Windows Admin Centre

Windows Admin center was built with the cloud in mind and lets you manage Azure IaaS machines

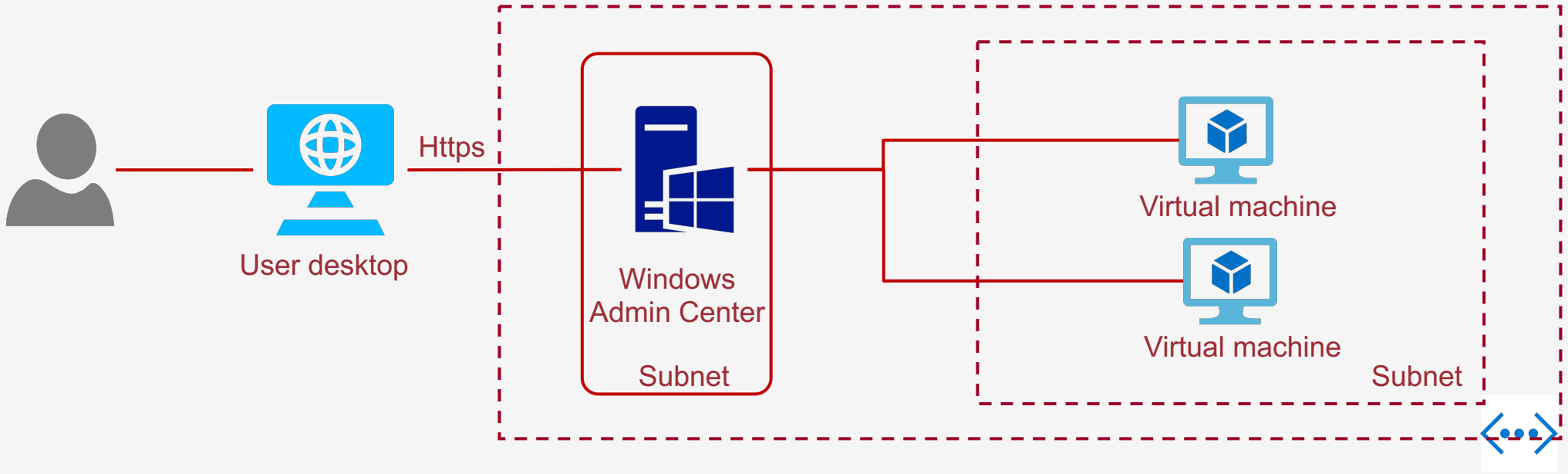
3rd Party solutions

There are several 3rd Party solution available in Azure Marketplace to deliver RAM

Windows Admin Center

- Windows Admin Center is a new, locally-deployed, browser-based management tool set that lets you manage your Windows Servers with no Azure or cloud dependency.

- Windows Admin Center gives you full control over all aspects of your server infrastructure and is particularly useful for managing servers on private networks that are not connected to the Internet.



Hardening workstation

- Active scanning and patching
- Limited functionality – Reduce number of apps and startup services
- Network hardening - Use Windows Firewall rules to allow only valid IP addresses, ports, and URLs related to Azure management.
- Execution restriction
- Least privilege
- IE Hardening
- Governance using GPO’s

Azure Cosmos DB security

Azure COSMOS DB security overview

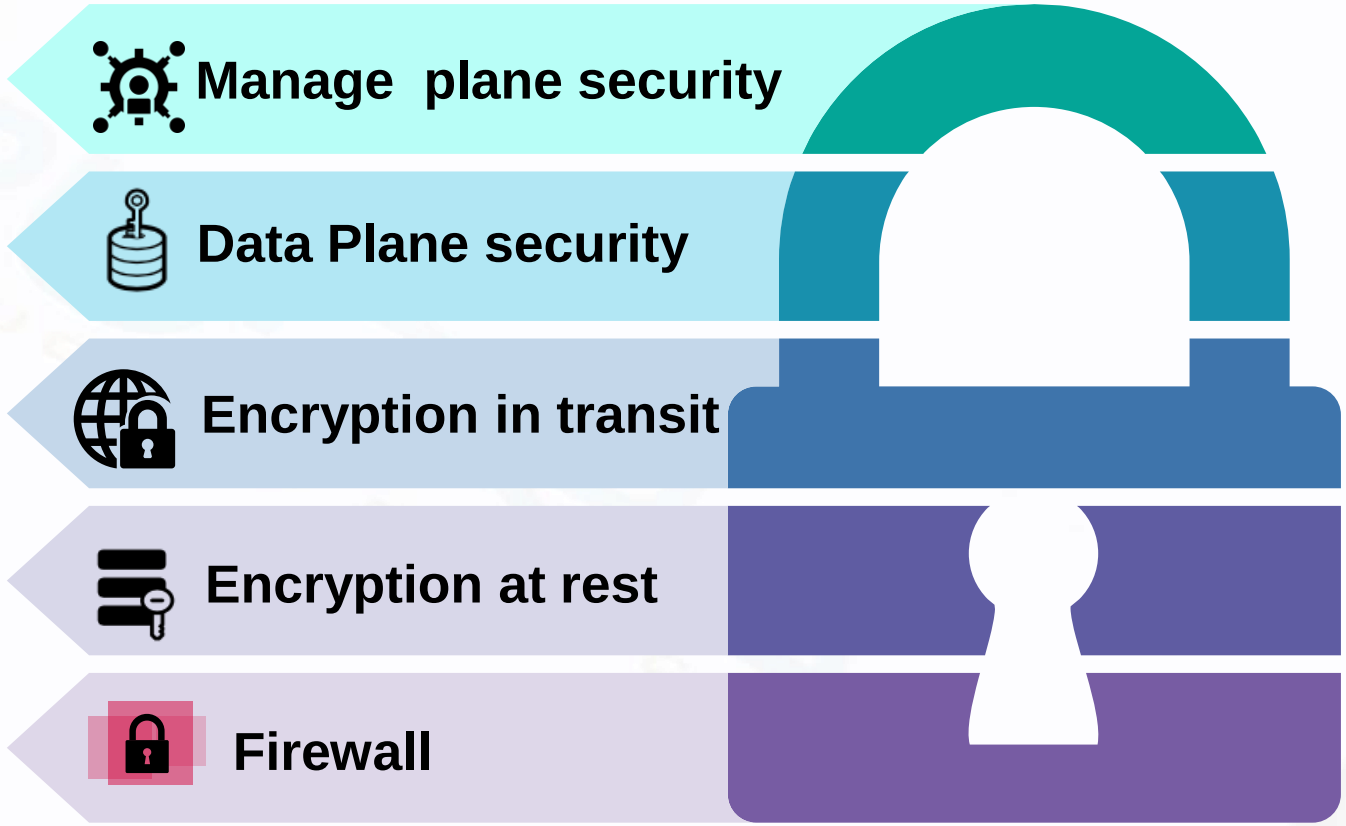
Securing your COSMOS DB account

Securing access to your data

Encryption in transit

Encryption at rest

Secure network level access



Management plane security

Management plane refers to the access to Azure COSMOS accounts, databases, containers and throughput.

- DocumentDB Accounts Contributor - Can manage Azure Cosmos DB accounts.
- Cosmos DB Account Reader - Can read Azure Cosmos DB account data.
- Cosmos Backup Operator - Can submit restore request for an Azure Cosmos database or a container.
- Cosmos DB Operator - Can provision Azure Cosmos accounts, databases, and containers but cannot access the keys that are required to access the data.

Data plane security

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources.

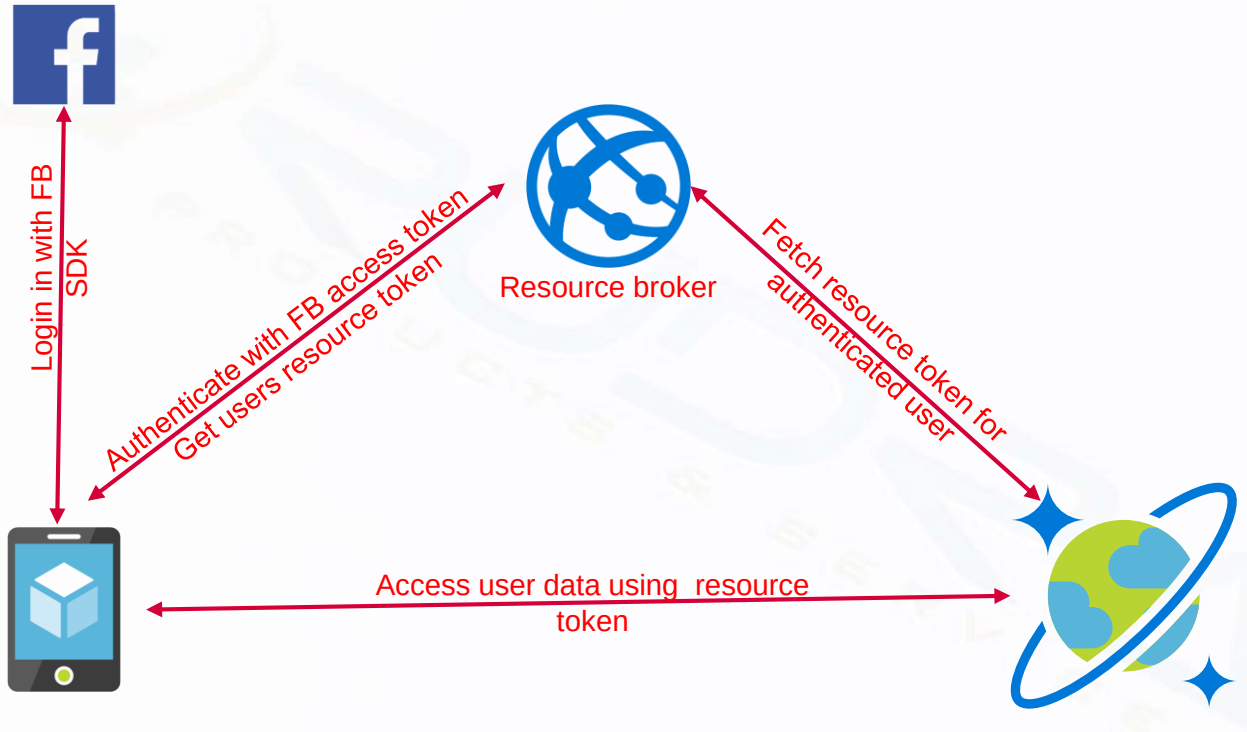
Master Keys

- Provide access to accounts, databases, users, and permissions.
- Cannot be used to provide granular access to containers and documents.
- Are created during the creation of an account.
- Can be regenerated at any time.

Resource Tokens

- Provide access to specific containers, partition keys, documents, attachments, stored procedures, triggers, and UDFs.
- Are created when a user is granted permissions to a specific resource.
- Are time bound with a customizable validity period. The default valid timespan is one hour. Token lifetime, however, may be explicitly specified, up to a maximum of five hours.
- Provide a safe alternative to giving out the master key.

Resource tokens usage approach



Introduction to Azure Active Directory Monitoring

AAD Reports overview

Azure Active Directory (Azure AD) reports provide a comprehensive view of activity in your environment.

Security reports

- **Users flagged for risk**

  Provide an overview of user accounts that might have been compromised.

- **Risky sign-ins**

  Provides an indicator for sign-in attempts that might have been performed by someone who is not the legitimate owner of a user account.

Activity reports

- **Audit logs**

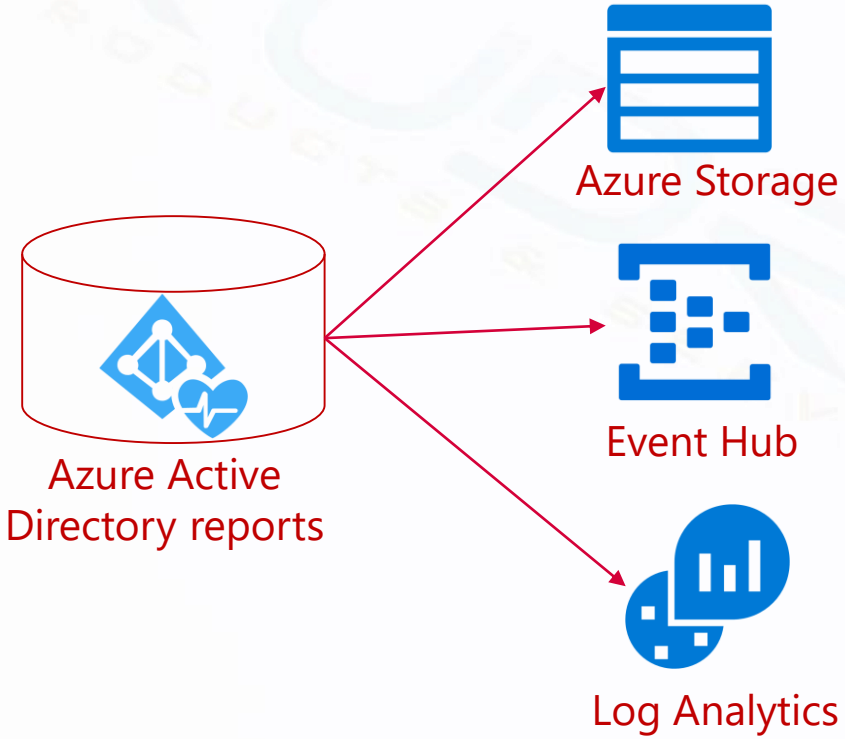
  Provides the history of every task performed in your tenant.

- **Sign-ins**

  Using this you can determine, who has performed the tasks reported by the audit logs report.

AAD Monitoring overview

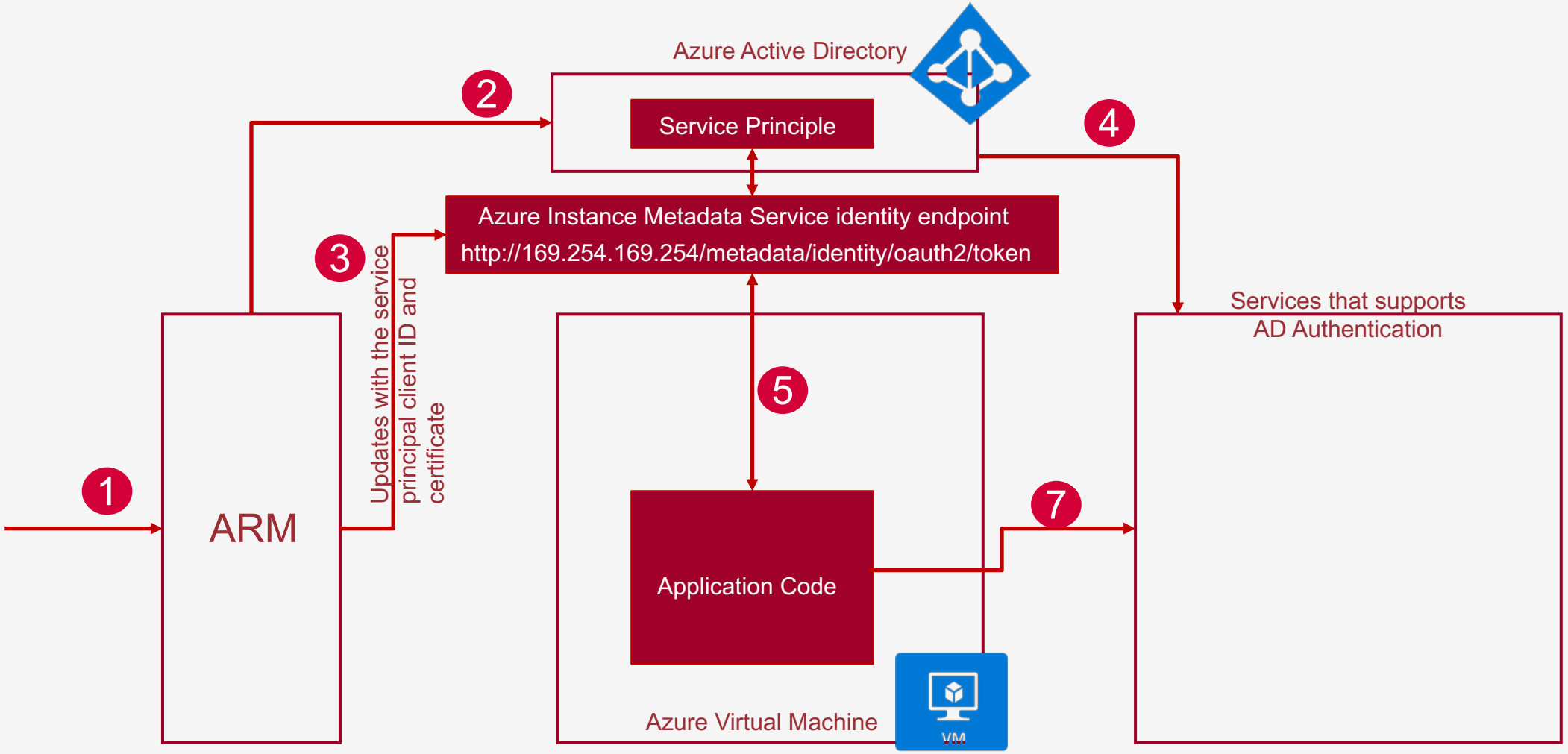
With Azure Active Directory (Azure AD) monitoring, you can now route your Azure AD activity logs to different endpoints. You can then either retain it for long-term use or integrate it with third-party Security Information and Event Management (SIEM) tools to gain insights into your environment.



Introduction to Managed identities

Managed Identities overview

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure AD.



Types of managed identities

System-assigned managed identity

- A system-assigned managed identity is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance.
- The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it's enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.

User-assigned managed identity

- A user-assigned managed identity is created as a standalone Azure resource. After the identity is created, the identity can be assigned to one or more Azure service instances.
- The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it's assigned.

Services that support managed identities

- Azure Virtual machines & Virtual machines scale set
- Container services
- Azure App service
- Azure functions, logic apps, API management
- Azure Data factory

Introduction to Azure Policies

Azure Policies overview

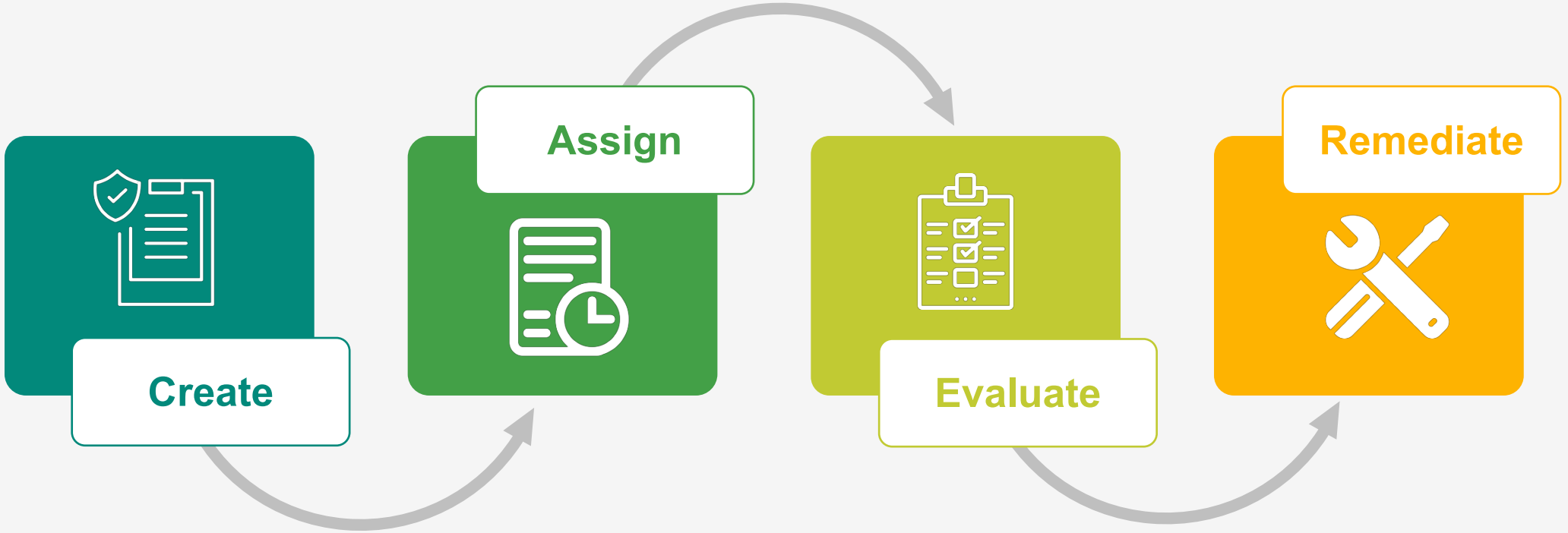
Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements.

Azure policies Vs RBAC

- RBAC controls user actions at different scopes.
  Example is start and stop virtual machine

- Policy enforce rules on resource properties during deployment and for existing resources.
  Example is to deploy resources at a specific location only

Azure Policy steps



Policy definition has conditions under which it's enforced. And, it has a defined effect that takes place if the conditions are met

A **policy assignment** is a policy definition that has been assigned to take place within a specific scope. This scope could range from a management group to a resource group.

Evaluations of assigned policies and initiatives happen as the result of various events. For e.g. creation of a resource, policy assignment to a scope etc.

Each policy definition in Azure Policy has a single effect. That **effect** determines what happens when the policy rule is evaluated to match

Policy definition

You use JSON to create a policy definition. The policy definition contains elements for:

- Mode – Determines which resource types will be evaluated for the policy
- Parameters - Parameters help simplify your policy management by reducing the number of policy definitions.
- Display name & Description
- Policy rule
    - Logical evaluation
    - Effect

Policy effects

There are currently six effects that are supported in a policy definition:

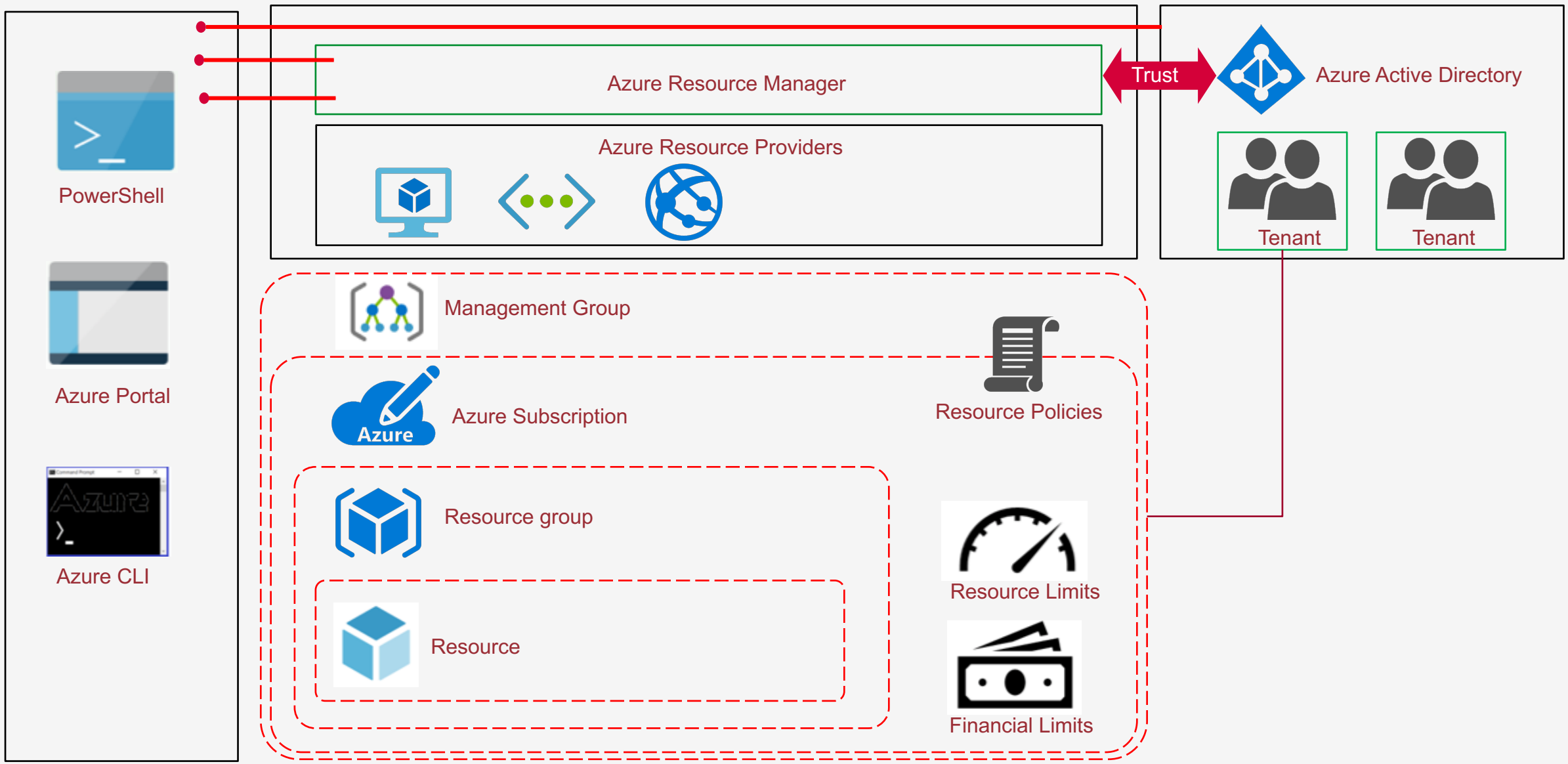
- **Append** - Append is used to add additional fields to the requested resource during creation or update. For e.g. tags.
- **Audit** - Audit is used to create a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
- **AuditIfNotExists** - AuditIfNotExists enables auditing on resources that match the if condition, but doesn't have the components specified in the details of the then condition.
- **Deny** - Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
- **DeployIfNotExists** - Similar to AuditIfNotExists, DeployIfNotExists executes a template deployment when the condition is met.
- Disabled

Initiatives

- **Initiative definition**
  - An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions
- **Initiative assignment**
  - Like a policy assignment, an initiative assignment is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope.

Introduction to Resource providers and locks

Overview of Azure resources management (ARM)



Azure Resource Providers

- Each resource provider offers a set of resources and operations for working with those resources.
- Before getting started with deploying your resources, you should gain an understanding of the available resource providers. Knowing the names of resource providers and resources helps you define resources you want to deploy to Azure.
- You need to know the valid locations and API versions for each resource type.
- Registering a resource provider configures your subscription to work with the resource provider. The scope for registration is always the subscription. By default, many resource providers are automatically registered.

Azure locks

- Locks enables you to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.
- You can set the lock level to CanNotDelete or ReadOnly.
  - **CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.
  - **ReadOnly** means authorized users can read a resource, but they can't delete or update the resource.
- **RBAC vs Locks**
  - Unlike role-based access control, you use management locks to apply a restriction across all users and roles.

Apps deployment overview

Apps deployment options

- ZIP or WAR file deployment
- Deploy via FTP
- Content sync deployment – OneDrive, Dropbox etc
- Deploy continuously using Azure DevOps, GitHub etc

Deployment credentials

Azure App Service supports two types of credentials for local Git deployment and FTP/S deployment.

- **User-level credentials** - One set of credentials for the entire Azure account. It can be used to deploy to App Service for any app, in any subscription, that the Azure account has permission to access. Each Azure user that receives access to an app can use his/her personal user-level credentials until access is revoked

- **App-level credentials** - one set of credentials for each app. It can be used to deploy to that app only. In order to give someone access to these credentials via Role Based Access Control (RBAC), you need to make them contributor or higher on the Web App

Deployment slots

- When you deploy your web app, web app on Linux, mobile back end, and API app to App Service, you can deploy to a separate deployment slot instead of the default production slot when running in the Standard or Premium App Service plan tier.

- App content and configuration elements can be swapped between two deployment slots, including the production slot.

- Deploying an app into a slot first and swapping into production will

  - enable you to validate the changes in staging slot

  - if the changes swapped into the production slot are not as you expected, you can perform the same swap immediately to get your "last known good site" back.

Swapped settings

Some configuration elements will follow the content across a swap (not slot specific) while other configuration elements will stay in the same slot after a swap (slot specific). The following lists show the settings that change when you swap slots.

Settings that are swapped :

- General settings - such as framework version, 32/64-bit, Web sockets
- App settings (can be configured to stick to a slot)
- Connection strings (can be configured to stick to a slot)
- Handler mappings
- Monitoring and diagnostic settings
- WebJobs content

Settings that are not swapped:

- Publishing endpoints
- Custom Domain Names
- SSL certificates and bindings
- Scale settings
- WebJobs schedulers

Azure App Service security

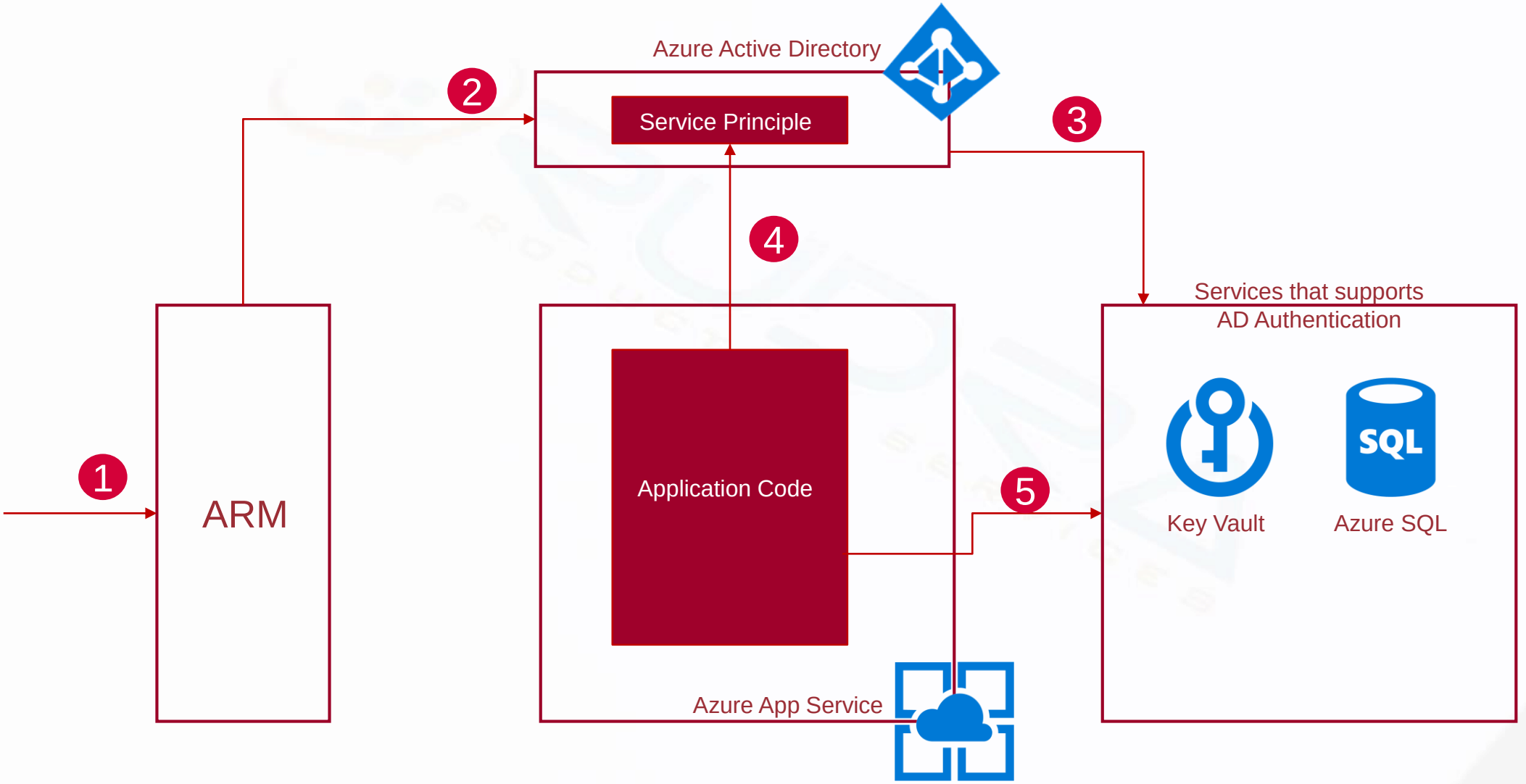
Authentication and authorization

- Authentication and authorization module handles several things for your app
  - Authenticates users with the specified provider
  - Validates, stores, and refreshes tokens
  - Manages the authenticated session
  - Injects identity information into request headers
- Token store
- Logging & tracing
  - If you enable application logging, you will see authentication and authorization traces directly in your log files

Other security areas

- App Service is ISO, SOC and PCI complaint
- IP Address & Virtual network whitelisting
- SSL communication

Managed service identity



App Service Environments security

- Network security groups
- Web Application Firewall
  - Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities.
  - Web application firewall is based on rules from the OWASP core rule sets 3.0 or 2.2.9

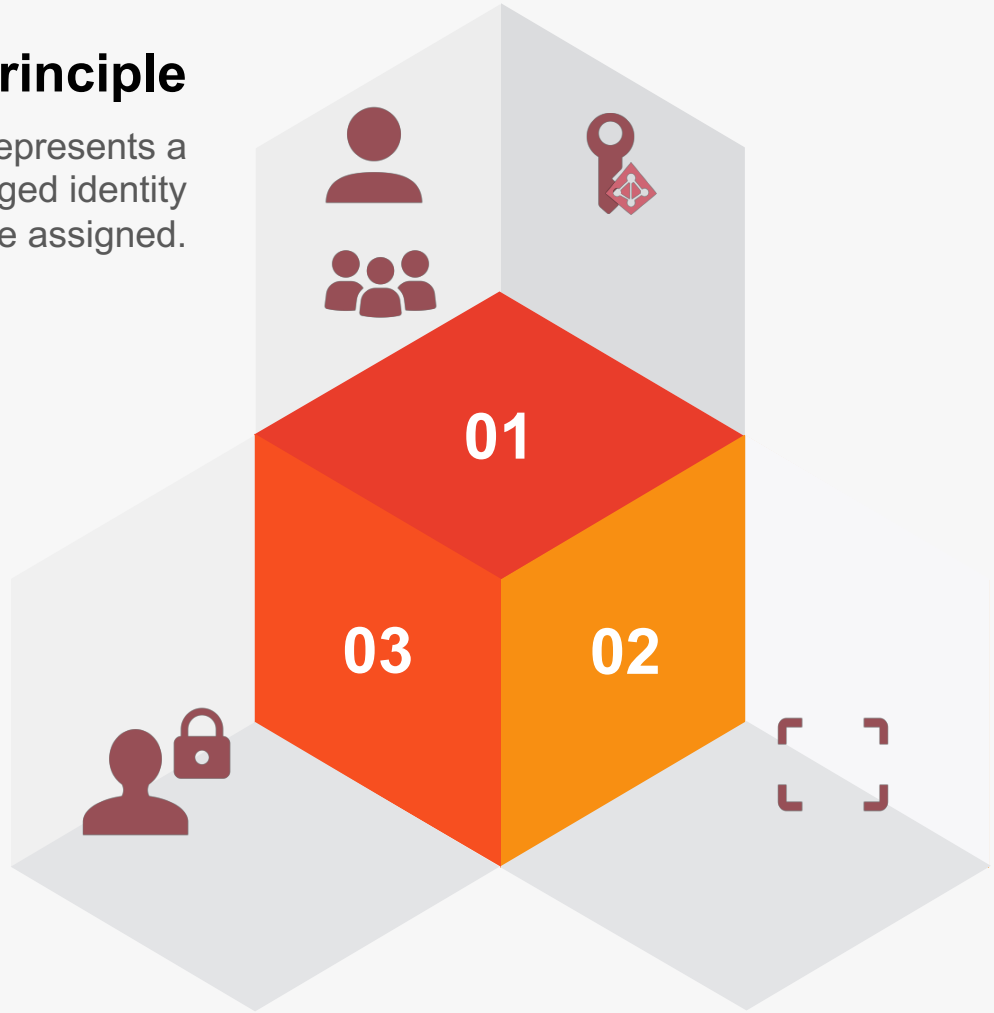
Introduction to Role based access control

Overview of Role based access control (RBAC)

RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources.

Security Principle

A security principle is an object that represents a user, group, service principle or managed identity to which access to resources are assigned.



Role definition

A role definition is a collection of permissions. It's sometimes just called a role. A role definition lists the operations that can be performed, such as read, write, and delete.

Scope

Scope is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope.

Security principle

- **User** - An individual who has a profile in Azure Active Directory. You can also assign roles to users in other tenants. For information about users in other organizations, see Azure Active Directory B2B.

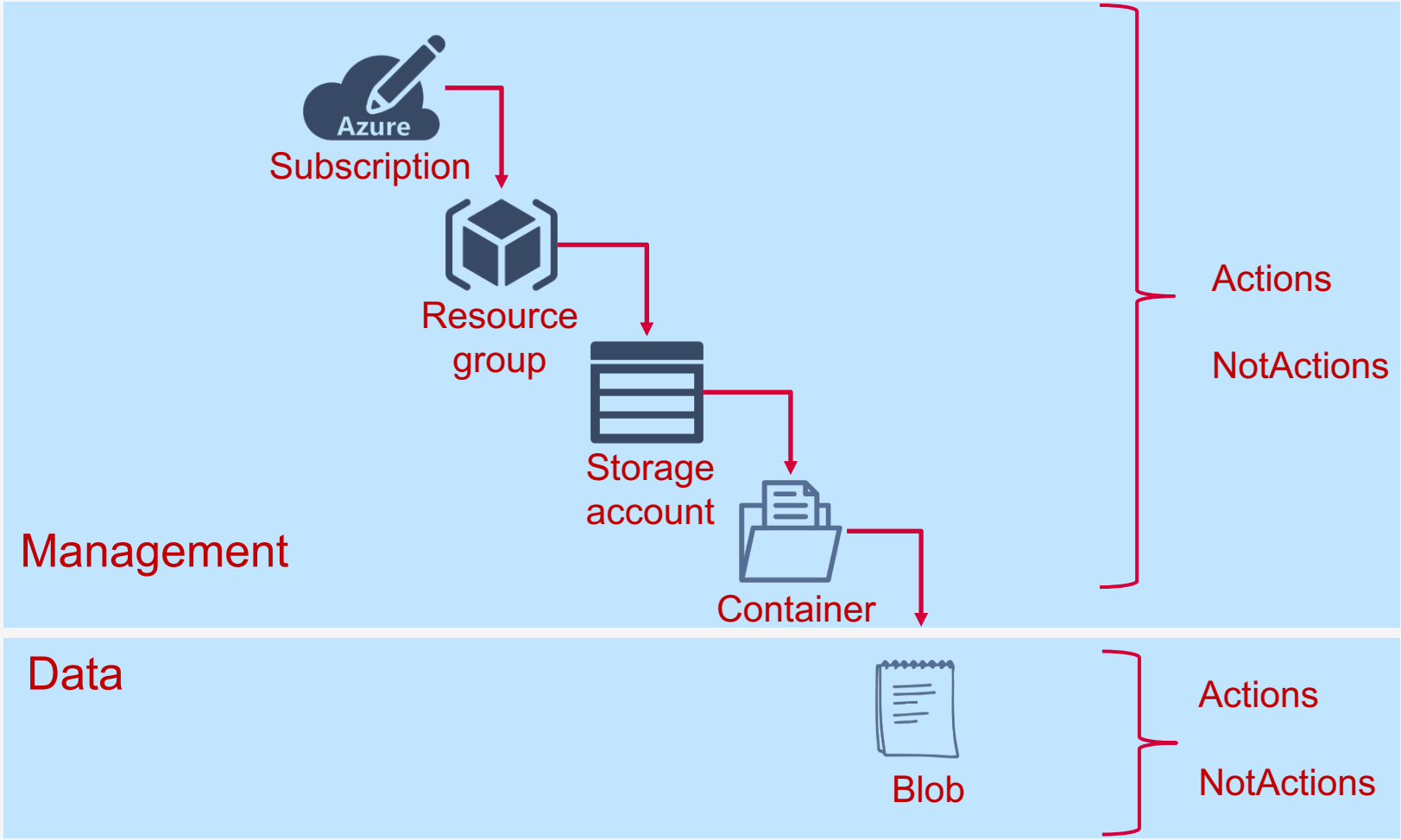
- **Group** - A set of users created in Azure Active Directory. When you assign a role to a group, all users within that group have that role.

- **Service principal** - A security identity used by applications or services to access specific Azure resources. You can think of it as a user identity (username and password or certificate) for an application.

- **Managed identity** - An identity in Azure Active Directory that is automatically managed by Azure. You typically use managed identities when developing cloud applications to manage the credentials for authenticating to Azure services.

Role definition

A role definition lists the operations that can be performed, such as read, write, and delete. It can also list the operations that can't be performed or operations related to underlying data.



Role types

RBAC roles - Azure RBAC includes over 70 built-in roles. There are four fundamental RBAC roles

- Owner
- Contributor
- Reader
- User Access administrator

Azure AD administrator roles - Azure AD administrator roles are used to manage Azure AD resources in a directory such as create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains.

Scope

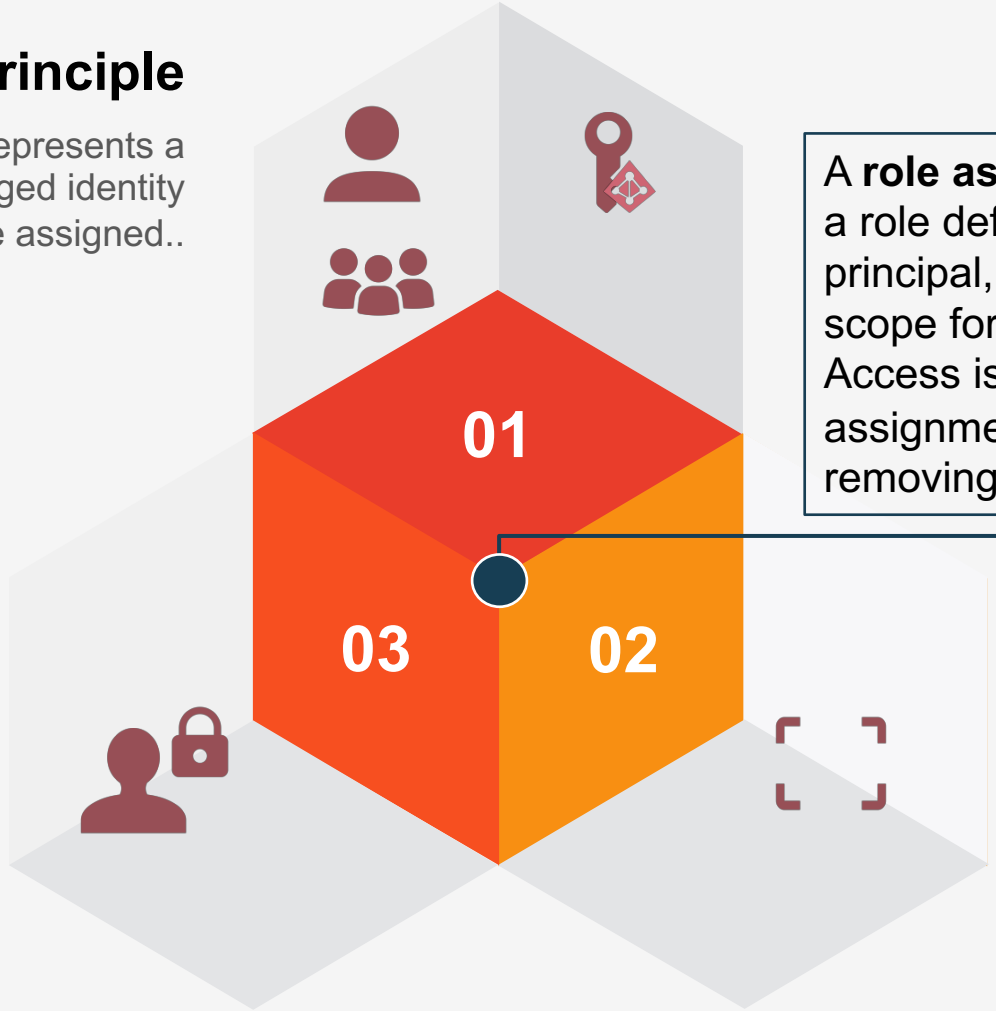
- *Scope* is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope

- In Azure, you can specify a scope at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent-child relationship.

Role assignment

Security Principle

A security principle is an object that represents a user, group, service principle or managed identity to which access to resources are assigned..



A **role assignment** is the process of attaching a role definition to a user, group, service principal, or managed identity at a particular scope for the purpose of granting access. Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

Role definition

A role definition is a collection of permissions. It's sometimes just called a role. A role definition lists the operations that can be performed, such as read, write, and delete.

Scope

Scope is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope.