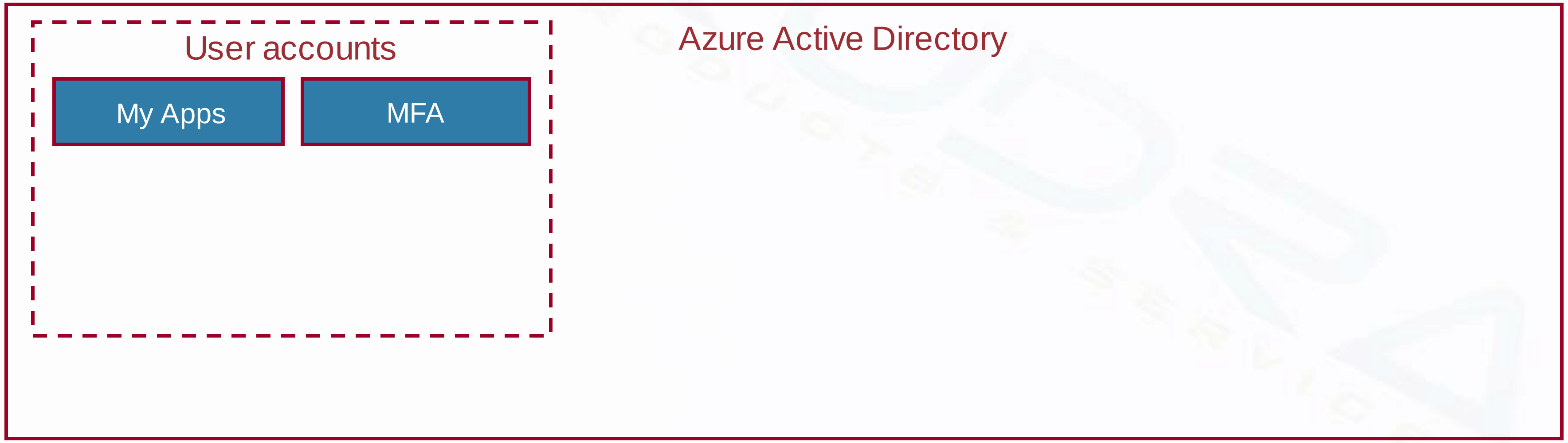
Step by step implementation of Azure Security Controls

Step 1 – Manage user accounts

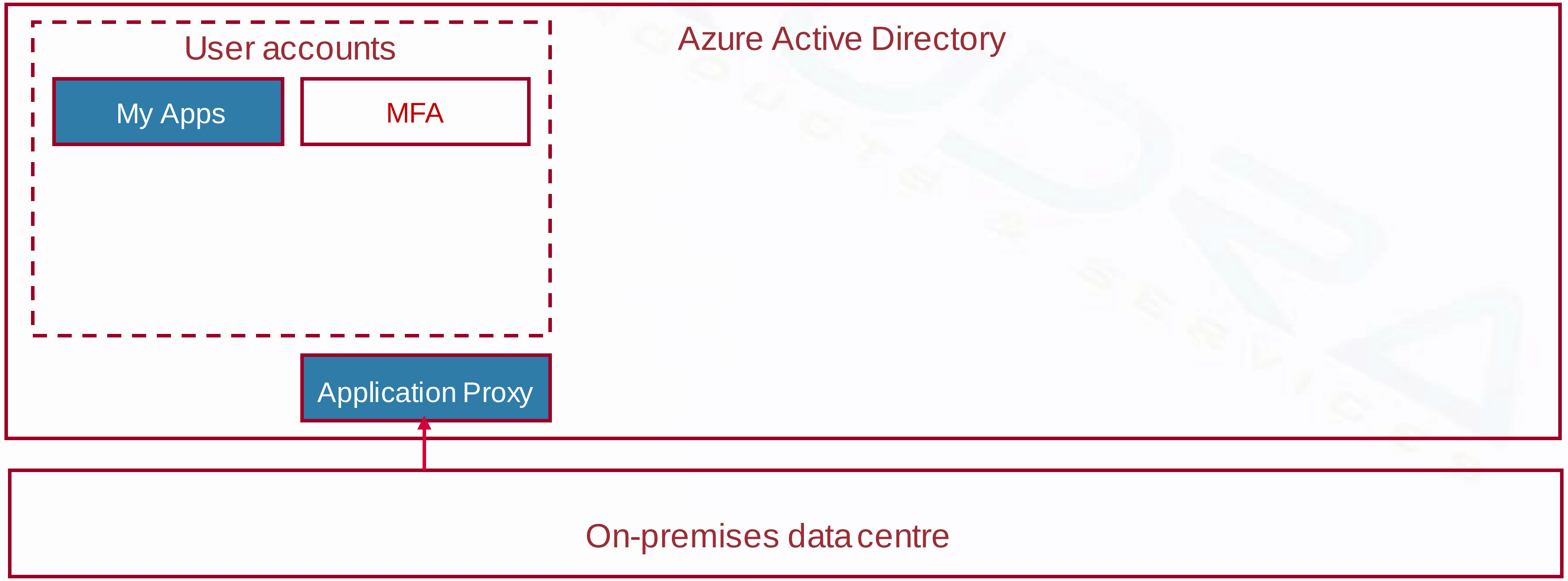
User accounts

Azure Active Directory

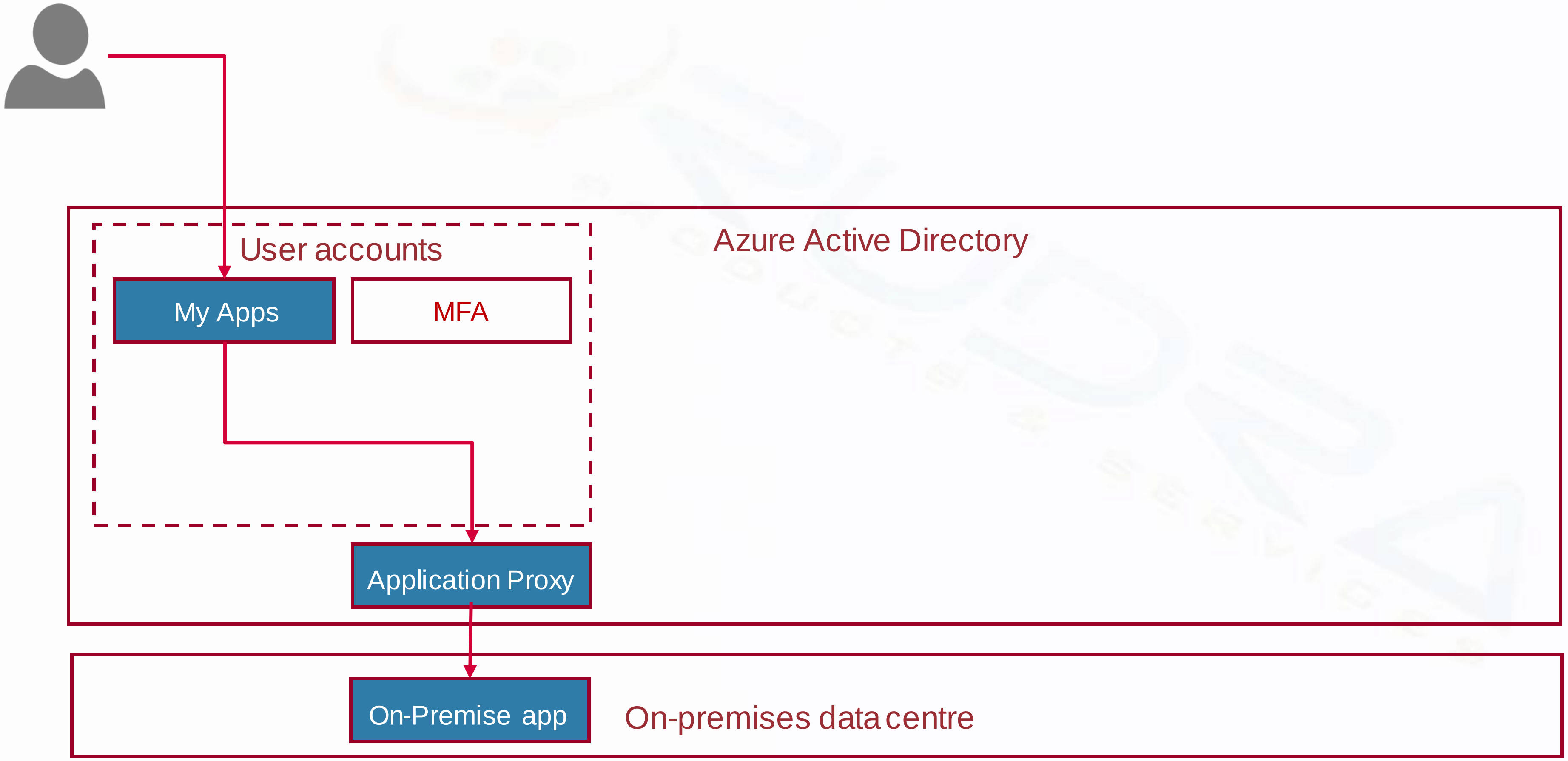
Step 2 – My Apps portal password reset, MFA and groups configuration



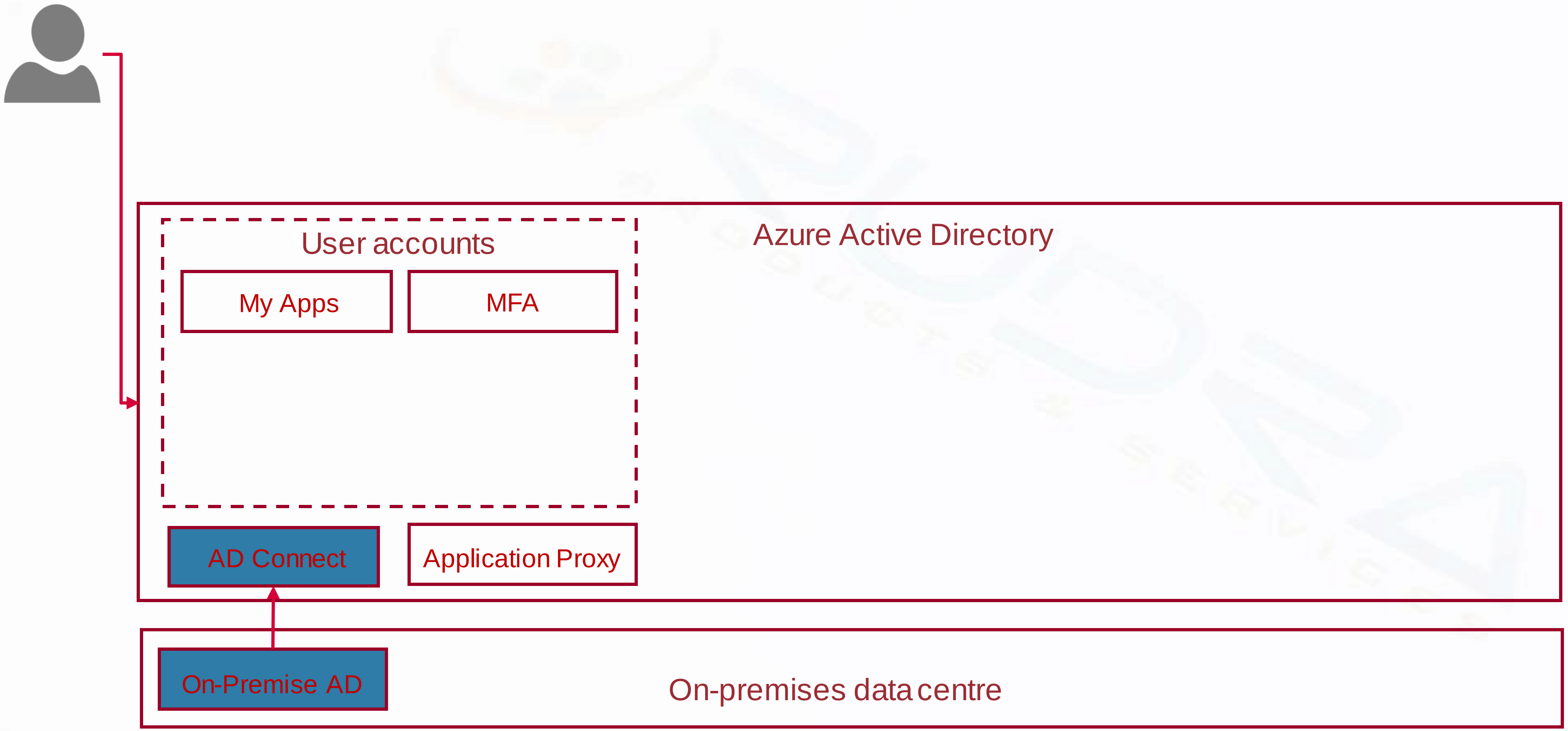
Step 3 – Publish an On-premise app into MyApps portal



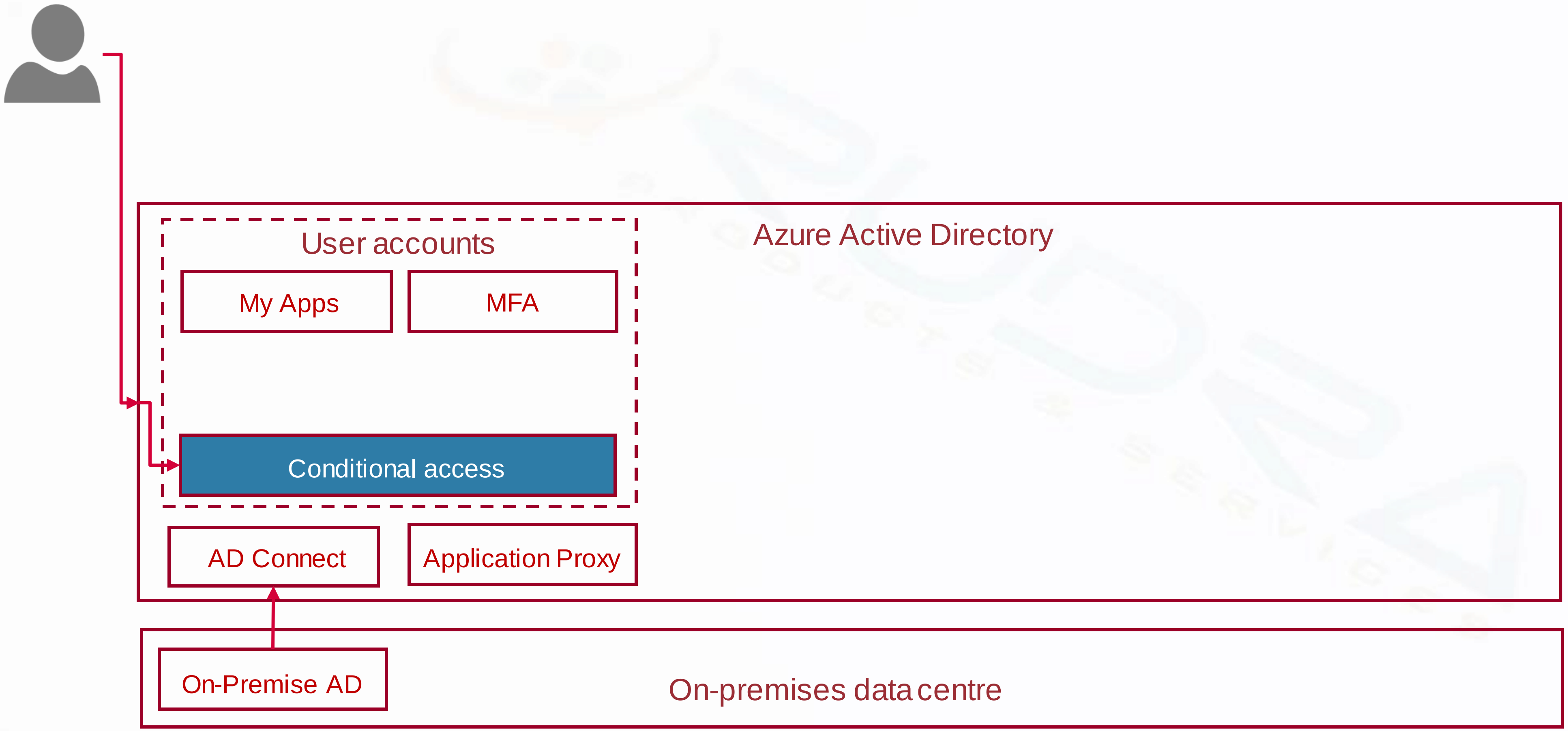
Step 4 – Enable Password based SSO for an on-premise app



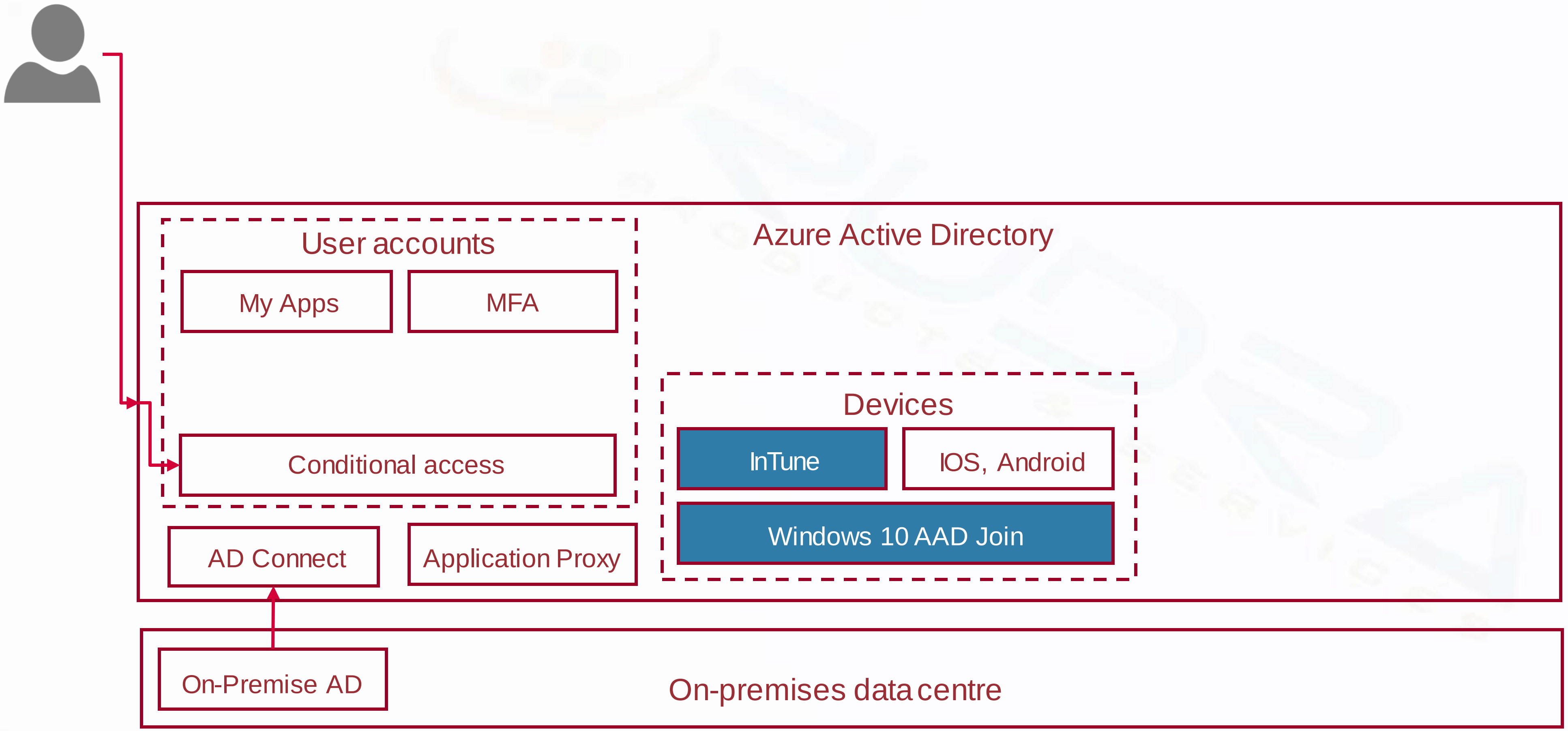
Step 5 – Synchronise users from On-premise AD into AAD



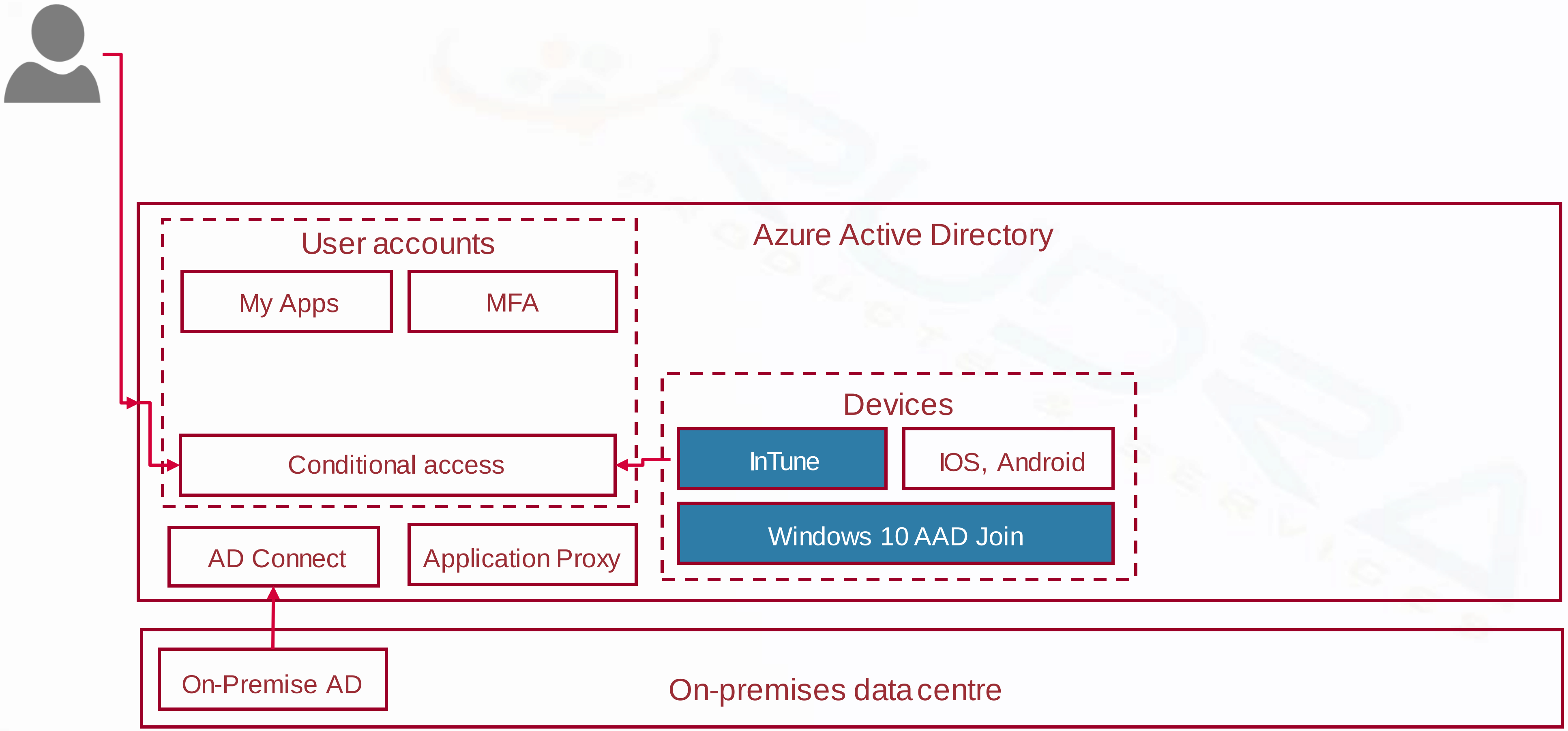
Step 6 – Implement location based conditional access policy



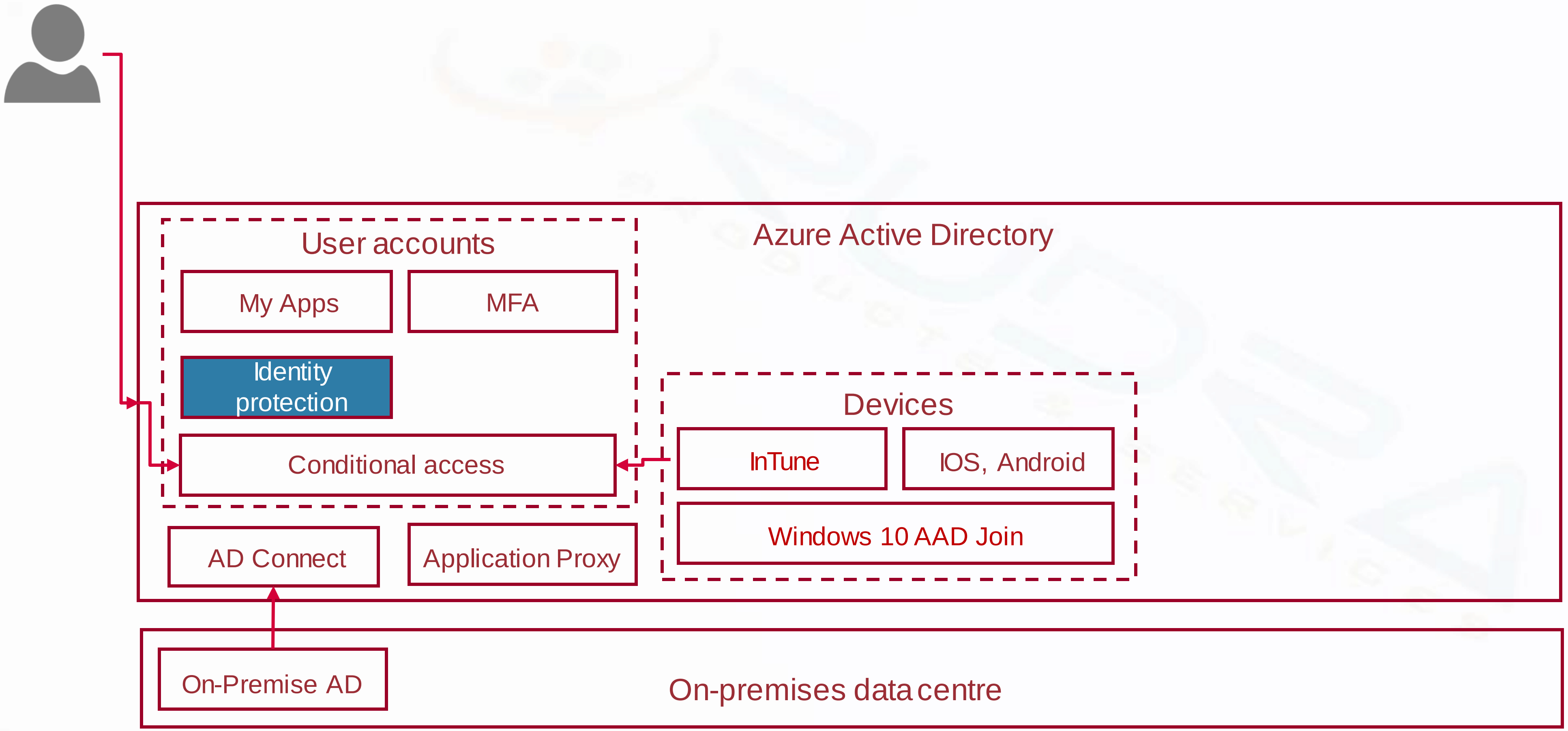
Step 7 – AAD join a Windows 10 device and enrol into Intune



Step 8 – Implement device based conditional access



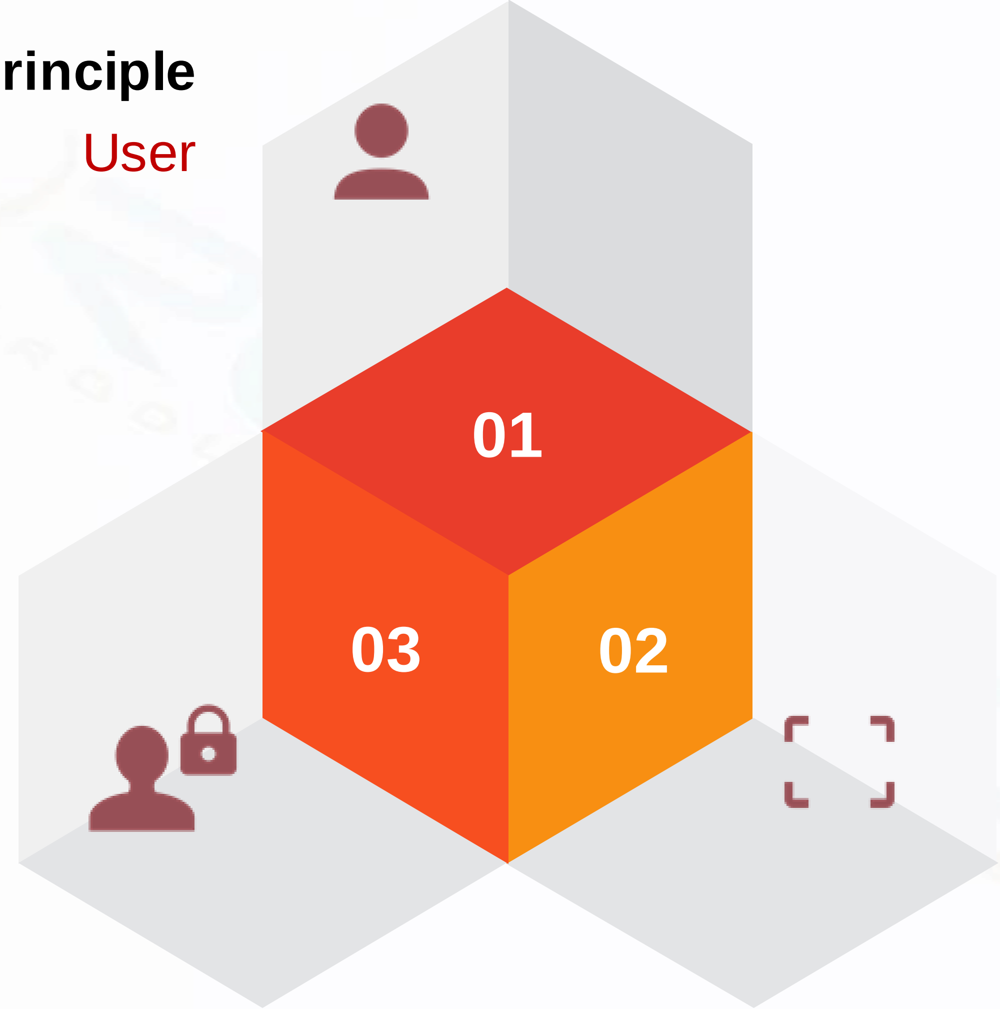
Step 8a – Implement AAD Identity protection



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

Security Principle

User



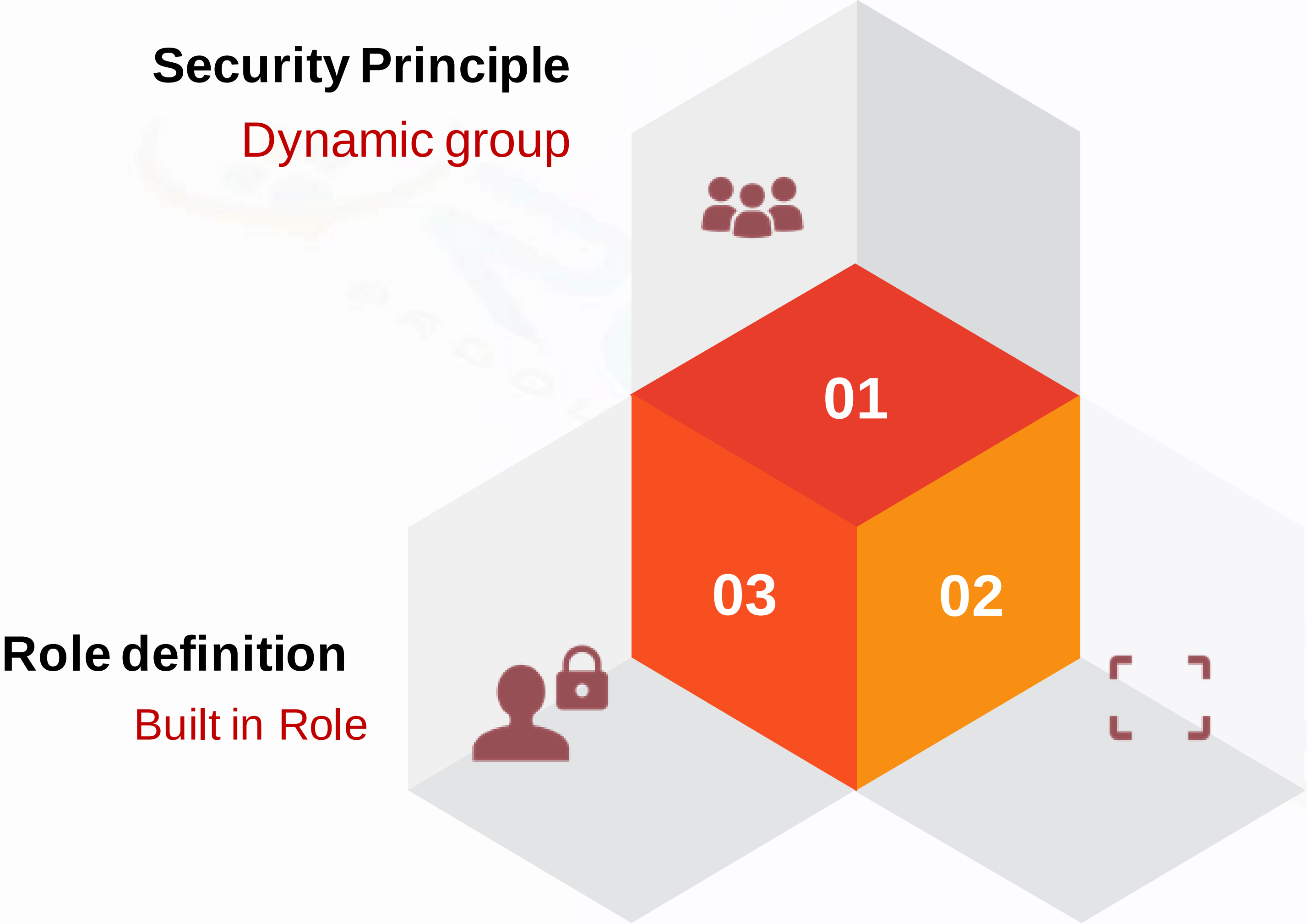
Role definition

Built in Role
Custom Role

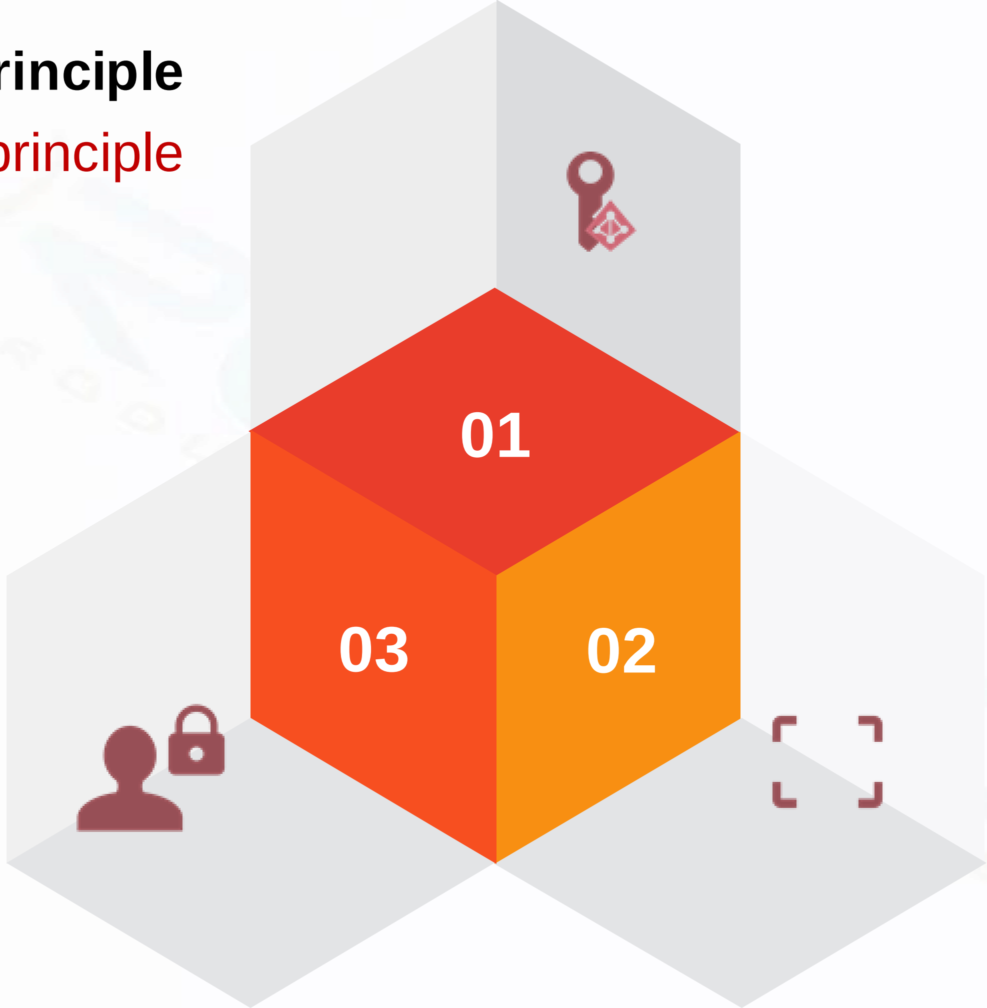
Scope

Subscription
Storage account

Step 10 – Dynamic group creation and role assignment



Step 11 – Service principle creation and role assignment



Security Principle

Service principle

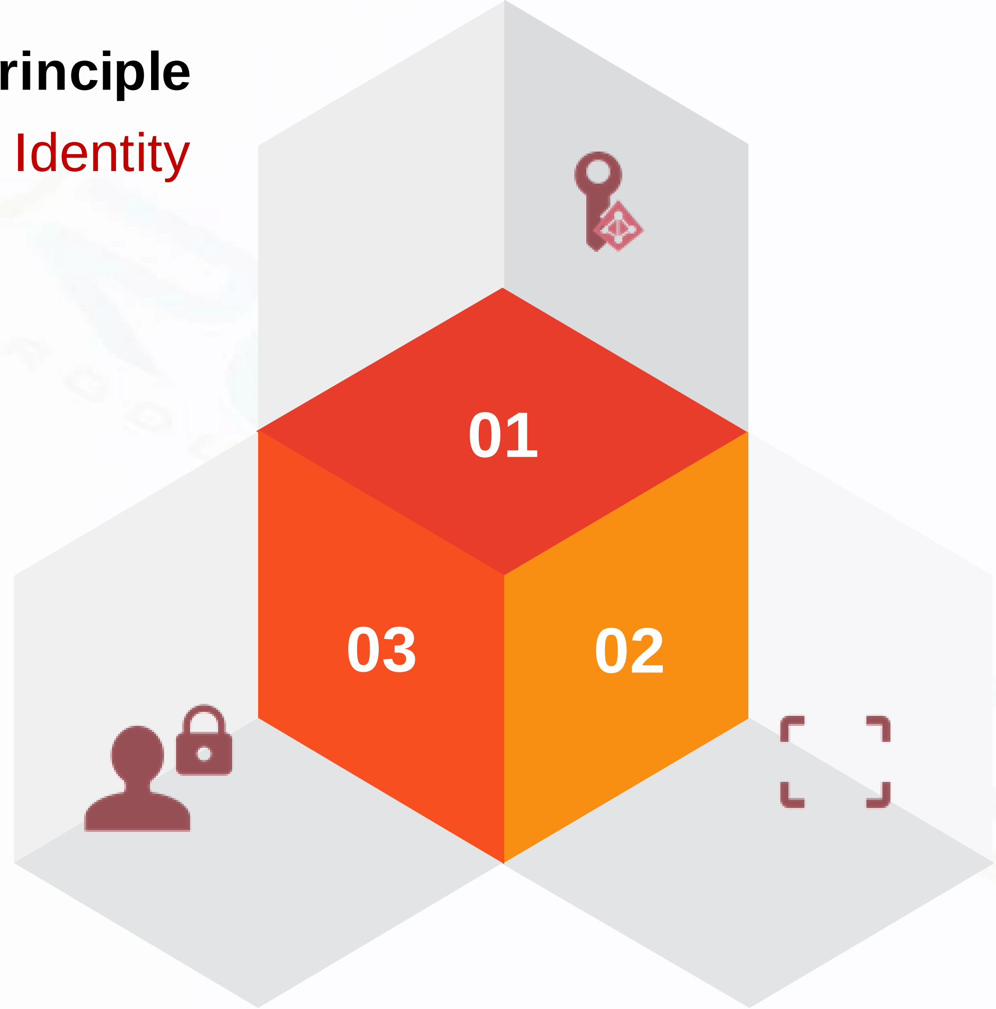
Scope

Storage account

Role definition

Built in Role

Step 12 – Managed identity creation and role assignment



Security Principle

Managed Identity

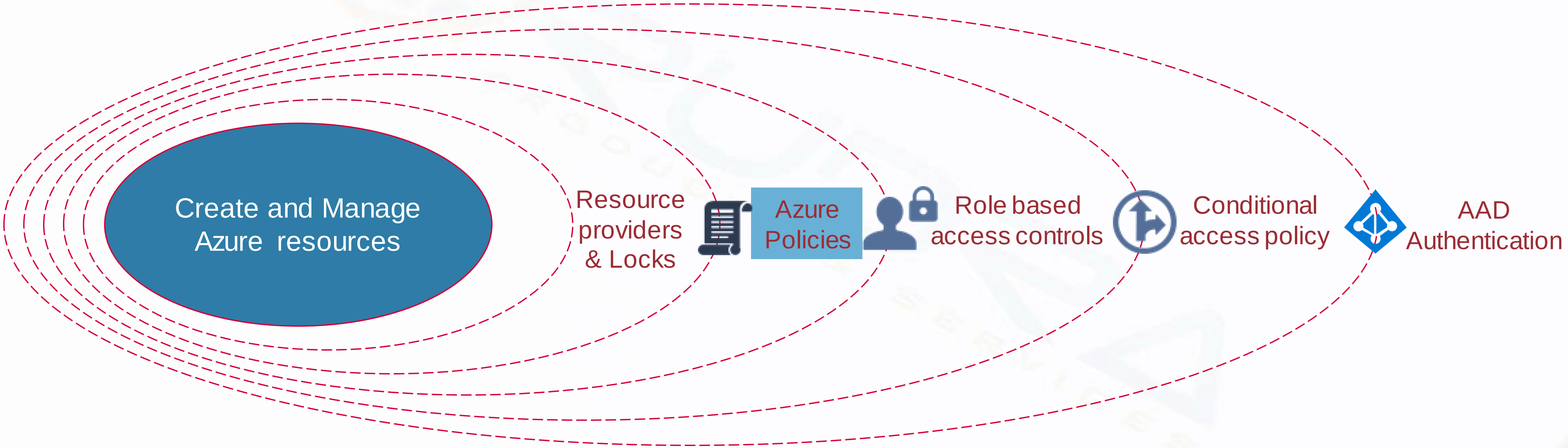
Scope

Storage account

Role definition

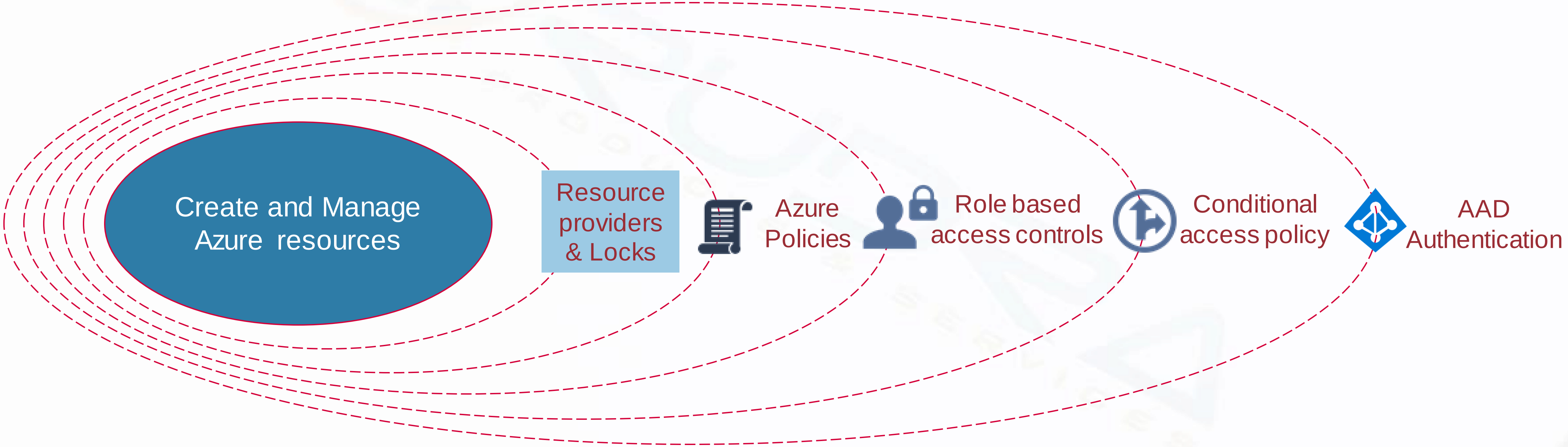
Built in Role

Step 13 – Implement Azure policies

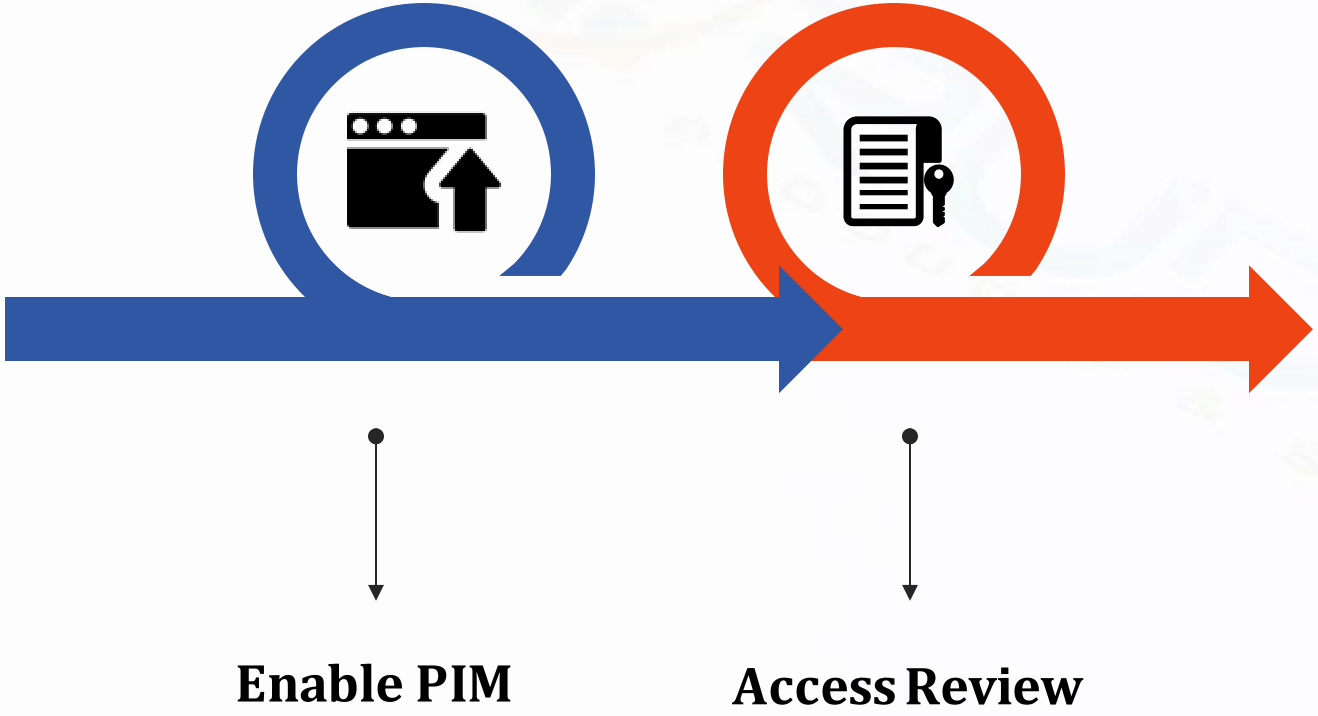


Create and Manage Azure resources
Resource providers & Locks
Azure Policies
Role based access controls
Conditional access policy
AAD Authentication

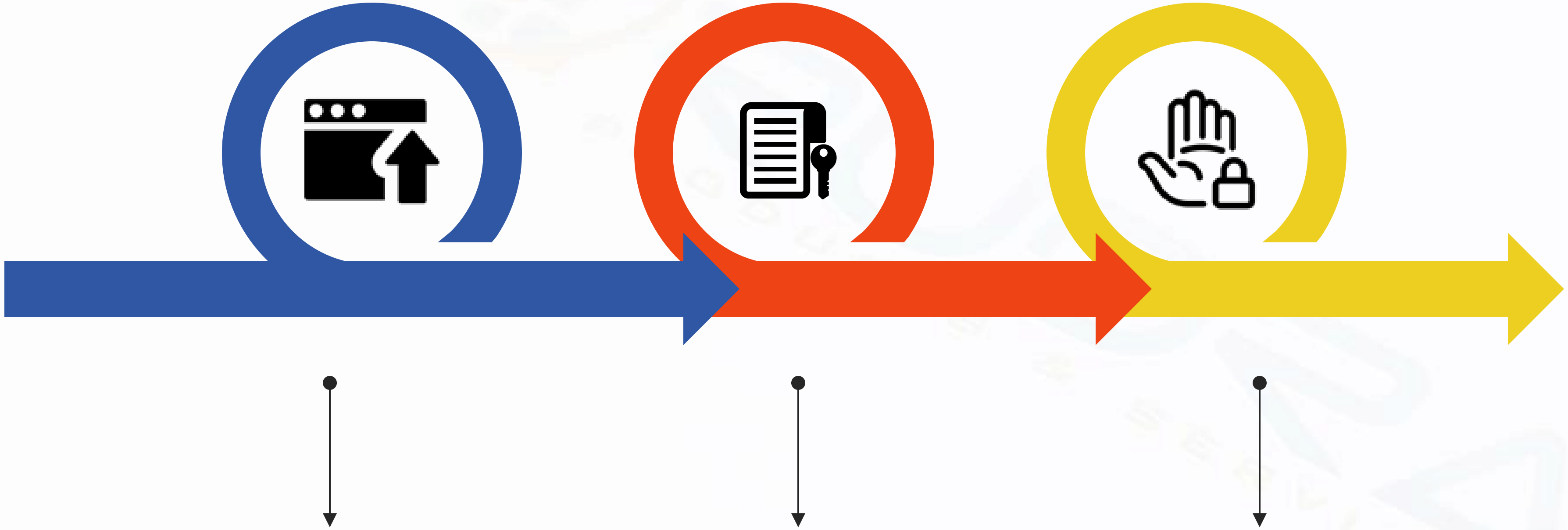
Step 14 – Resource providers & locks


Create and Manage
Azure resources
Resource providers & Locks
Azure Policies
Role based access controls
Conditional access policy
AAD Authentication

Step 15 – Initiate PIM and conduct access review



Step 16 – Protect AD role assignments using PIM

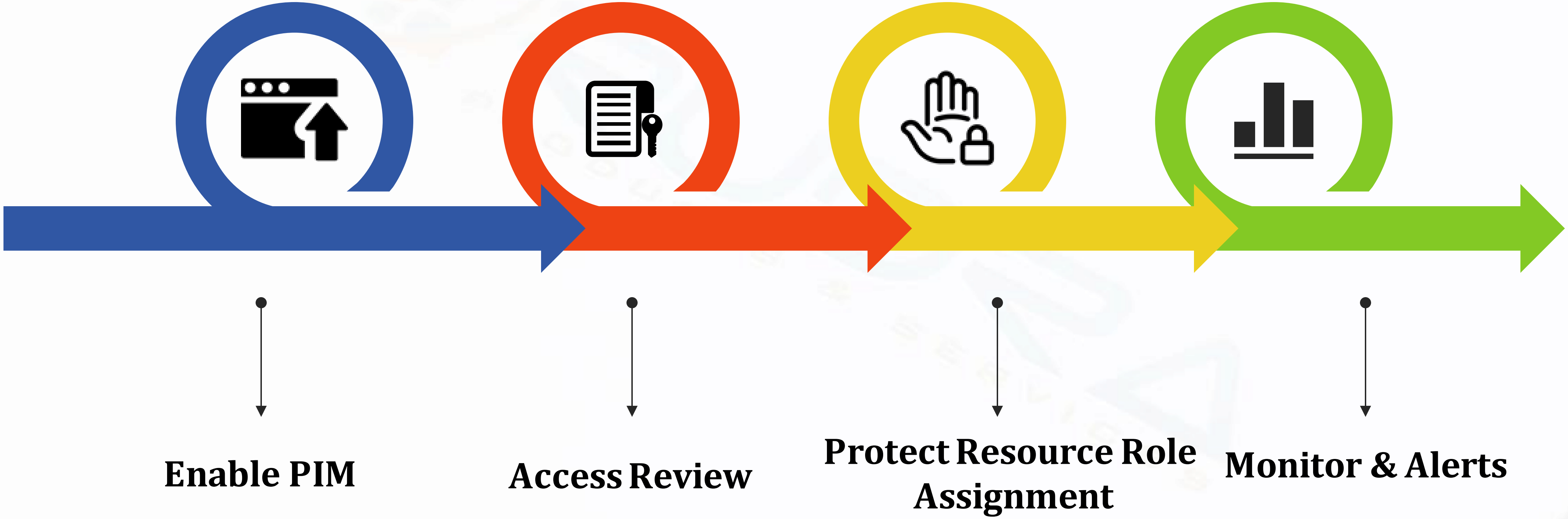


Enable PIM

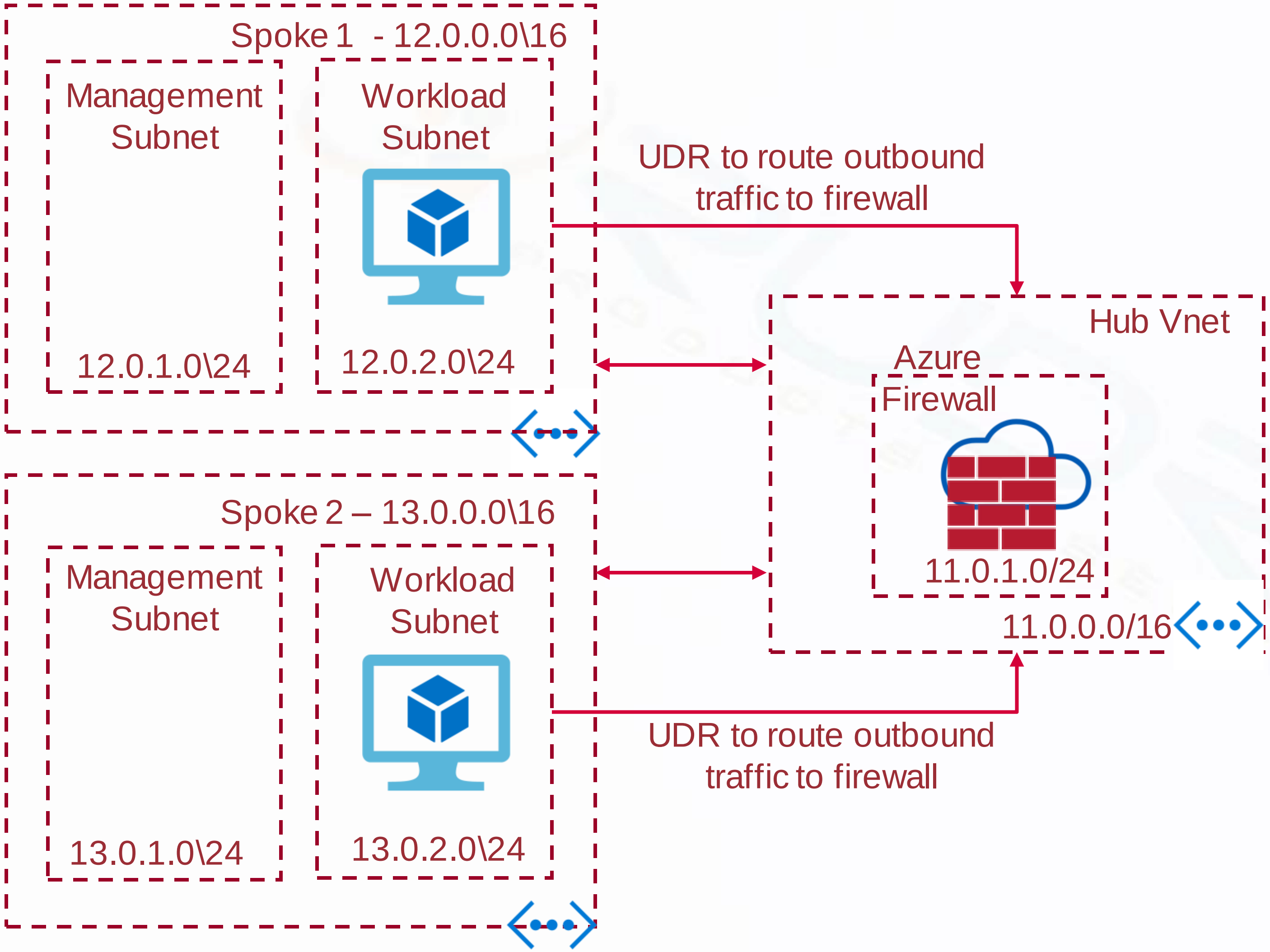
Access Review

Protect AD Role Assignments

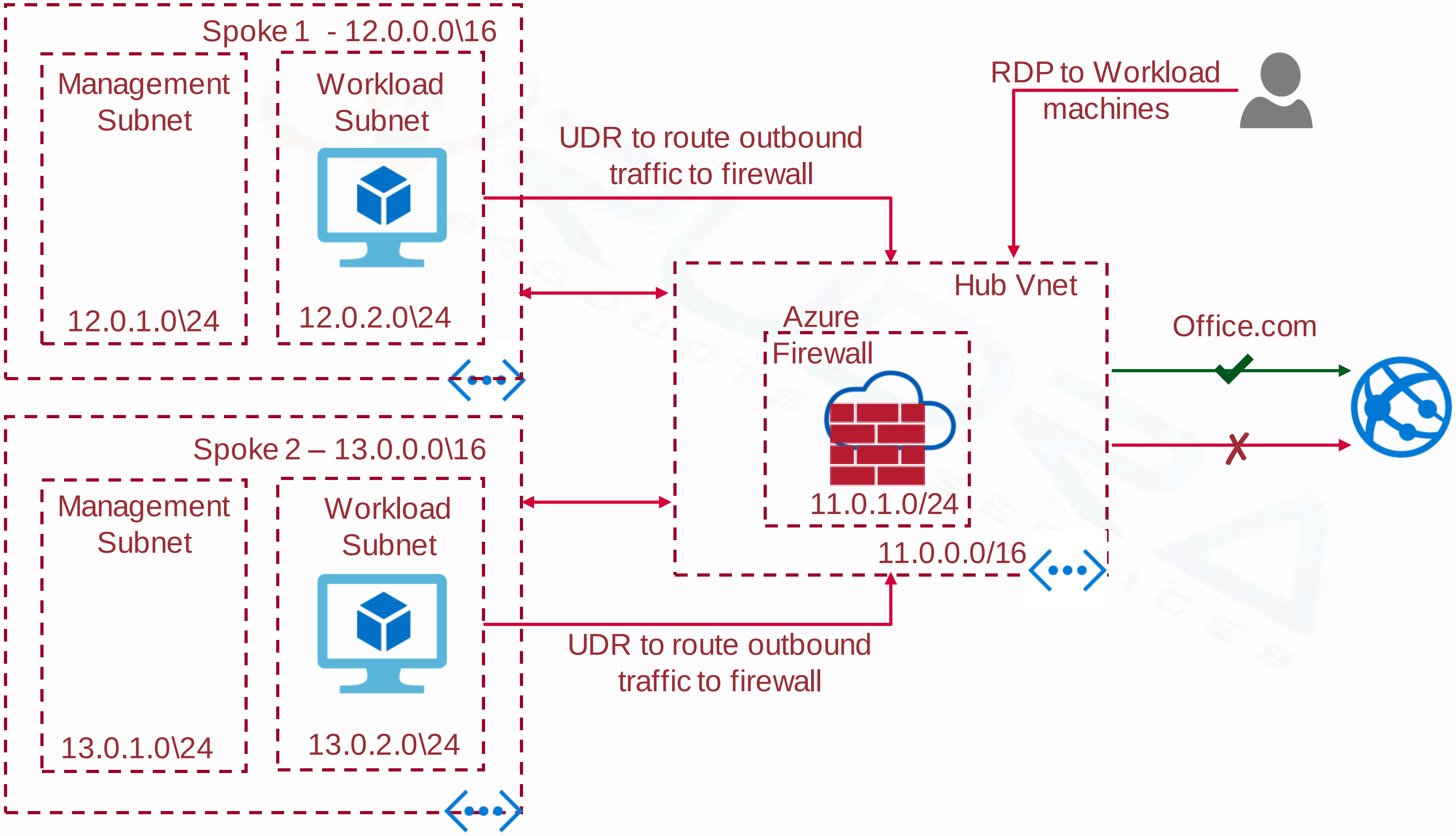
Step 17 – Protect resource role assignment and monitor PIM



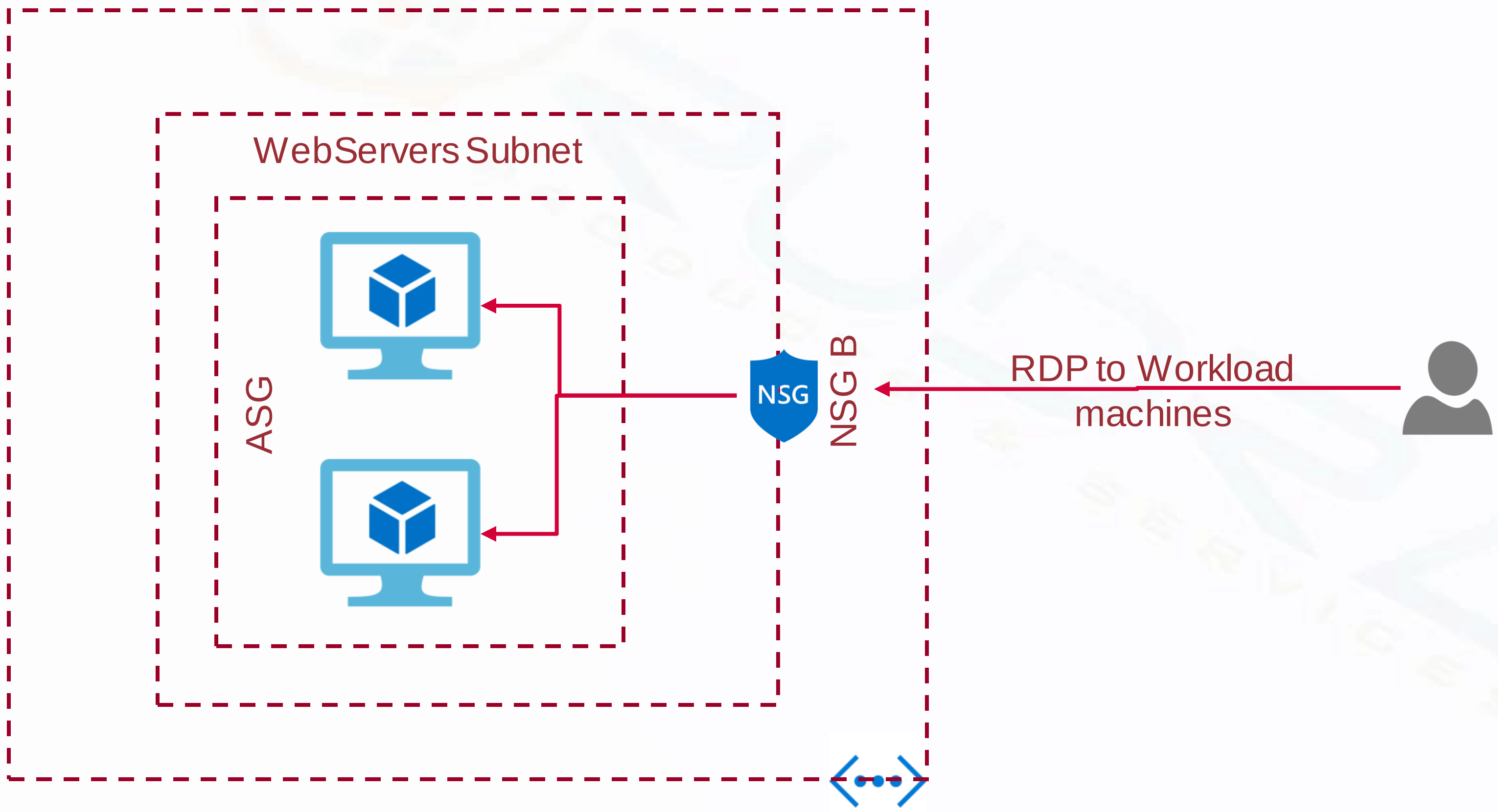
Step 18a – Deploy Azure Firewall in Hub and Spoke model



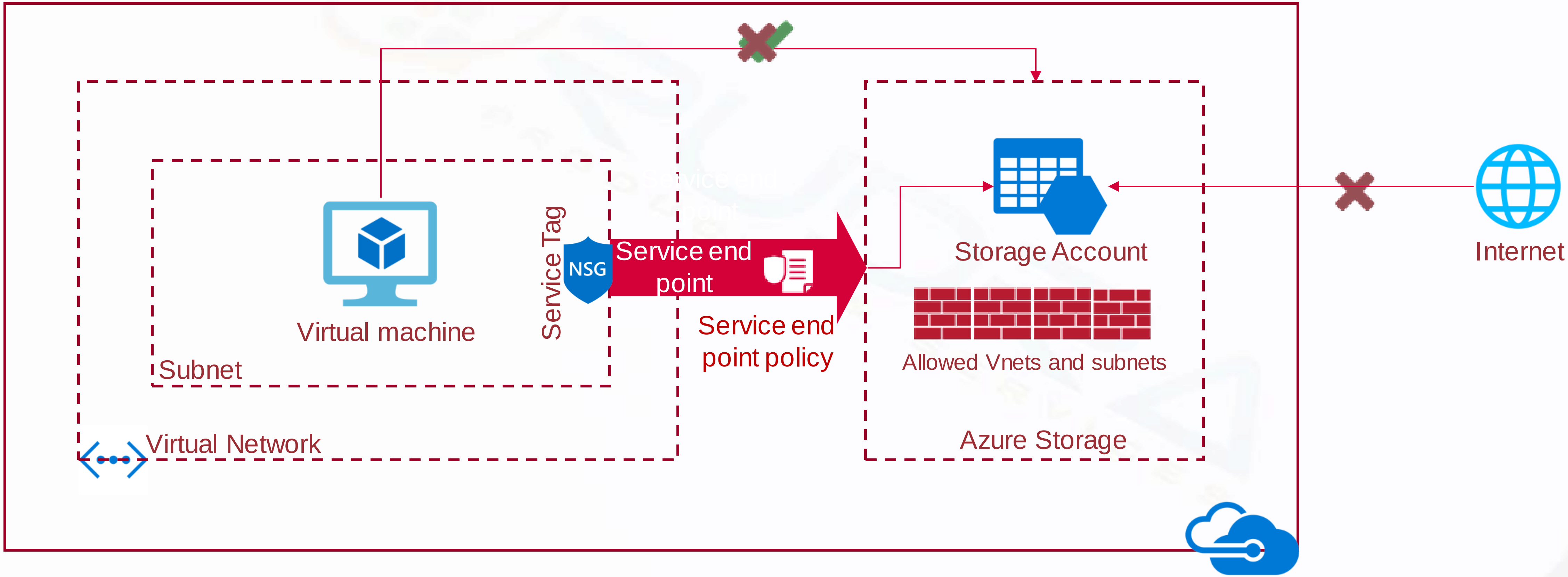
Step 18b – Configure Azure Firewall to allow RDP and control outbound traffic



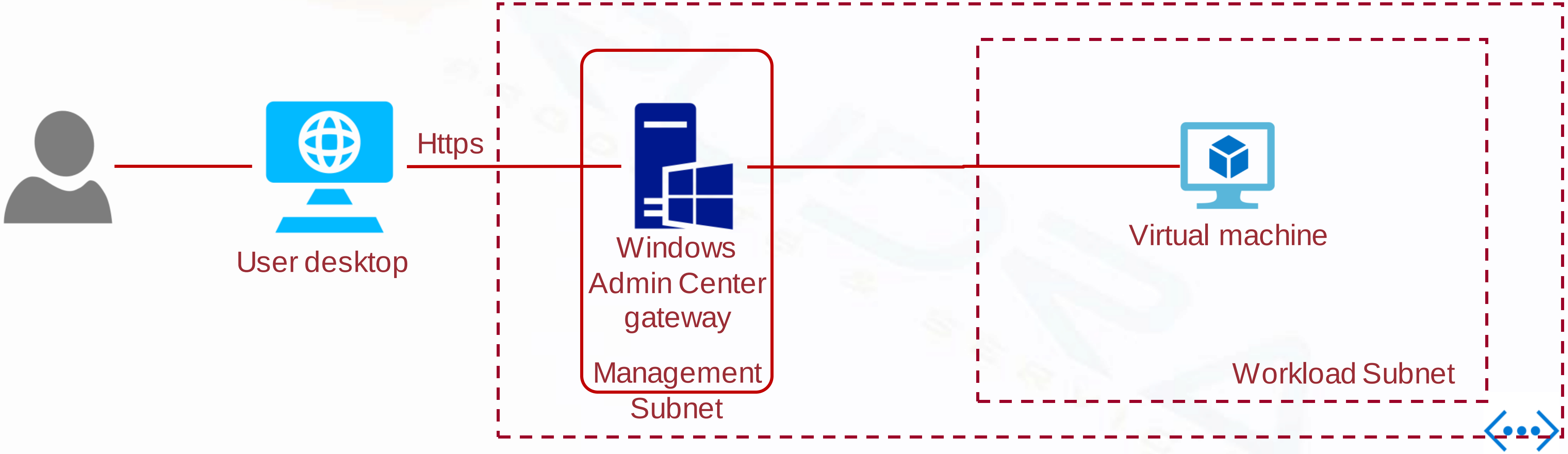
Step 19 – Configure NSG & ASG to control inbound RDP traffic



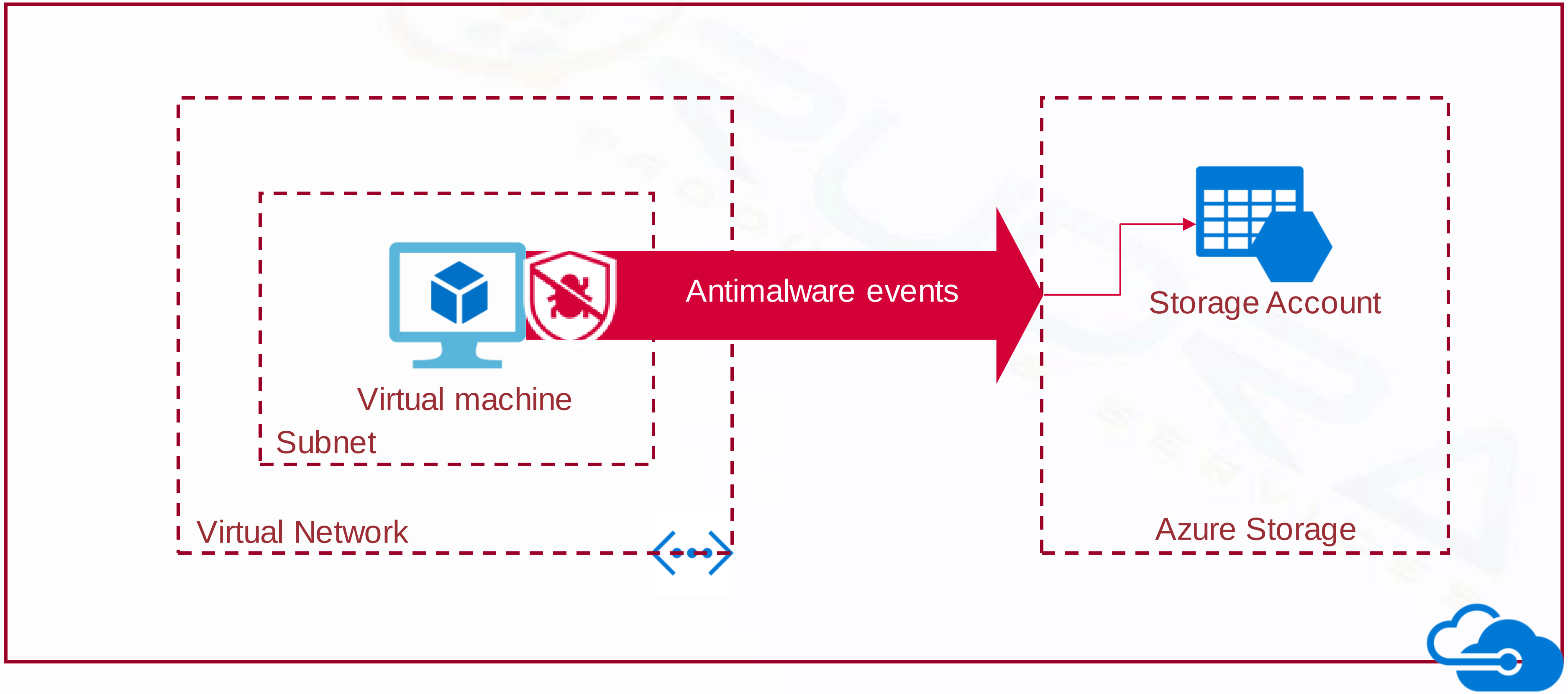
Step 20 – Configure service endpoint and policy



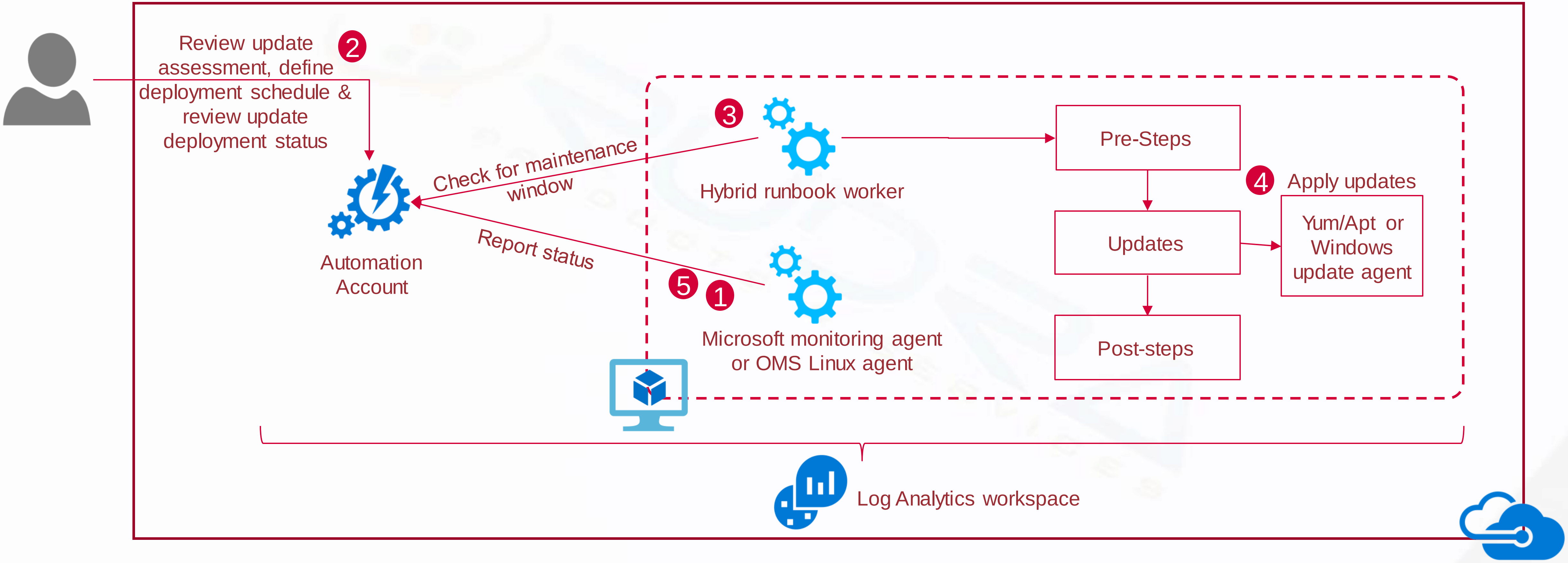
Step 21 – Remote access Azure VM using Windows Admin Centre



Step 22 – IaaS security – Endpoint protection

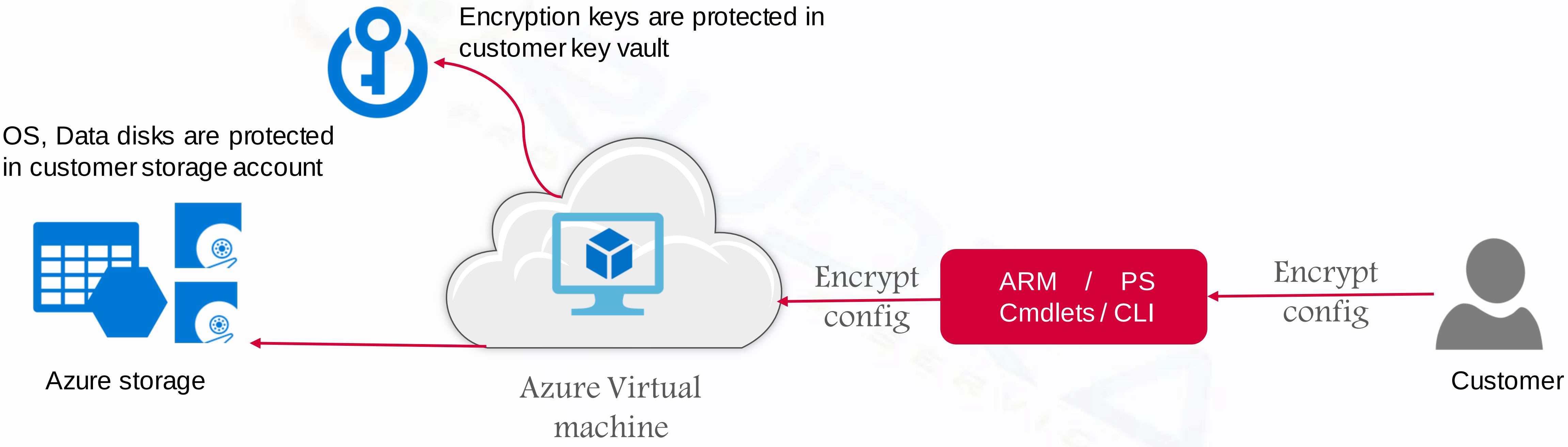


Step 23 – IaaS Security – Update management



Review update assessment, define deployment schedule & review update deployment status
2
Check for maintenance window
3
Hybrid runbook worker
Pre-Steps
4
Apply updates
Updates
Yum/Apt or Windows update agent
Post-steps
Automation Account
Report status
5
1
Microsoft monitoring agent or OMS Linux agent
Log Analytics workspace

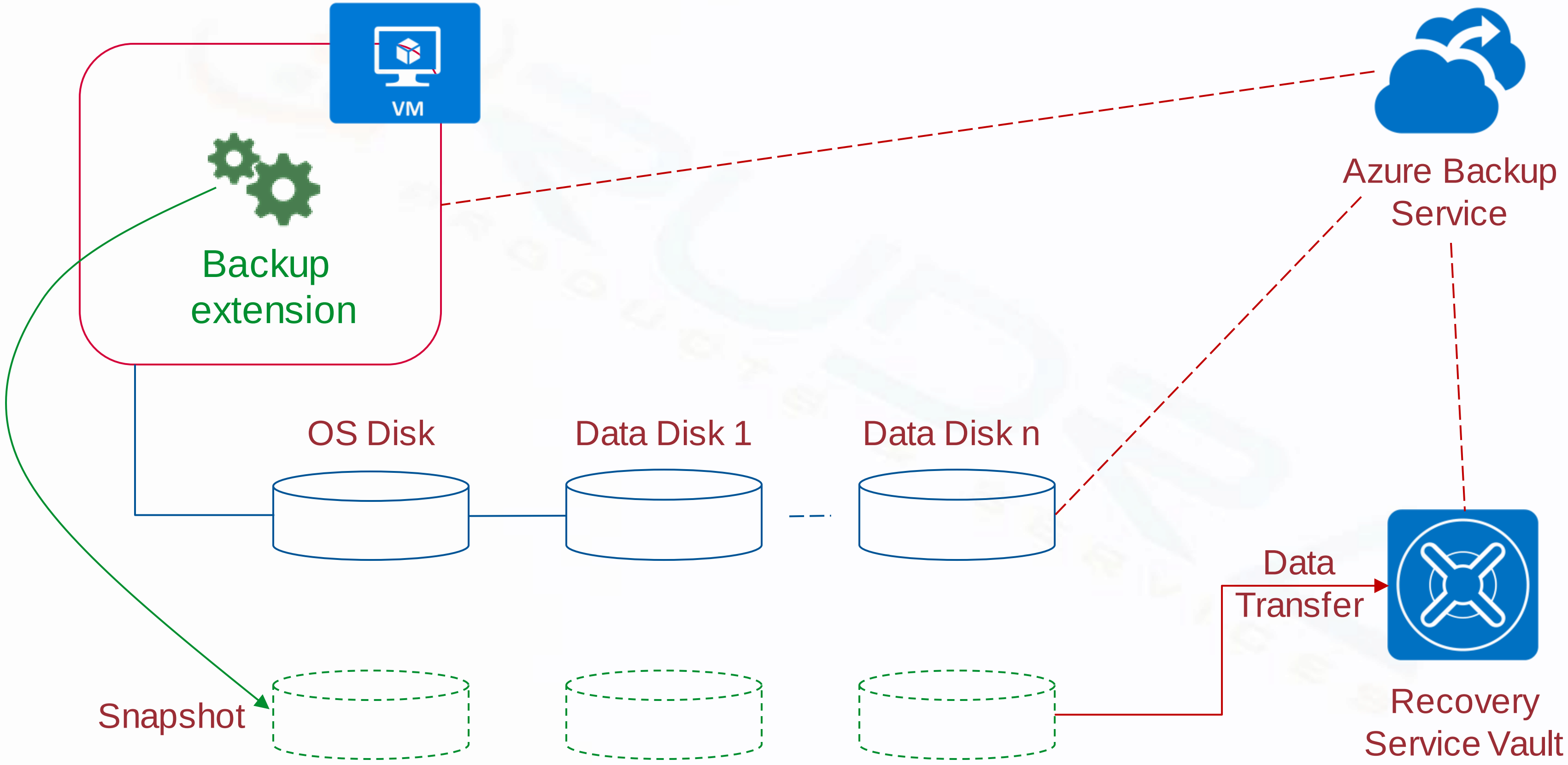
Step 24 – IaaS Security – Disk encryption



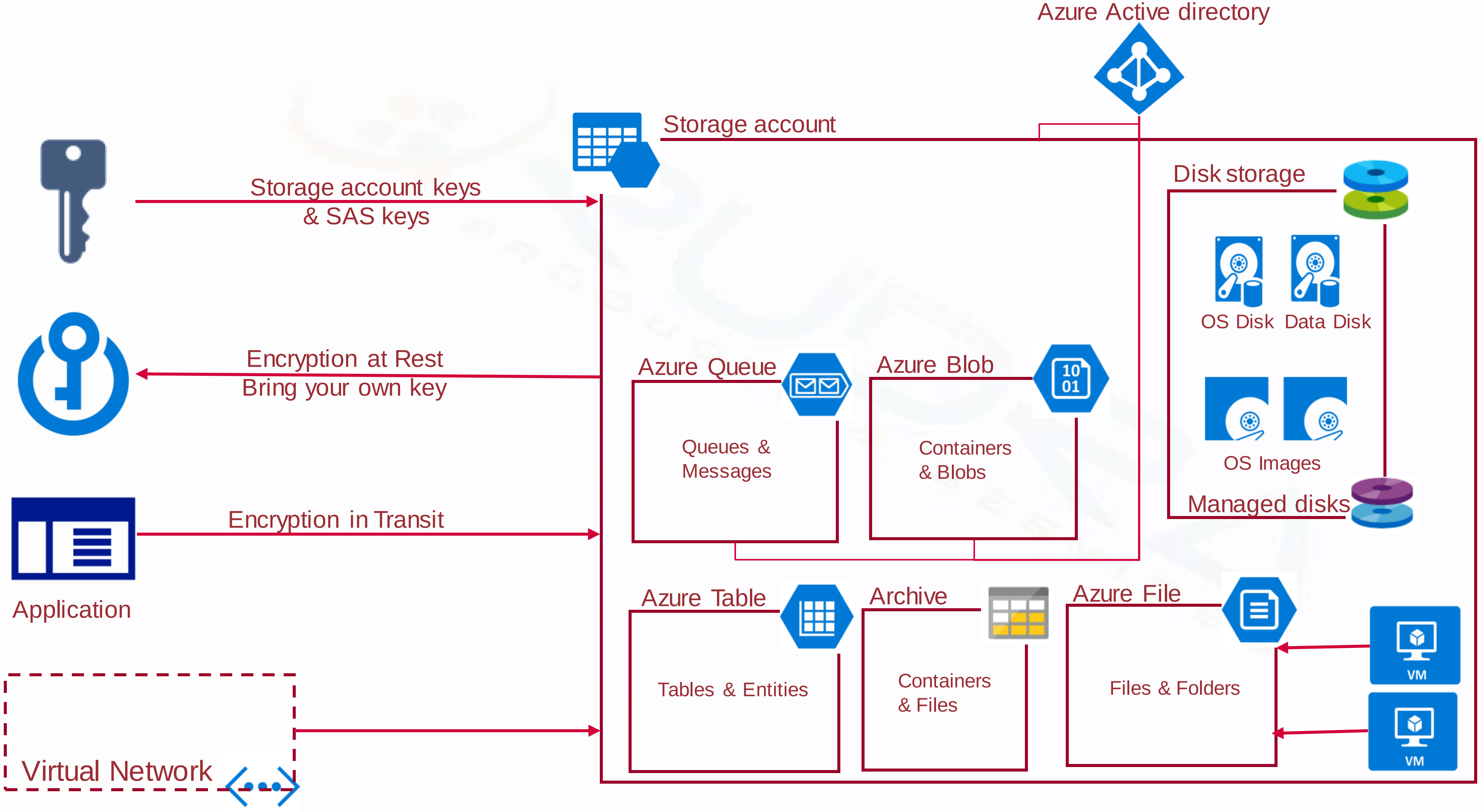
Encryption keys are protected in customer key vault

OS, Data disks are protected in customer storage account

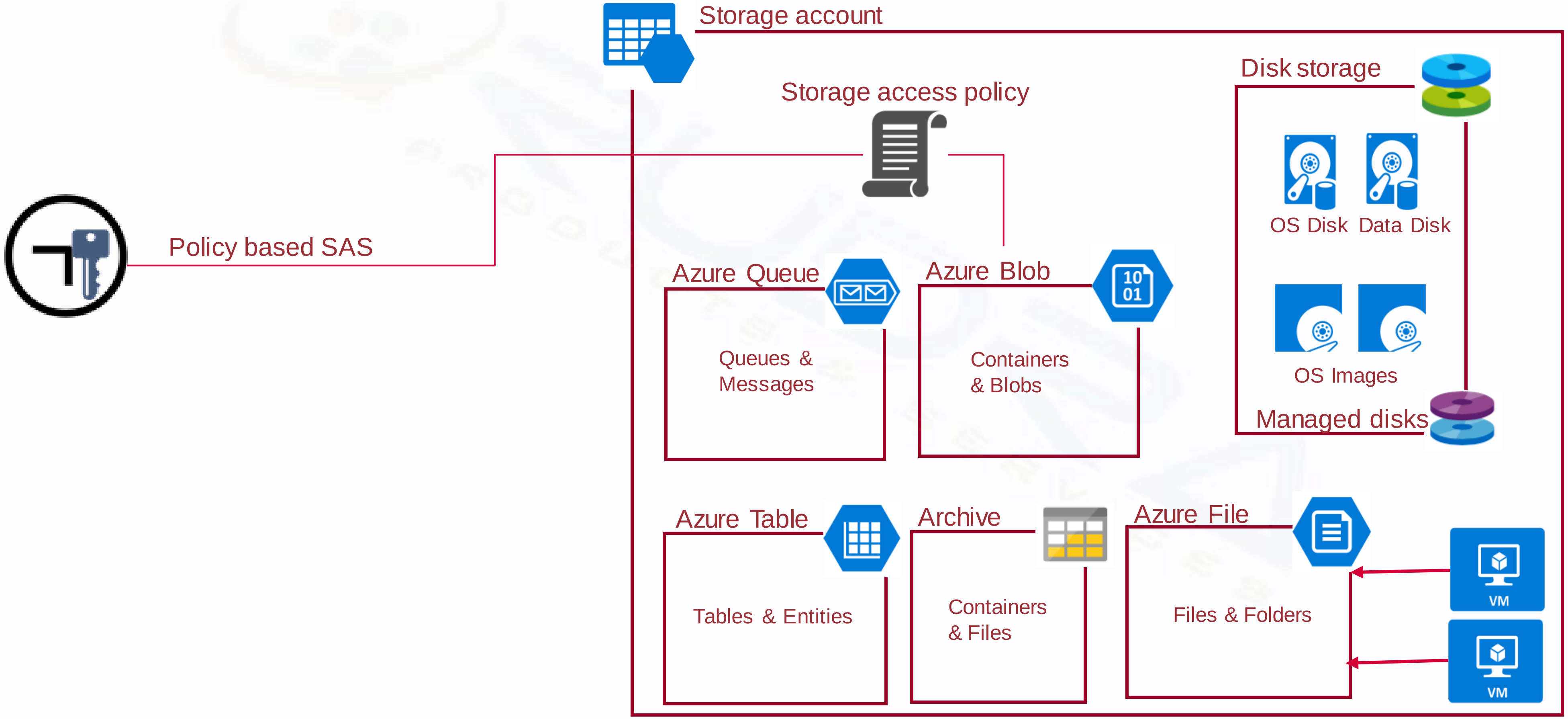
Step 25 - IaaS Security – Backup encryption



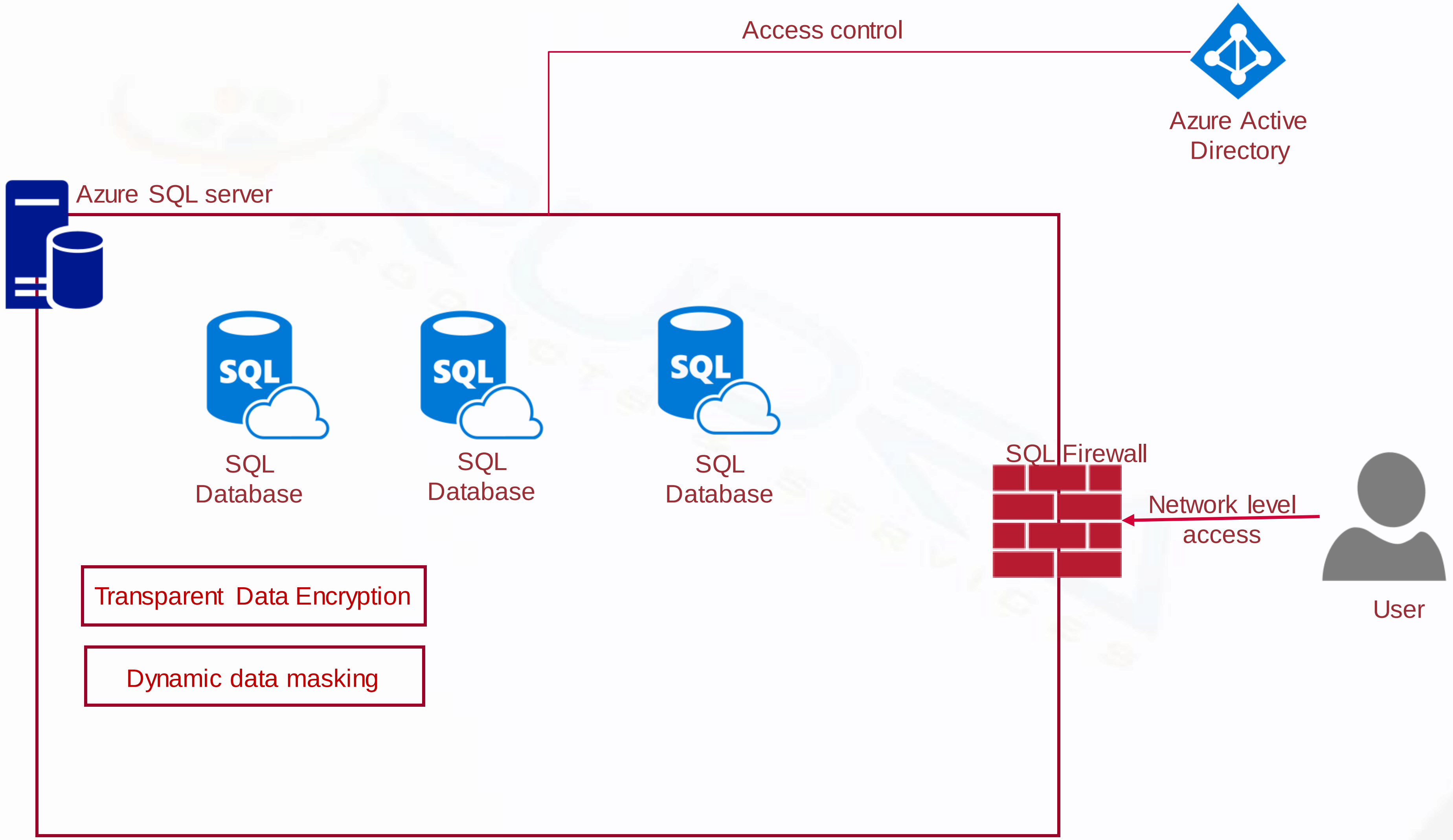
Step 26 – Walkthrough of Azure storage security features



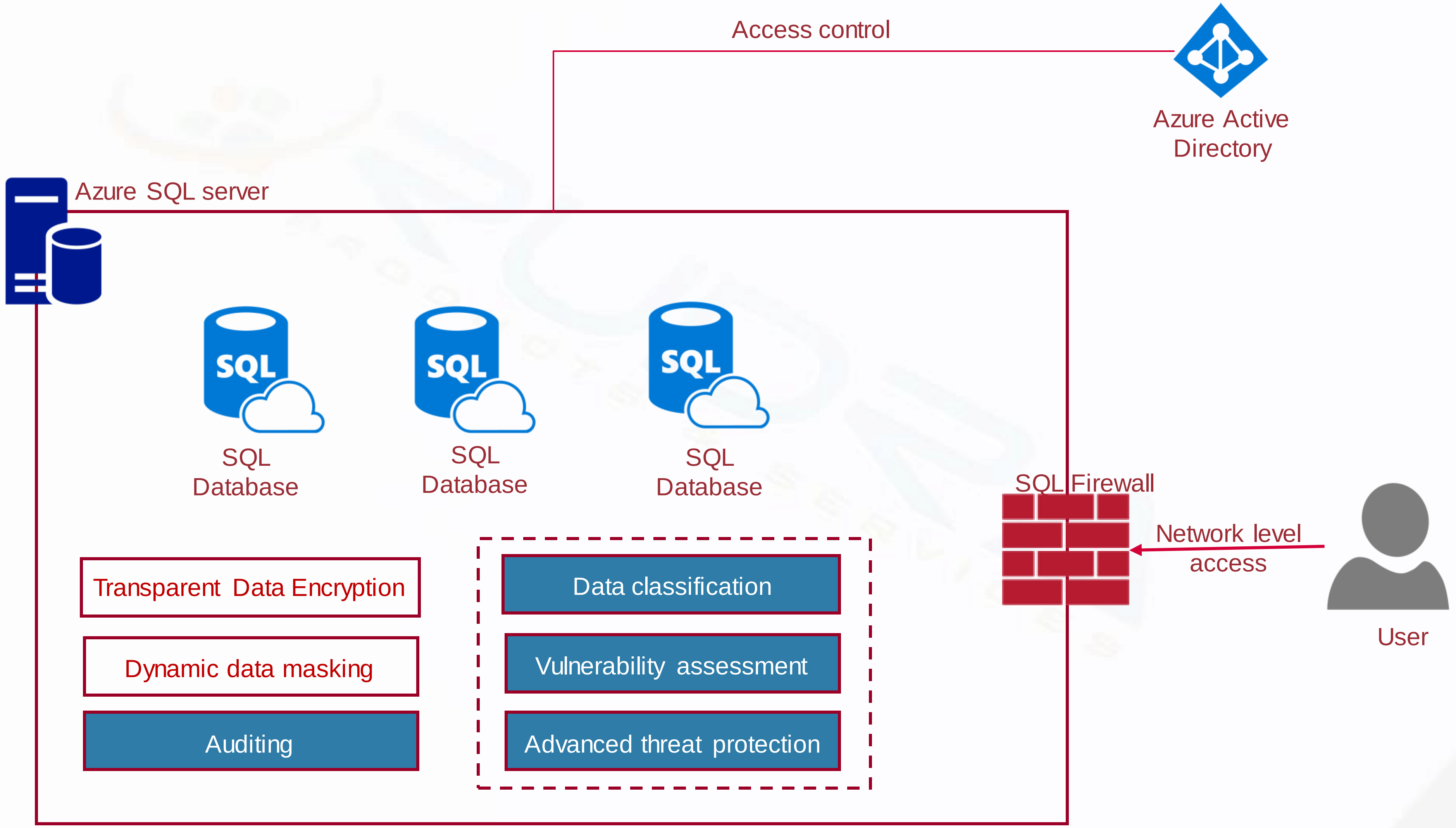
Step 27 - Create and use SAS Keys based on Storage access policies



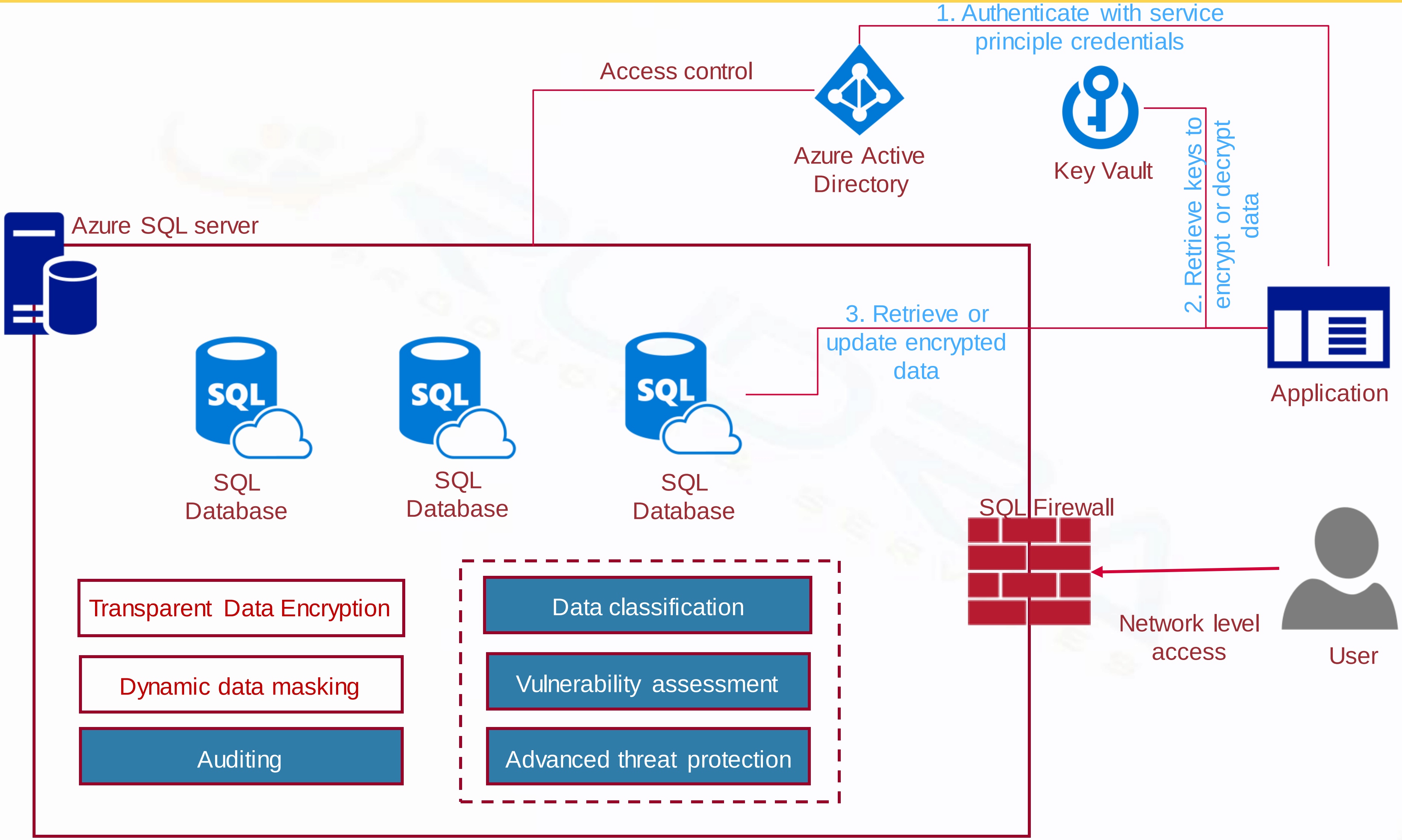
Step 28 – Implement access control, Firewall rules, TDE and dynamic data masking



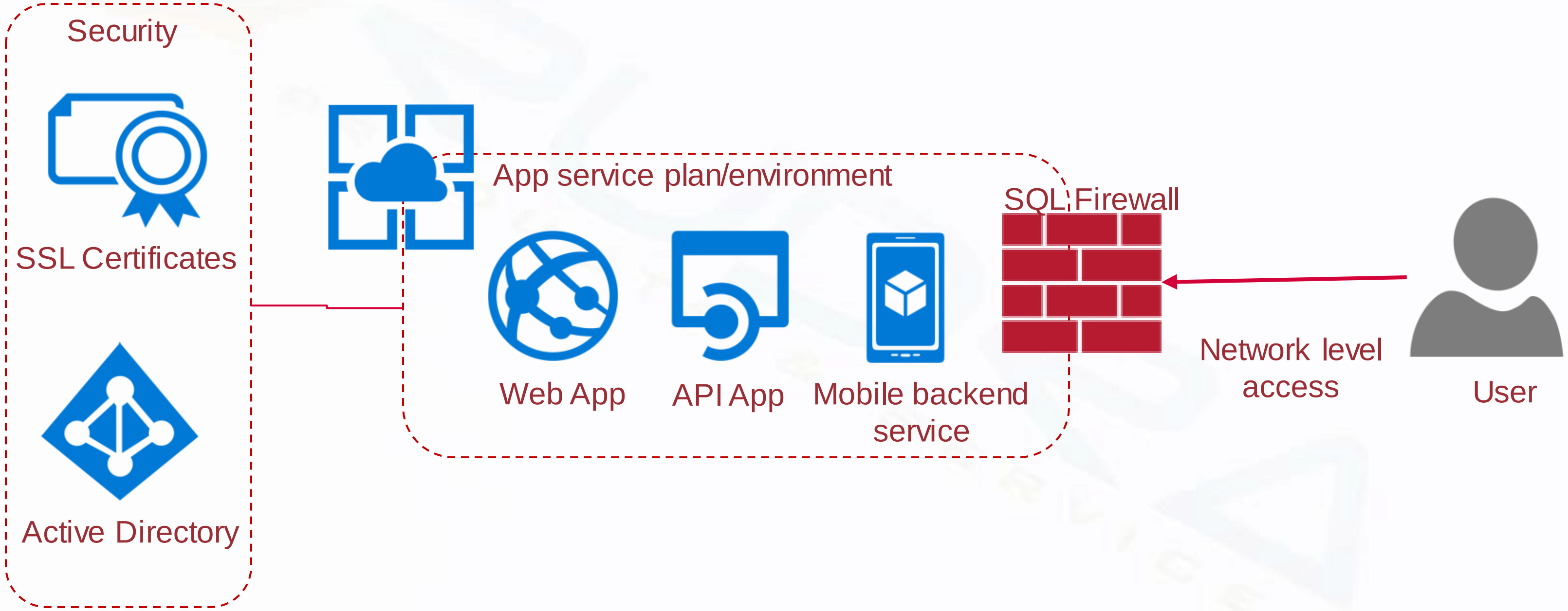
Step 29 – Implement Advanced Data Security and Auditing



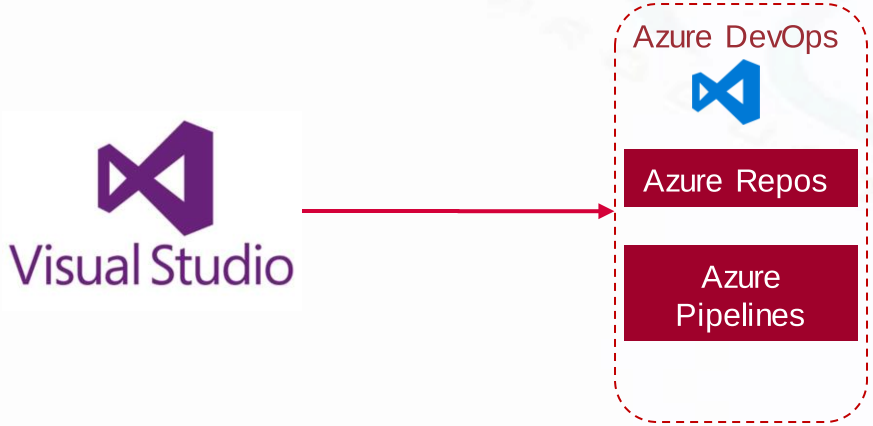
Step 30 - Implement Always encrypted in Azure SQL database



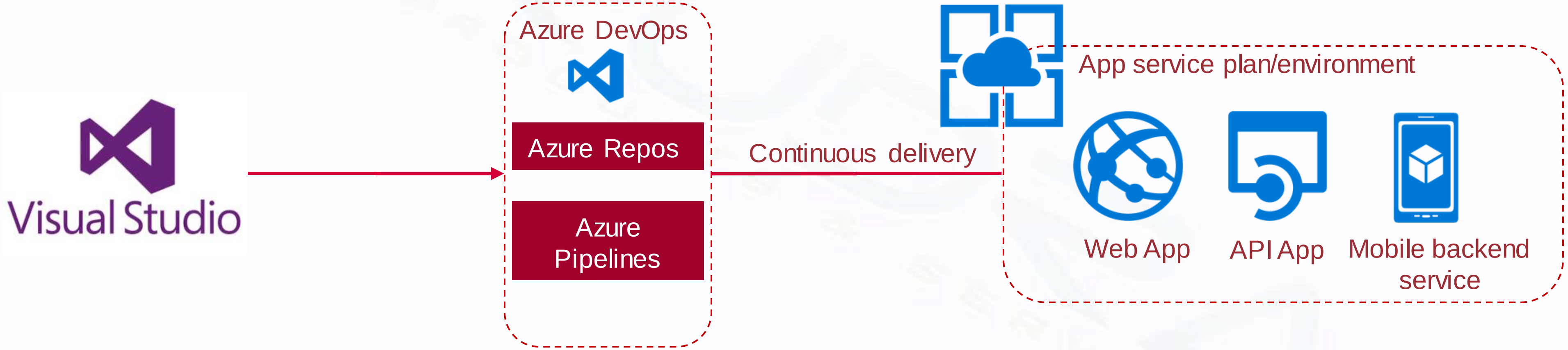
Step 31 - Authentication with AAD and configure SSL for Azure App service



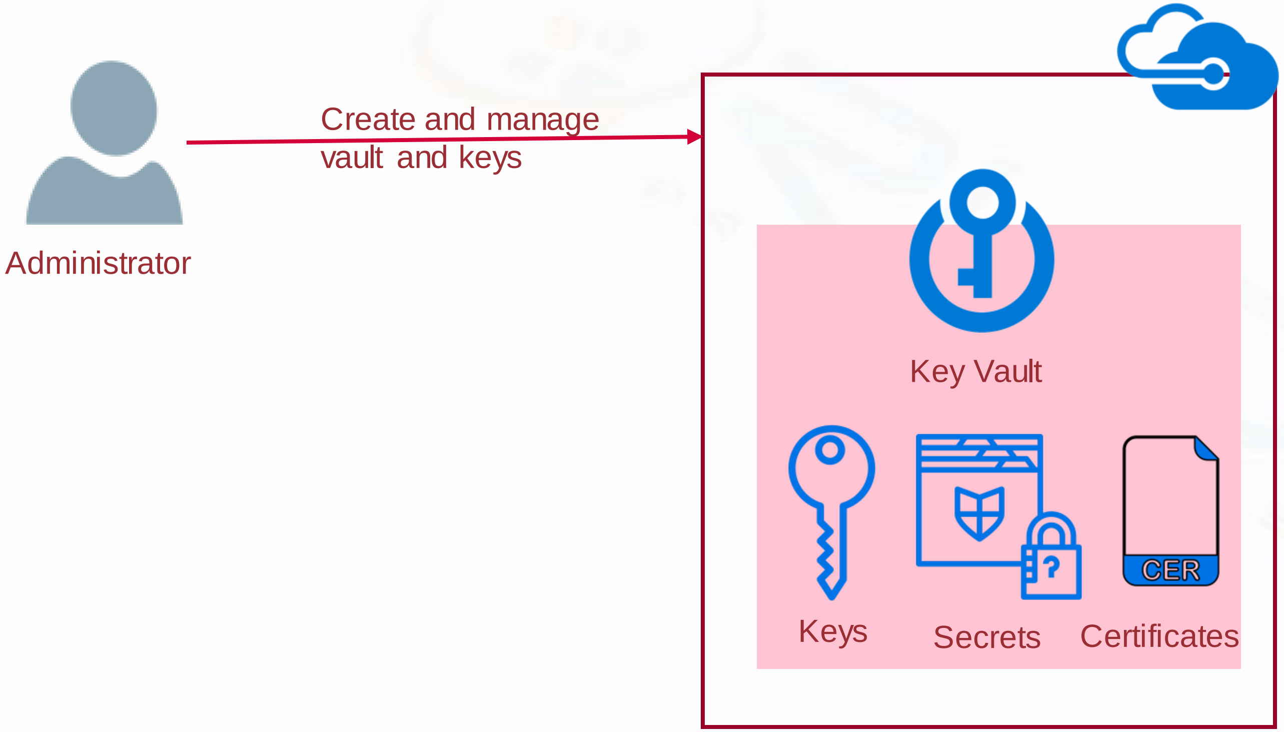
Step 32a – Securely deploying code using Azure Devops



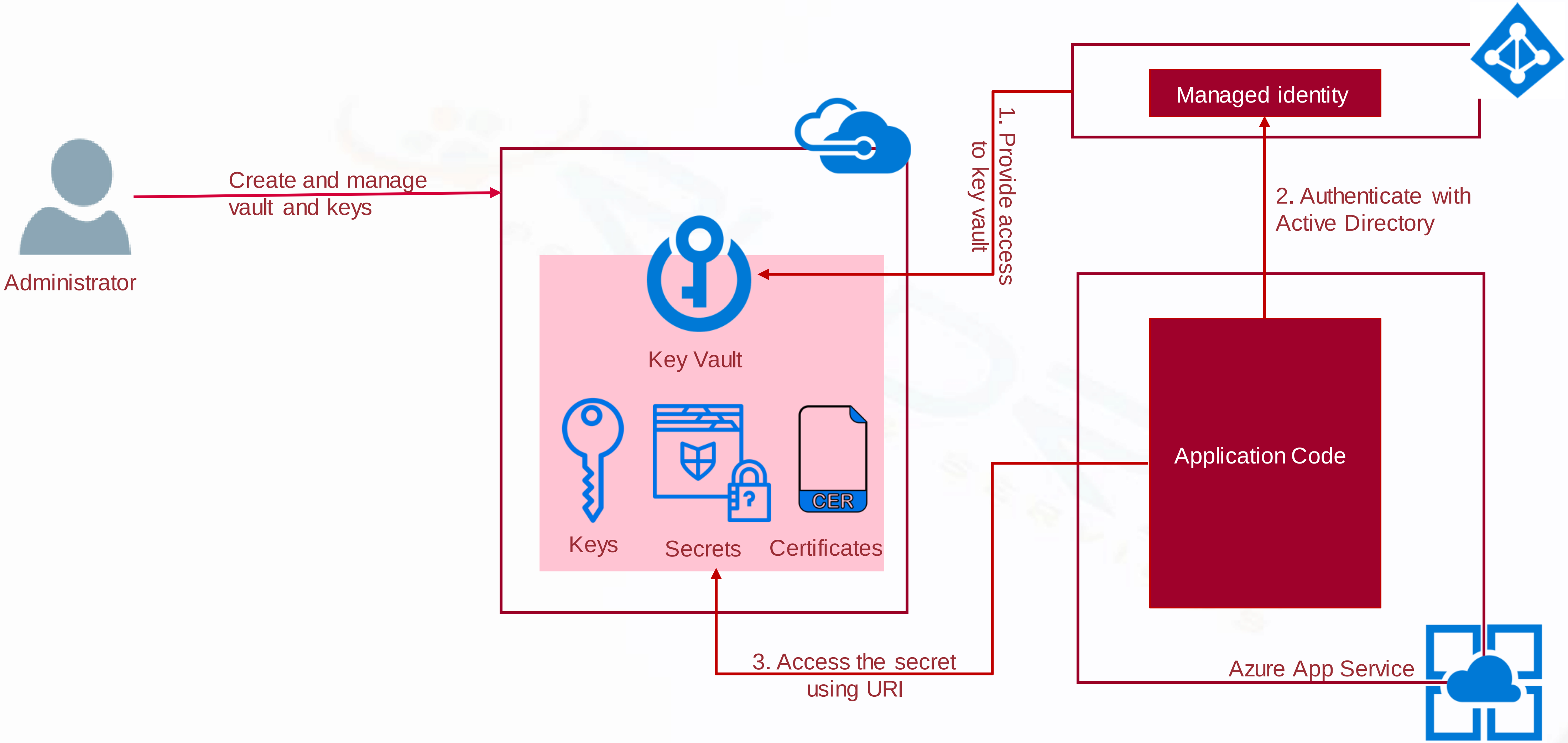
Step 32b – Securely deploying code using Azure Devops



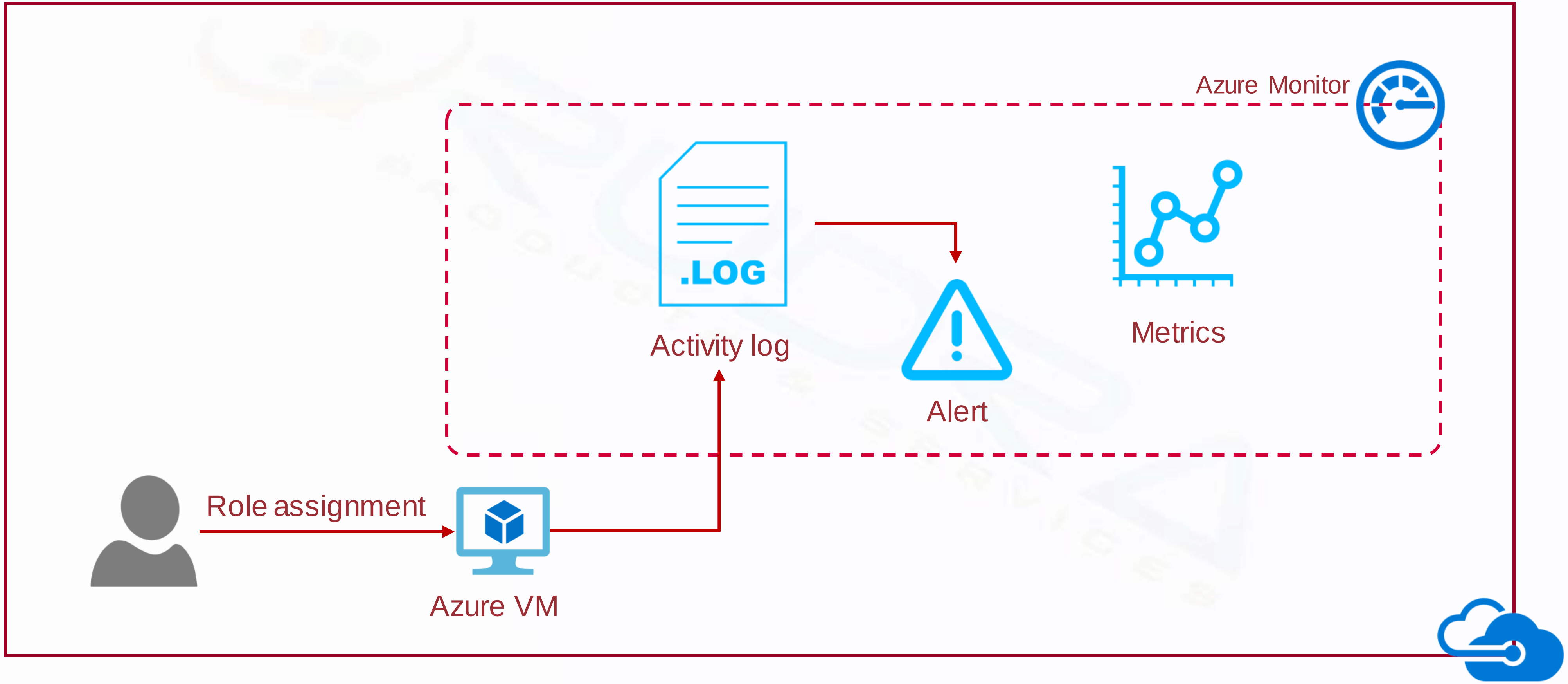
Step 33 – Create and manage Key Vault using Azure portal



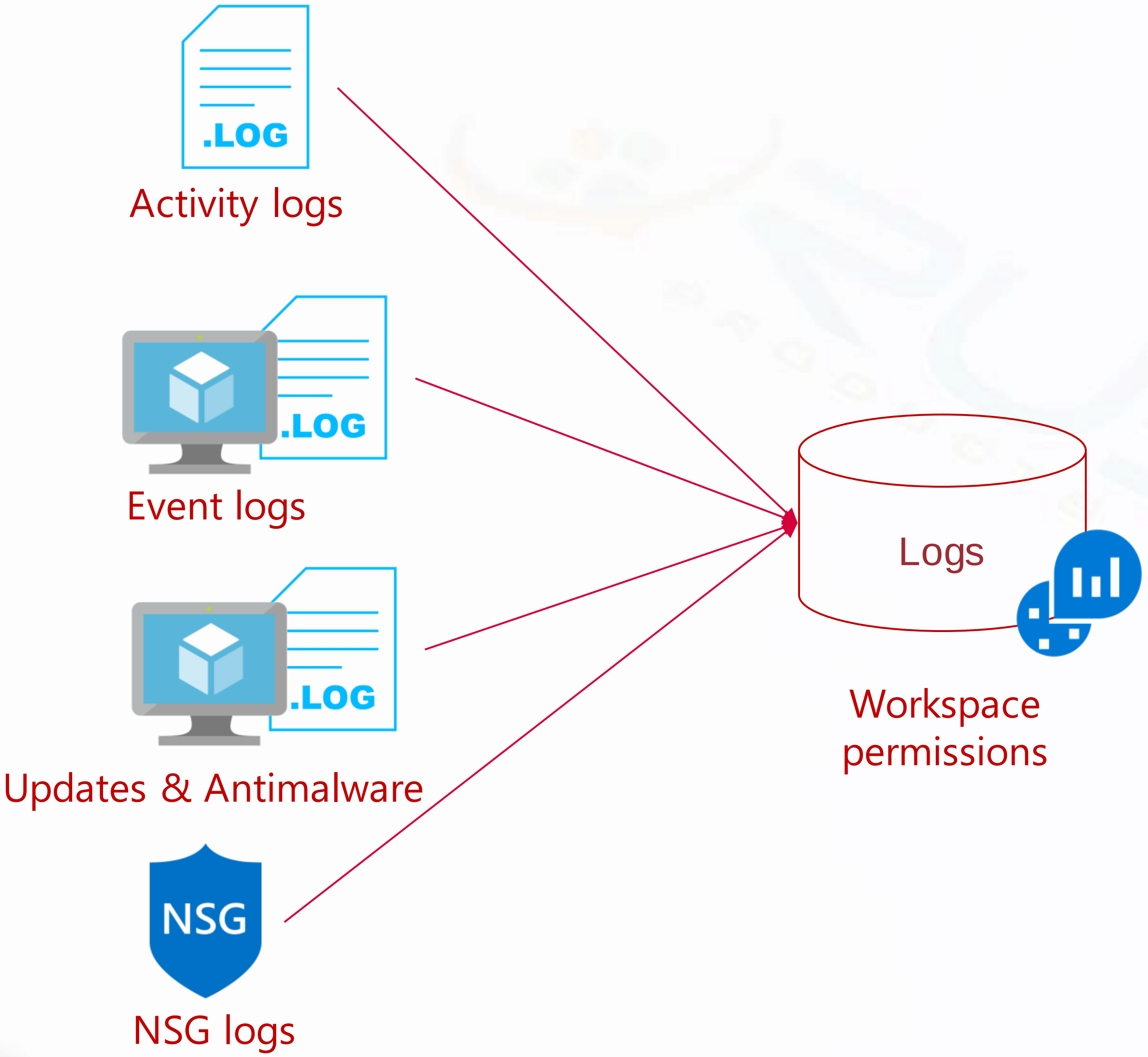
Step 34 – Access secret in Key Vault from Azure web app


Administrator
Create and manage vault and keys
Key Vault
Keys
Secrets
CER
Certificates
1. Provide access to key vault
Managed identity
2. Authenticate with Active Directory
Application Code
3. Access the secret using URI
Azure App Service

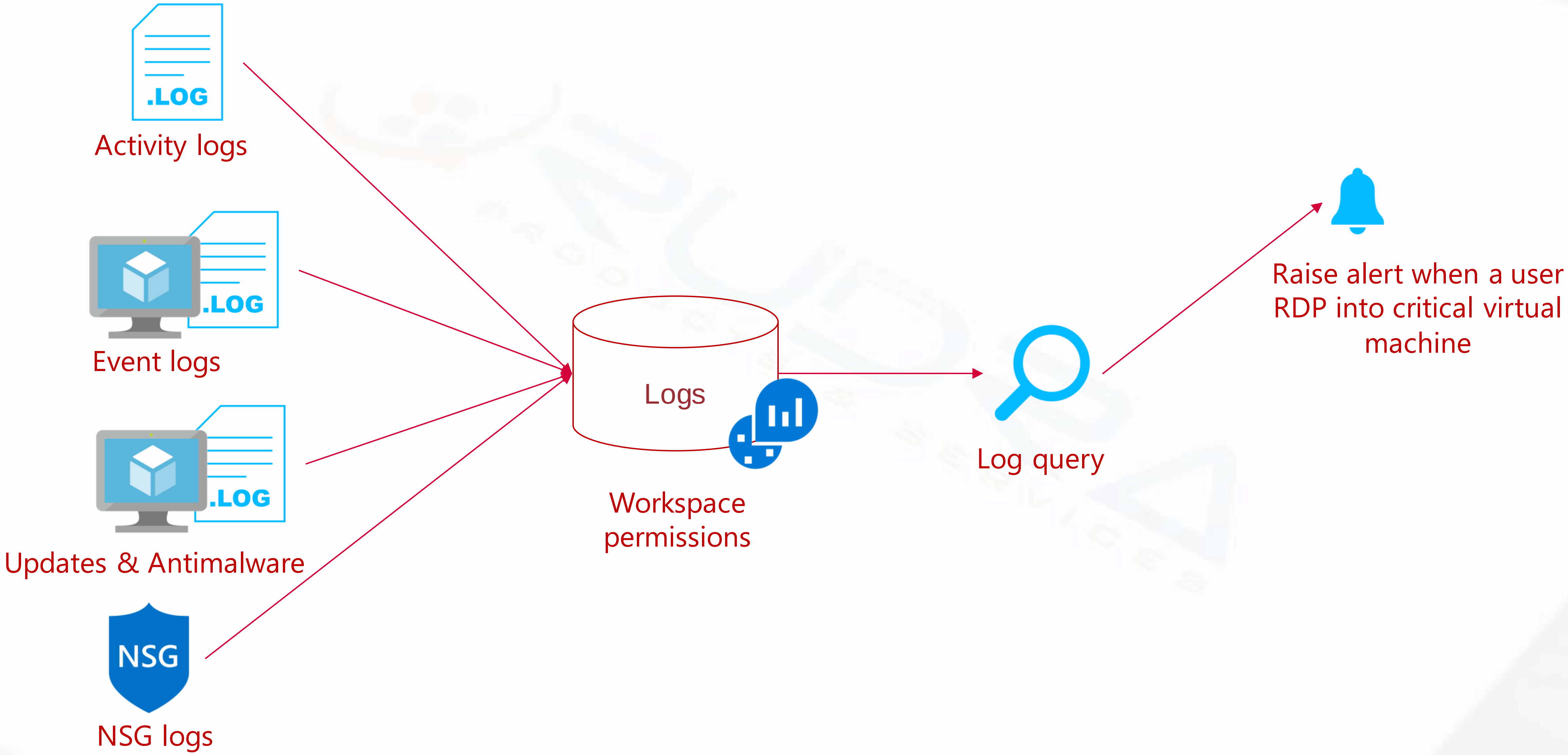
Step 35 – Monitoring – Metrics, Activity logs and Alerts



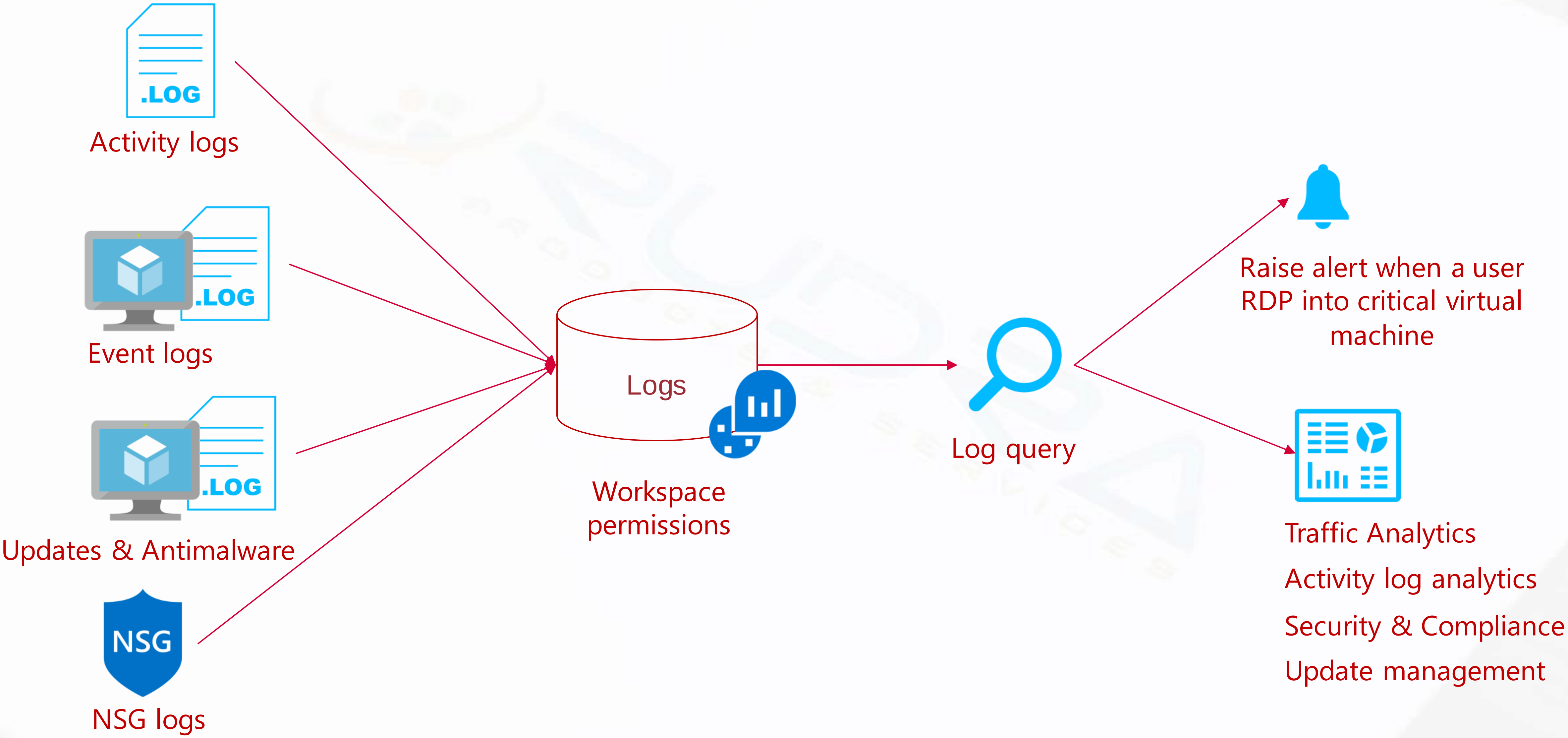
Step 36a – Monitoring – Azure monitor logs



Step 36b – Monitoring – Azure monitor logs



Step 36c – Monitoring – Azure monitor logs



Activity logs

Event logs

Updates & Antimalware

NSG logs

Logs

Workspace permissions

Log query

Raise alert when a user RDP into critical virtual machine

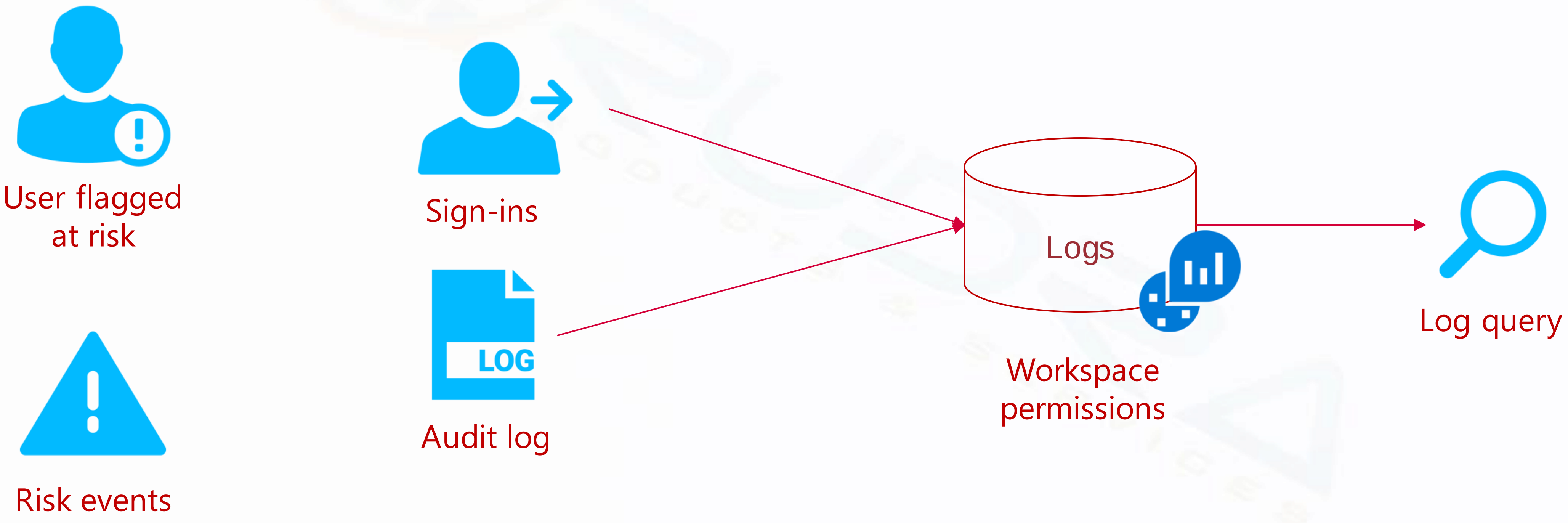
Traffic Analytics

Activity log analytics

Security & Compliance

Update management

Step 37 – Monitoring – Azure Active Directory monitoring


User flagged at risk

Risk events

Sign-ins

Audit log

Logs

Workspace permissions

Log query

Step 38 – Security center – Preventive monitoring and remediation

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

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.*

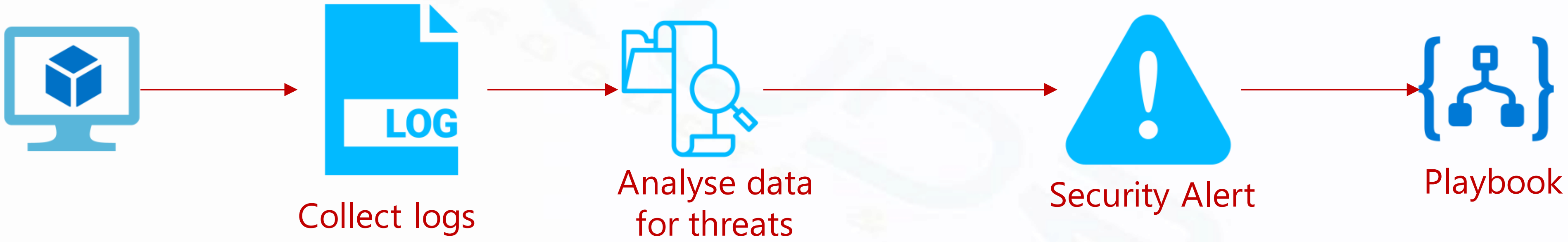
Implement the recommendations

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


LOG
Collect logs
Analyse data for threats
Security Alert
Playbook