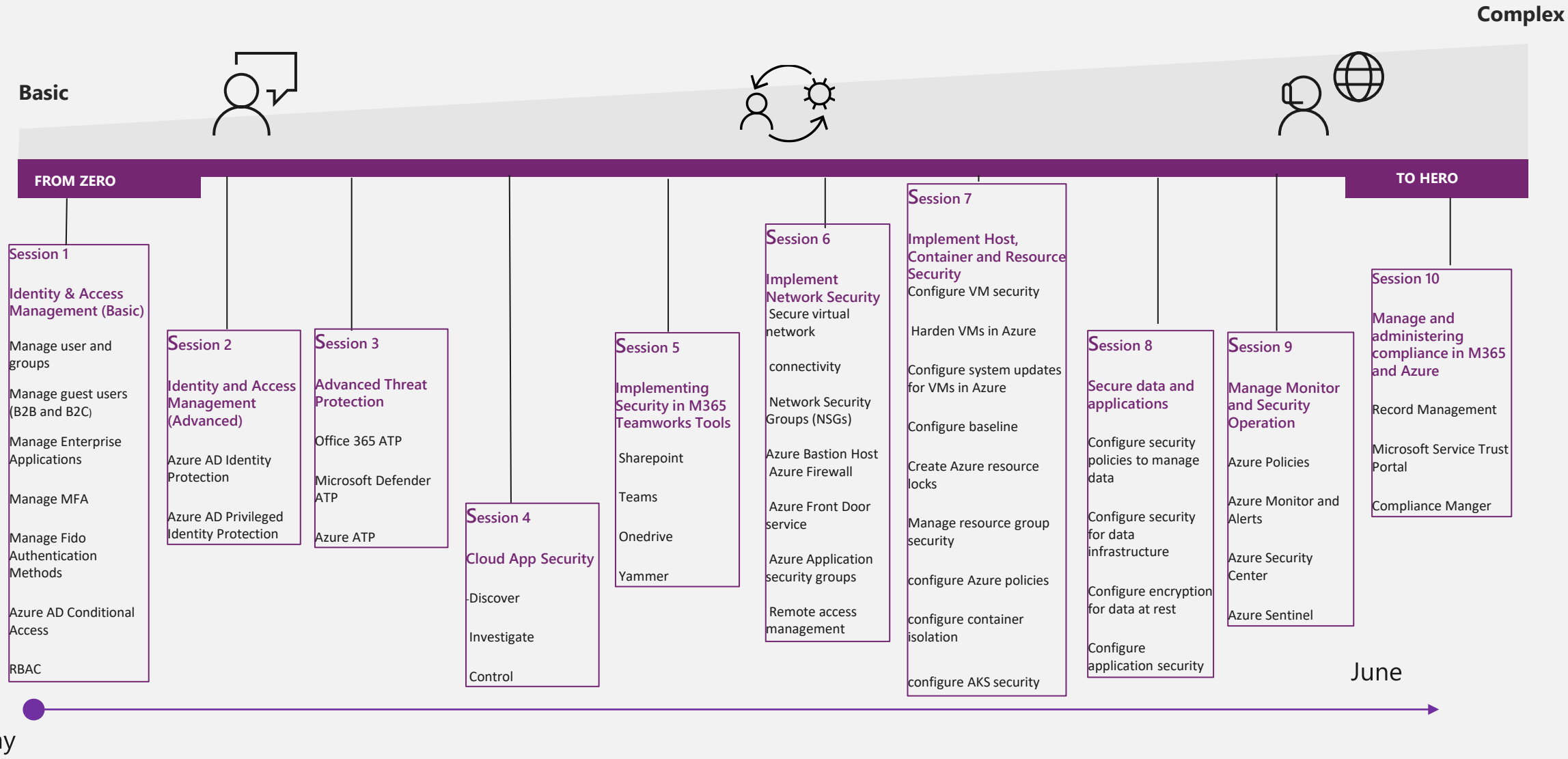
Security Sailing

Session 7 – Implement Host, Container and Resource Security

Michele

- Senior Consultant – Speaker – Trainer (22 anni)
- Dipendente 50% su tecnologie Microsoft Dipartimento di Informatica – Università degli Studi di Milano
- Freelance 50/70%
- Mi occupo di: AD, SCCM, W10, Win Server, AzureAD, O365, M365, Azure, Enterprise Mobility & Security
- Speaker da 12 anni di WPC e da 5 responsabile agenda ITPRO e Security
- Certificato MCT, MCSE, MCSA, MCITP
- Contatti:
  - michele@sensalari.com
  - michele.sensalari@overneteducation.it
  - Twitter: @ilsensa7
  - Linkedin: https://www.linkedin.com/in/michele-sensalari-4988b7/

Content and Timeline Details



Microsoft Security

Agenda

Virtual Machine Security

Subscription and Resource Security

Container Security

Virtual Machine Security

So you have migrated your VMs to azure,
but you are asking …

“How do we make sure they are secure?”

Key pillars to secure!

Secure identity authentication & authorization

Protect against malware & attacks

Update management

Virtual machine security posture

Control Networking

Secure identity authentication & authorization

Use Multi-factor authentication (MFA) on accounts

All accounts should have MFA

Why? Prevents attackers from taking over an account.

Ensure least privilege access using role-based access control (RBAC)

Resource, Resource Group, Subscription, Management Groups

Why? If by some chance, attacker gets an account they are limited to which resources that user can access

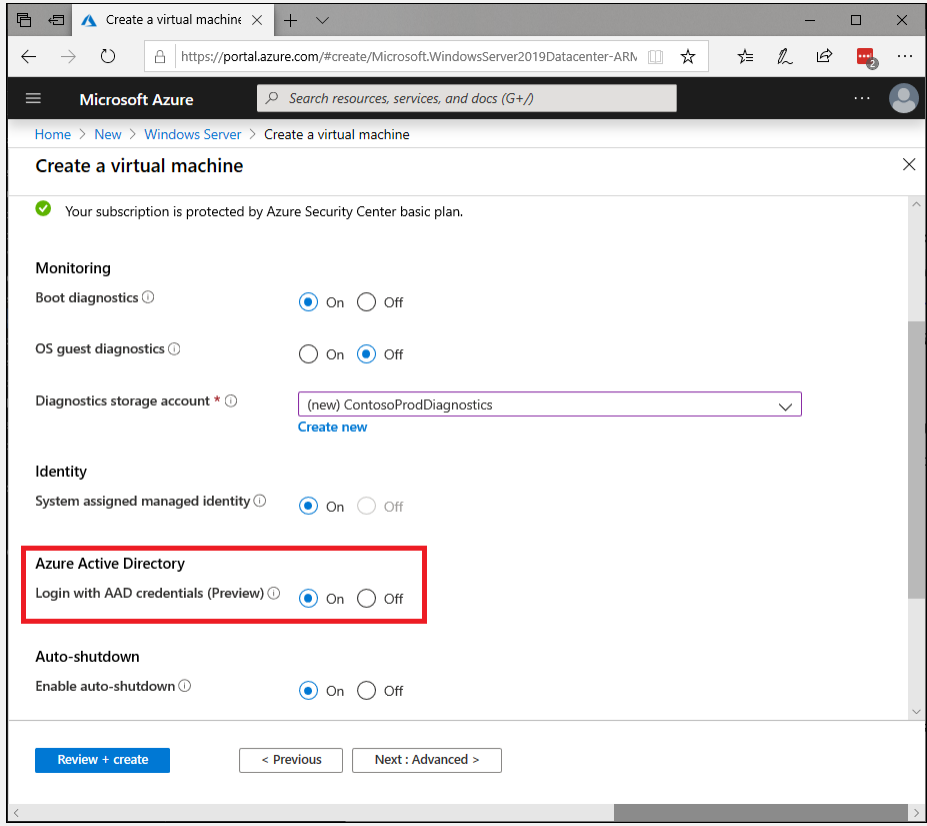
Use Privileged Identity Management (PIM)

Limit standing administrator access to privileged roles

Why? For admin accounts, ensures they don’t have permanent access and can enforce approval process.

Sign in to Windows virtual machine in Azure using Azure Active Directory authentication (Preview)

- You need to configure Azure RBAC policy to determine who can log in to the VM. Two RBAC roles are used to authorize VM login:
  - **Virtual Machine Administrator Login**: Users with this role assigned can log in to an Azure virtual machine with administrator privileges.
  - **Virtual Machine User Login**: Users with this role assigned can log in to an Azure virtual machine with regular user privileges
- You can enforce **Conditional Access policies** such as **multi-factor authentication** or user sign-in risk check before authorizing access to Windows VMs in Azure that are enabled with Azure AD sign in. To apply Conditional Access policy, you must select "Azure Windows VM Sign-In" app from the cloud apps or actions assignment option and then use Sign-in risk as a condition and/or require multi-factor authentication as a grant access control.



Protect against malware & attacks

Use Antimalware and monitor with Azure Security Center (ASC)

AV/AM to cover all the basic attacks (viruses, spyware)

Why? The basics still exist out there

Use ASC Standard for Adaptive Application Control

Next level to prevent malware.

Why? It will (if you let it) block the malicious applications

Configure endpoint security

- Computer systems that interact directly with users are considered endpoint systems
- Endpoint systems are typically vulnerable to security attacks
- Azure Security Center provides the tools you need to harden your network, secure your services, and solidify your security posture
- **First step**: Protect against malware
  - Install and integrate your antimalware solution with Security Center
- **Second step**: Monitor the status of antimalware
  - Security Center monitors the status of antimalware protection and reports this under the **Endpoint protection issues** blade

Update Management

Apply System Updates

Use Update Management to automate deployment

Why? Patch security vulnerabilities and reduces your risk

Use the latest Operating System images when deploying new machines

Why? Latest OS includes new security features

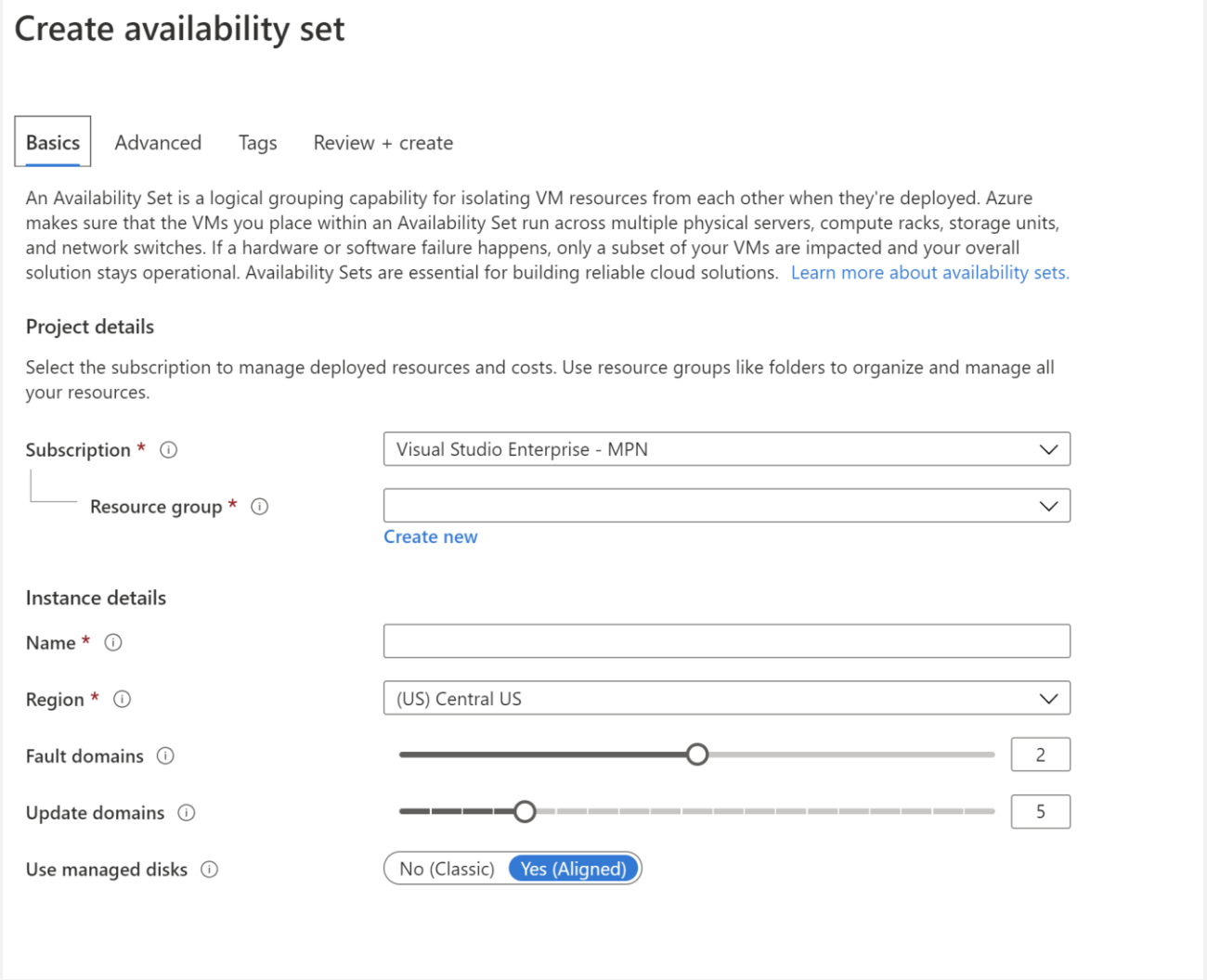
Plan for Business Continuity and Disaster Recovery (BCDR)

Backup your VMs using Azure Backup OR Have a plan to rapidly redeploy (ARM / DevOps)

Why? Recovery may be required dependent on the attack

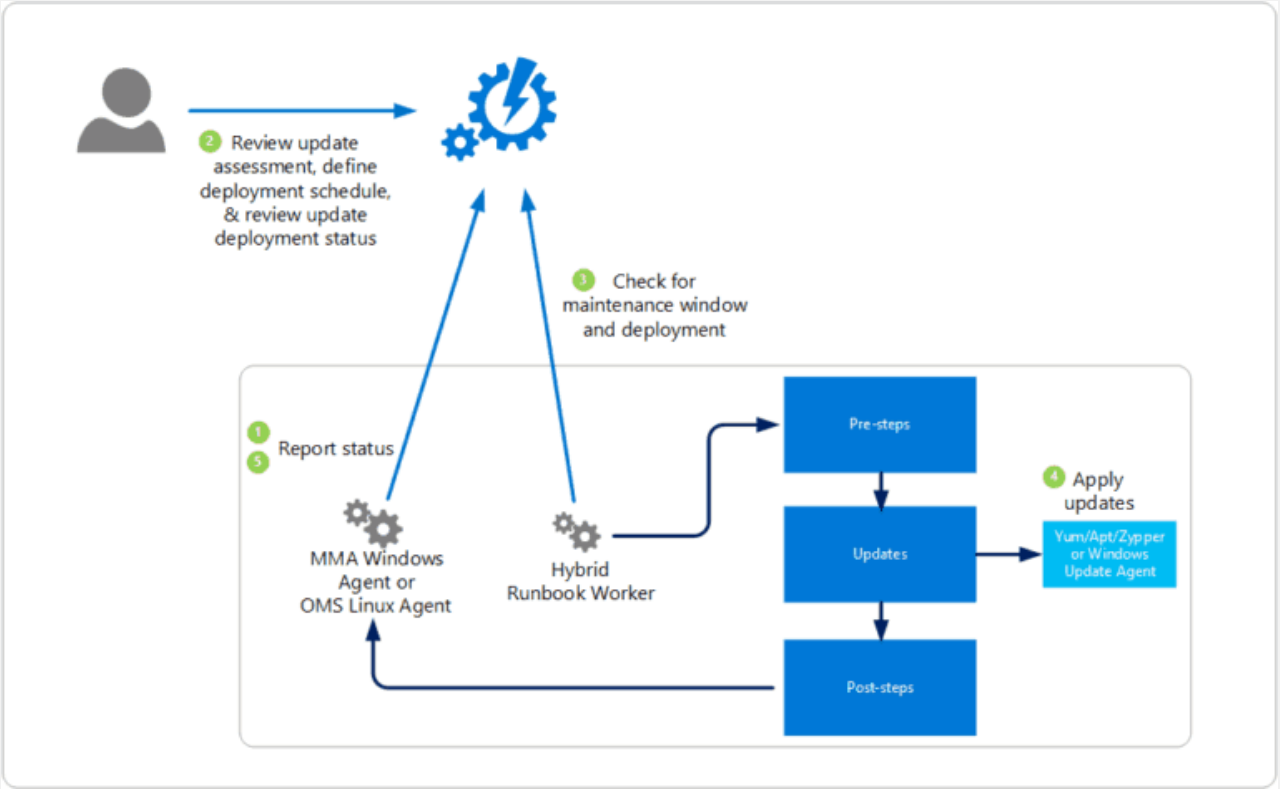
Configure update domains

- Microsoft does not automatically update your IaaS VMs
- Update domains manage intentional moves to take down one (or more) of your servers to provide critical updates
- To provide redundancy to your application, we recommend that you group two or more virtual machines in an availability set
- The underlying Azure platform assigns an update domain and a fault domain to each virtual machine in your availability set



Azure Update Management

The Azure Update Management solution is part of Azure Automation. And with Azure Update Management you can manage operating system updates for your Windows and Linux computers in Azure, in on-premises environments, or in other cloud providers. That is right, it is not only for your Azure VMs, it also works with all your environment and provides you with a single pane of glass for your Update Management. It allows you to quickly assess the status of available updates on all virtual machines and servers, and manage the process of installing required updates for servers.



Automation Account

Home > Automation Accounts >

Add Automation Account

Name * ⓘ

LabAutomation ✓

Subscription *

Visual Studio Enterprise - MPN

Resource group *

SensaLab

Create new

Location *

West Europe

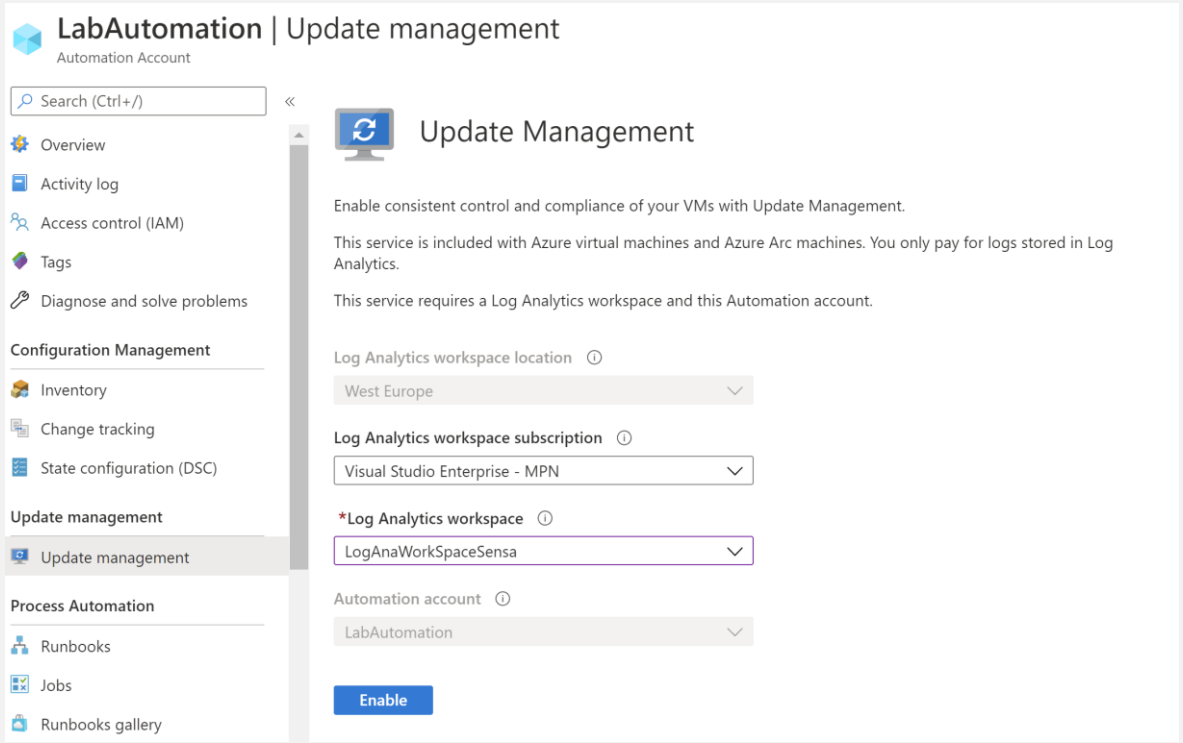
Create Azure Run As account * ⓘ

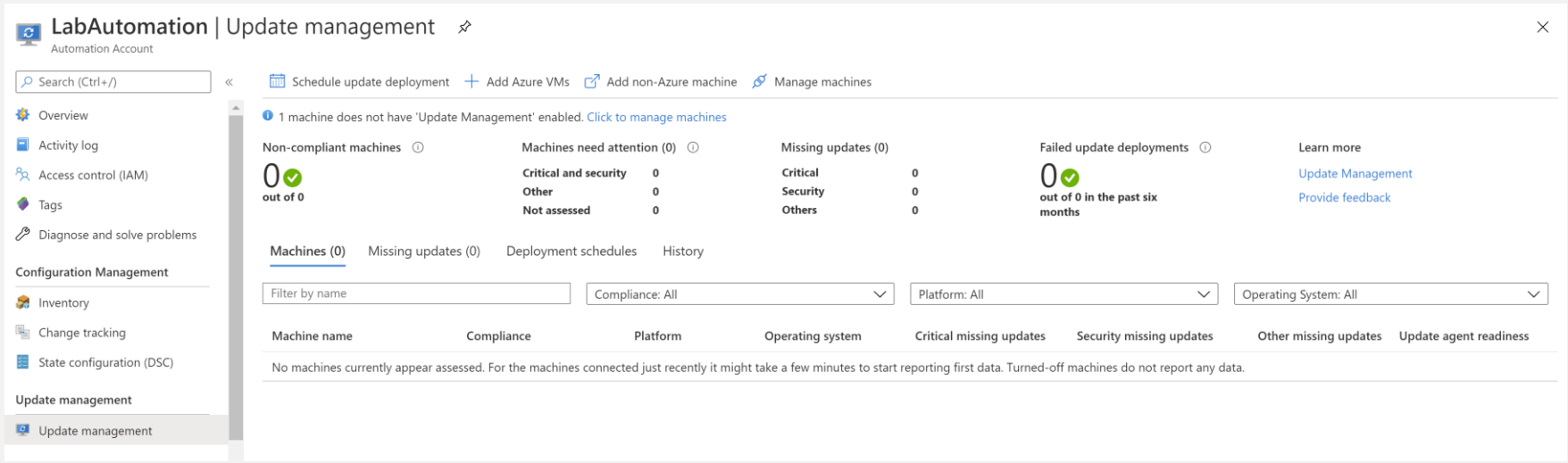
Yes | No

This will create Azure Run As account in the Automation account which are useful for authenticating with Azure to manage Azure resources from Automation runbooks. Note that the creation of Azure Run As account may affect the security of the subscription.Learn more

Learn more about Automation pricing.

Create



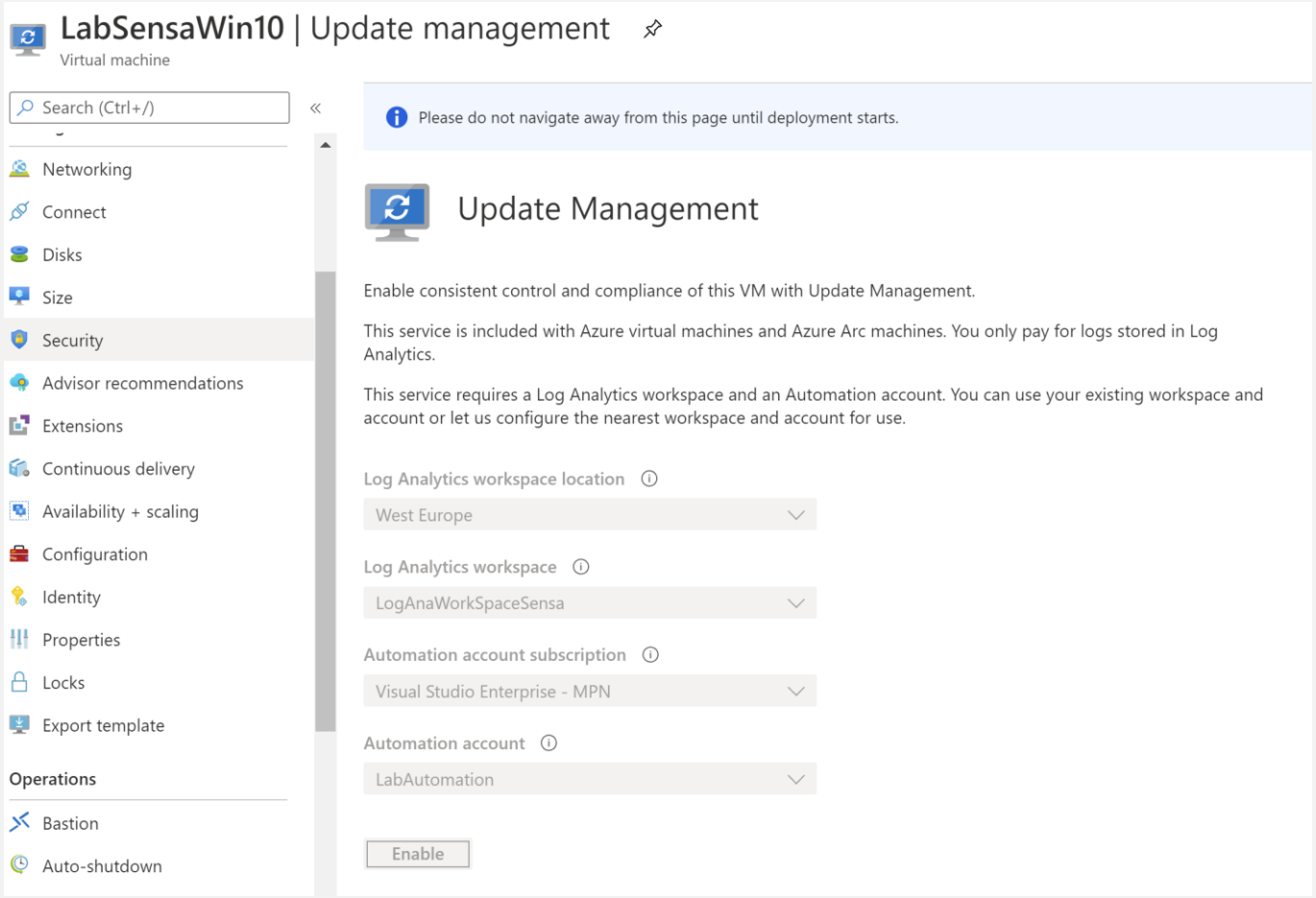


With an Automation account, you can authenticate runbooks by managing resources in either Azure Resource Manager or the classic deployment model. One Automation Account can manage resources across all regions and subscriptions for a given tenant.

How to onboard Azure IaaS VMs

Onboarding Azure VMs to Azure Update Management is fairly simple and there are many different ways you can enable Update Management for an Azure VM:

- From a virtual machine
- From browsing multiple machines
- From your Automation account
- With an Azure Automation runbook



VM Security Posture

Review missing OS security settings

Remediate using Group Policy, DSC, Deploy VM custom image with policy built in

Use disk encryption

Protect data at rest

Assess and remediate vulnerabilities

Why? Vulnerable applications provide a target for attackers

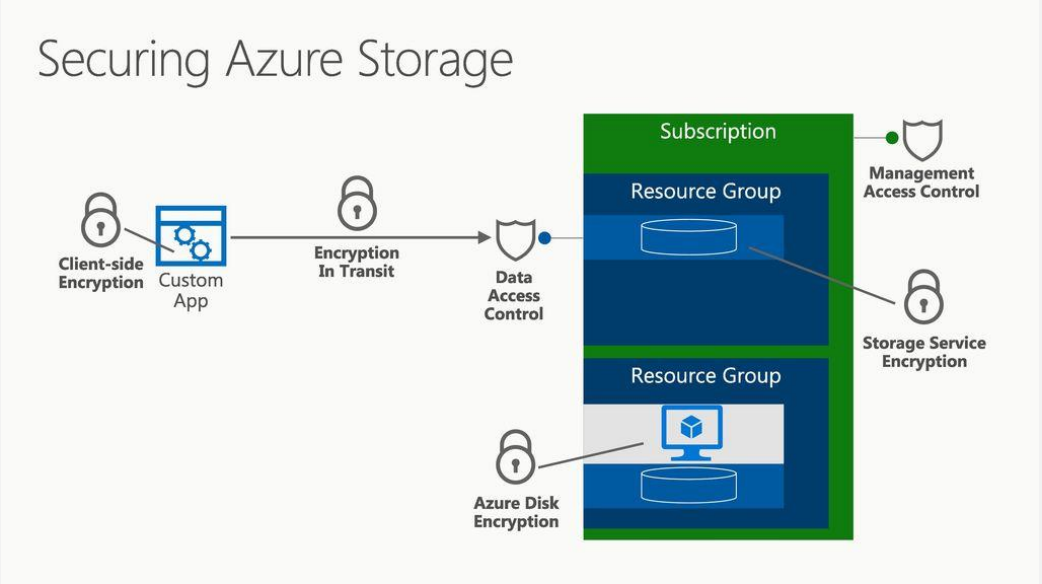
Detect threats with ASC Standard which includes MDATP for servers

Provides advanced detections and endpoint detection and response

Why? Endpoints are still where most attacks occur

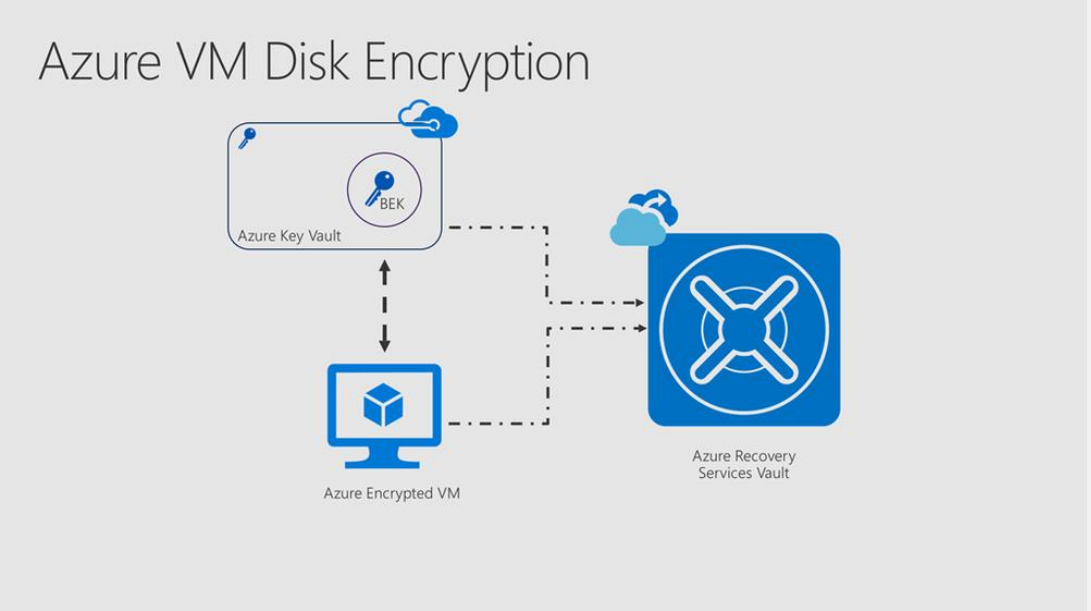
Azure Storage encryption for data at rest

- Azure Storage automatically encrypts your data when it is persisted it to the cloud. Azure Storage 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. Azure Storage encryption is similar to BitLocker encryption on Windows.
- Azure Storage encryption is enabled for all new storage accounts, including both Resource Manager and classic storage accounts. Azure Storage encryption cannot be disabled
- Encryption does not affect Azure Storage performance. There is no additional cost for Azure Storage encryption
- You can rely on Microsoft-managed keys for the encryption of your storage account, or you can manage encryption with your own keys.



Azure Disk Encryption for VMs

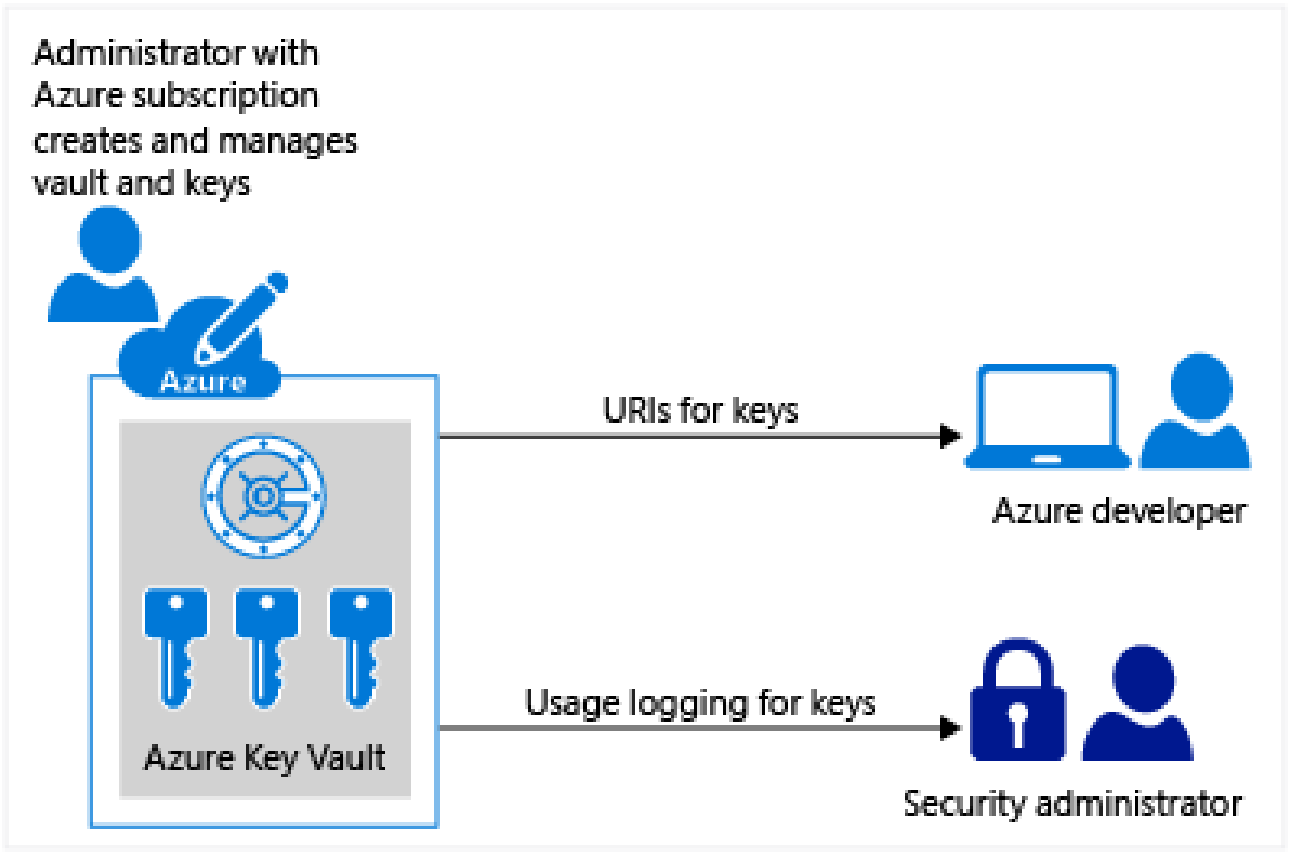
- Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the Bitlocker feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.
- We can use BitLocker to encrypt Windows VM running on Azure, for Linux VMs, we can use DM-Crypt to encrypt virtual disks
- Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines with a less than 2 GB of memory.
- Azure Disk Encryption is also available for VMs with premium storage



Azure Key Vault

Azure Key Vault enables Microsoft Azure applications and users to store and use several types of secret/key data:

- ✓ Cryptographic keys: Supports multiple key types and algorithms, and enables the use of Hardware Security Modules (HSM) for high value keys.
- ✓ Secrets: Provides secure storage of secrets, such as passwords and database connection strings.
- ✓ Certificates: Supports certificates, which are built on top of keys and secrets and add an automated renewal feature.
- ✓ Azure Storage: Can manage keys of an Azure Storage account for you. Internally, Key Vault can list (sync) keys with an Azure Storage Account, and regenerate (rotate) the keys periodically.



Bitlocker

- Connect-AzAccount
- Register-AzResourceProvider -ProviderNamespace "Microsoft.KeyVault«
- New-AzKeyVault -Location " West Europe" -ResourceGroupName MyRG -VaultName SensaVMKV1 –EnabledForDiskEncryption
- Set-AzKeyVaultAccessPolicy -VaultName SensaVMKV1 -ObjectId xxxxxxxxxxxxxxx -PermissionsToKeys create,import,delete,list -PermissionsToSecrets set,delete –PassThru

objectid should replace with the actual **objectid** value of the currently logged in global admin account

Add-AzKeyVaultKey -VaultName SensaVMKV1 -Name "SensaVMKey" -Destination "Software«

The next step of the configuration is to encrypt the VM.

1. Azure Key Vault Resource ID
2. Azure Key Vault URI

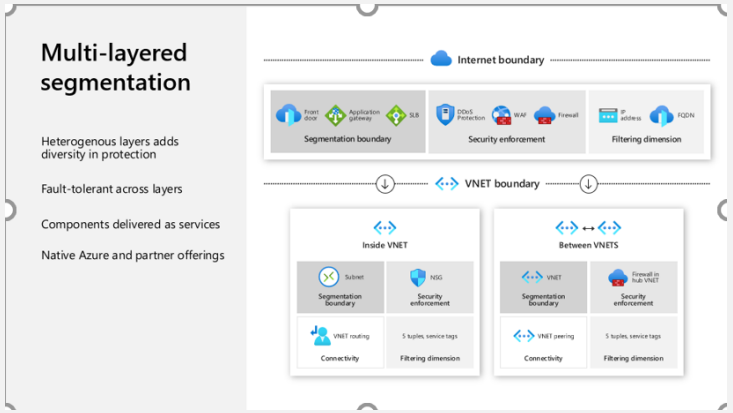
   Get-AzKeyVaultKey -VaultName SensaVMKV1 -Name SensaVMKey
3. Azure Key vault key ID

   Get-AzKeyVaultKey -VaultName SensaVMKV1 -Name SensaVMKey

Set-AzVMDiskEncryptionExtension -ResourceGroupName MyRG -VMName "SensaVM01" -DiskEncryptionKeyVaultUrl (value of Azure Key Vault URI) -DiskEncryptionKeyVaultId (value of Azure Key Vault Resource ID) -KeyEncryptionKeyUrl (value of Azure Key vault key ID) -KeyEncryptionKeyVaultId (value of Azure Key Vault Resource ID)

Control Networking

Govern your VM's traffic patterns with multi-dimensional segmentation



Limit Access to Management Ports

Use Just in time VM Access (Integrated with Azure Firewall and NSG) or use Azure Bastion

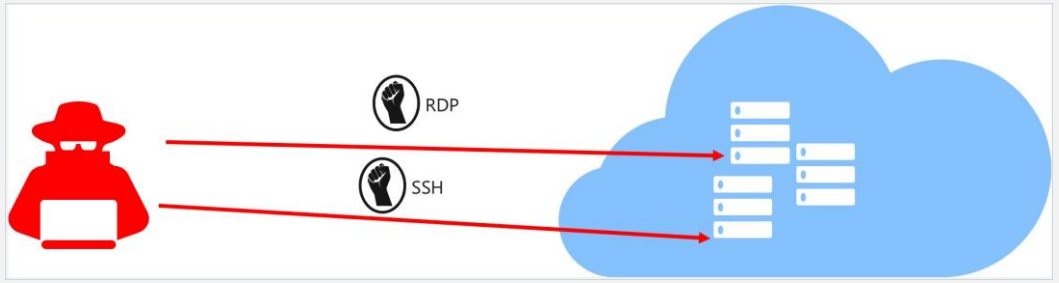
Why? Reduce the risk of exposed management access

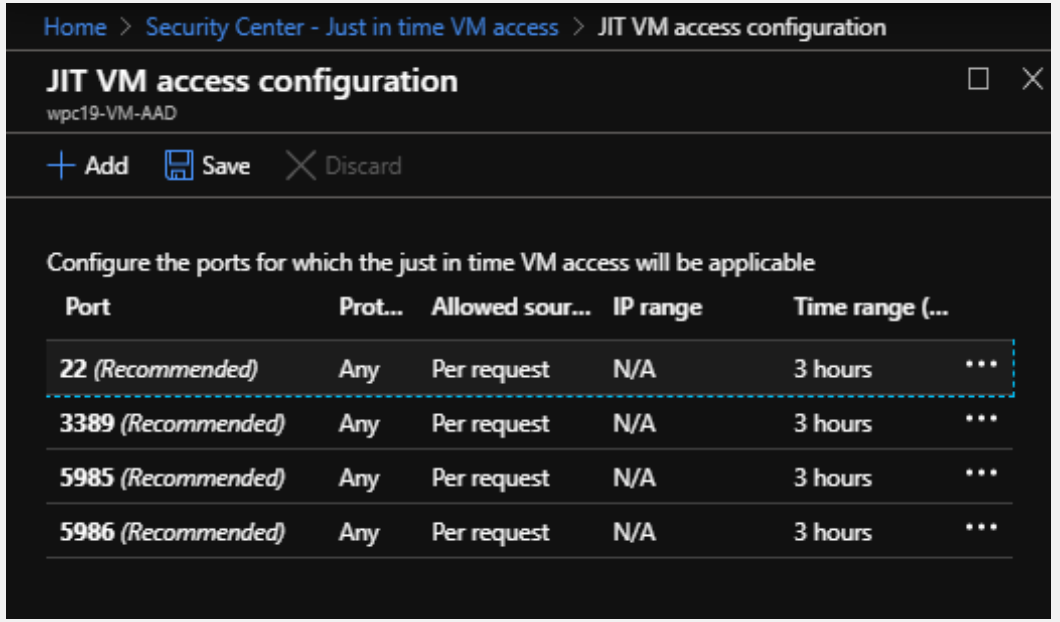
Use Adaptive Network Hardening

ML makes your job easier

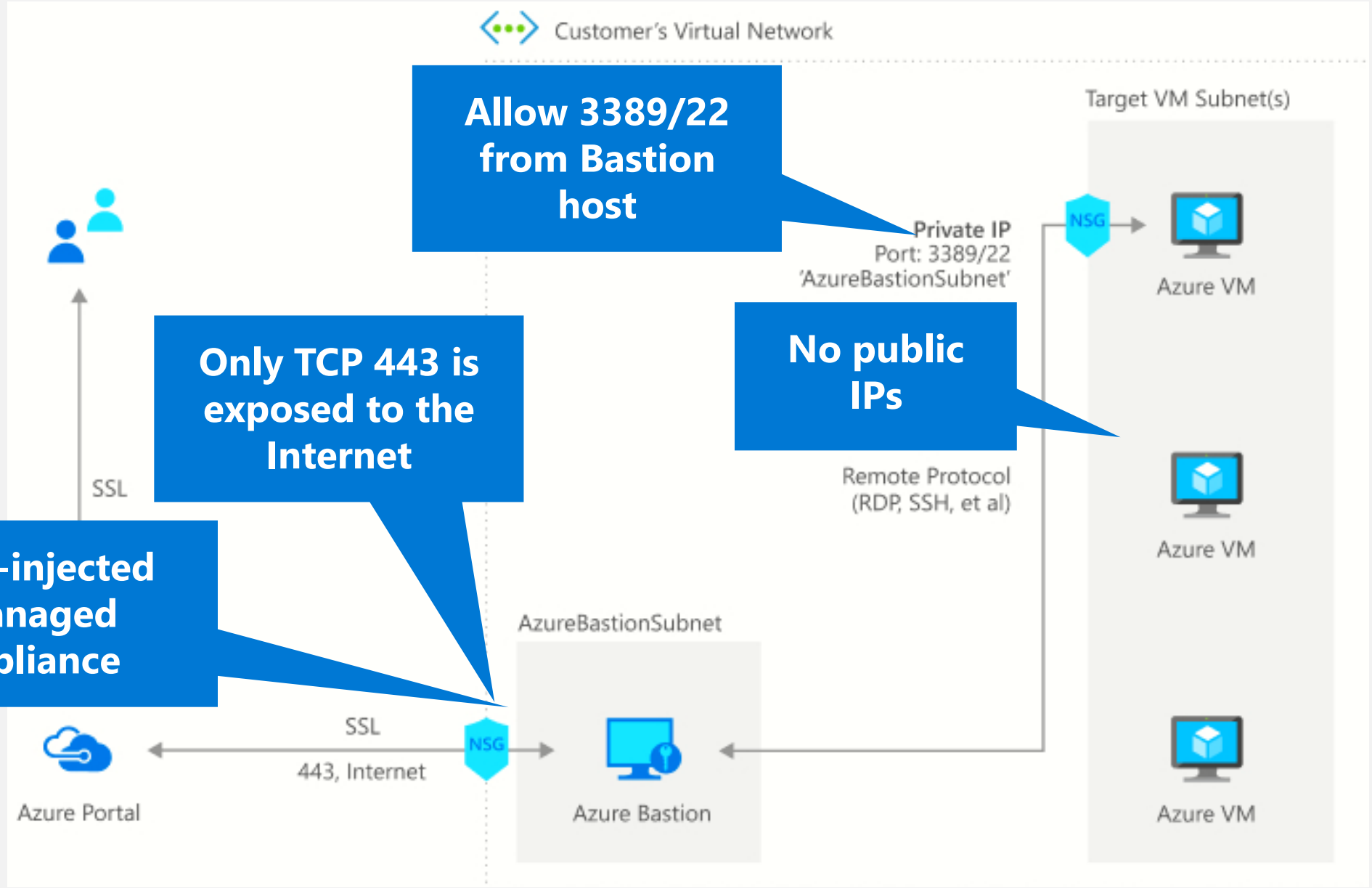
Manage virtual machine access using just-in-time

- Brute force attacks commonly target management ports as a means to gain access to a VM. If successful, an attacker can take control over the VM and establish a foothold into your environment.
- One way to reduce exposure to a brute force attack is to limit the amount of time that a port is open. Management ports don't need to be open at all times. They only need to be open while you're connected to the VM, for example to perform management or maintenance tasks. When just-in-time is enabled, Security Center uses network security group (NSG) and Azure Firewall rules, which restrict access to management ports so they cannot be targeted by attackers.



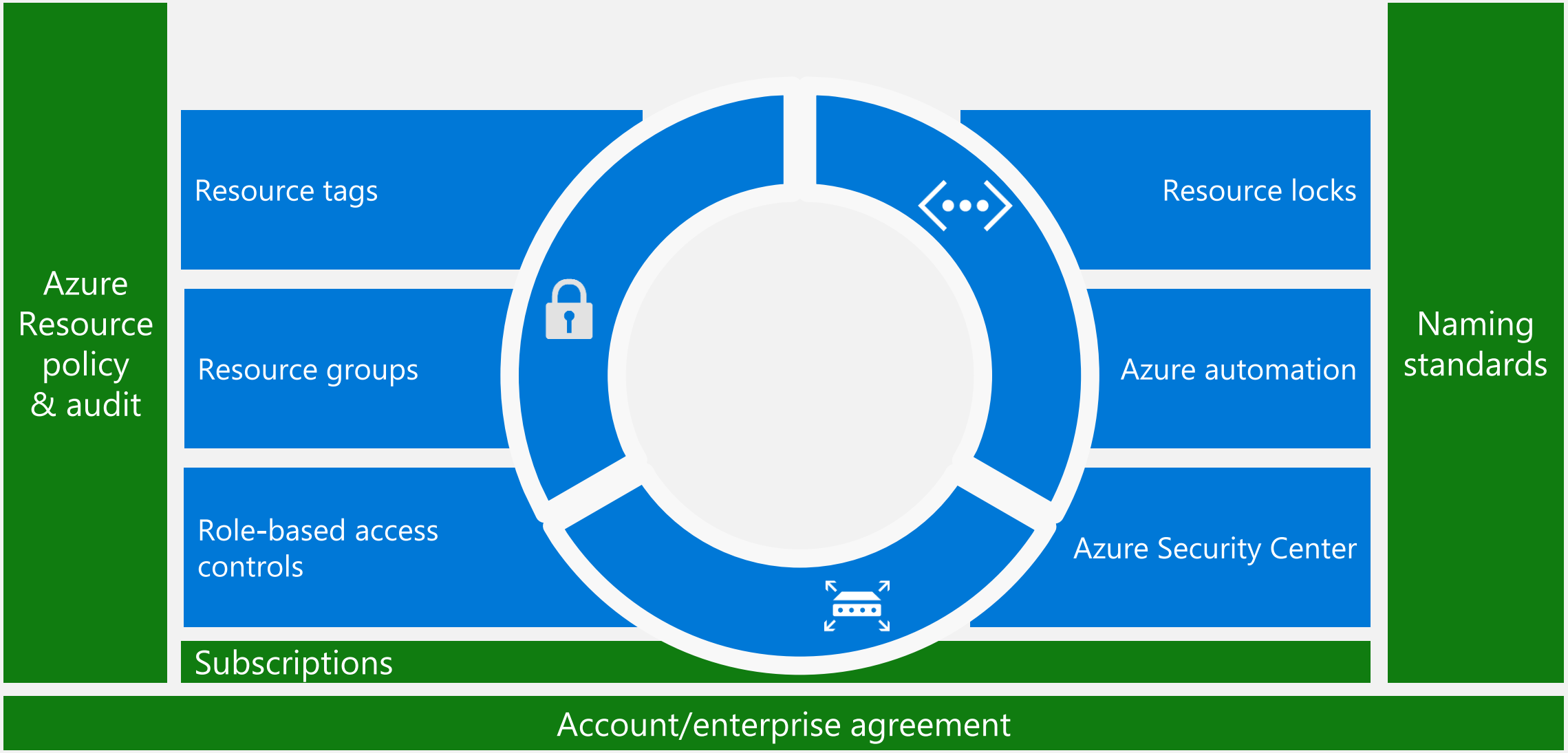


Azure Bastion – Managed jump box

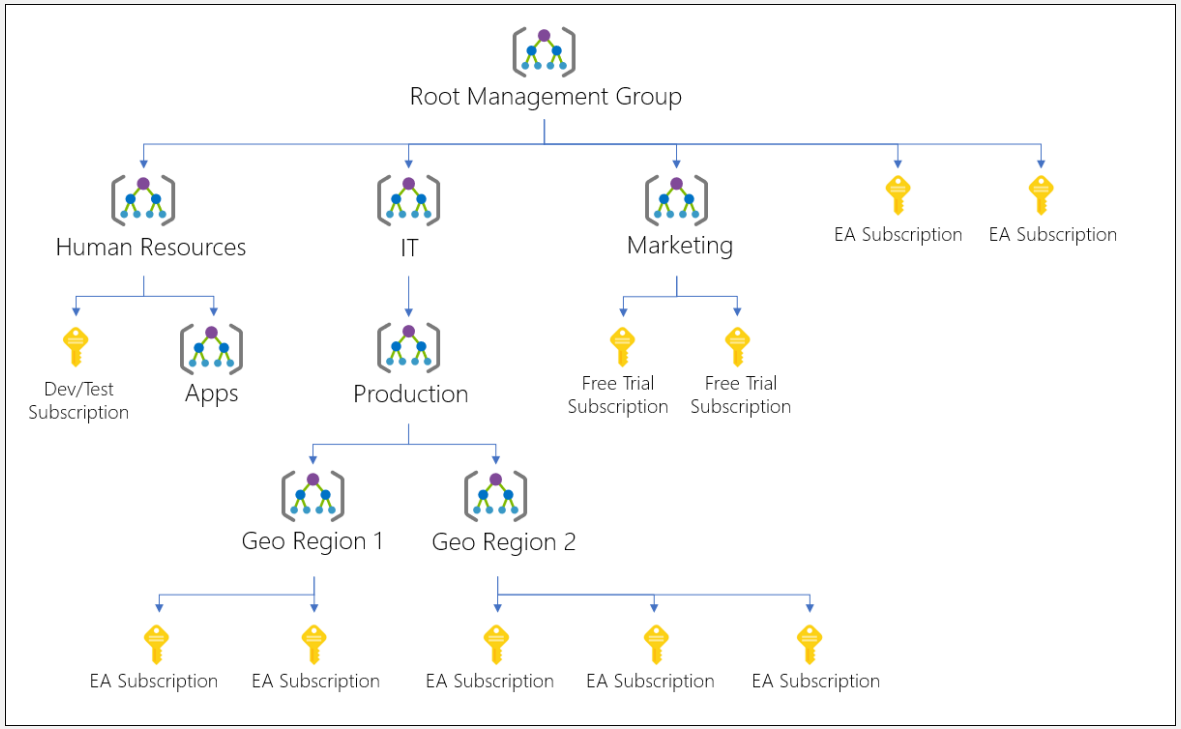


Subscription Security

Manage Azure Subscriptions

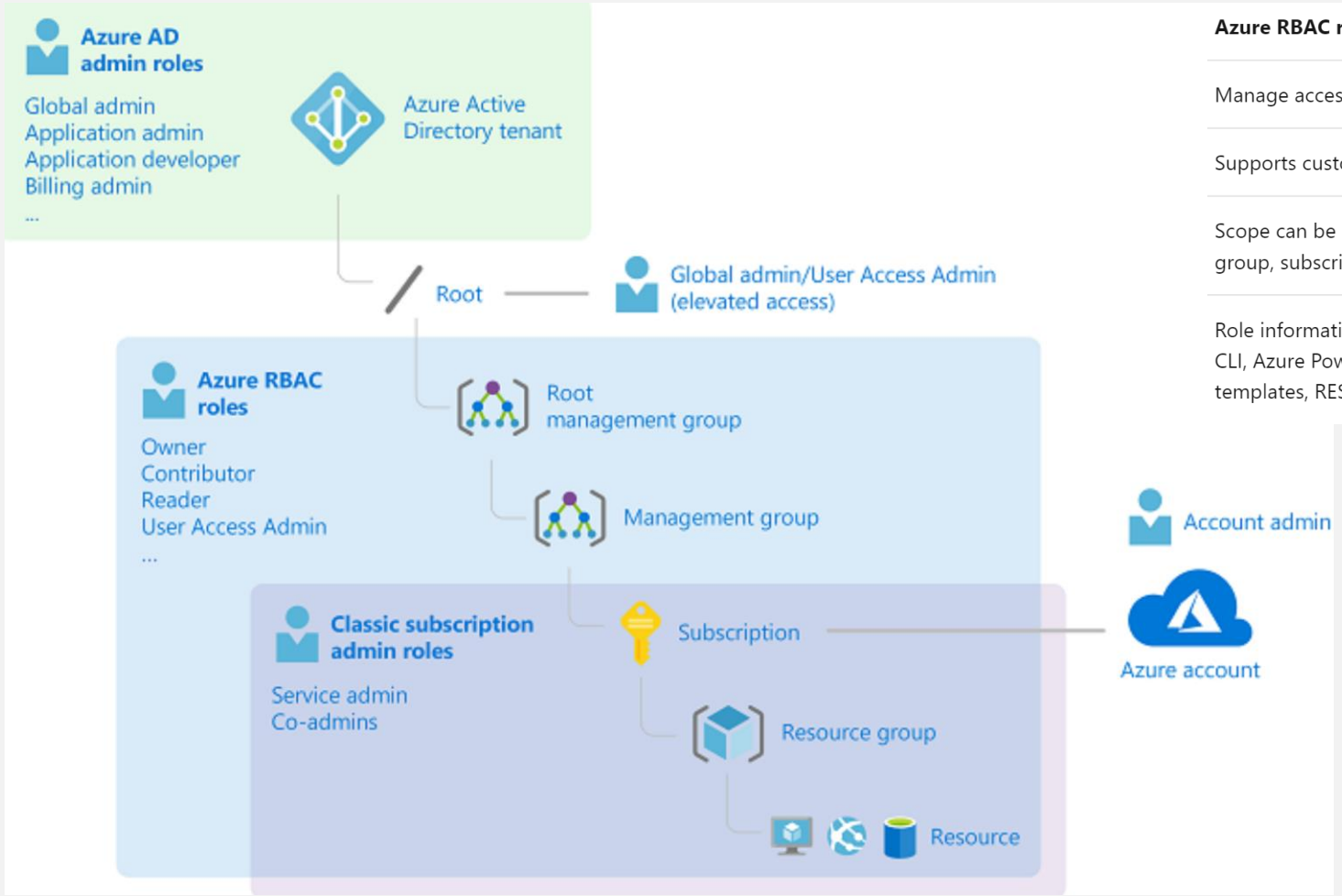


Azure management groups

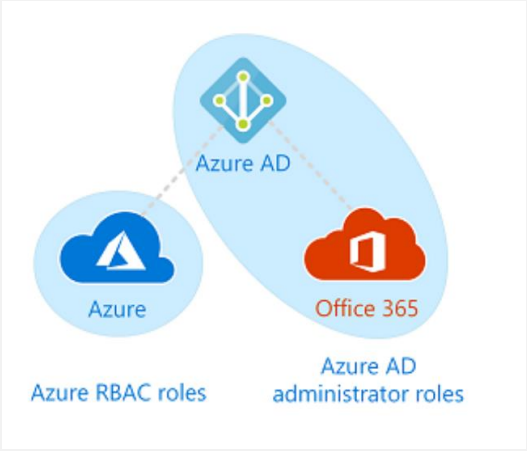


- Organizations with many subscriptions may need a way to efficiently manage access, policies, and compliance for those subscriptions.
- **Azure management groups** provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups.
- All subscriptions within a management group automatically inherit the conditions applied to the management group.
- Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. All subscriptions within a single management group must trust the **same Azure Active Directory tenant**.

RBAC Roles



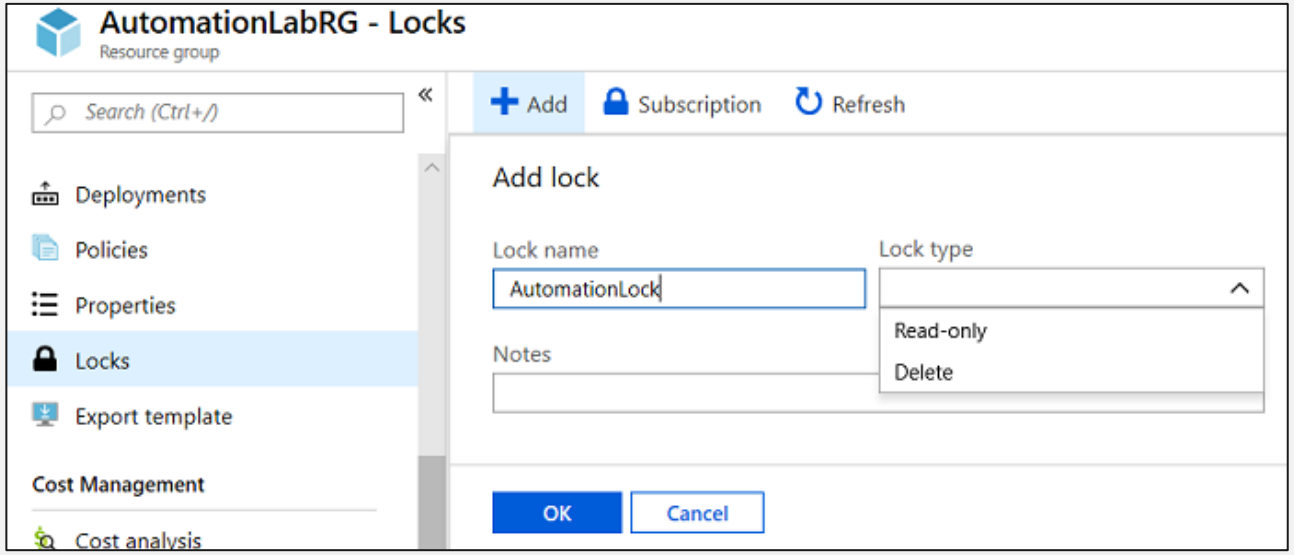
Azure RBAC roles	Azure AD administrator roles
Manage access to Azure resources	Manage access to Azure Active Directory resources
Supports custom roles	Supports custom roles
Scope can be specified at multiple levels (management group, subscription, resource group, resource)	Scope is at the tenant level
Role information can be accessed in Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure admin portal, Microsoft 365 admin center, Microsoft Graph, AzureAD PowerShell



Resource Manager Locks

You may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

- Associate the lock with a subscription, resource group, or resource
- Locks are inherited by child resources
- Read-Only locks prevent any changes to the resource
- Delete locks prevent deletion



Container and Serverless Security

Understand virtualization, containers, and serverless computing

- **Virtualization** creates a simulated, or virtual, computing environment, as opposed to a physical environment
- Each virtual machine can then interact independently and run different operating systems or applications

- A **container** is a modified runtime environment that prevents a program from accessing protected resources
- A container interacts directly with the host operating system (OS) and augments the containment functions

- **Serverless** computing is the abstraction of servers, infrastructure, and operating systems
- When you build serverless apps, you don’t need to provision and manage any servers
- Azure Functions is a serverless application platform
- Azure Logic Apps allows developers to add workflows to support their Azure functions

Azure compute services – container services

Containers are a virtualization environment. However, unlike virtual machines, they do not include an operating system. Containers are meant to be lightweight, and are designed to be created, scaled out, and stopped dynamically. Examples of Azure services for containers include:

- **Azure Container Instances**: A PaaS offering that allows you to upload your containers, which it then will run for you

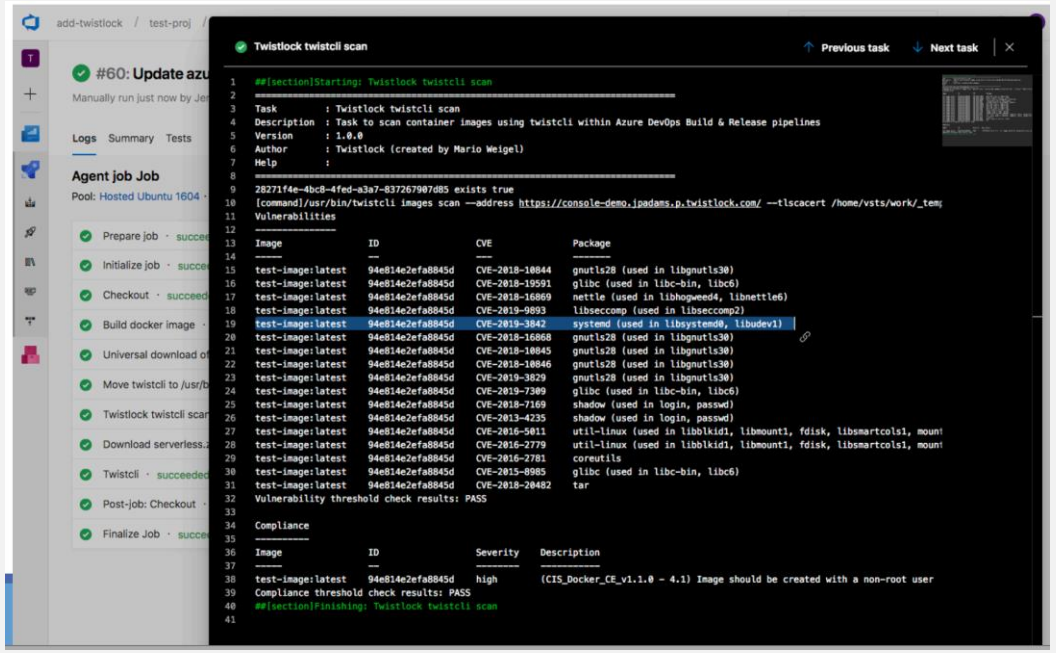
- **Azure Kubernetes Service**: A container orchestrator service for managing large numbers of containers

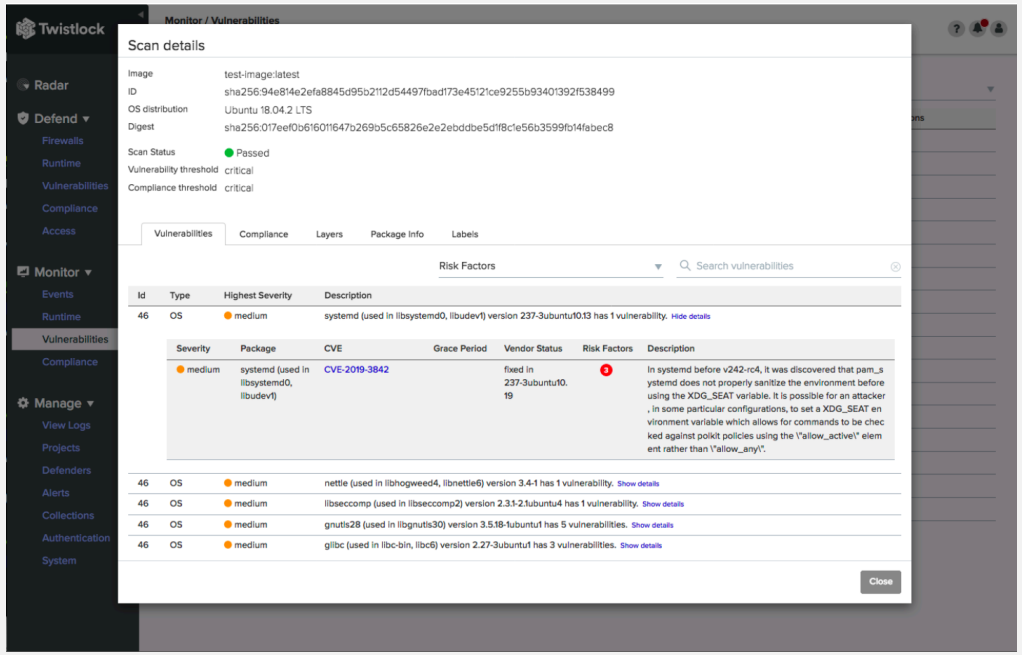
Configure container security

- Networking in a container deployment is a special area that you must address in security scenarios
- A container image is a lightweight, standalone, executable package that includes everything needed to run an application
- When an app is containerized, the app and the components needed to run the app are combined in a single image
- Containers are not inherently vulnerable
- The kernel is shared among all containers and the host
- An attacker who gains access to a container should not be able to gain access to other containers or the host

Scanning Containers

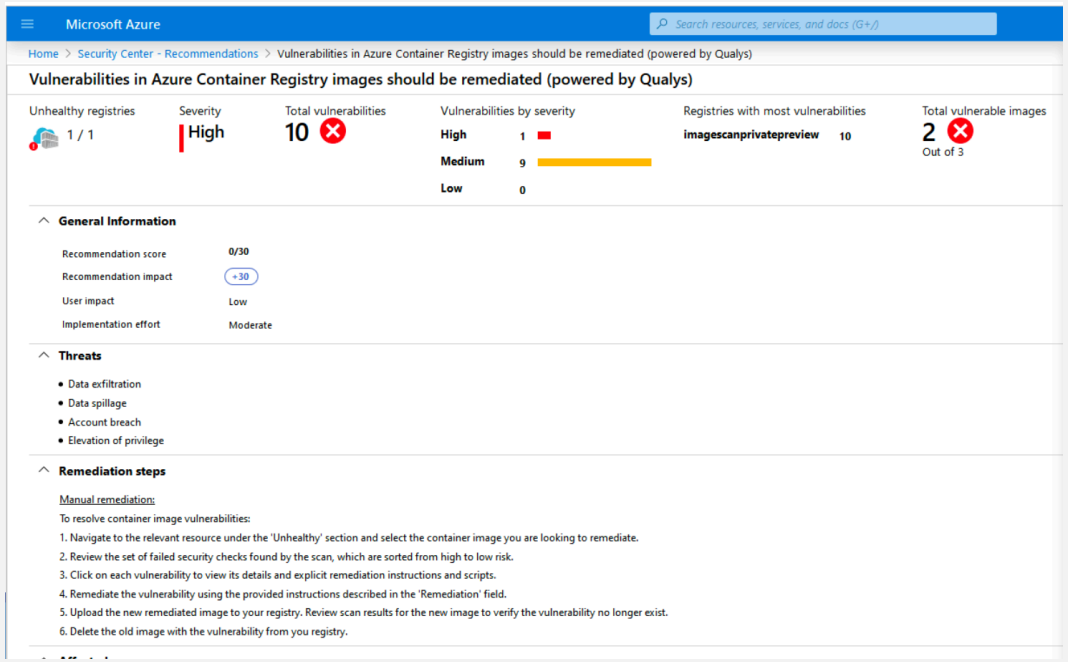
- Secure DevOps Kit for Azure (AzSK) (https://azsk.azurewebsites.net/) + Twitslock
- Scan dell'immagine durante CI

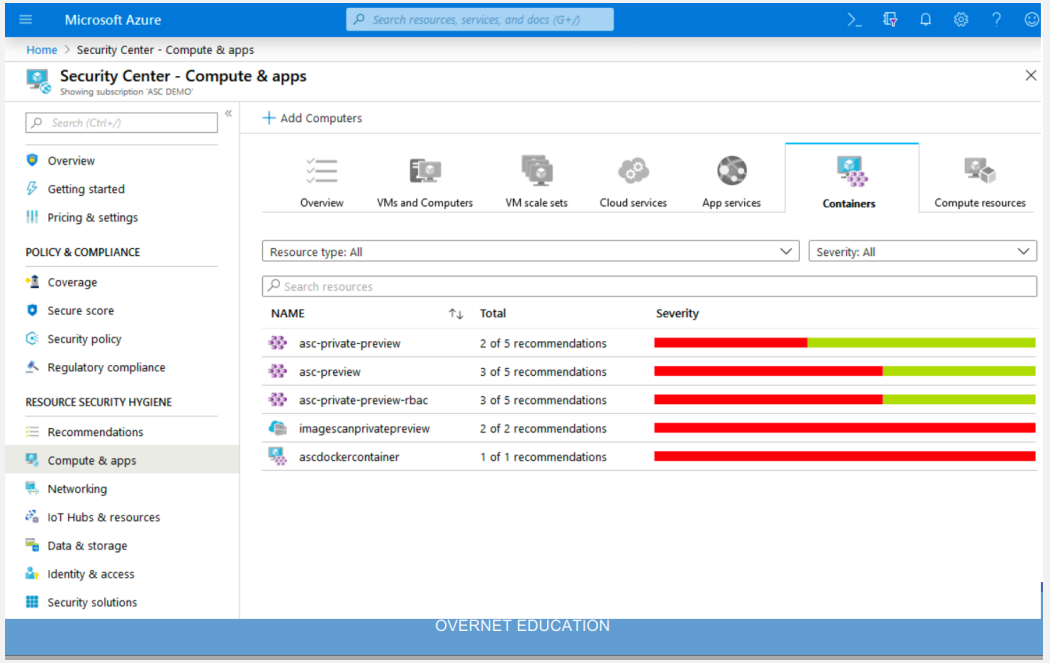




Scanning Containers

- Azure Security Center + Qualys
- Image Quarantine
- Integrazione del processo in Azure DevOps (API-Powershell)





Configure security for serverless computing

- Serverless computing moves the responsibility for server management from the application owner to the platform provider
- This helps eliminate security issues, such as servers with known security variabilities that have not been updated
- However, there are some security issues and challenges in serverless computing, as you're still responsible for:
  - Your application code
  - Data management
  - Data encryption
  - Identity management
  - Authentication/authorization
  - Configuration of services and role-based access control (RBAC)

Microsoft

OverNet EDUCATION

Contatti

OverNet Education
+39 02 365738
info@overneteducation.it
www.overneteducation.it

ROZZANO - MILANO
BOLOGNA
ROMA
GENOVA
TORINO

Grazie! – Q&A