AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Monitor and manage performance and health
14. Plan and implement updates, backups, and disaster recovery

Microsoft

Manage security for Azure Virtual Desktop

Introduction

The topics covered in this module include:

- Security recommendations for Azure Virtual Desktop.
- Connecting your Azure subscriptions to Microsoft Defender for Cloud.
- Planning Microsoft Defender for Endpoint for Azure Virtual Desktop sessions.
- Applying Zero Trust principles to an Azure Virtual Desktop deployment.
- Understanding security posture management and threat protection.

Azure +more

Defender M365

Endpoint
Identity
Office
Cloud Apps

Shared responsability

Security recommendations for Azure Virtual Desktop

Shared security responsibilities

Bring your own key

KV

OTI

For Azure Virtual Desktop, most components are Microsoft-managed, but session hosts and some supporting services and components are customer-managed or partner-managed.

Bastion

Data Security Customer

The components of which you're responsible for the security in your Azure Virtual Desktop deployment:

Component	Responsibility
Identity	Customer or partner Entra Sync
User devices (mobile and PC)	Customer or partner
App security	Customer or partner
Session host operating system	Customer or partner
Deployment configuration	Customer or partner
Network controls NSG	Customer or partner
Virtualization control plane	Microsoft Hyper-V
Physical hosts	Microsoft
Physical network	Microsoft
Physical datacenter	Microsoft

Security boundaries

- Security boundaries separate the code and data of security domains with different levels of trust.
  - For example, there's usually a security boundary between kernel mode and user mode.
- Most Microsoft software and services depend on multiple security boundaries to isolate devices on networks, virtual machines (VMs), and applications on devices.

Security boundary	Description
Network boundary	An unauthorized network endpoint can't access or tamper with code and data on a customer’s device.
Kernel boundary	A non-administrative user mode process can't access or tamper with kernel code and data. Administrator-to-kernel is not a security boundary.
Process boundary	An unauthorized user mode process can't access or tamper with the code and data of another process.
AppContainer sandbox boundary	An AppContainer-based sandbox process can't access or tamper with code and data outside of the sandbox based on the container capabilities.
User boundary	A user can't access or tamper with the code and data of another user without being authorized.
Session boundary	A user session can't access or tamper with another user session without being authorized.
Web browser boundary	An unauthorized website can't violate the same-origin policy, nor can it access or tamper with the native code and data of the Microsoft Edge web browser sandbox.
Virtual machine boundary	An unauthorized Hyper-V guest virtual machine can't access or tamper with the code and data of another guest virtual machine; this includes Hyper-V isolated containers.
Virtual Secure Mode (VSM) boundary	Code running outside of the VSM trusted process or enclave can't access or tamper with data and code within the trusted process.

Connect your Azure subscriptions to Microsoft Defender for Cloud

ASC

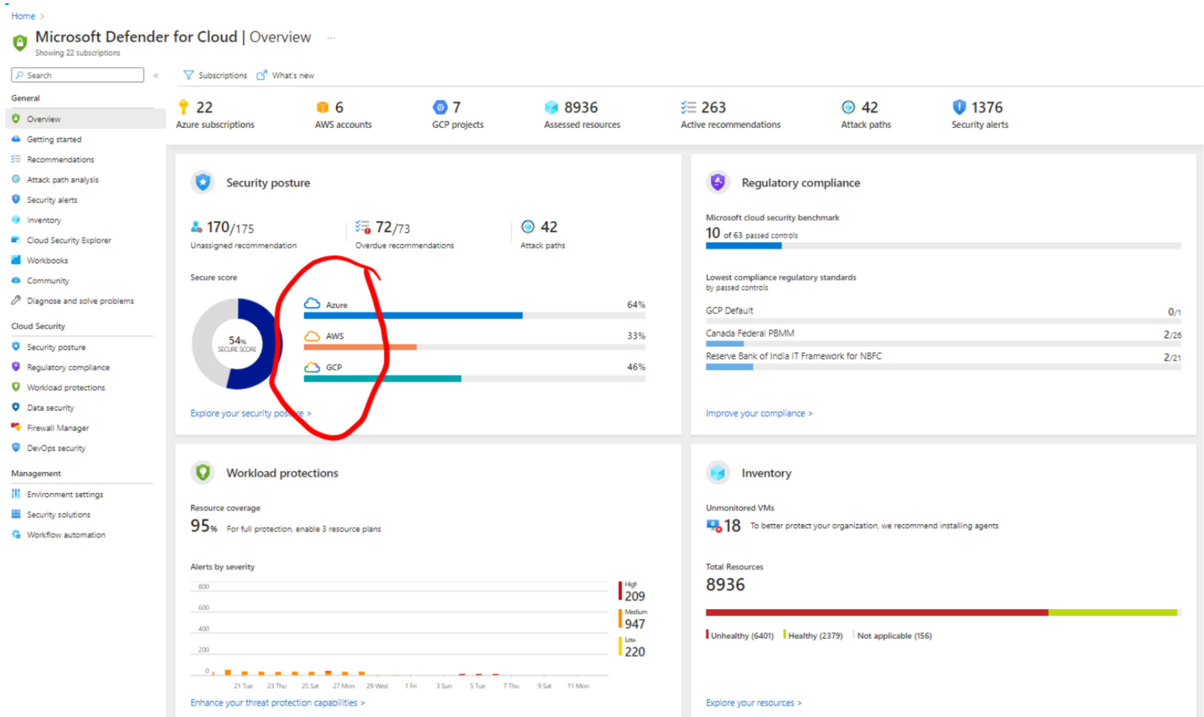
42 Posture Mgmt free

Recommeandiations ∈ Plans

Connect your Azure subscriptions to Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications:

- A **development security operations (DevSecOps)** solution that unifies security management at the code level across multicloud and multiple-pipeline environments
- A **cloud security posture management (CSPM)** solution that surfaces actions that you can take to prevent breaches.
  - Defender for Cloud includes Foundational CSPM capabilities and access to Microsoft Defender XDR for free.
- A **cloud workload protection platform (CWPP)** with specific protections for servers, containers, storage, databases, and other workloads



Microsoft Defender for Cloud | Overview

Showing 22 subscriptions

22 Azure subscriptions

6 AWS accounts

7 GCP projects

8936 Assessed resources

263 Active recommendations

42 Attack paths

1376 Security alerts

Security posture

170/175 Unassigned recommendation

72/73 Overdue recommendations

42 Attack paths

Secure score

54% SECURE SCORE

Azure	64%
AWS	33%
GCP	46%

Explore your security posture >

Regulatory compliance

Microsoft cloud security benchmark

10 of 63 passed controls

Lowest compliance regulatory standards by passed controls

GCP Default	0/1
Canada Federal PBMM	2/26
Reserve Bank of India IT Framework for NBFC	2/21

Improve your compliance >

Workload protections

Resource coverage

95% For full protection, enable 3 resource plans

Alerts by severity

High 209

Medium 947

Low 220

Enhance your threat protection capabilities >

Inventory

Unmonitored VMs

18 To better protect your organization, we recommend installing agents

Total Resources

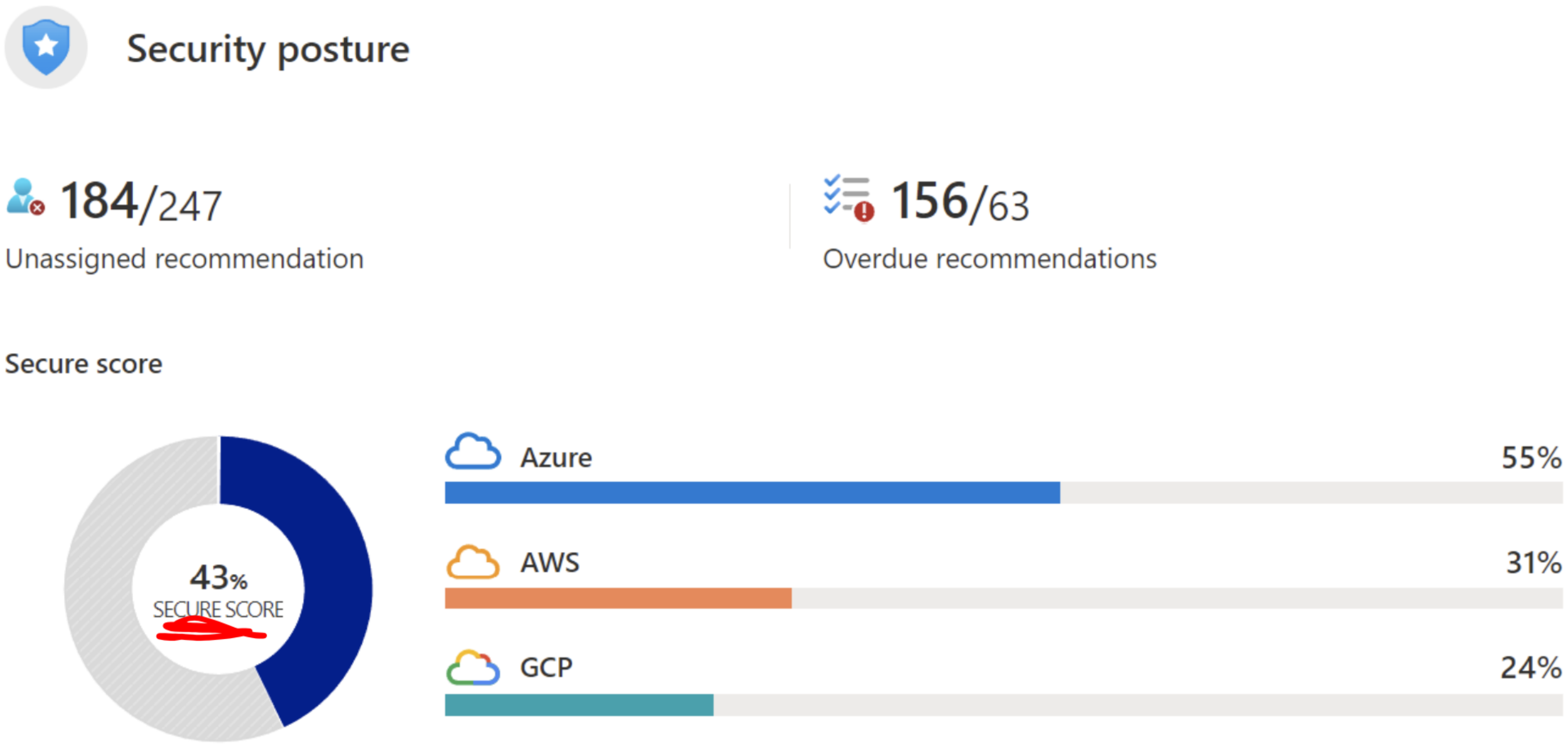
8936

Unhealthy (6401) Healthy (2379) Not applicable (156)

Explore your resources >

Security posture management and threat protection

The secure score in Microsoft Defender for Cloud helps improve your cloud security posture by aggregating security findings into a single score.



Security posture

184/247
Unassigned recommendation

156/63
Overdue recommendations

Secure score

43%
SECURE SCORE

Azure	55%
AWS	31%
GCP	24%

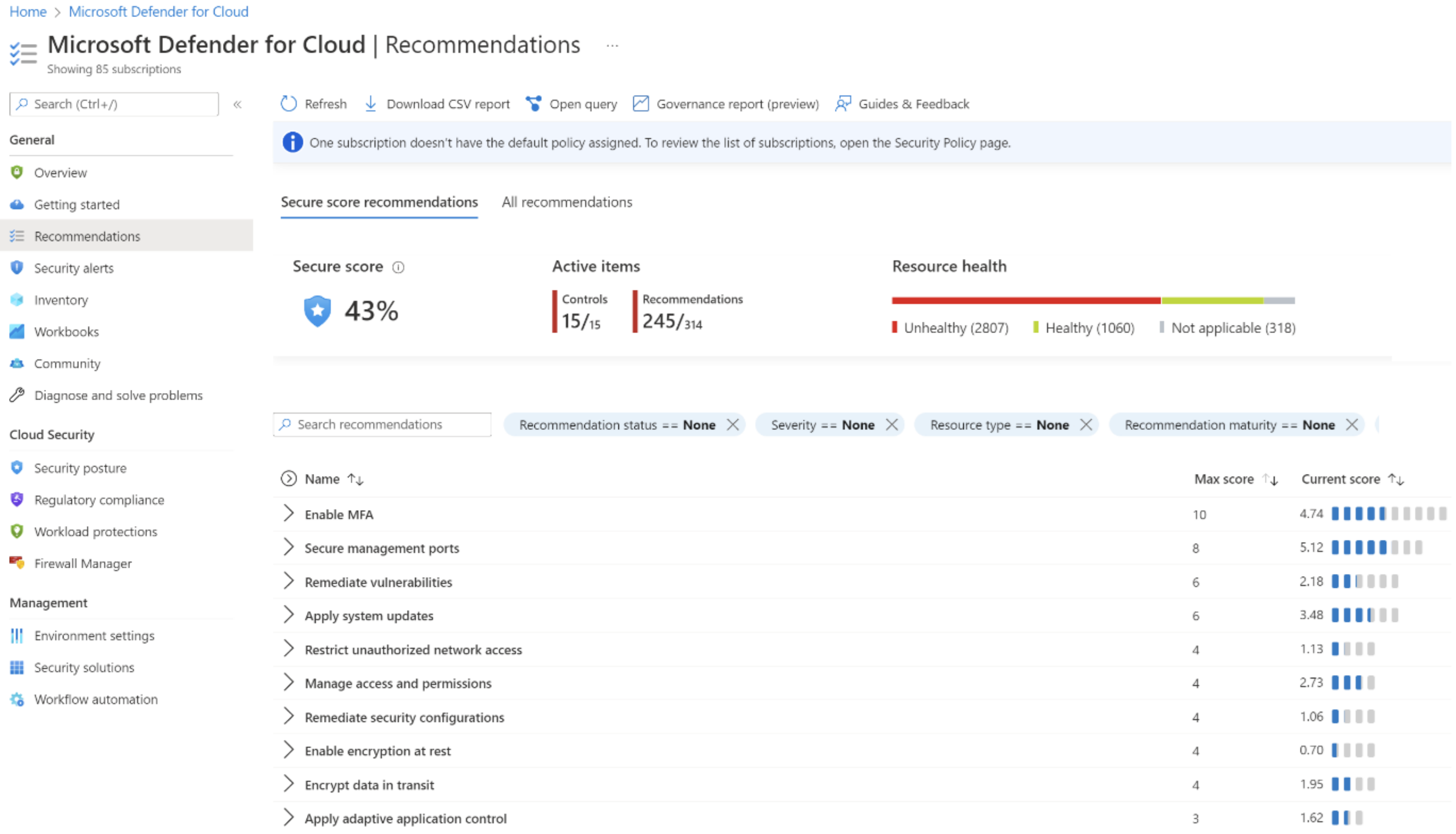
ARC

Arcns

vm
SQL
K8S

Calculation of the secure score

- Defender for Cloud calculates each control every eight hours for each Azure subscription or for each AWS or GCP cloud connector.
- Recommendations within a control are updated more often than the control itself.



Microsoft Defender for Cloud | Recommendations

Showing 85 subscriptions

One subscription doesn't have the default policy assigned. To review the list of subscriptions, open the Security Policy page.

Secure score 43%

Active items: Controls 15/15, Recommendations 245/314

Resource health: Unhealthy (2807), Healthy (1060), Not applicable (318)

Name	Max score	Current score
Enable MFA	10	4.74
Secure management ports	8	5.12
Remediate vulnerabilities	6	2.18
Apply system updates	6	3.48
Restrict unauthorized network access	4	1.13
Manage access and permissions	4	2.73
Remediate security configurations	4	1.06
Enable encryption at rest	4	0.70
Encrypt data in transit	4	1.95
Apply adaptive application control	3	1.62

Microsoft Defender for Endpoint for Azure Virtual Desktop sessions

Microsoft Defender for Endpoint for Azure Virtual Desktop sessions

There are multiple ways to onboard an AVD host machine:

- Run the script in the golden image (or from a shared location) during startup.
- Use a management tool to run the script.
- Through Integration with Microsoft Defender for Cloud

Scenario 1: Using local group policy
This scenario requires placing the script in a golden image and uses local group policy to run early in the boot process.

Scenario 2: Using domain group policy
This scenario uses a centrally located script and runs it using a domain-based group policy. You can also place the script in the golden image and run it in the same way.

Scenario 3: Onboarding using management tools
If you plan to manage your machines using a management tool, you can onboard devices with Microsoft Endpoint Configuration Marectly.

- After onboarding the device, you can choose to run a detection test to verify that the device is properly onboarded to the service.

Apply Zero Trust principles to an Azure Virtual Desktop deployment

Apply Zero Trust principles to an Azure Virtual Desktop deployment

Step 1: Secure your identities with Zero Trust

To apply Zero Trust principles to the identities used in Azure Virtual Desktop:

- Azure Virtual Desktop supports different types of identities. Use the information in Securing identity with Zero Trust to ensure that your chosen identity types adhere to Zero Trust principles.
- Create a dedicated user account with least privileges to join session hosts to a Microsoft Entra Domain Services or AD DS domain during session host deployment.

Step 2: Secure your endpoints with Zero Trust

Endpoints are the devices through which users access the Azure Virtual Desktop environment and session host virtual machines.

Step 3: Apply Zero Trust principles to Azure Virtual Desktop storage resources

Implement the steps in Apply Zero Trust principles to Storage in Azure for the storage resources being used in your Azure Virtual Desktop deployment.

Step 4: Apply Zero Trust principles to hub and spoke Azure Virtual Desktop VNets

A hub VNet is a central point of connectivity for multiple spoke virtual networks. Implement the steps in Apply Zero Trust principles to a hub virtual network in Azure for the hub VNet being used to filter outbound traffic from your session hosts.

Apply Zero Trust principles to an Azure Virtual Desktop deployment (continued)

Step 5: Apply Zero Trust principles to Azure Virtual Desktop session hosts

Session hosts are virtual machines that run inside a spoke VNet. Implement the steps in Apply Zero Trust principles to virtual machines in Azure for the virtual machines being created for your session hosts.

Step 6: Deploy security, governance, and compliance to Azure Virtual Desktop

Azure Virtual Desktop service allow you to use Azure Private Link to privately connect to your resources by creating private endpoints.

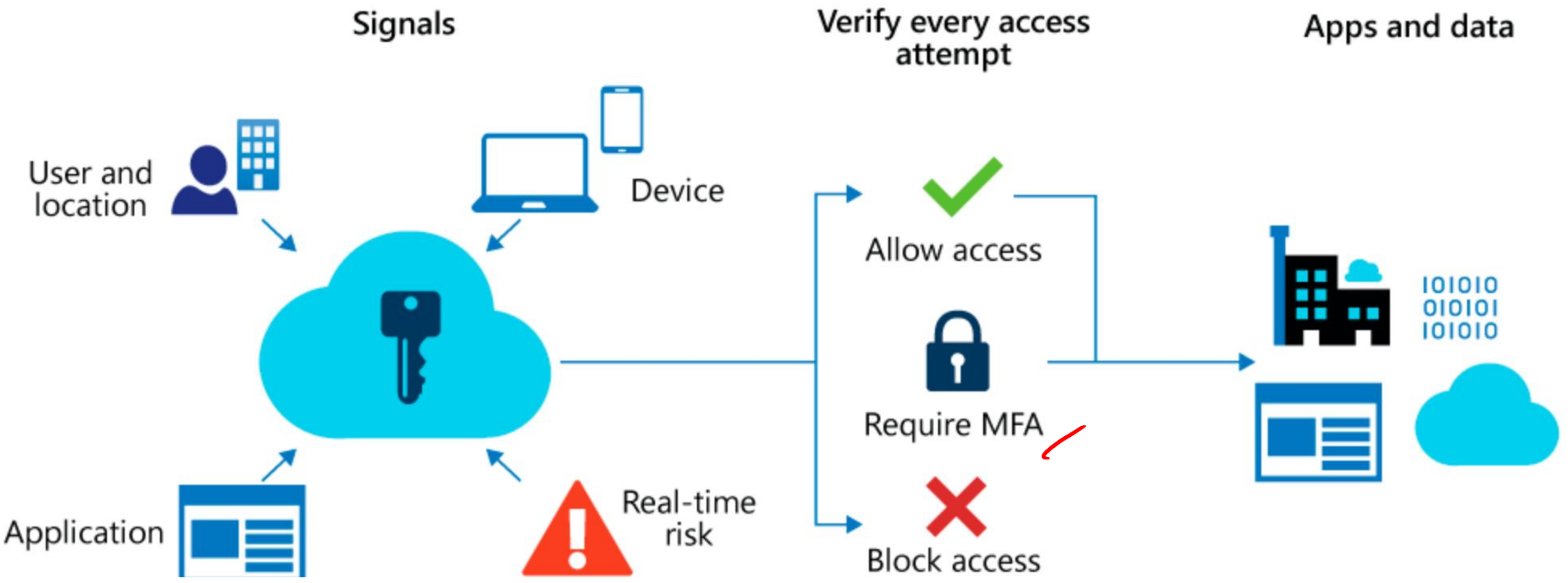
Step 7: Deploy secure management and monitoring to Azure Virtual Desktop

Management and continuous monitoring are important to ensure that your Azure Virtual Desktop environment is not engaging in malicious behavior. Use Azure Virtual Desktop Insights to log data and report diagnostic and usage data.

Plan and implement Conditional Access policies for connections to Azure Virtual Desktop

Plan and implement Conditional Access policies for connections to Azure Virtual Desktop

Use Conditional Access policies to automate decisions and enforce organizational access policies. Apply access controls like MFA and customize security defaults.



PIM = Roles temporär 6h
Antrag
Approver

Benefits of Conditional Access

Increase productivity. Only interrupt users with a sign-in condition like MFA when one or more signals warrants it. Conditional Access policies allow you to control when users are prompted for MFA, when access is blocked, and when they must use a trusted device.

Manage risk. Automating risk assessment with policy conditions means risky sign-ins are at once identified and remediated or blocked. Coupling Conditional Access with Identity Protection, which detects anomalies and suspicious events, allows you to target when access to resources is blocked or gated.

Address compliance and governance. Conditional Access enables you to audit access to applications, present terms of use for consent, and restrict access based on compliance policies.

Manage cost. Moving access policies to Entra ID reduces the reliance on custom or on-premises solutions for Conditional Access, and their infrastructure costs.

Knowledge check

Knowledge check

A system administrator is setting up a multi-session environment for users from different organizations. What is the recommended solution to ensure security and prevent unauthorized data access?

Choices:

1. Use a Windows Enterprise multi-session operating system ✗

2. Grant each user administrative privileges ✗

[✓ 3.] Separate Azure tenant and Azure subscription

Knowledge check

A team is deploying Azure Virtual Desktop and wants to ensure the environment is secure. They are considering using Microsoft Defender for Endpoint for session hosts. What does Microsoft Defender for Endpoint provide?

Choices:

1. It provides a platform for managing group policies on Active Directory Domain Services (AD DS). ✗

2. It allows the creation of private endpoints through Azure Private Link. ✗

[✓ 3.] It is an enterprise endpoint security platform designed to help prevent, detect, investigate, and respond to advanced threats.

Knowledge check

A system administrator is setting up a multi-session environment for users from different organizations. What is the recommended solution to ensure security and prevent unauthorized data access?

Choices:

1. Grant each user administrative privileges ✗

2. Use a Windows Enterprise multi-session operating system ✗

[✓ 3.] Separate Azure tenant and Azure subscription

Knowledge check

An administrator is tasked with setting up a secure multi-session environment for users from different organizations. What is the recommended solution to ensure security and prevent unauthorized data access?

Choices:

1. Grant each user administrative privileges
2. Use a Windows Enterprise multi-session operating system
3. Separate Azure tenant and Azure subscription

Summary

Summary

What you learned:

- Describe security recommendations for Azure Virtual Desktop
- Connect Azure subscriptions to Microsoft Defender for Cloud
- Plan Microsoft Defender for Endpoint for Azure Virtual Desktop sessions
- Apply Zero Trust principles to an Azure Virtual Desktop deployment
- Describe security posture management and threat protection