Mastering Defender for Servers

by Gregor Reimling

#CloudBrew

AZUG
Azure User Group Belgium

Thank you partners! 😍

ae

AXXES_

Arxus

codit

delaware

devoteam

DEXMACH
A CEGEKA COMPANY

Microsoft

ORDINA

inetum.
realdolmen
Positive digital flow

proximus

ZURE

Integration.team
Connecting anything, anytime, anywhere

NOEST

dataroots

JET BRAINS

U2U

About “Gregor Reimling”

Azure Meetup
BONN
www.azurebonn.de

Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

https://www.Reimling.eu

www.cloudinspires.me

Certifications

Cloud Security Architect

MVP for MS Azure & Security

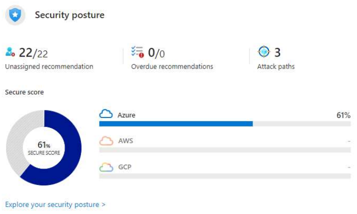
Hobbies

Family, Community, Worldtraveler

Contact

@GregorReimling

Gregor Reimling



Security posture

22/22 Unassigned recommendation

0/0 Overdue recommendations

3 Attack paths

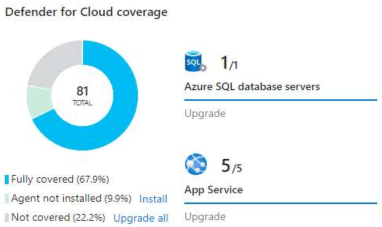
Secure score

61% SECURE SCORE

Azure	61%
AWS	-
GCP	-

Explore your security posture >

Defender for Cloud Overview



Defender for Cloud coverage

81 TOTAL

- Fully covered (67.9%)
- Agent not installed (9.9%) Install
- Not covered (22.2%) Upgrade all

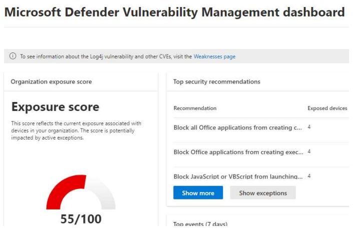
1/1 Azure SQL database servers

Upgrade

5/5 App Service

Upgrade

Defender for Server



Microsoft Defender Vulnerability Management dashboard

To see information about the Log4j vulnerability and other CVEs, visit the Weaknesses page

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.

55/100

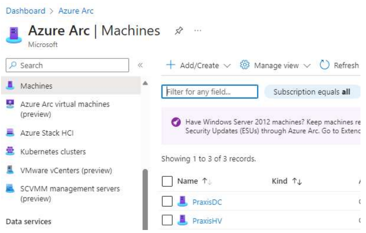
Top security recommendations

Recommendation	Exposed devices
Block all Office applications from creating c...	4
Block Office applications from creating exec...	4
Block JavaScript or VBScript from launching...	4

Show more | Show exceptions

Top events (7 days)

Defender for Endpoint



Dashboard > Azure Arc

Azure Arc | Machines

Microsoft

Search

- Machines
- Azure Arc virtual machines (preview)
- Azure Stack HCI
- Kubernetes clusters
- VMware vCenters (preview)
- SCVMM management servers (preview)

Data services

+ Add/Create | Manage view | Refresh

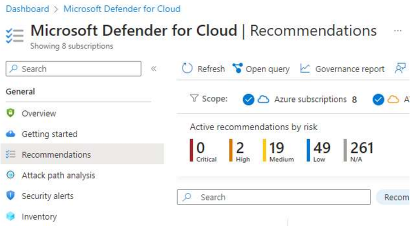
Filter for any field... | Subscription equals **all**

Have Windows Server 2012 machines? Keep machines re
Security Updates (ESUs) through Azure Arc. Go to Extenc

Showing 1 to 3 of 3 records.

□	Name ↑↓	Kind ↑↓
□	PraxisDC	
□	PraxisHV	

Multicloud Capabilities



Dashboard > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Recommendations

Showing 8 subscriptions

Search

General

- Overview
- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory

Refresh | Open query | Governance report

Scope: Azure subscriptions 8

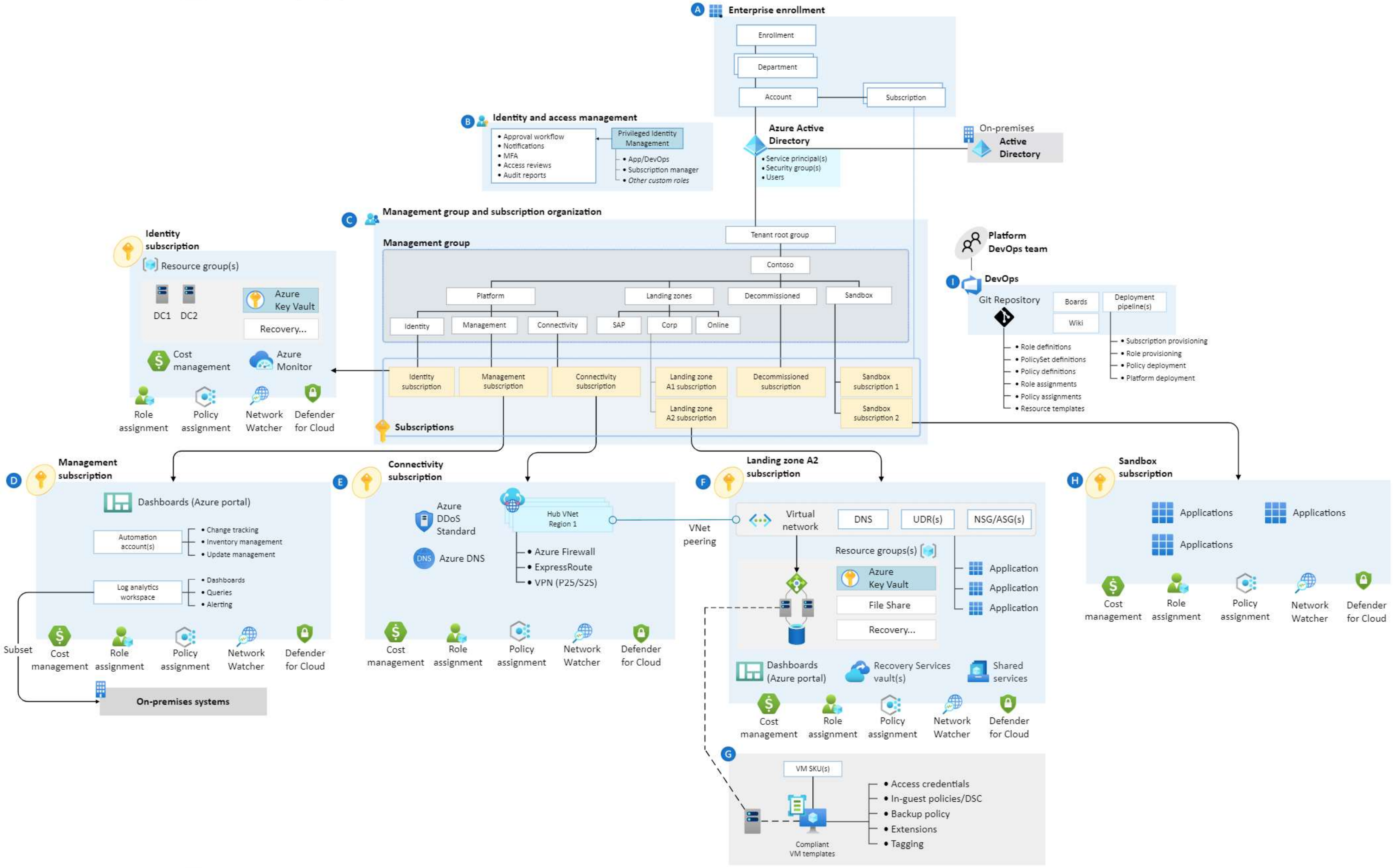
Active recommendations by risk

0	2	19	49	261
Critical	High	Medium	Low	N/A

Search | Recom

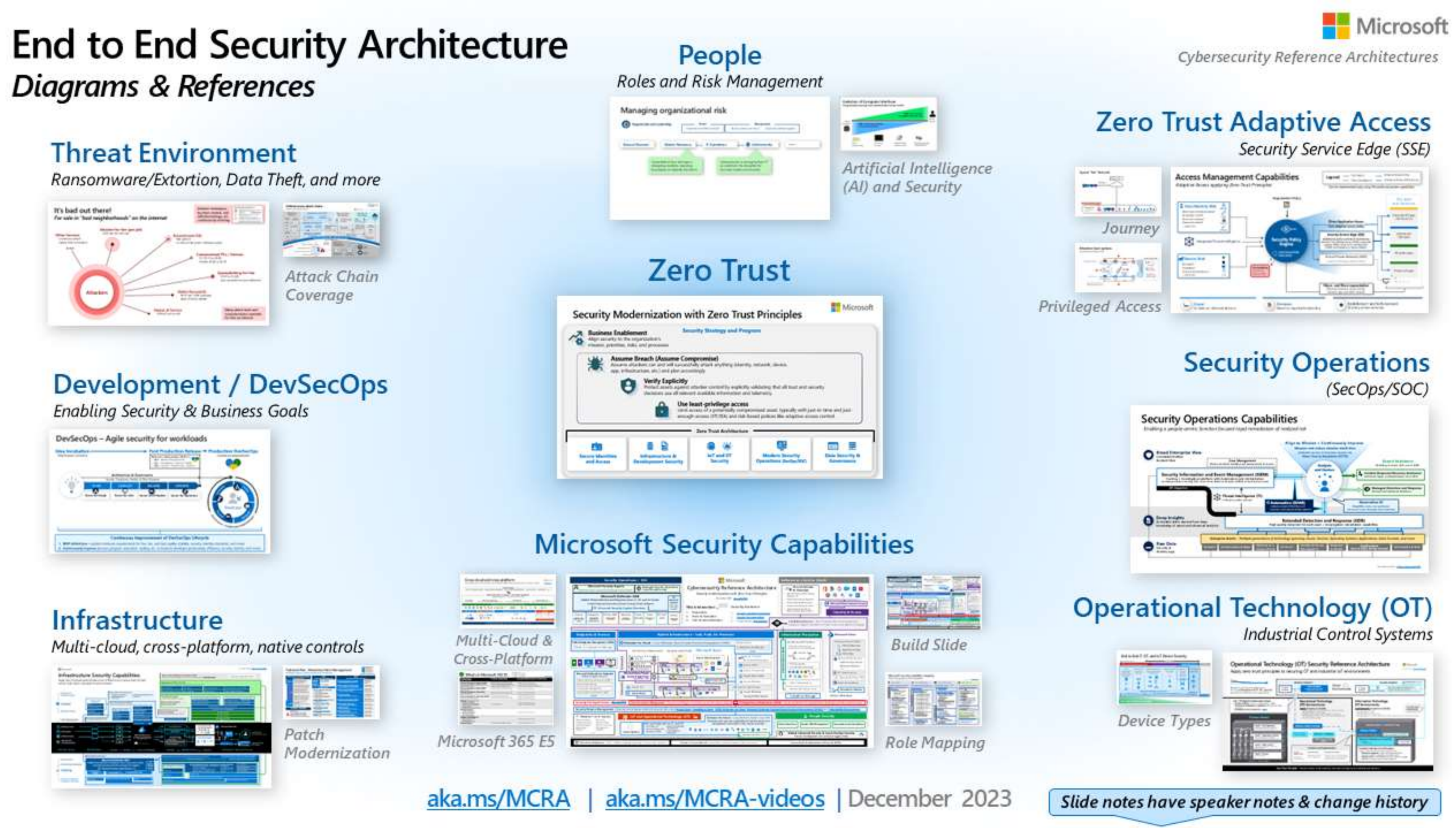
New Defender features

Enterprise Scale



https://aka.ms/landingzones

Cybersecurity Reference Architecture



Managing organizational risk
Security Modernization with Zero Trust Principles
Business Enablement
Assume Breach (Assume Compromise)
Verify Explicitly
Use least-privilege access
Zero Trust Architecture
It's bad out there!
Attacker
DevSecOps – Agile security for workloads
Infrastructure Security Capabilities
Access Management Capabilities
Security Operations Capabilities
Operational Technology (OT) Security Reference Architecture
Cybersecurity Reference Architecture

End to End Security Architecture

Diagrams & References

Microsoft

Cybersecurity Reference Architectures

People

Roles and Risk Management

Artificial Intelligence (AI) and Security

Threat Environment

Ransomware/Extortion, Data Theft, and more

Attack Chain Coverage

Zero Trust Adaptive Access

Security Service Edge (SSE)

Journey

Privileged Access

Zero Trust

Development / DevSecOps

Enabling Security & Business Goals

Security Operations

(SecOps/SOC)

Microsoft Security Capabilities

Multi-Cloud & Cross-Platform

Microsoft 365 E5

Build Slide

Role Mapping

Infrastructure

Multi-cloud, cross-platform, native controls

Patch Modernization

Operational Technology (OT)

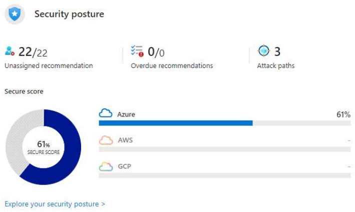
Industrial Control Systems

Device Types

aka.ms/MCRA | aka.ms/MCRA-videos | December 2023

Slide notes have speaker notes & change history

Defender for Cloud overview



Security posture

22/22
Unassigned recommendation

0/0
Overdue recommendations

3
Attack paths

Secure score

61%
SECURE SCORE

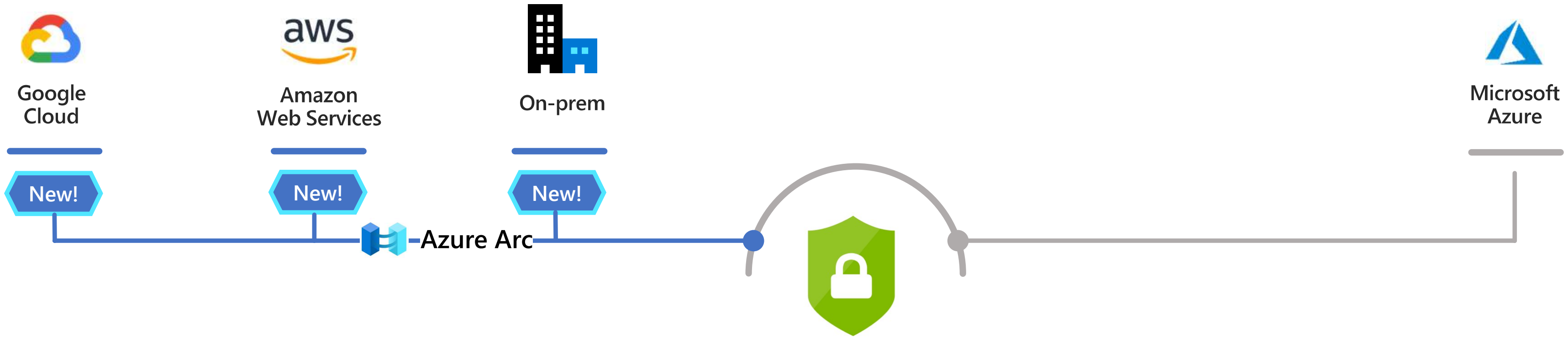
Azure 61%

AWS -

GCP -

Explore your security posture >

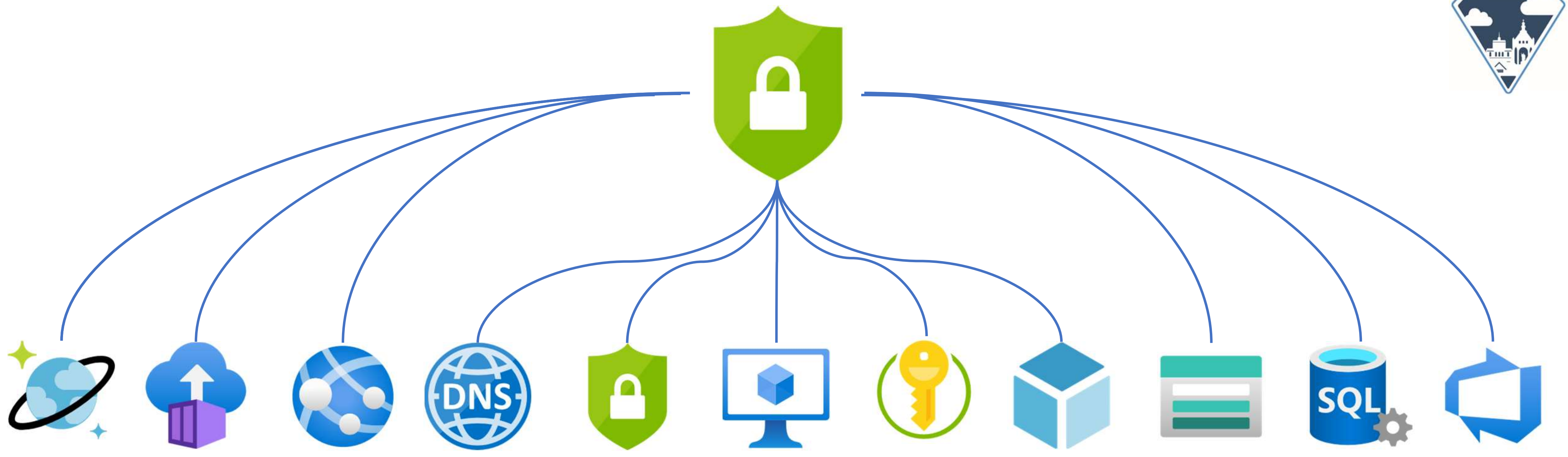
MS Defender for Cloud



Security posture & compliance	Secure score	Asset management	Policy
Server protection (Microsoft Defender for Cloud for VMs)	Threat detection	VA (power by Qualys)	Application control
Automation & management at scale	Automation	SIEM integration	Export

AZUG
Azure User Group Belgium

Microsoft Defender for Cloud



Defender for Azure Cosmos DB

Defender for Containers

Defender for App Service

Defender for DNS

Defender for CSPM

Defender for Servers

Defender for Key Vault

Defender for Resource Manager

Defender for Storage

Defender for SQL

Defender for DevOps

Log Analytics Considerations

Per default Defender for Cloud creates Log Analytics Workspace in each VM region

Note
Default workspaces created by Defender for Cloud **can not be used for Sentinel**

Note
Without defined LAW – Azure creates a Default LAW in every Azure VM region

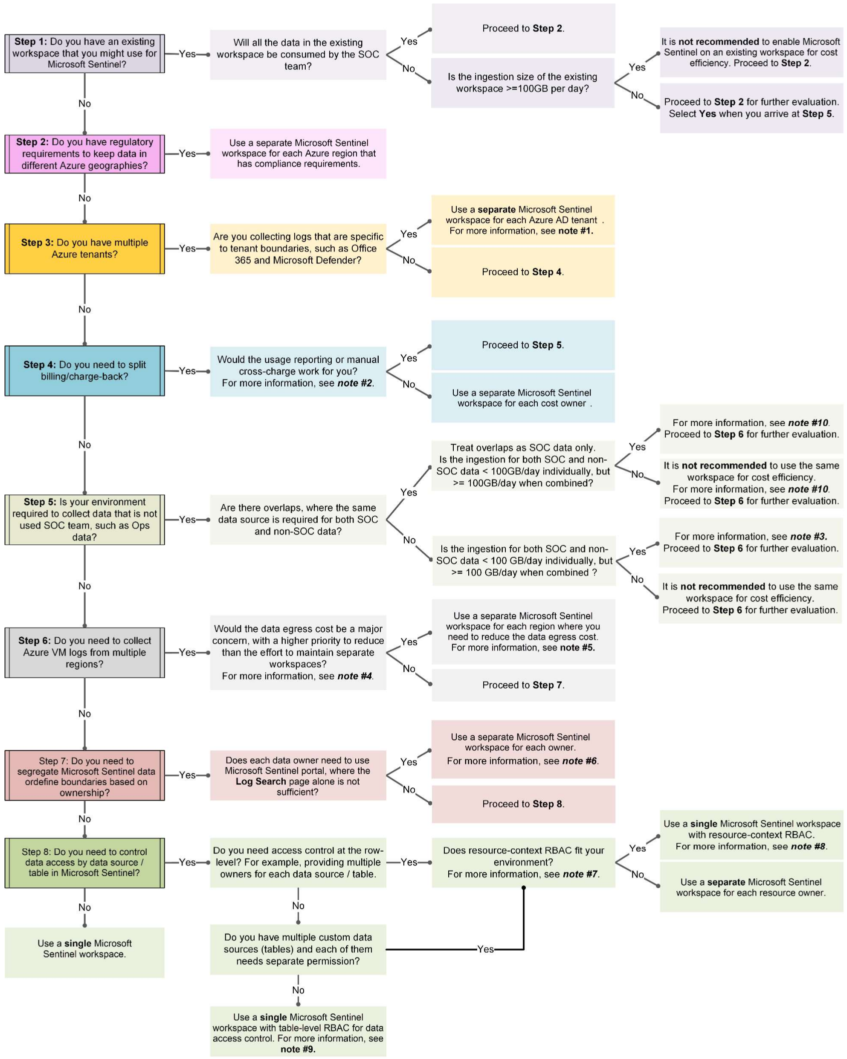
Think about pricing and ingestion data

Using VMs in different regions – maybe different LAWs make sense in case of ingress and egress traffic cost and compliance reasons

Before start with Defender for Cloud create a **own** Default LAW for all Security related Logs

This can then also used later for Sentinel

LAW decision tree



Step 1: Do you have an existing workspace that you might use for Microsoft Sentinel?

Yes → Will all the data in the existing workspace be consumed by the SOC team?

Yes → Proceed to **Step 2**.

No → Is the ingestion size of the existing workspace >=100GB per day?

Yes → It is **not recommended** to enable Microsoft Sentinel on an existing workspace for cost efficiency. Proceed to **Step 2**.

No → Proceed to **Step 2** for further evaluation. Select **Yes** when you arrive at **Step 5**.

No

Step 2: Do you have regulatory requirements to keep data in different Azure geographies?

Yes → Use a separate Microsoft Sentinel workspace for each Azure region that has compliance requirements.

No

Step 3: Do you have multiple Azure tenants?

Yes → Are you collecting logs that are specific to tenant boundaries, such as Office 365 and Microsoft Defender?

Yes → Use a **separate** Microsoft Sentinel workspace for each Azure AD tenant . For more information, see **note #1.**

No → Proceed to **Step 4**.

No

Step 4: Do you need to split billing/charge-back?

Yes → Would the usage reporting or manual cross-charge work for you? For more information, see ***note #2***.

Yes → Proceed to **Step 5**.

No → Use a separate Microsoft Sentinel workspace for each cost owner .

No

Step 5: Is your environment required to collect data that is not used SOC team, such as Ops data?

Yes → Are there overlaps, where the same data source is required for both SOC and non-SOC data?

Yes → Treat overlaps as SOC data only. Is the ingestion for both SOC and non-SOC data < 100GB/day individually, but >= 100GB/day when combined?

Yes → For more information, see ***note #10***. Proceed to **Step 6** for further evaluation.

No

It is **not recommended** to use the same workspace for cost efficiency. For more information, see ***note #10***. Proceed to **Step 6** for further evaluation.

No → Is the ingestion for both SOC and non-SOC data < 100 GB/day individually, but >= 100 GB/day when combined ?

Yes → For more information, see ***note #3.*** Proceed to **Step 6** for further evaluation.

No → It is **not recommended** to use the same workspace for cost efficiency. Proceed to **Step 6** for further evaluation.

No

Step 6: Do you need to collect Azure VM logs from multiple regions?

Yes → Would the data egress cost be a major concern, with a higher priority to reduce than the effort to maintain separate workspaces? For more information, see ***note #4***.

Yes → Use a separate Microsoft Sentinel workspace for each region where you need to reduce the data egress cost. For more information, see **note #5.**

No → Proceed to **Step 7**.

No

Step 7: Do you need to segregate Microsoft Sentinel data ordefine boundaries based on ownership?

Yes → Does each data owner need to use Microsoft Sentinel portal, where the **Log Search** page alone is not sufficient?

Yes → Use a separate Microsoft Sentinel workspace for each owner. For more information, see ***note #6***.

No → Proceed to **Step 8**.

No

Step 8: Do you need to control data access by data source / table in Microsoft Sentinel?

Yes → Do you need access control at the row-level? For example, providing multiple owners for each data source / table.

Yes → Does resource-context RBAC fit your environment? For more information, see ***note #7***.

Yes → Use a **single** Microsoft Sentinel workspace with resource-context RBAC. For more information, see ***note #8***.

No → Use a **separate** Microsoft Sentinel workspace for each resource owner.

No

Do you have multiple custom data sources (tables) and each of them needs separate permission?

Yes

No

Use a **single** Microsoft Sentinel workspace with table-level RBAC for data access control. For more information, see **note #9.**

No → Use a **single** Microsoft Sentinel workspace.

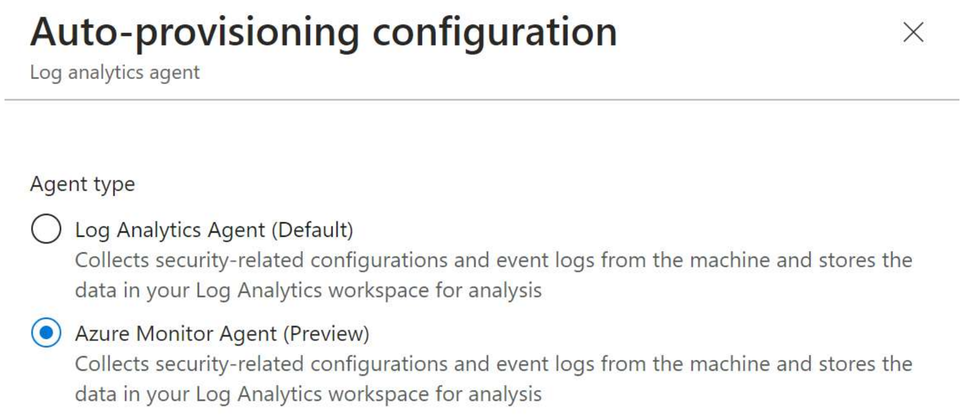
Design your Microsoft Sentinel workspace architecture | Microsoft Learn

Timeline

Sep	Oct	Nov	Dec	Jan	Feb	Mar	April	May	June	July	Aug
Previous implementation (before April of 2022) uses MMA for WS2012/WS2016											
				MMA will be retired on 31 August 2024							
				all Defender for Servers features and capabilities currently relying on Log Analytics Agent (MMA) will be deprecated							
				all Defender for Servers features and capabilities will be provided through either Microsoft Defender for Endpoint (MDE) integration or agentless scanning							

Auto-provisioning configuration

- Switch from MMA to AMA does not uninstall the MMA-agent
- Duplicate agents results in doubled events or recommendations and appear twice in Defender
- Monitoring workbook – AMA migration tracker workbook



Auto-provisioning configuration

Log analytics agent

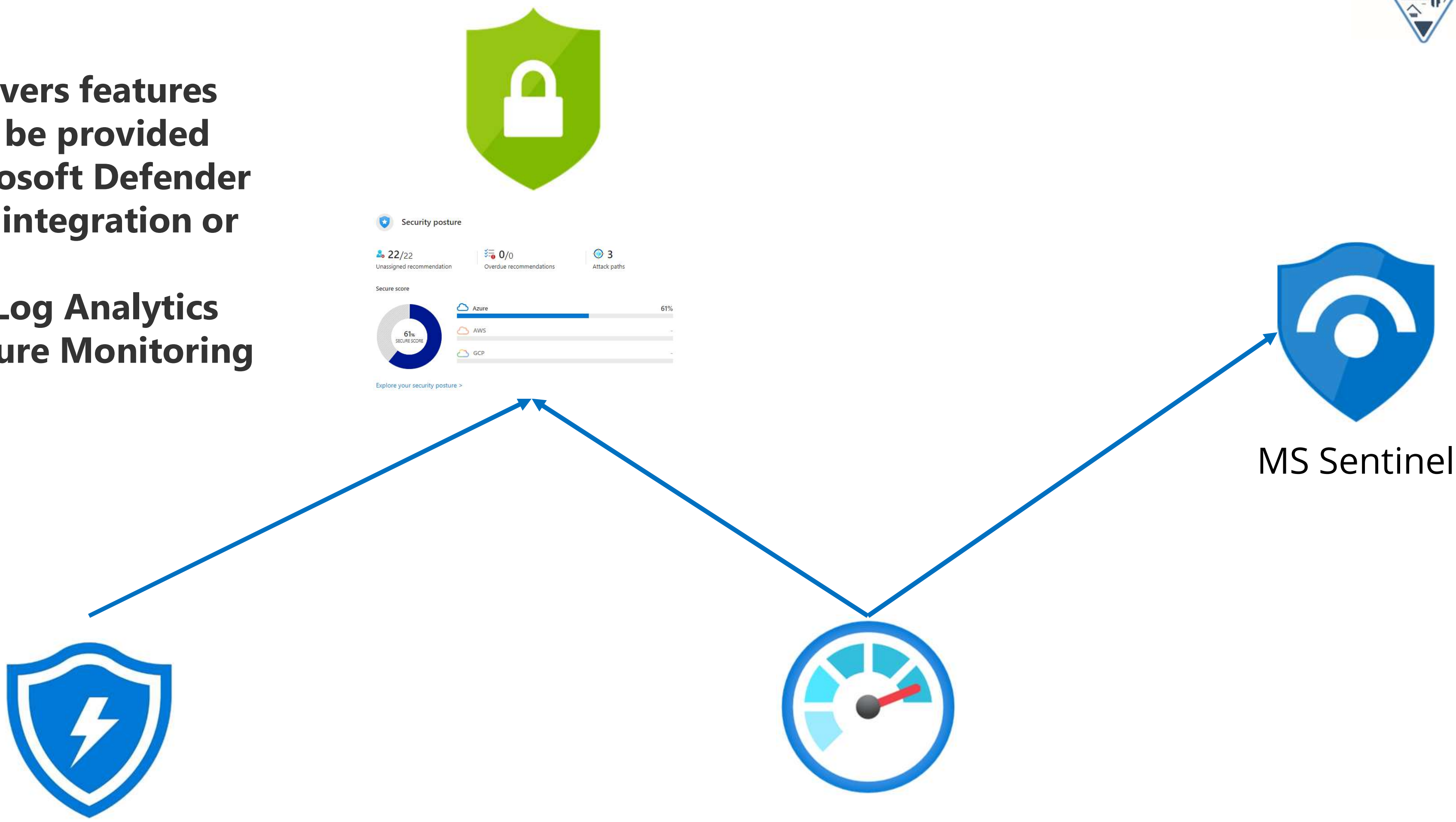
Agent type

○ Log Analytics Agent (Default)
Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis

● Azure Monitor Agent (Preview)
Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis

AMA and Defender for Server

- All Defender for Servers features and capabilities will be provided through either Microsoft Defender for Endpoint (MDE) integration or agentless scanning
- No dependency on Log Analytics Agent (MMA) or Azure Monitoring Agent (AMA)



Security posture

22/22 Unassigned recommendation

0/0 Overdue recommendations

3 Attack paths

Secure score

61% SECURE SCORE

Azure	61%
AWS	-
GCP	-

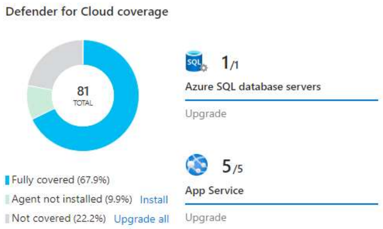
Explore your security posture >

MS Sentinel

Defender for Endpoint

Azure Monitoring Agent

Defender for Server



Defender for Cloud coverage

- Fully covered (67.9%)
- Agent not installed (9.9%) Install
- Not covered (22.2%) Upgrade all

1/1 Azure SQL database servers

Upgrade

5/5 App Service

Upgrade

Why Defender for Servers?

VMs needs security on the control plane

Preventing Lateral Movement

Threat detections must be managed and validated centrally

Real-time scanning and protection

Protecting Servers on different level is important

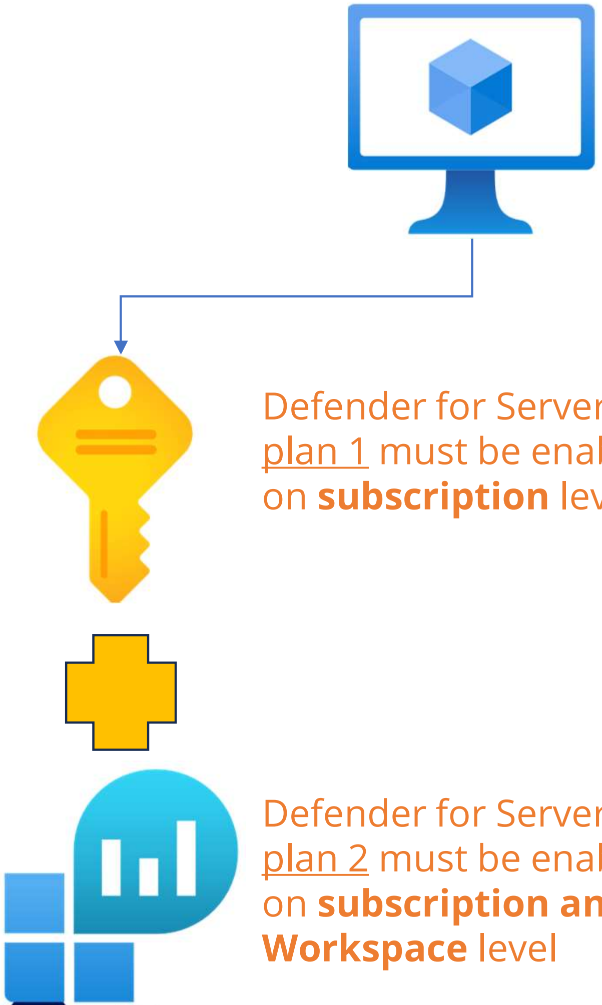
Reducing the attack surface

Defender for Servers Plan comparison

Plan 1	Features	Plan 2
✓	Unified View	✓
✓	Automatic MDE provisioning	✓
✓	MS Threat and Vulnerability management	✓
	Security Policy and Regulatory Compliance	✓
	Integrated Vulnerability by Qualys	✓
	Log Analytics 500MB free data ingestion per day	✓
	Threat detection	✓
	Adaptive application control	✓
	File integrity monitoring	✓
	Just-in-Time VM access	✓
	Adaptive Network hardening	✓
	Docker host hardening	✓
	Fileless attack detection	✓

AZUG
Azure User Group Belgium

Considerations for activation of Defender for Server

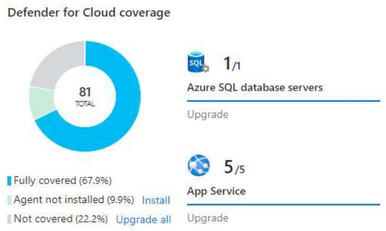


Defender for Servers plan 1 must be enabled on **subscription** level

Defender for Servers plan 2 must be enabled on **subscription and Workspace** level

- Defender for Servers plan 1 must be enabled on **subscription** level
- Defender for Servers plan 2 must be enabled on **subscription** and **Workspace** level
- Mixing of the plans only possible with different subscription
- License cost for plan 2 is incurred for each machine connected to the Workspace where plan 2 is activated

Demo Defender for Server



Defender for Cloud coverage

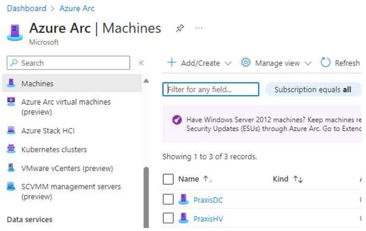
- Fully covered (67.9%)
- Agent not installed (9.9%) Install
- Not covered (22.2%) Upgrade all

1/1
Azure SQL database servers
Upgrade

5/5
App Service
Upgrade

Defender
for Server

Multicloud Capabilities



Have Windows Server 2012 machines? Keep machines re
Security Updates (ESUs) through Azure Arc. Go to Extenc

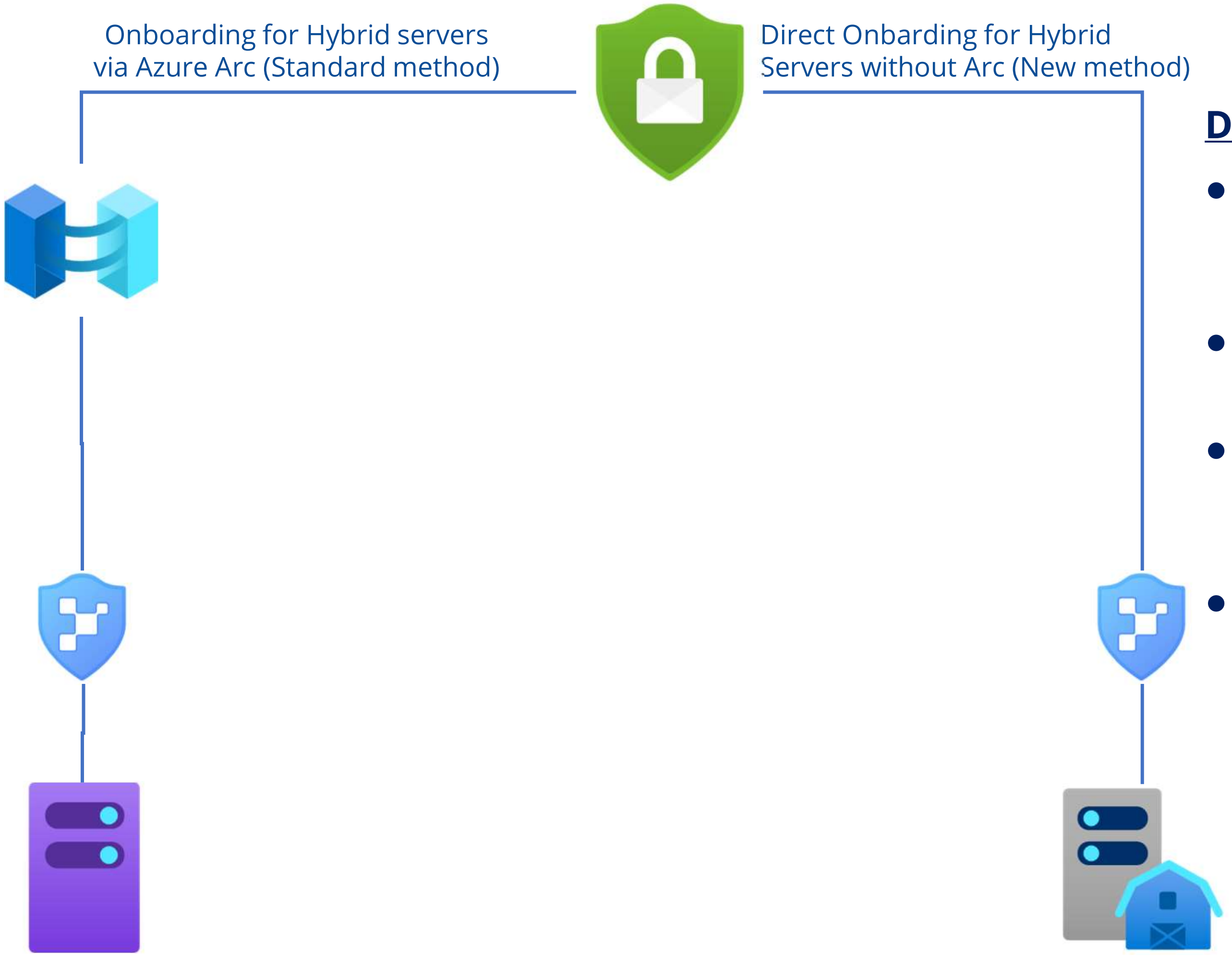
Showing 1 to 3 of 3 records.

□	Name ↑↓	Kind ↑↓
□	PraxisDC	
□	PraxisHV	

Hybrid Server Onboarding (Azure Arc)

Azure Arc

- Will automatically install
- Direct onboarding of VMs in AWS and GCP is also supported, but do you plan to use multicloud connectors is recommended to use Azure Arc



Onboarding for Hybrid servers via Azure Arc (Standard method)

Direct Onbarding for Hybrid Servers without Arc (New method)

Direct Onboarding

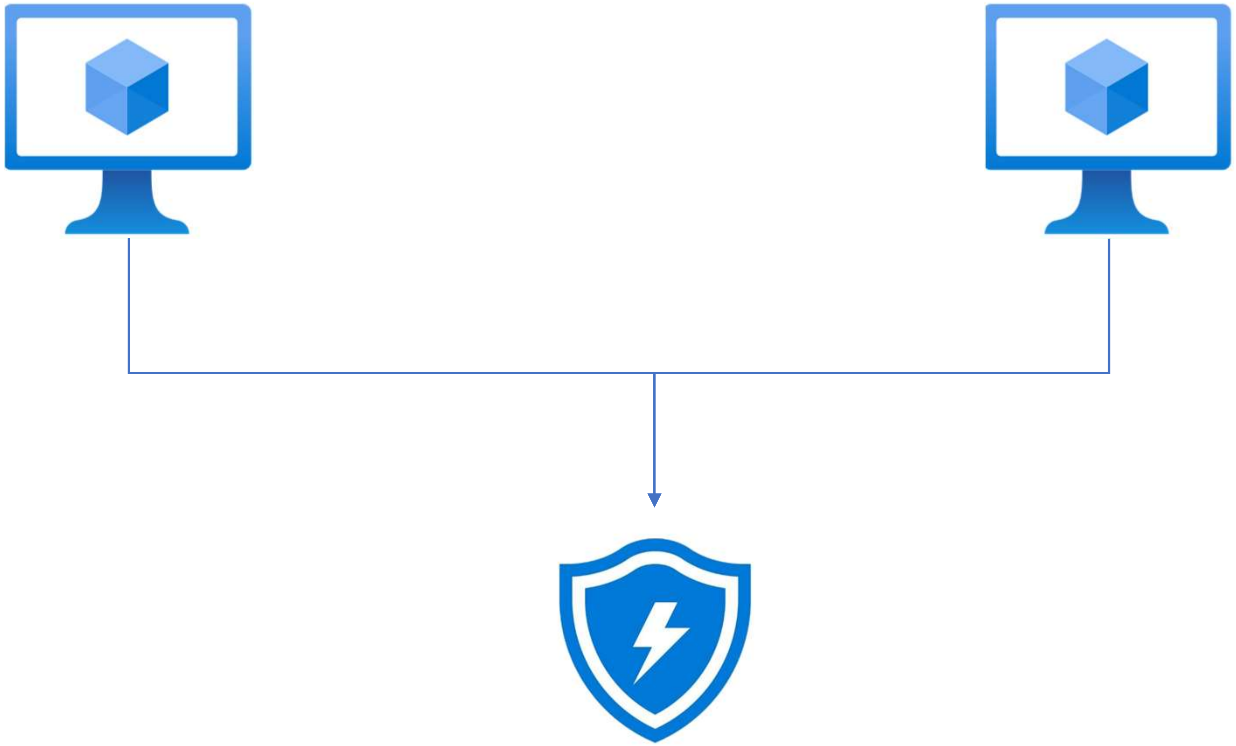
- Ideal for customers which focussing only on Defender for Server
- Needs a separate subscription
- Direct onboard support all features of Plan 1 and Plan 2
- Direct onboarding of VMs in AWS and GCP is also supported, but do you plan to use multicloud connectors is recommended to use Azure Arc

Defender for Endpoint

Defender for Endpoint Plan comparisation

MS Defender for Endpoint Plan comparisation	Plan 1	Plan 2
Next-generation protection	✓	✓
Attack surface reduction	✓	✓
Manual response actions	✓	✓
Centralized management	✓	✓
Security reports	✓	✓
APIs	✓	✓
Support for Windows 10, Windows 11, iOS, Android OS, and macOS devices	✓	✓
Device discovery		✓
Device inventory		✓
Core Defender Vulnerability Management capabilities		✓
Threat Analytics		✓
Automated investigation and response		✓
Advanced hunting		✓

MDE is an essential part of Defender for Server



Defender for Servers Plan 1

Defender for Servers Plan 2

Microsoft Defender for Endpoint Plan 2

MDE AV with existing AV solutions

- MS AV is per default available on devices running Win10/11 and WS2016/2019/2022
- Unified solution packages brings it also on WS2012 R2 in **Active** mode
- AV can be uninstalled via Powershell which is **not possible** when device is enrolled **for MDE**
- Which means using a Non-Microsoft AV solutions needs to set MS AV in passive mode for alls Windows Server versions

Configure passive mode for MS AV

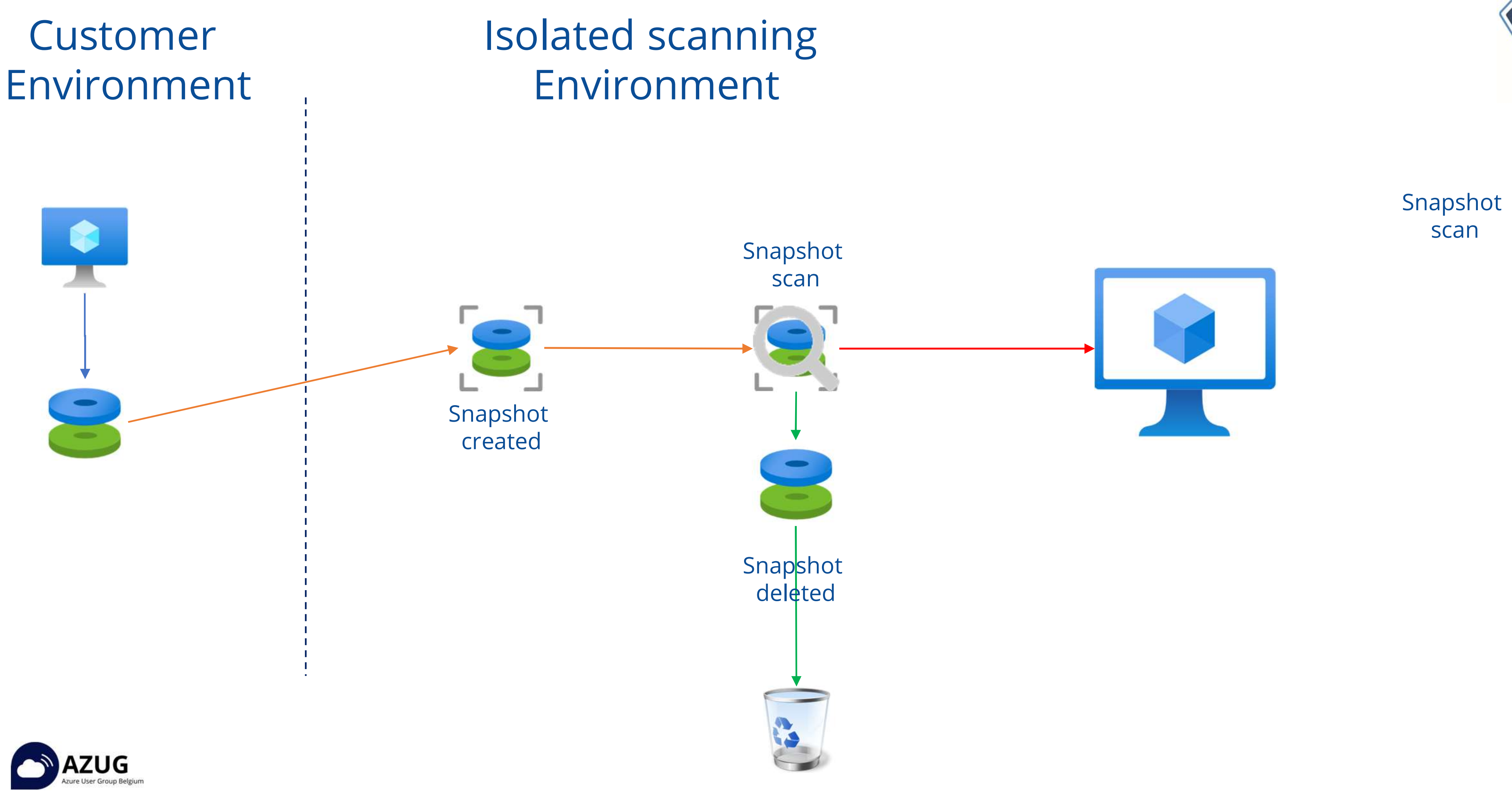
- Registry path: HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection
- Name: **ForceDefenderPassiveMode**
- Type: REG_DWORD
- Value: 1

Passive mode works on WS2012R2/2016 only when device is enrolled in MDE

New Defender features

Agentless scanning for VMs

How Agentless scanning works



Customer Environment

Isolated scanning Environment

Snapshot scan

Snapshot scan

Snapshot created

Snapshot deleted

Why agentless scanning for VMs?

Securing servers that are not onboarded in Defender for Endpoint

Because Policy is not run / or access to the VM for installing additional software

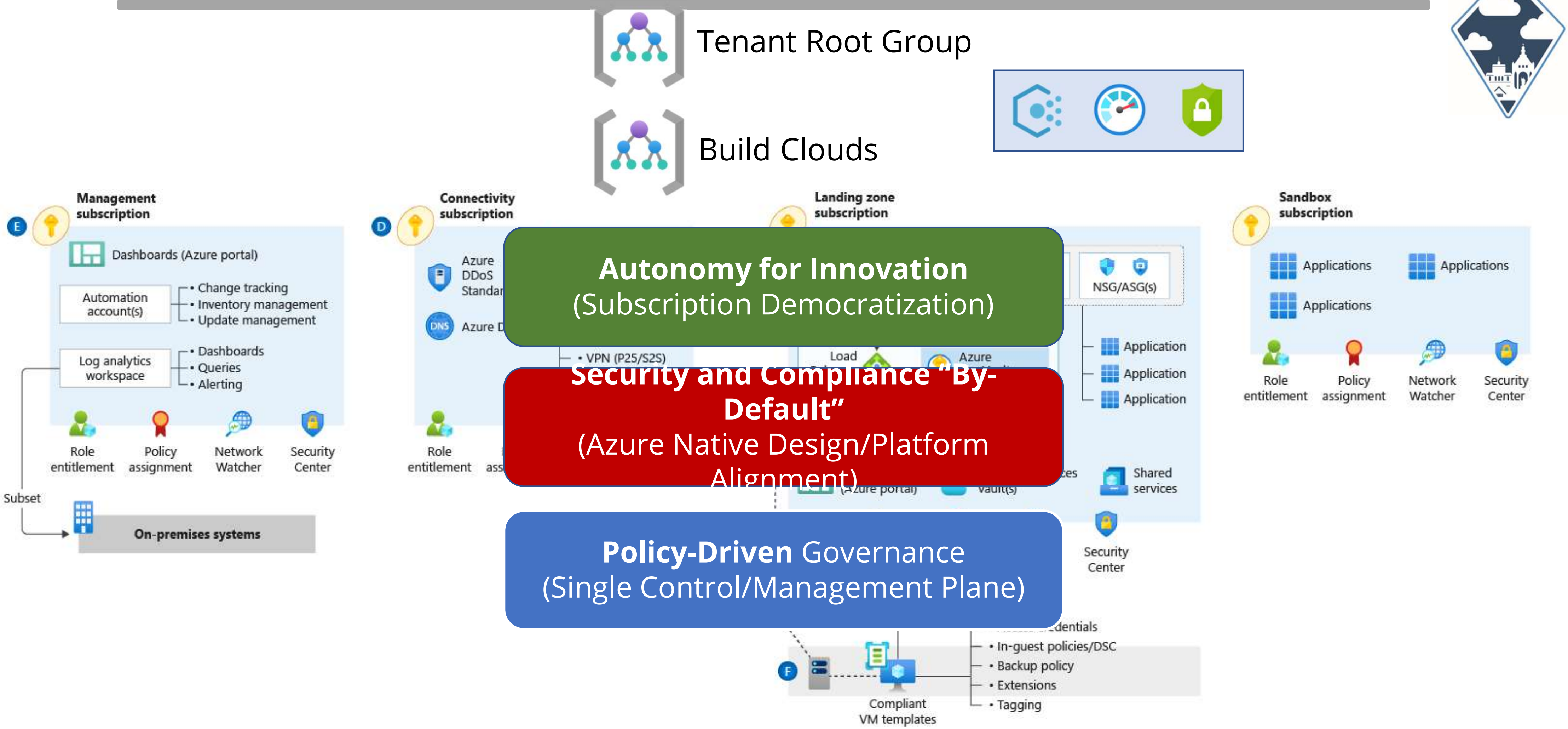
No performance impact

Security team does not depend on workload owners

Agentless scanning for VMs

- Available in Defender for **CSPM** or Defender for Servers **Plan 2**
- Available for Windows and Linux OS
- Instance types:
    - Azure: Standard VMs, VMSS
    - AWS: EC2 and Autoscale instances
- Encryption
    - Azure: Unencrypted and Encrypted (managed disk with PMK – **actual no CMK support**)
    - AWS: Unencrypted and Encrypted (PMK and CMK)

Deployment at Scale

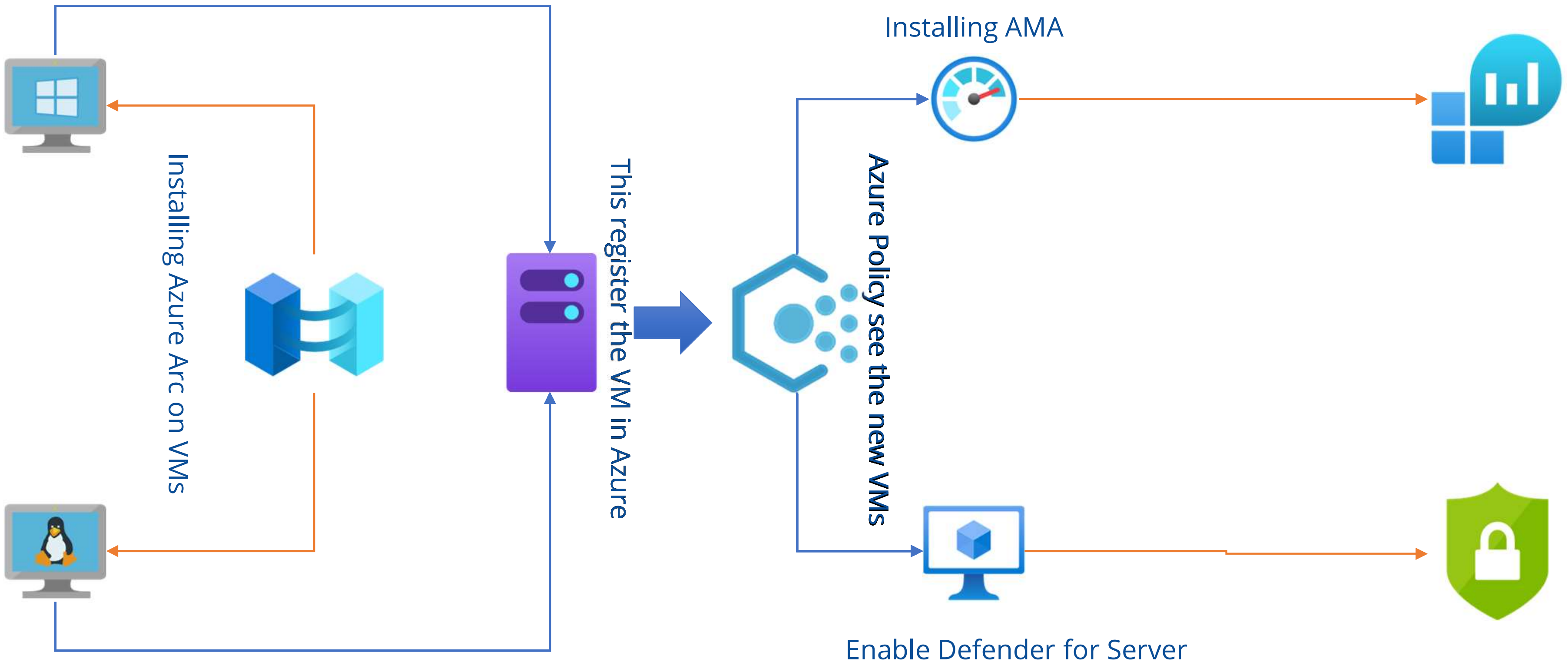


Autonomy for Innovation
(Subscription Democratization)

Security and Compliance "By-Default"
(Azure Native Design/Platform Alignment)

Policy-Driven Governance
(Single Control/Management Plane)

Deployment at Scale


Installing AMA
Installing Azure Arc on VMs
This register the VM in Azure
Azure Policy see the new VMs
Enable Defender for Server

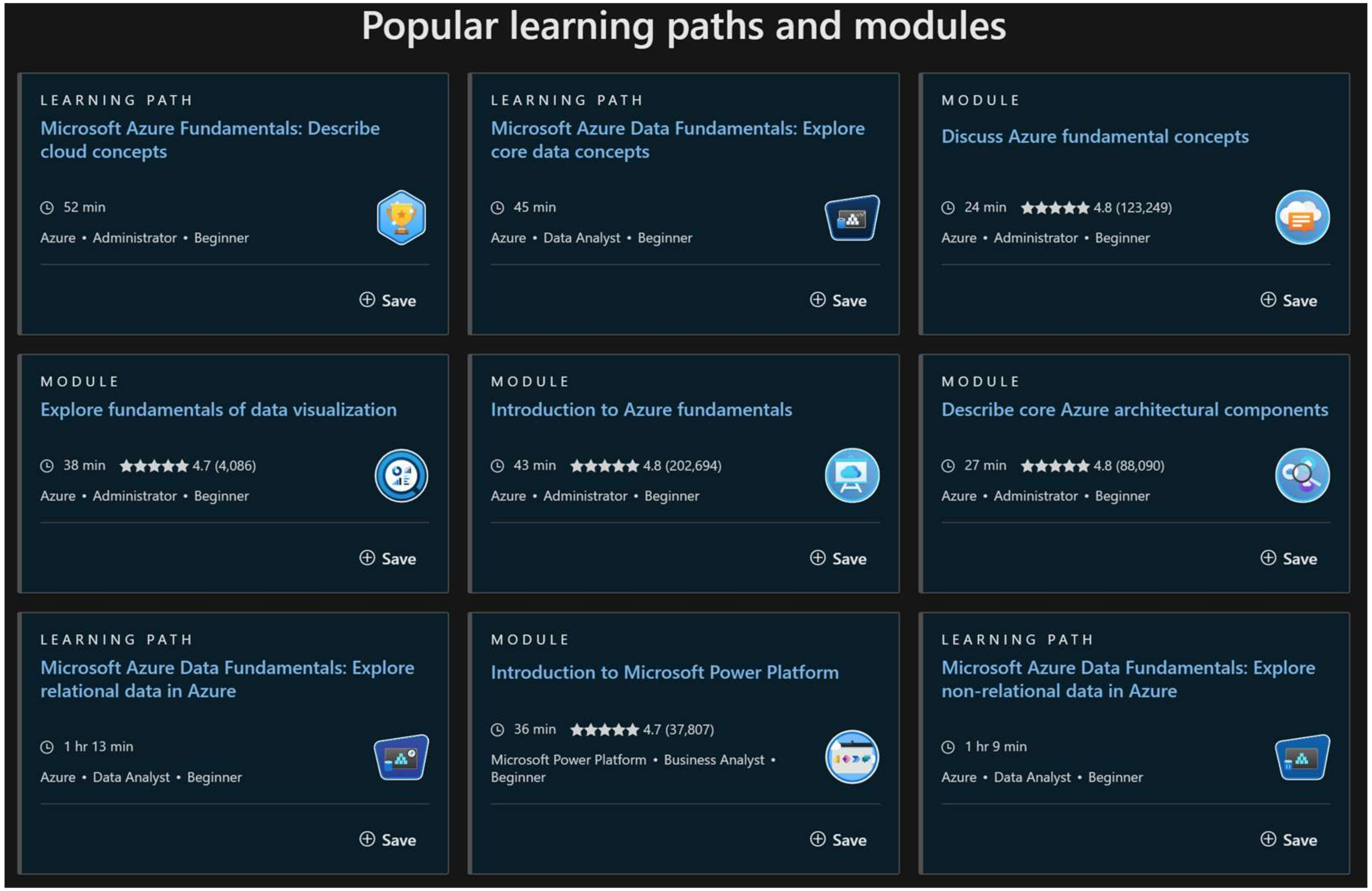
- Deploy Microsoft Defender for Endpoint agent on Windows virtual machines
- Deploy Microsoft Defender for Endpoint agent on Windows Azure Arc machines
- Deploy Microsoft Defender for Endpoint agent on Linux hybrid machines
- Deploy Microsoft Defender for Endpoint agent on Linux virtual machines

Deployment at Scale

- Change from MMA to AMA and to the USP are important for scalable deployment
- Now the full solution are integrated into Azure Arc
- For scalable deployment over different environments (On-Prem, AWS, etc.) Azure Arc is important
- Azure Arc integrates the VMs inside the Azure Controle plane
- From there Azure Policy see the VMs and integrate them inside the Defender for Cloud environment

Learning

Training | Microsoft Learn



Popular learning paths and modules

LEARNING PATH
Microsoft Azure Fundamentals: Describe cloud concepts
52 min
Azure • Administrator • Beginner
Save

LEARNING PATH
Microsoft Azure Data Fundamentals: Explore core data concepts
45 min
Azure • Data Analyst • Beginner
Save

MODULE
Discuss Azure fundamental concepts
24 min ★★★★★ 4.8 (123,249)
Azure • Administrator • Beginner
Save

MODULE
Explore fundamentals of data visualization
38 min ★★★★★ 4.7 (4,086)
Azure • Administrator • Beginner
Save

MODULE
Introduction to Azure fundamentals
43 min ★★★★★ 4.8 (202,694)
Azure • Administrator • Beginner
Save

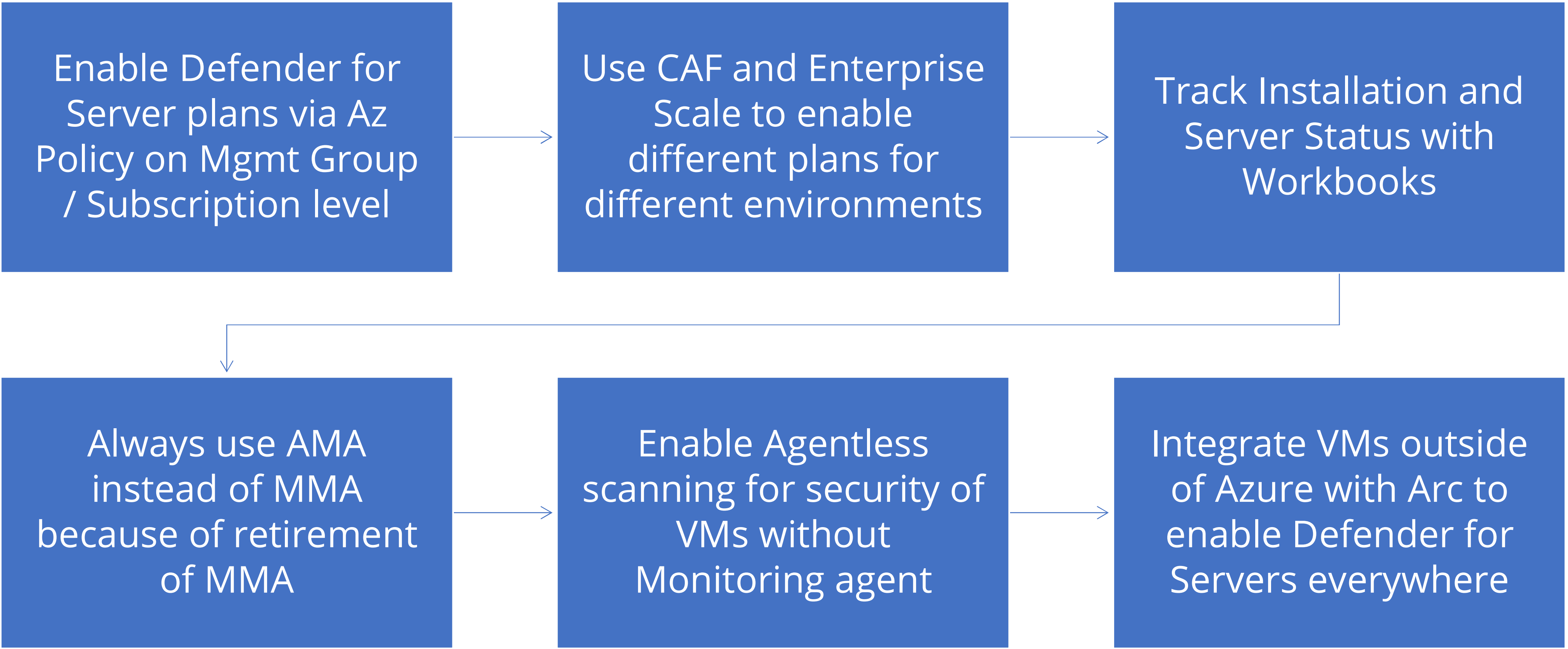
MODULE
Describe core Azure architectural components
27 min ★★★★★ 4.8 (88,090)
Azure • Administrator • Beginner
Save

LEARNING PATH
Microsoft Azure Data Fundamentals: Explore relational data in Azure
1 hr 13 min
Azure • Data Analyst • Beginner
Save

MODULE
Introduction to Microsoft Power Platform
36 min ★★★★★ 4.7 (37,807)
Microsoft Power Platform • Business Analyst • Beginner
Save

LEARNING PATH
Microsoft Azure Data Fundamentals: Explore non-relational data in Azure
1 hr 9 min
Azure • Data Analyst • Beginner
Save

Join Our Security Community - Microsoft Tech Community



Enable Defender for Server plans via Az Policy on Mgmt Group / Subscription level

Use CAF and Enterprise Scale to enable different plans for different environments

Track Installation and Server Status with Workbooks

Always use AMA instead of MMA because of retirement of MMA

Enable Agentless scanning for security of VMs without Monitoring agent

Integrate VMs outside of Azure with Arc to enable Defender for Servers everywhere

Future information

- Plan Defender for Servers data residency and workspaces | Microsoft Learn
- GitHub - Azure/Microsoft-Defender-for-Cloud: Welcome to the Defender for Cloud community repository
- Microsoft Defender PoC Series – Defender CSPM - Microsoft Community Hub
- Onboard Windows servers to the Microsoft Defender for Endpoint service | Microsoft Learn
- Microsoft Defender for Endpoint | Microsoft Learn
- Microsoft Defender for Endpoint: Defending Windows Server 2012 R2 and 2016
- We're retiring the Log Analytics agent in Azure Monitor on 31 August 2024 | Azure updates
- https://aka.ms/CVEDashboard
- Microsoft Defender Antivirus compatibility with other security products | Microsoft Learn
- Agentless scanning of cloud machines using Microsoft Defender for Cloud | Microsoft Learn
- Workbooks/Defender for Endpoint Deployment Status · MS-Defender-for-Cloud · GitHub
- Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
- Join Our Security Community - Microsoft Community Hub
- Security Copilot with Microsoft Intune Early Access Program | Microsoft Intune Blog
- Microsoft Defender for Endpoint - Streamline device connectivity
- Defender-for-Cloud/Policy/Enable Defender for Servers plans at main · Azure/Defender-for-Cloud (github.com)

Azure Meetup
BONN
www.azurebonn.de

Thank You

Cloud Inspires Podcast
Stories and people behind Cloud Transformation
www.cloudinspires.me

- @GregorReimling
- Gregor Reimling

AZUG
Azure User Group Belgium

Enjoy the conference!

#CloudBrew

AZUG
Azure User Group Belgium