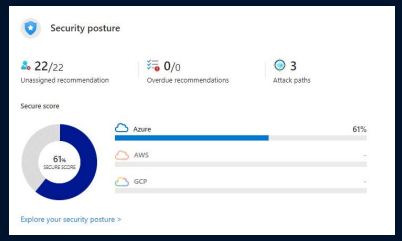
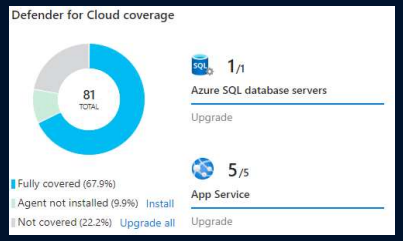
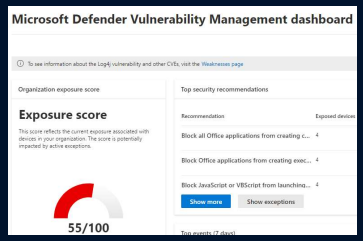
nic Cloud Connect

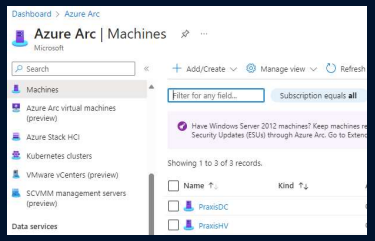
Mastering Defender for Servers

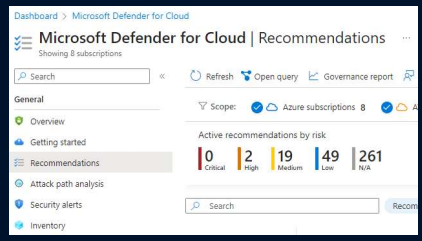
by Gregor Reimling











About “Gregor Reimling”

Azure Meetup BONN

www.azurebonn.de

Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

https://www.Reimling.eu

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

www.cloudinspires.me

Certifications

Cloud Security Architect, MVP for MS Azure & Security

Hobbies

Family, Community, Worldtraveler

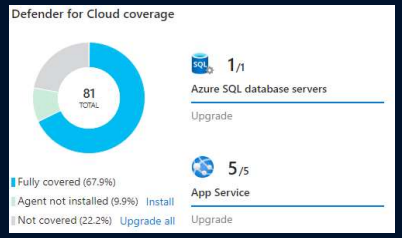
Contact

@GregorReimling

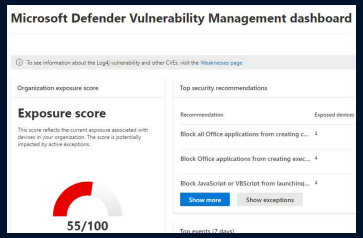
@CloudInspires

nic Cloud Connect

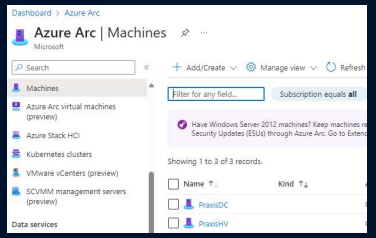
Defender for Cloud Overview



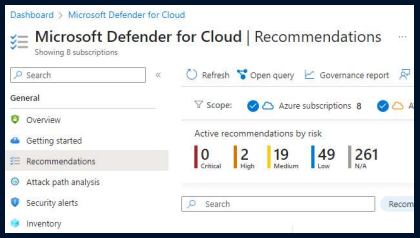
Defender for Server



Defender for Endpoint

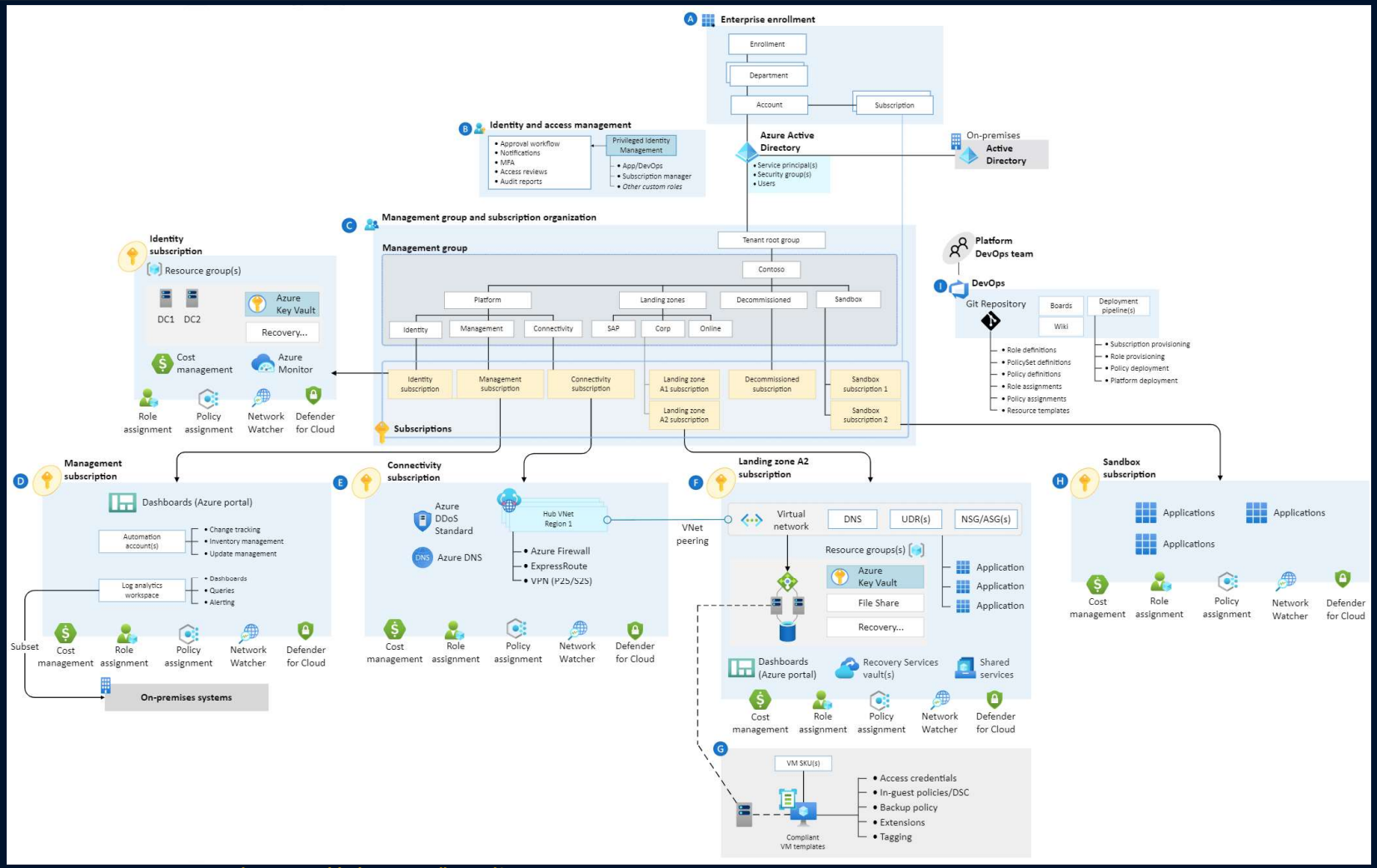


Multicloud Capabilities



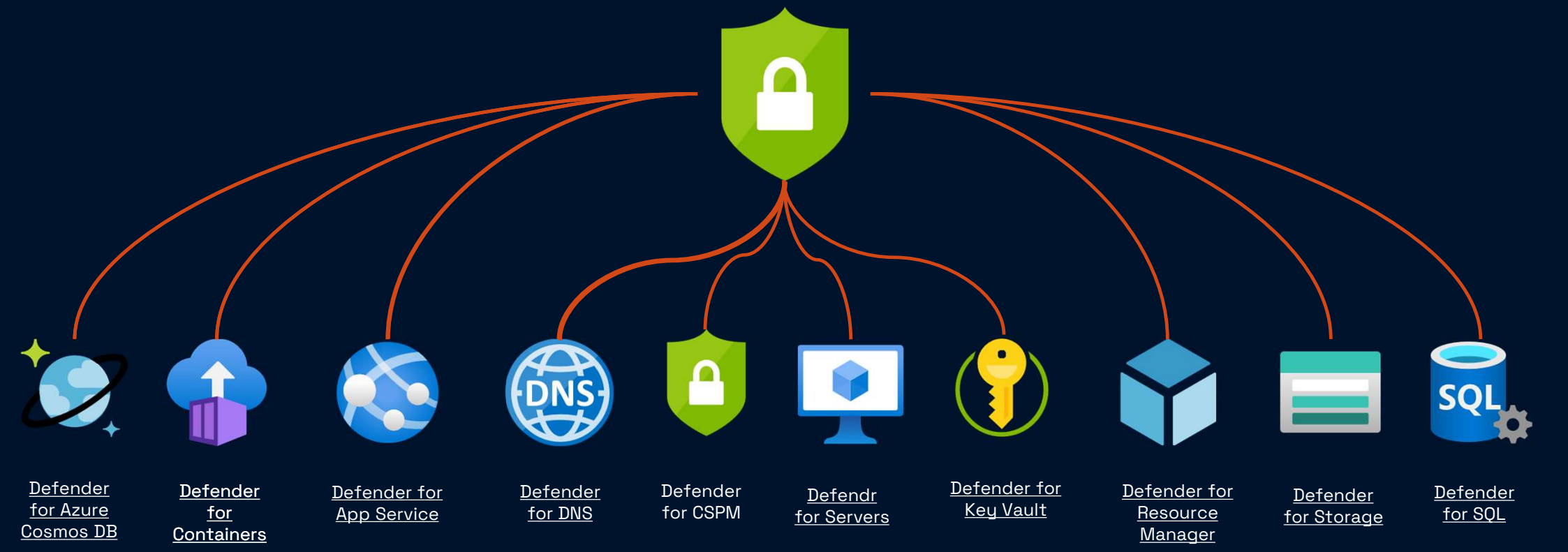
New Defender features

Enterprise Scale



https://aka.ms/landingzones

Microsoft Defender for Cloud



Defender for Azure Cosmos DB

Defender for Containers

Defender for App Service

Defender for DNS

Defender for CSPM

Defendr for Servers

Defender for Key Vault

Defender for Resource Manager

Defender for Storage

Defender for SQL

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

Why Defender for Servers?

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	✓

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

[Design your Microsoft Sentinel workspace architecture | Microsoft Learn]

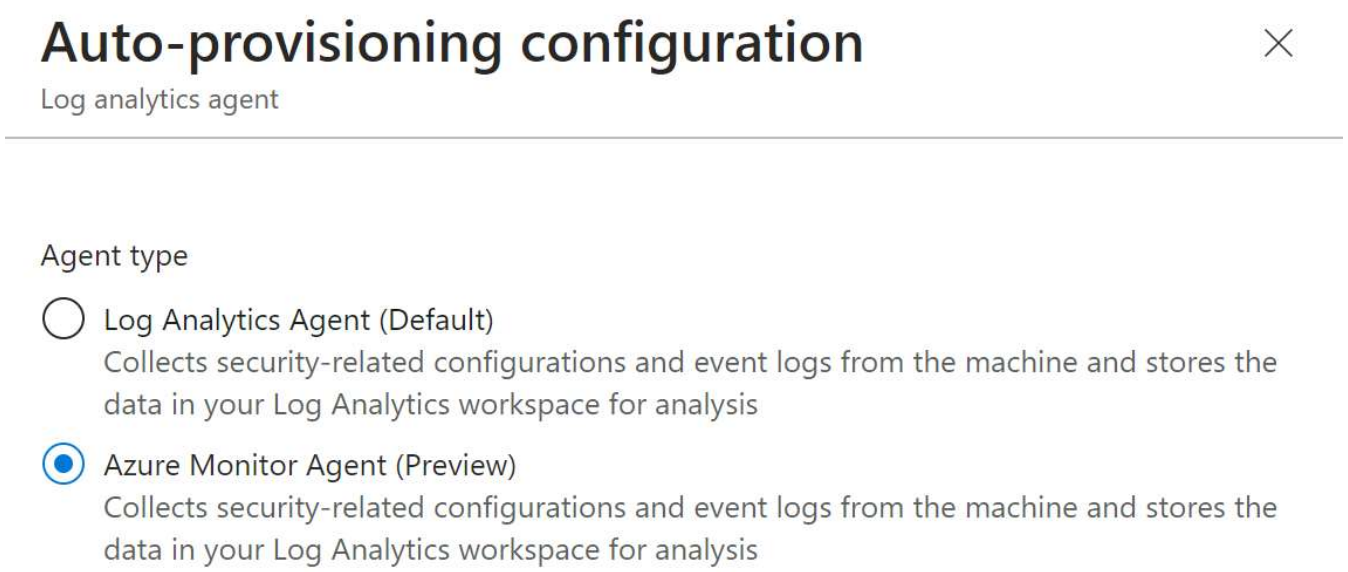
Considerations for activation of Defender for Server

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

Auto-provisioning configuration

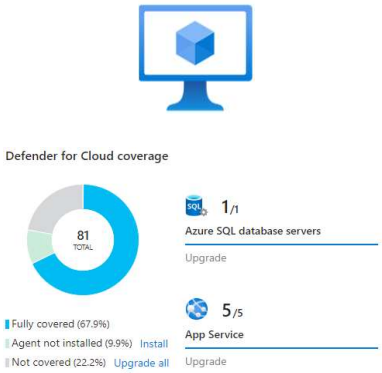


- Switch from MMA to AMA does not uninstall the MMA-agent
  - Duplicate agents results in doubled events or recommendations and appear twice in Defender
- Monitoring workbook – AMA migration tracker workbook

Timeline

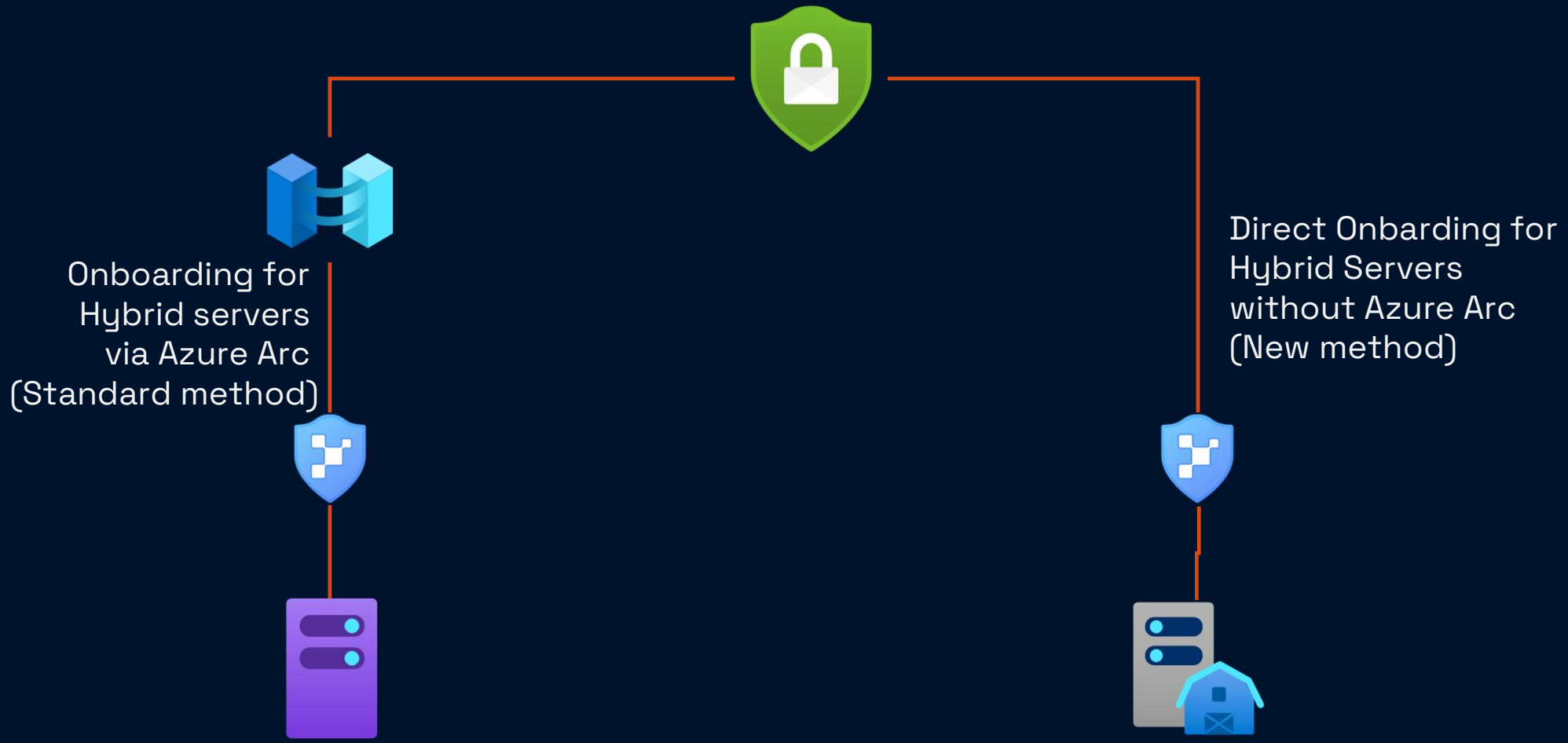
Sep	Oct	Nov	Dec	Jan	Feb	Mar	April	May	June	July	Aug
Previous implementation (before April of 2022) uses MMA for WS2012/WS2016											
				MMA will be retired on 31 August 2024							
				all Defender for Servers features and capabilities currently relying on Log Analytics Agent (MMA) will be deprecated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

Demo Defender for Server



Defender
for Server

Hybrid Server Onboarding (Azure Arc)



Hybrid Server Onboarding

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

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
    - However, Plan 2 requires some features of AMA and AMA is only supported via Azure Arc
- 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

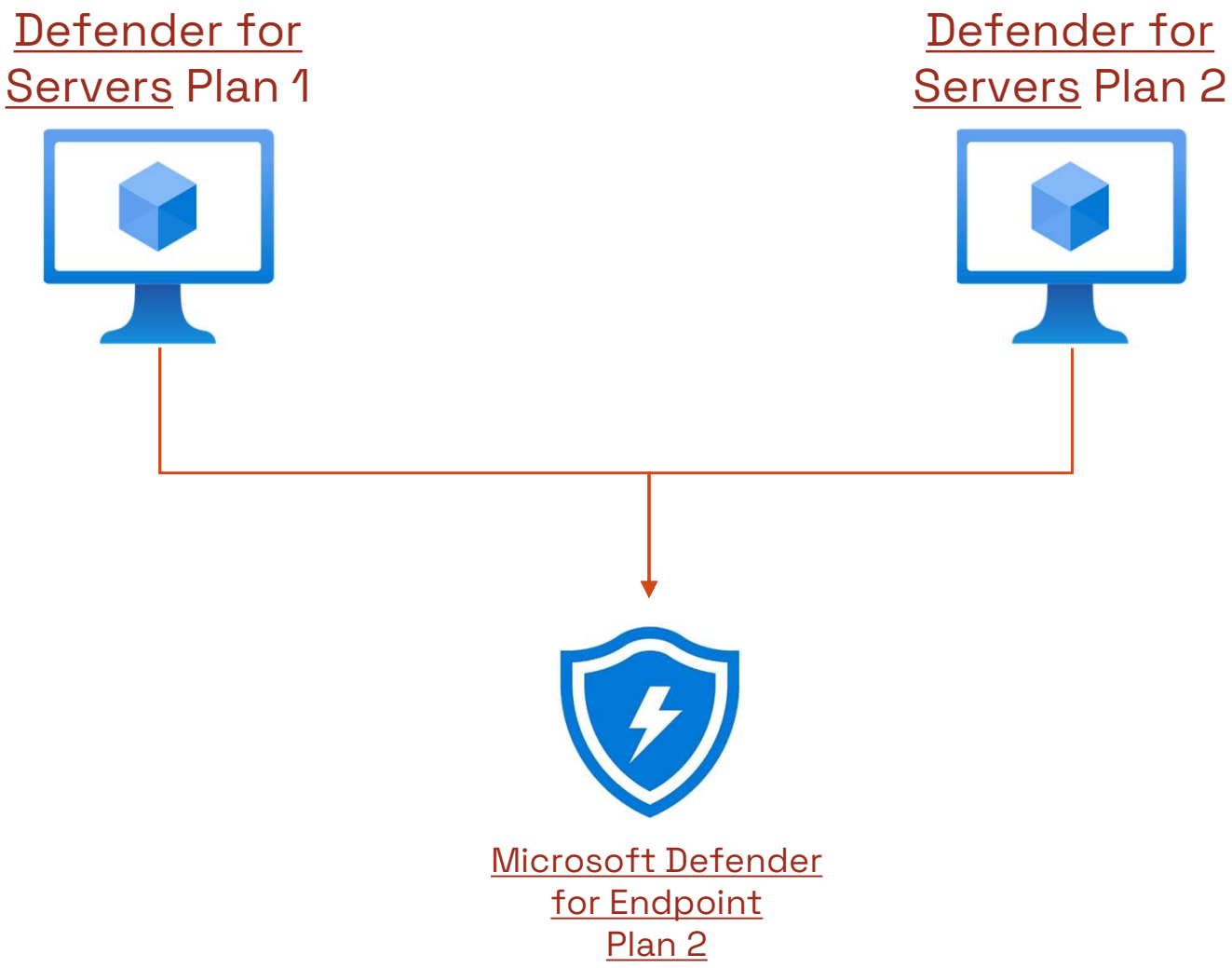
nic Cloud Connect

Defender for Endpoint

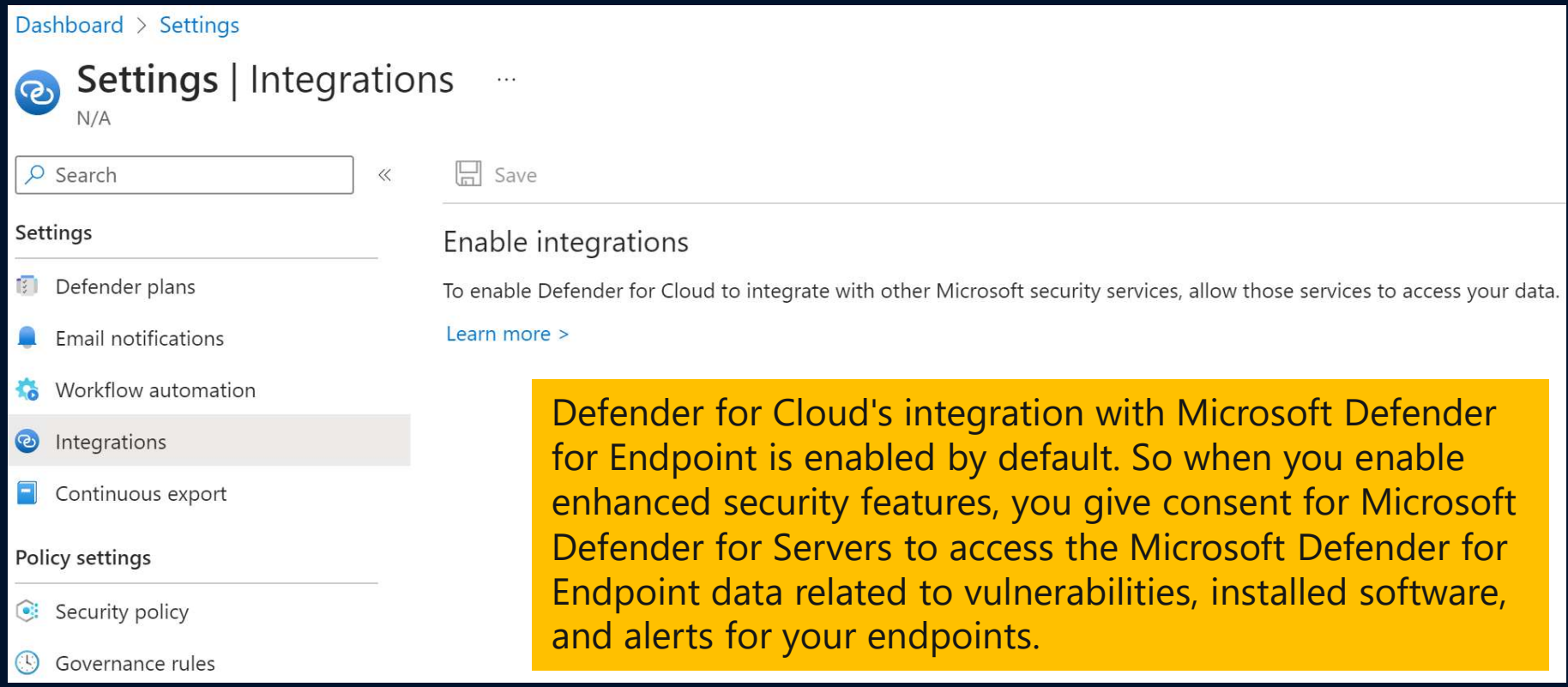
Defender for Endpoint Plan comparisation

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



MS Defender for Endpoint (MDE)



MDE

- Defender for Endpoint protects Windows and Linux machines
- In Azure or with Azure Arc everywhere (Multicloud capability)
- Contains
    - **Advanced post-breach detection sensors**
    - **Vulnerability assessment from Microsoft Defender Vulnerability Management**
    - **Analytics-based, cloud-powered, post-breach detection**
    - **Threat intelligence**
    - **Automated onboarding**
    - **Single pane of glass**
- How MMA will be affected by MDE
    - Installing unified, modern solution (MDE) MMA will no longer be used
    - But MMA stay as is and will work together with other connected workspaces

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

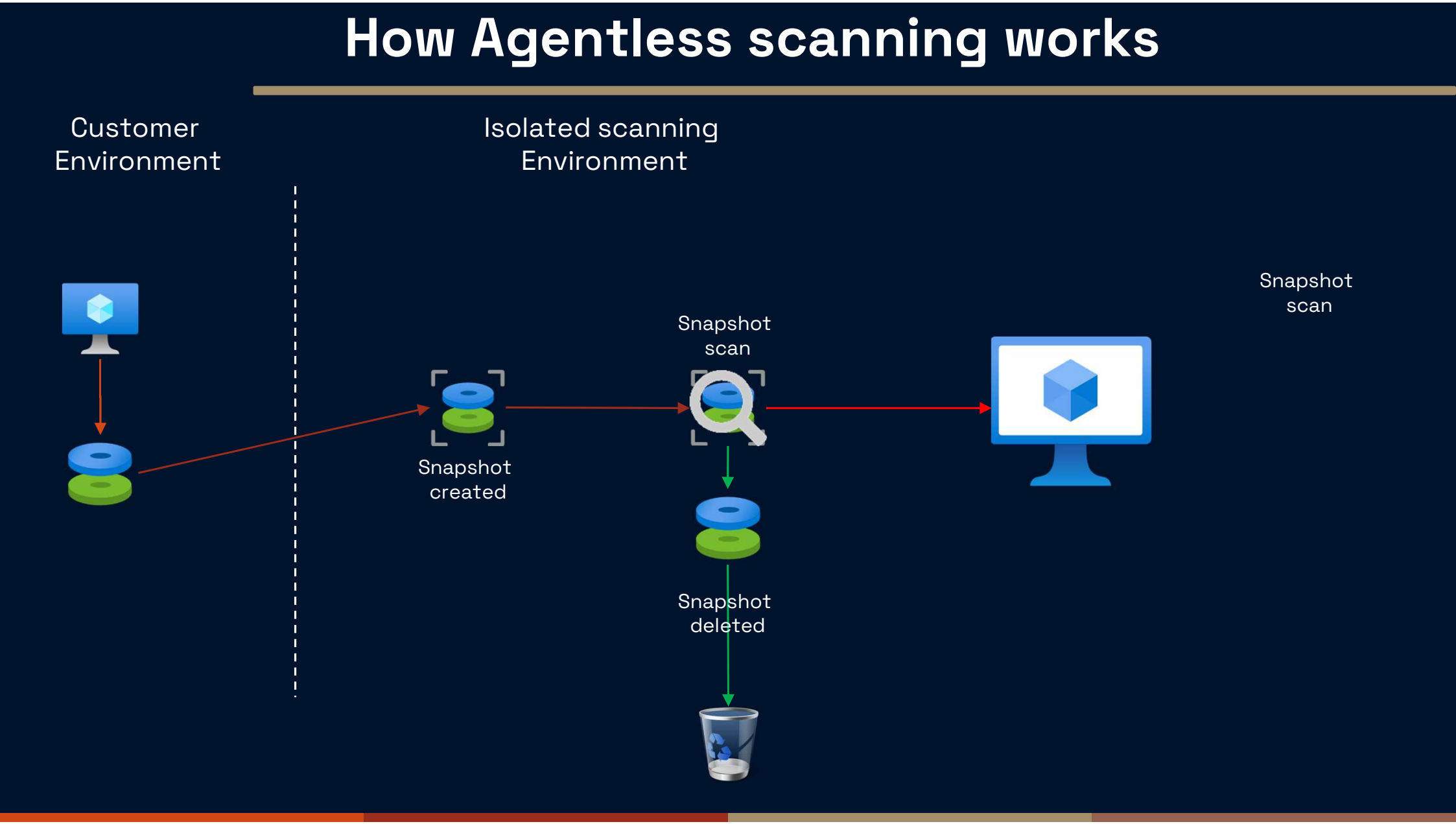
Agentless scanning for VMs

How Agentless scanning works

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)

How Agentless scanning works



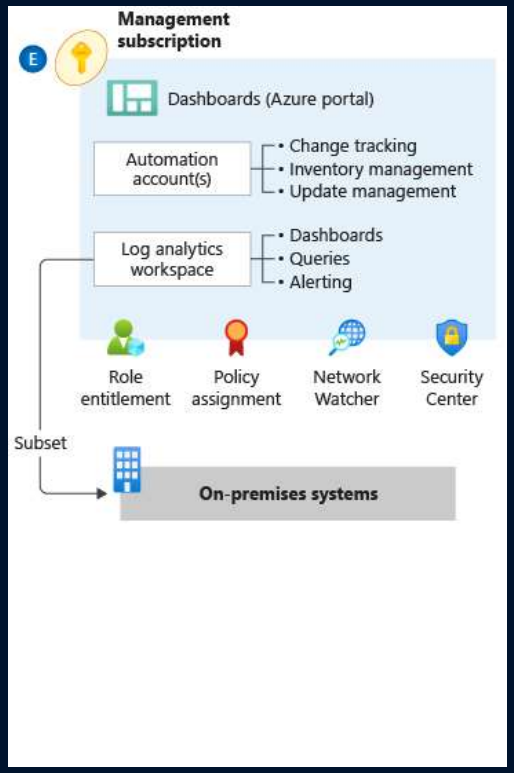
Why agentless scanning for VMs?

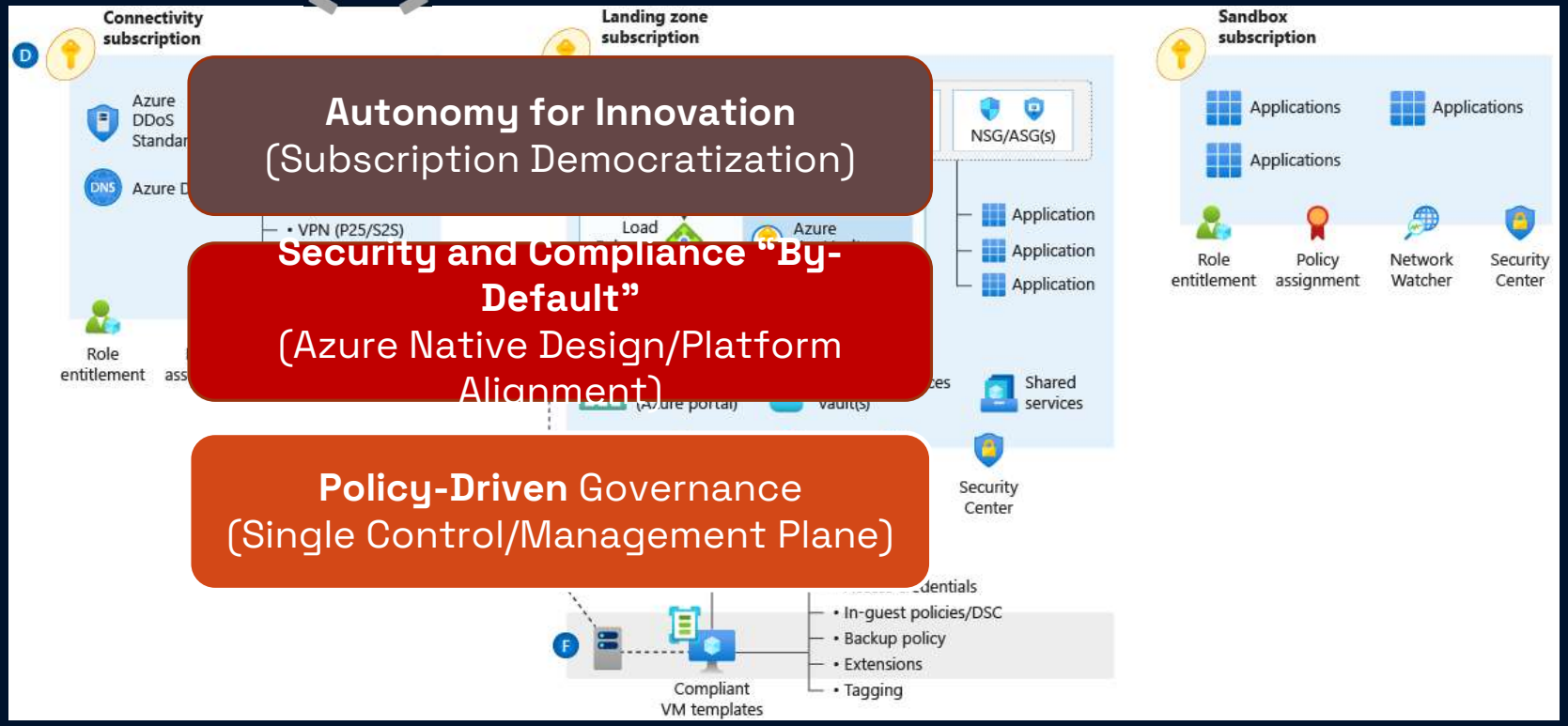
- Securing servers that are not onboarded in Defender for Endpoint
    - Because Policy is not run / o access to the VM for installing additional software
- No performance impact
- Security team does not depend on workload owners

Deployment at Scale

Tenant Root Group

Build Clouds



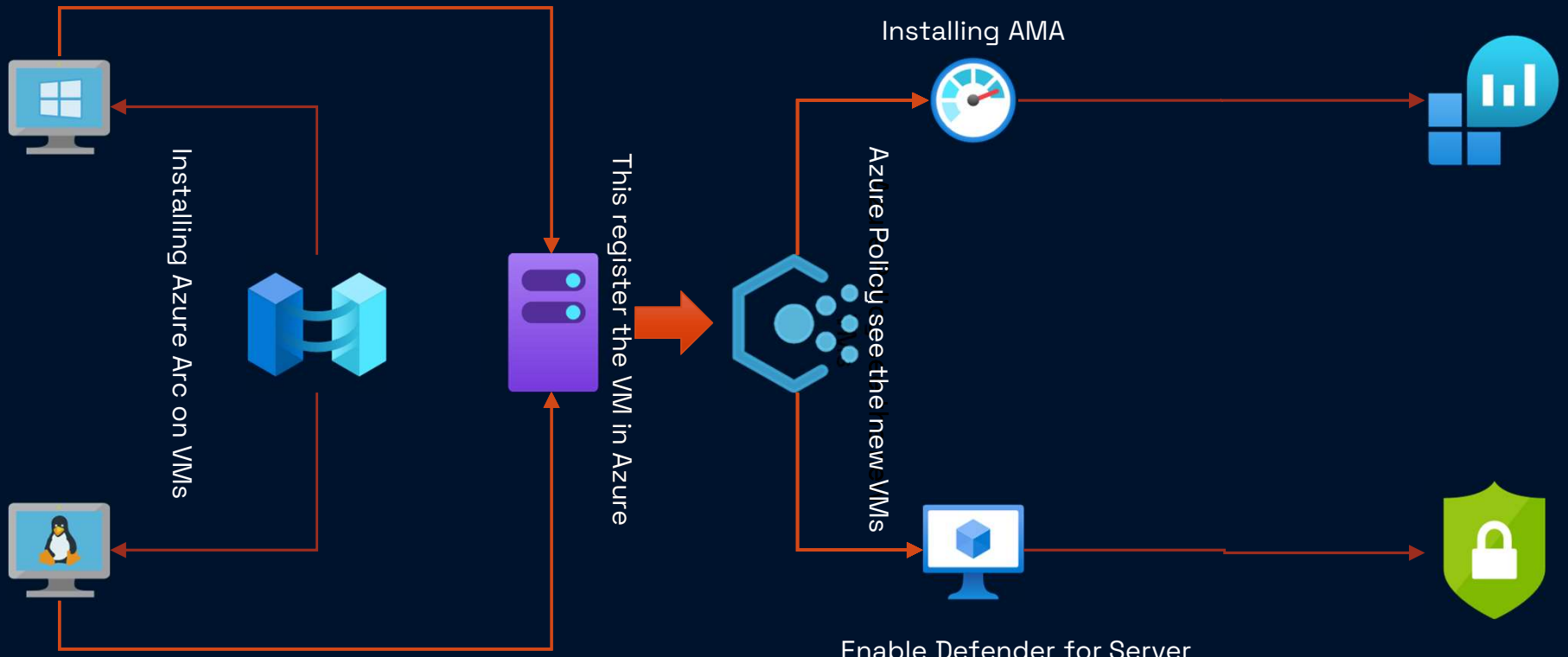


Autonomy for Innovation
(Subscription Democratization)

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

Policy-Driven Governance
(Single Control/Management Plane)

Deployment at Scale

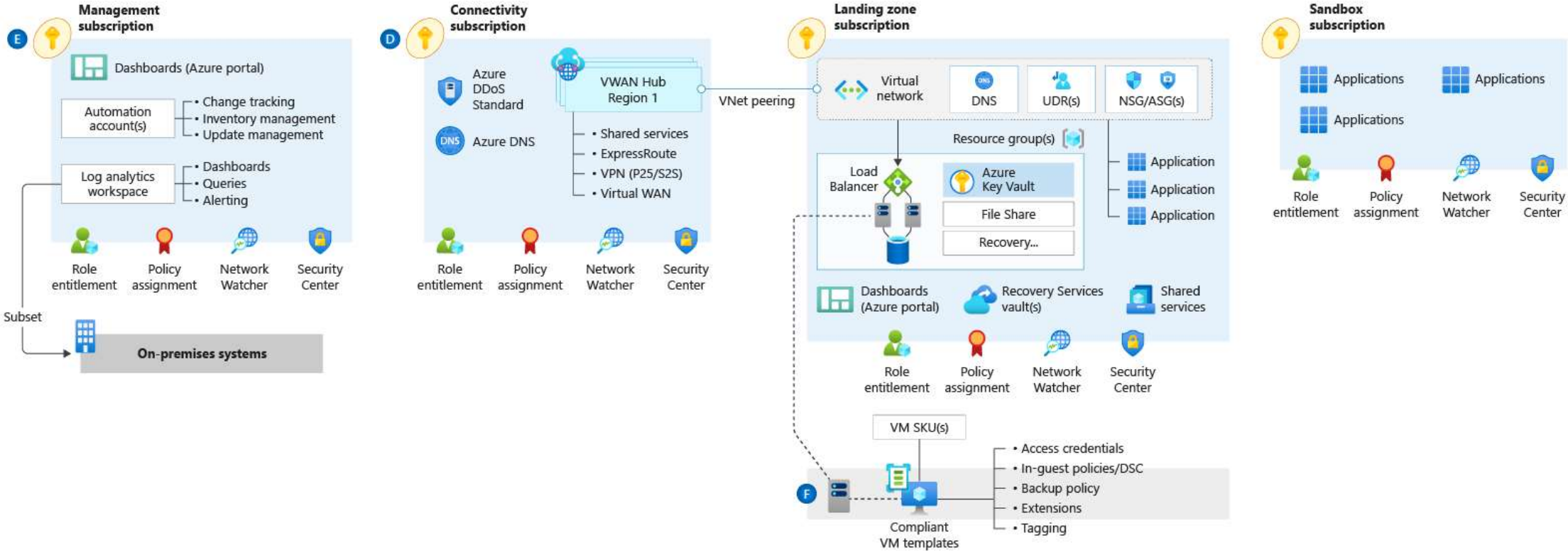


- Deploy Microsoft Defender for Endpoint agent on Windows virtual machines
- Deploy Microsoft Defender for Endpoint agent on Windows Azure Arc machines
- Deploy Microsoft Defender for Endpoint agent on Linux hybrid machines
- Deploy Microsoft Defender for Endpoint agent on Linux virtual machines

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

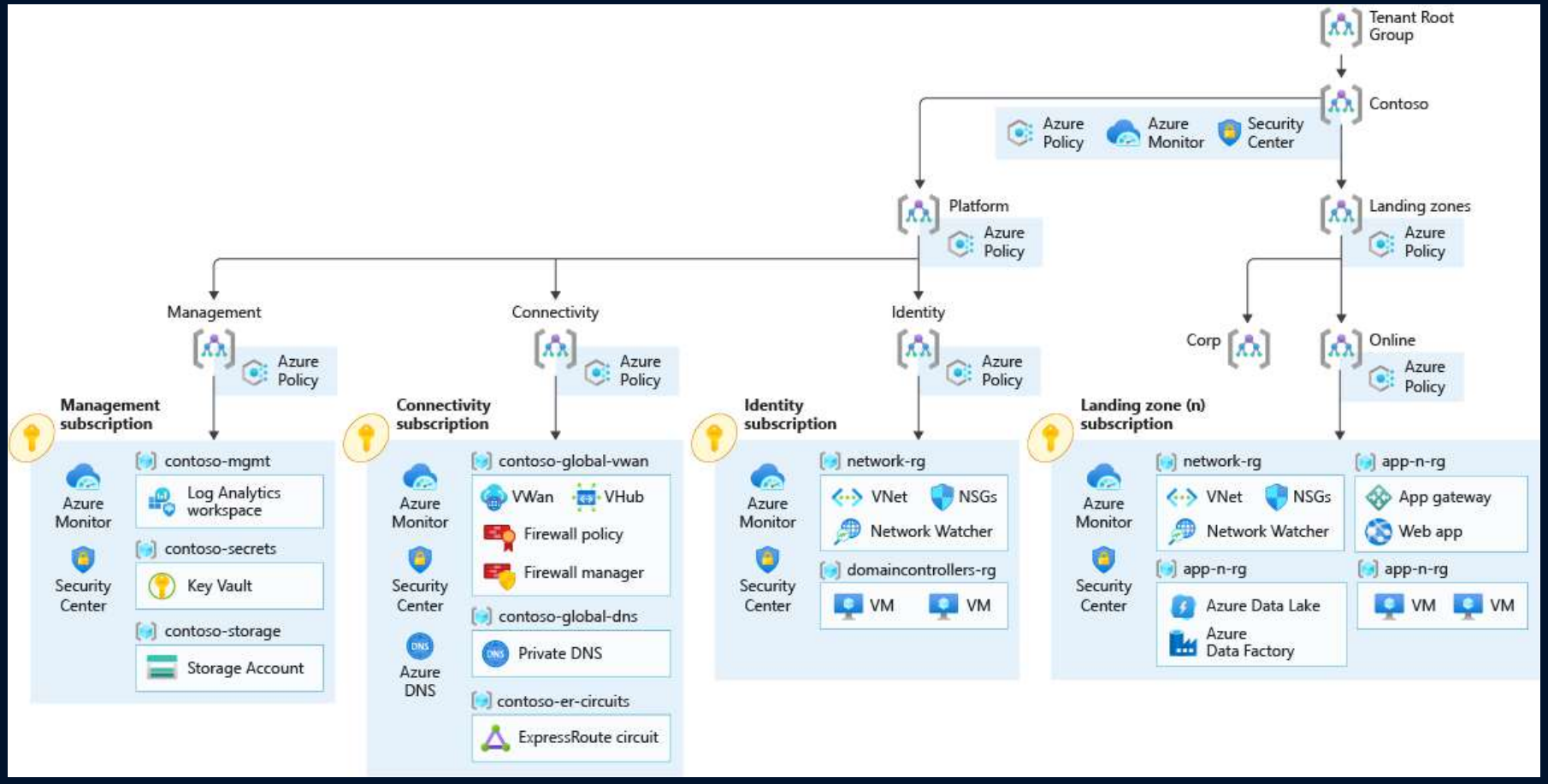
Enterprise-Scale Design Principles



Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

GitHub Enterprise Scale Templates

Deploy Enterprise-Scale with Azure VWAN



GitHub - Azure/Enterprise-Scale: The Azure Landing Zones (Enterprise-Scale) architecture provides prescriptive guidance coupled with Azure best practices, and it follows design principles across the critical design areas for organizations to define their Azure architecture

Learning

Training | Microsoft Learn

Join Our Security Community - Microsoft Tech Community

Microsoft Cybersecurity Reference Architectures (MCRA)

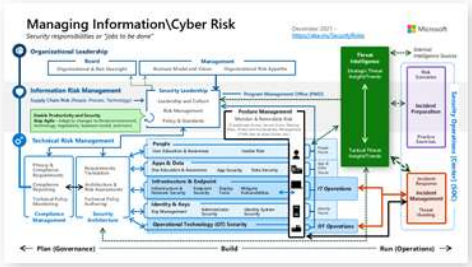
Capabilities

What cybersecurity capabilities does Microsoft have?

Build Slide

People

How are roles & responsibilities evolving with cloud and zero trust?



Zero Trust User Access

How to validate trust of user/devices for all resources?

Azure Native Controls

What native security is available?

Security Operations

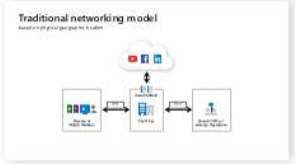
How to enable rapid incident response?

Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?

Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?



Attack Chain Coverage

How does this map to insider and external attacks?

Build Slide

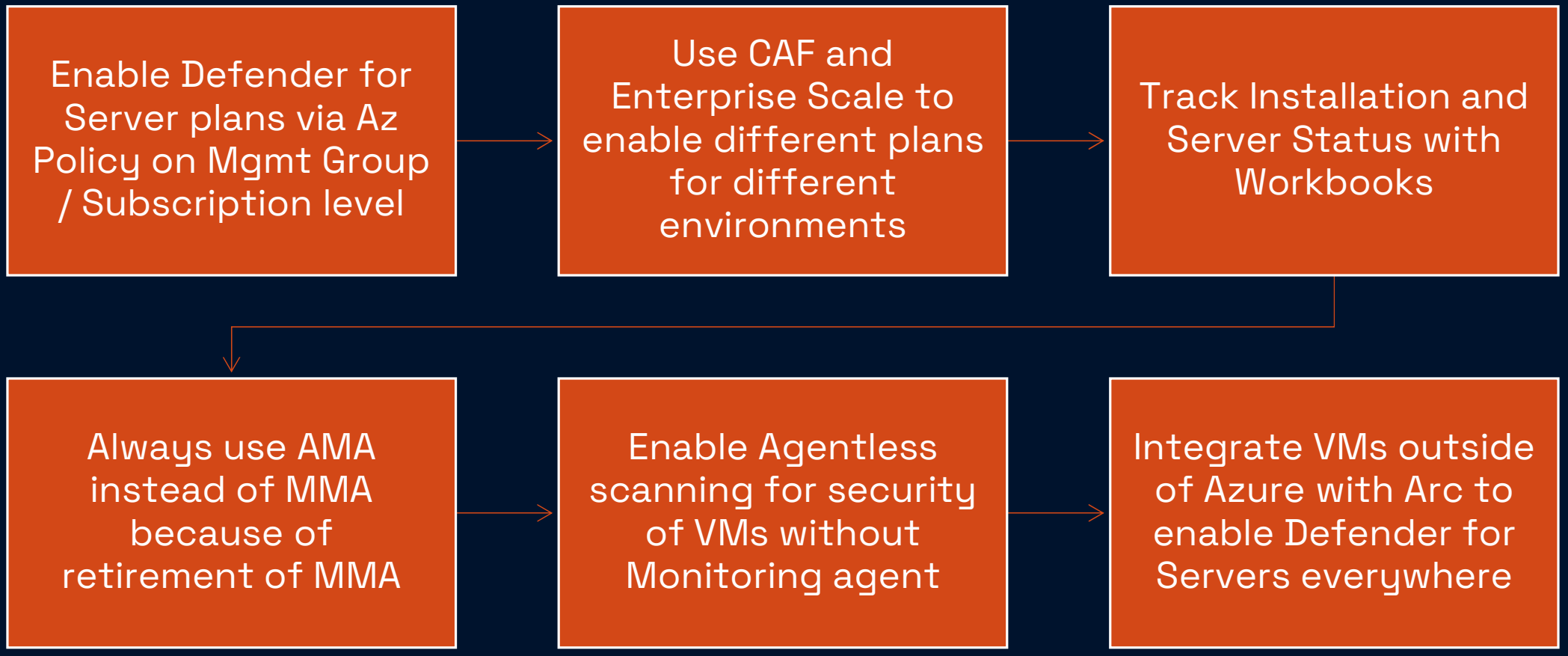
Operational Technology

How to enable Zero Trust Security for OT?

aka.ms/MCRA | December 2021 | Microsoft

Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

Abstract


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 Microsoft 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
- Microsoft-Defender-for-Cloud/Policy/Enable Defender for Servers plans at main · Azure/Microsoft-Defender-for-Cloud [github.com]

Thank You

Azure Meetup BONN

www.azurebonn.de

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

www.cloudinspires.me

Blog

https://www.Reimling.eu

Contact

- @GregorReimling
- Gregor Reimling