Mastering Defender for Servers

Gregor Reimling

Experts Live Netherlands

About "Gregor Reimling"

Azure Meetup BONN

www.azurebonn.de

Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

https://www.Reimling.eu

Certifications

Cloud Security Architect, MVP for MS Azure

Hobbies

Family, Community, Worldtraveler

Contact

@GregorReimling

@CloudInspires

www.cloudinspires.me

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC


CLOUD IDENTITY
SUMMIT '23
Thu, September 7th, 2023
Deep-Dive and Q&A sessions on #AzureAD
Hybrid Event in Bonn, Germany
www.identitysummit.cloud
Follow us on Twitter:
@identitysummit
Azure Meetup
BONN
regeka
INSPARK
Partner Network
PATCH MY PC
PINK
YDENTIC

Agenda

Defender for Cloud

Defender for Server

Log Analytics Workspace

Defender for Endpoint

Agentless scanning

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Topics of this Session

MMA

MCSB

MDE

AV

USP

CWPP

ES

CSPM

CNAA

EDR

AMA

CAF

ASC

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Defender for Cloud

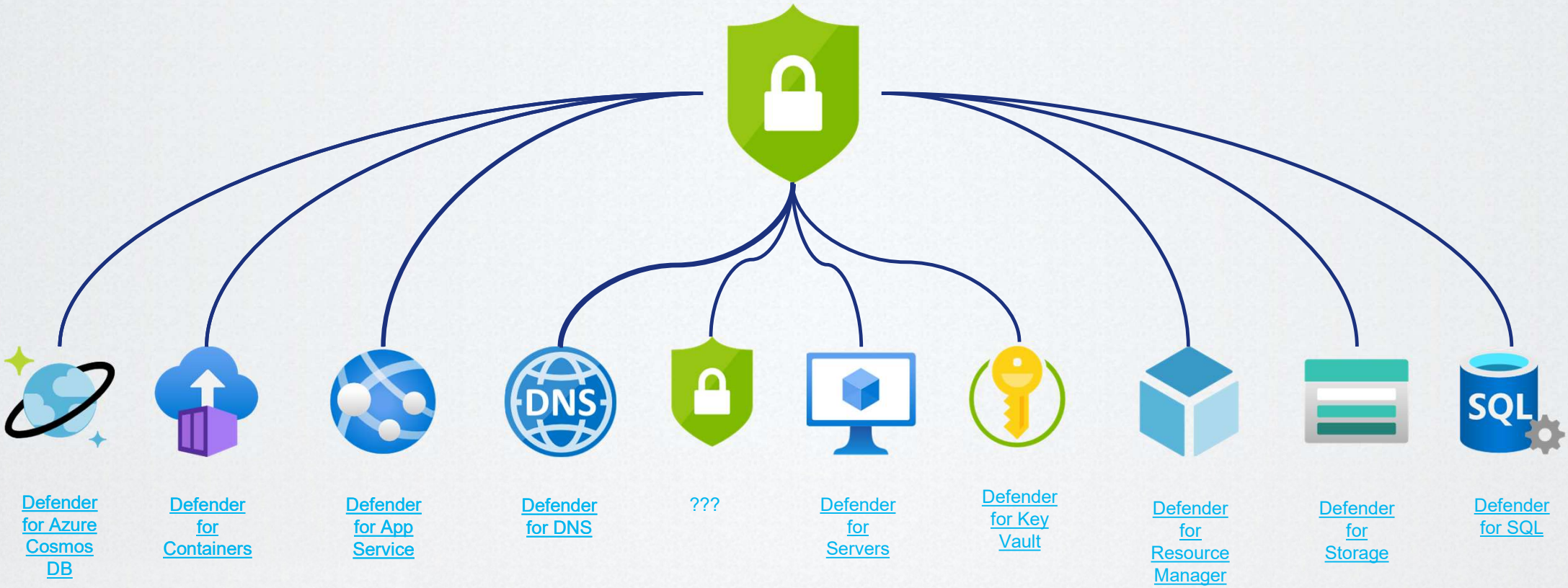
Overview

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

cegeka INSPARK Partner Network PATCH MY PC YDENTIC

Microsoft Defender for Cloud



Defender for Azure Cosmos DB

Defender for Containers

Defender for App Service

Defender for DNS

???

Defender for Servers

Defender for Key Vault

Defender for Resource Manager

Defender for Storage

Defender for SQL

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Which is new plan is available since end of March?

Defender for CSPM

Cloud Security Posture Management

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Defender for CSPM

Features	Foundational CSPM	Defender for CSPM
Security recommendations to fix misconfigurations	✓	✓
Asset inventory	✓	✓
Secure score	✓	✓
Data exporting	✓	✓
Workflow automation	✓	✓
Tools for remediation	✓	✓
Microsoft Cloud Security Benchmark	✓	✓
Governance		✓
Regulatory compliance		✓
Cloud security explorer		✓
Attack path analysis		✓
Agentless scanning for machines		✓
Agentless discovery for Kubernetes		✓
Data aware security posture		✓

Defender for CSPM Pricing

- GA since end of March
- Billing starts on **Aug 1 2023**
- **Billable** workloads will be VMs, Storage Accounts, OSS DBs, & SQL PaaS & Servers on VMs
- Price $15 per **billable** resource/month

Current Defender for Cloud Customer	Automatic Discount	Defender CSPM Price
Defender for Servers P2	25%	$11.25/ Compute or Data workload / month
Defender for Containers	10%	$13.50/ Compute or Data workload / month
Defender for DBs / Defender for Storage	5%	$14.25/ Compute or Data workload / month

Defender for Servers

Plan overview

Defender for Servers Plans

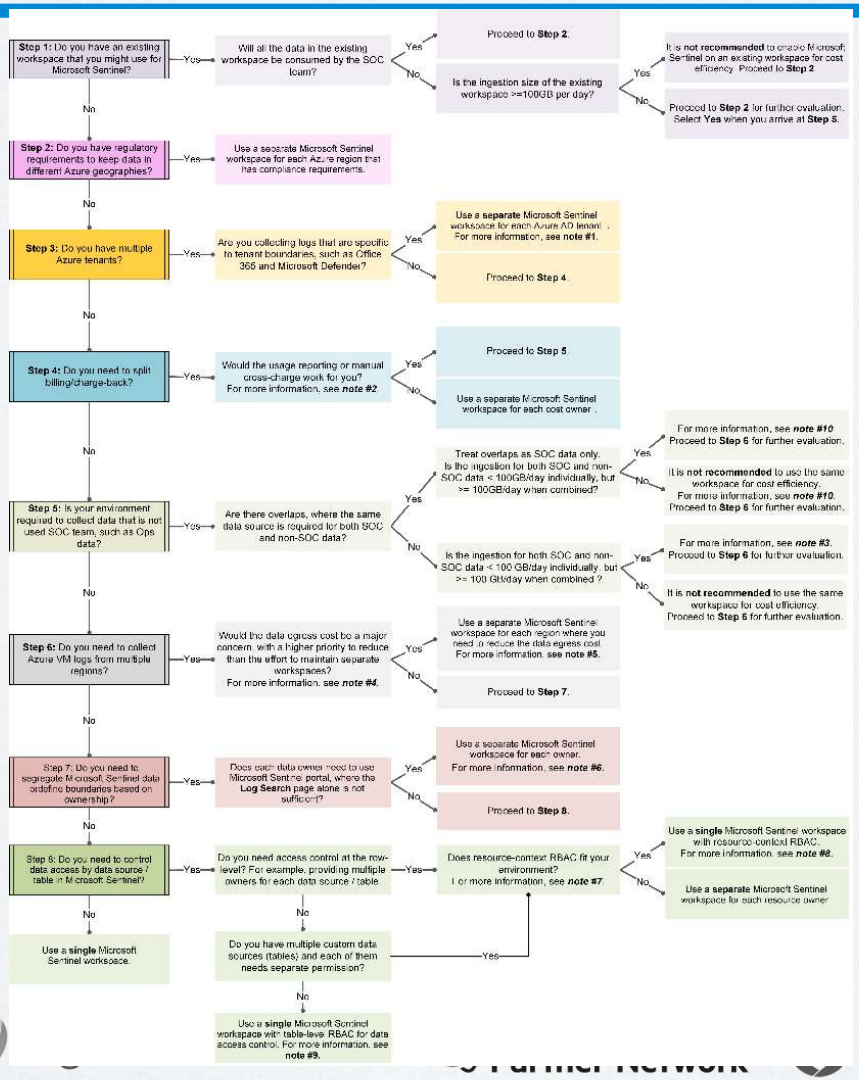
	Plan 1	Plan 2
Unified View	✓	✓
Automatic MDE provisioning	✓	✓
MS Threat and Vulnerability management	✓	✓
Security Policy and Regulatory Compliance		✓
Integrated Vulnerability by Qualys		✓
Log Analytics 500MB free data ingestion per day		✓
Threat detection		✓
Adaptive application control		✓
File integrity monitoring		✓
Just-in-Time VM access		✓
Adaptive Network hardening		✓
Docker host hardening		✓
Fileless attack detection		✓
Price	5$ per Server	15$ per Server

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

MS Defender for Endpoint

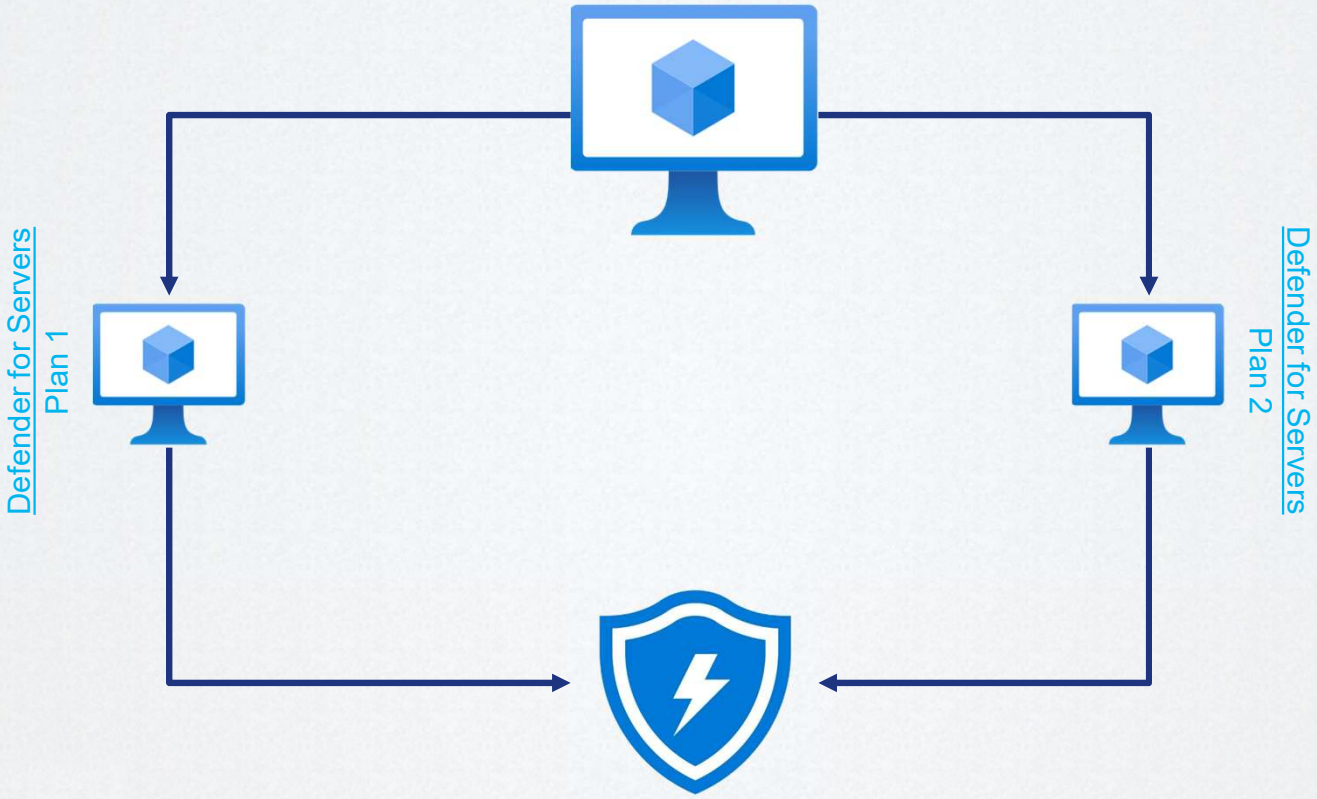
Introduction to MDE

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Defender for Endpoint plan overview

	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		✓
Price	5$ per Server	15$ per Server

Defender for Servers and MDE

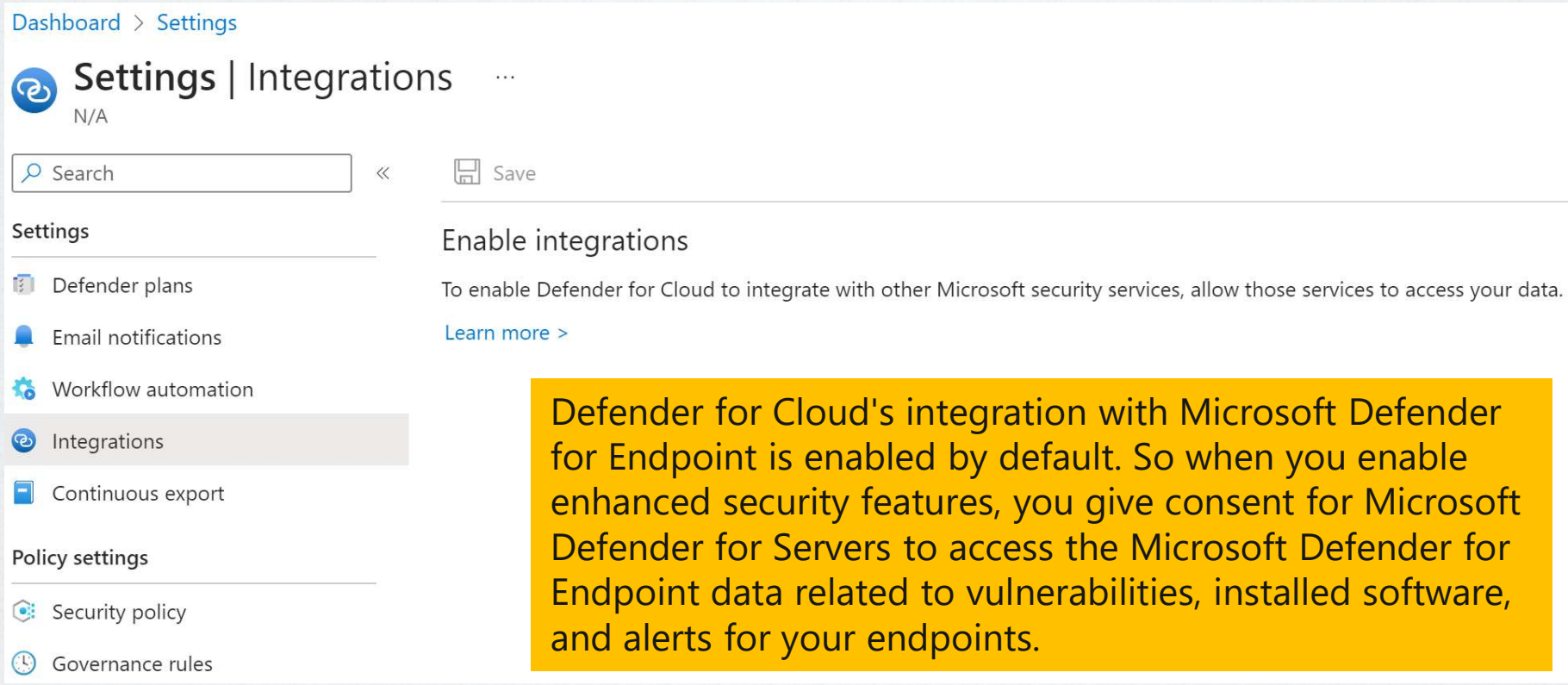


cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Activation of Defender for Servers

- 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

MS Defender for Endpoint (MDE)



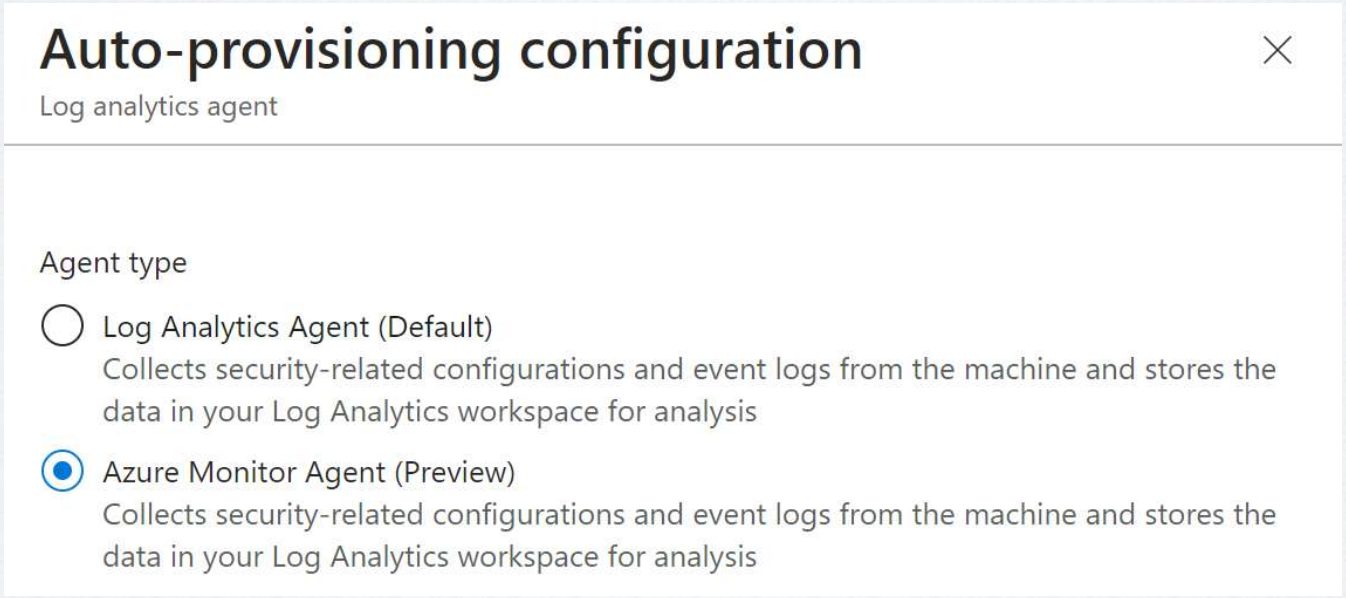
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Windows Server onboarding

- Previous implementation (before April of 2022) uses MMA for WS2012/WS2016
- New solution(Unified Agent integration) does not use or require the MMA
- Please note **MMA will be retired on 31 August 2024**
- New Unified Solution packages standardizes the capabilities and functionality
    - Installs AV (Anti Virus) and EDR (Endpoint Detection and Response) sensor

Server version	AV	EDR
WS2012 R2 SP1	USP	USP
WS2016	Built-in	USP
WS2019	Built-in	Built-in

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

Question

If an agent reports to multiple workspaces, am I charged twice?

Yes

No

If a machine reports to multiple workspaces and all of them have Defender for Servers enabled, the machines are billed for each attached workspace.

MMA vs AMA

	AMA	MMA
Environments	Azure Other Cloud & On-Prem via Arc	Azure Other Cloud & On-prem
Events per second (EPS)	5K	1K
Events	All security events Common Minimal Custom	All security events Common Minimal None
Support for file-based logs	Yes	No
Support for DCR (Data Collection Rules)	Yes	No

- Monitoring workbook – AMA migration tracker workbook

AMA Migration Tracker Workbook

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

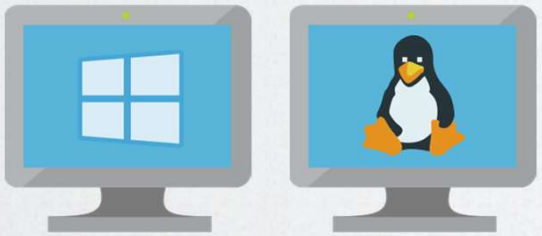
MDE AV with existing AV solutions

- 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

Defender for Endpoint integration



Agentless scanning for VMs

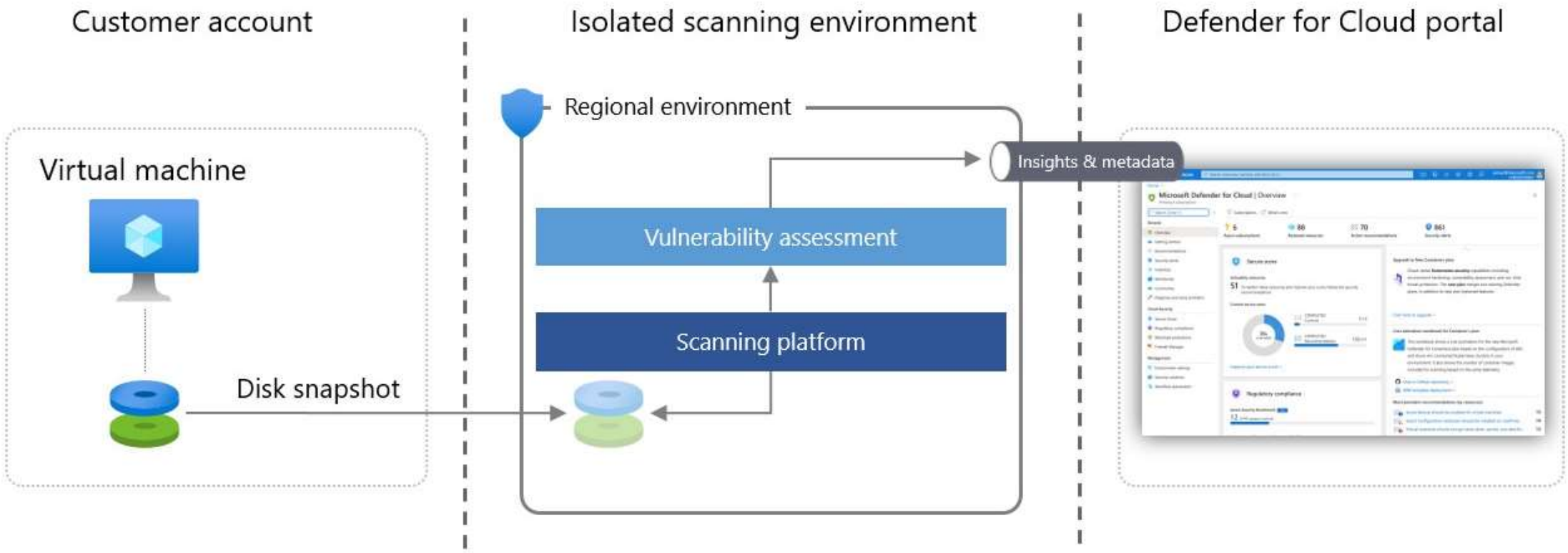
How Agentless scanning works

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

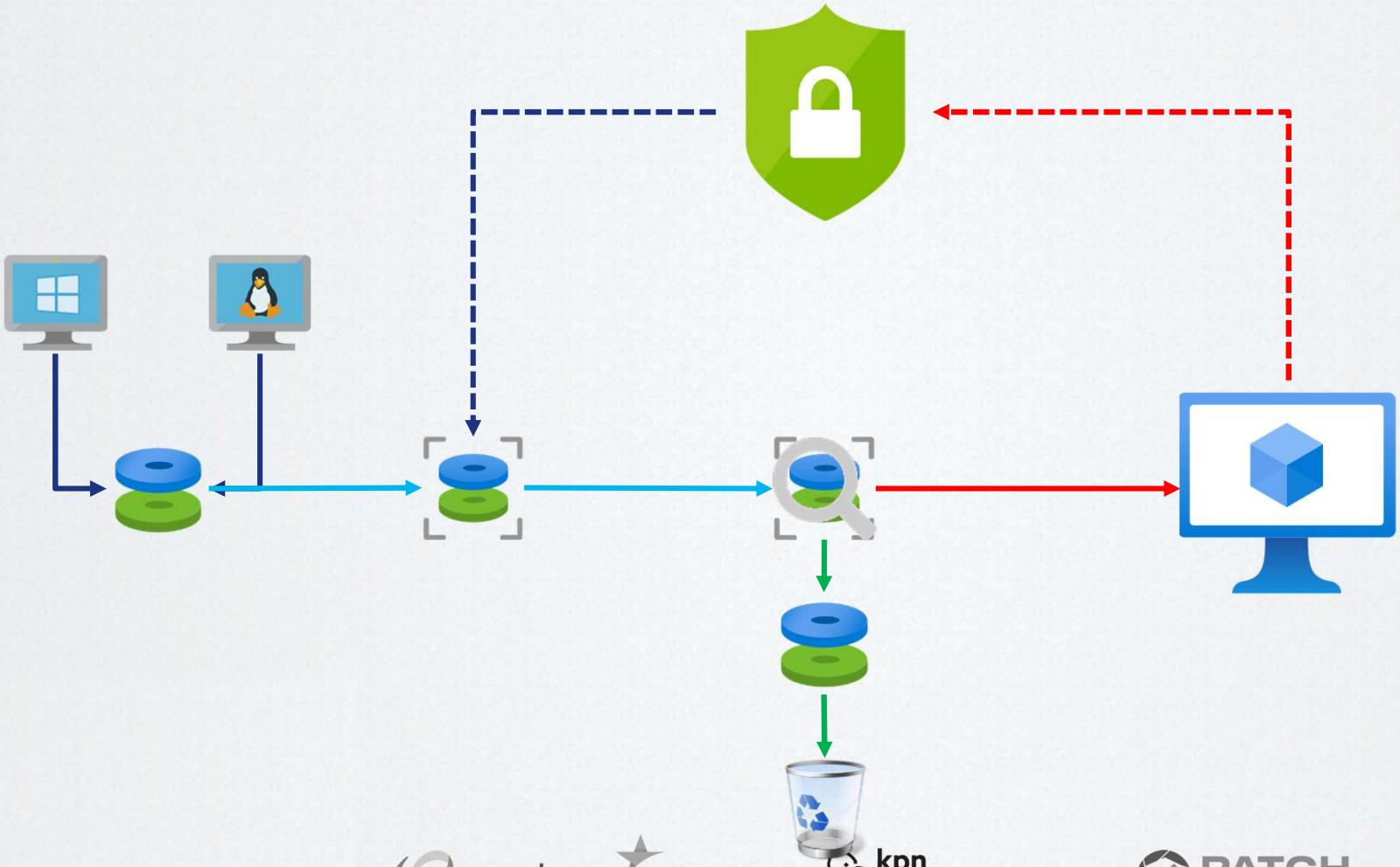
Agentless scanning for VMs

- 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



How Agentless scanning works



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

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

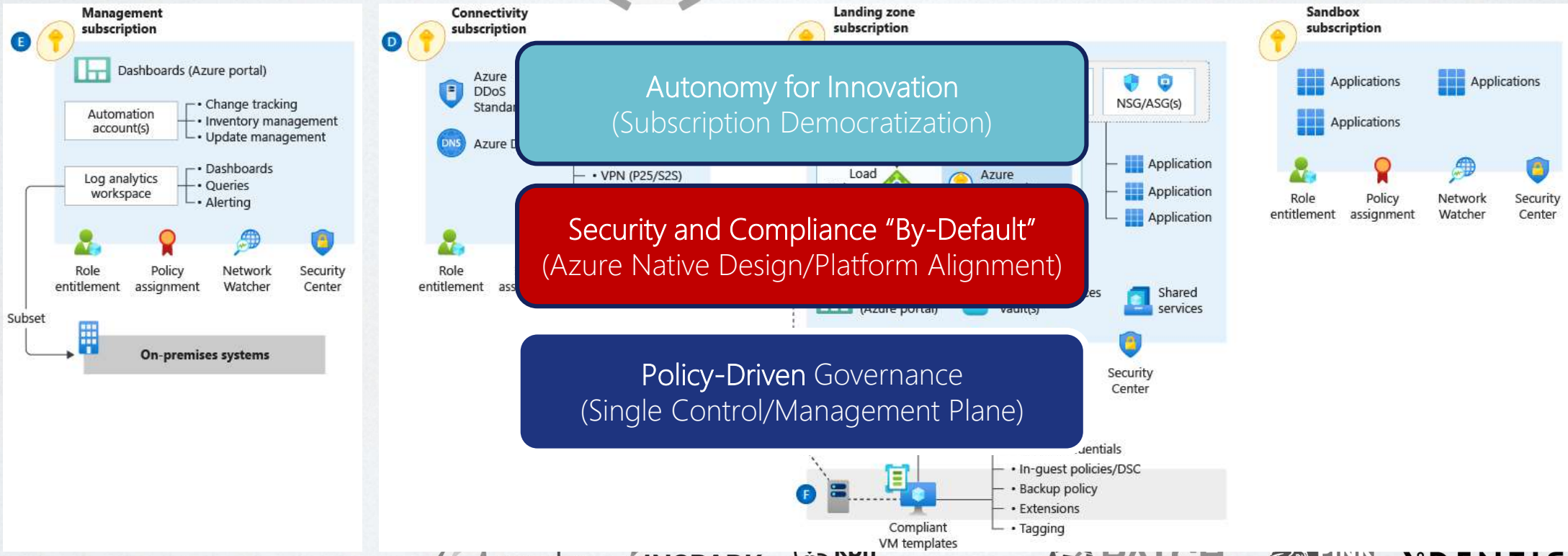
How Agentless scanning works

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Enterprise-Scale - Design Principles

Tenant Root Group

Build Clouds



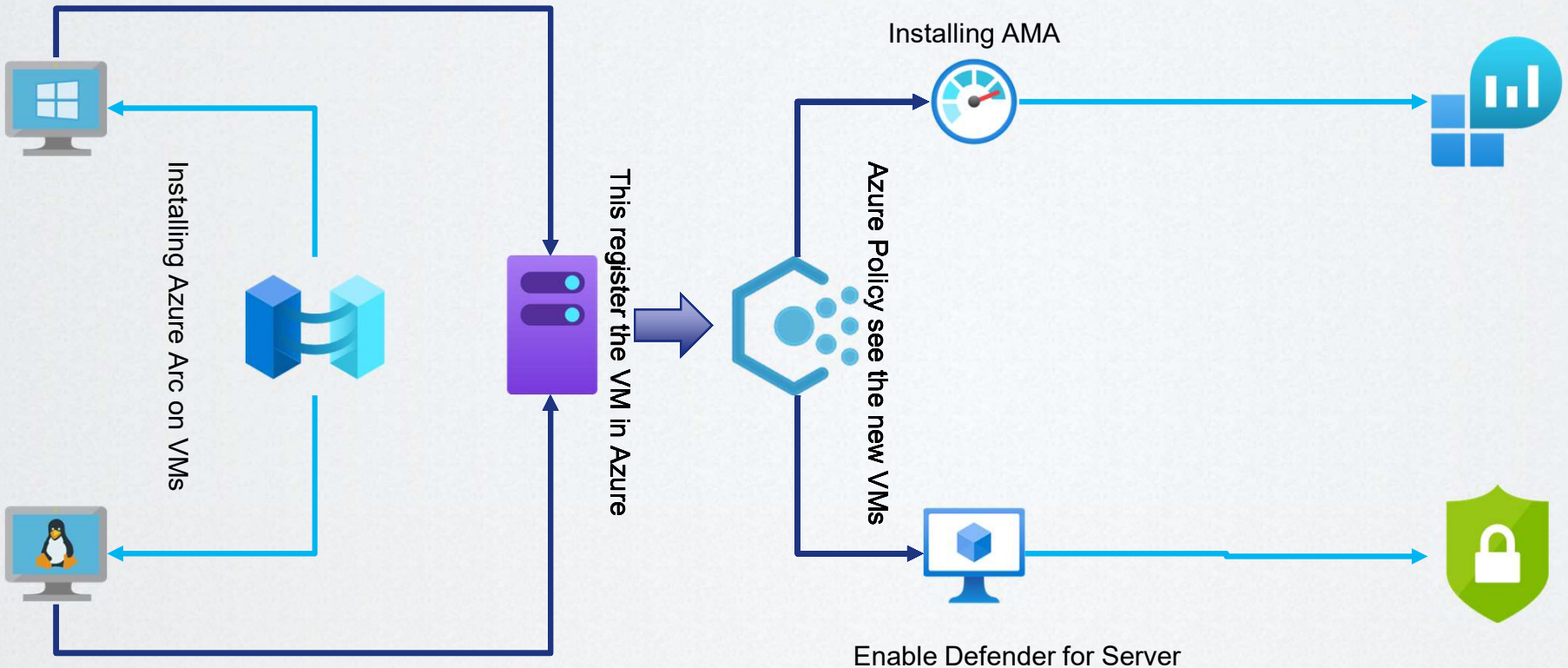
Autonomy for Innovation
(Subscription Democratization)

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

Policy-Driven Governance
(Single Control/Management Plane)

cegeka INSPARK Partner Network PATCH MY PC YDENTIC

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

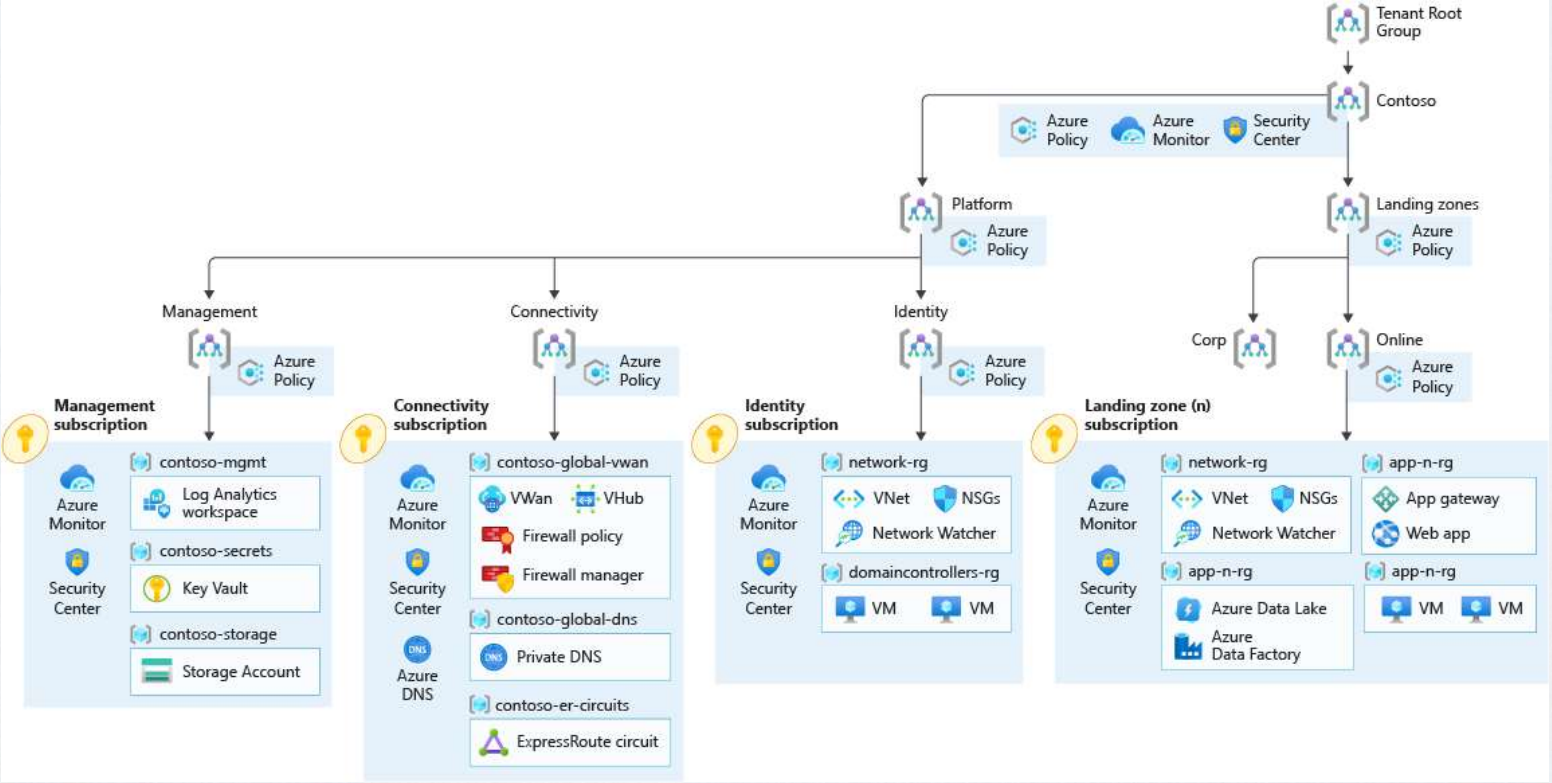
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

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

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

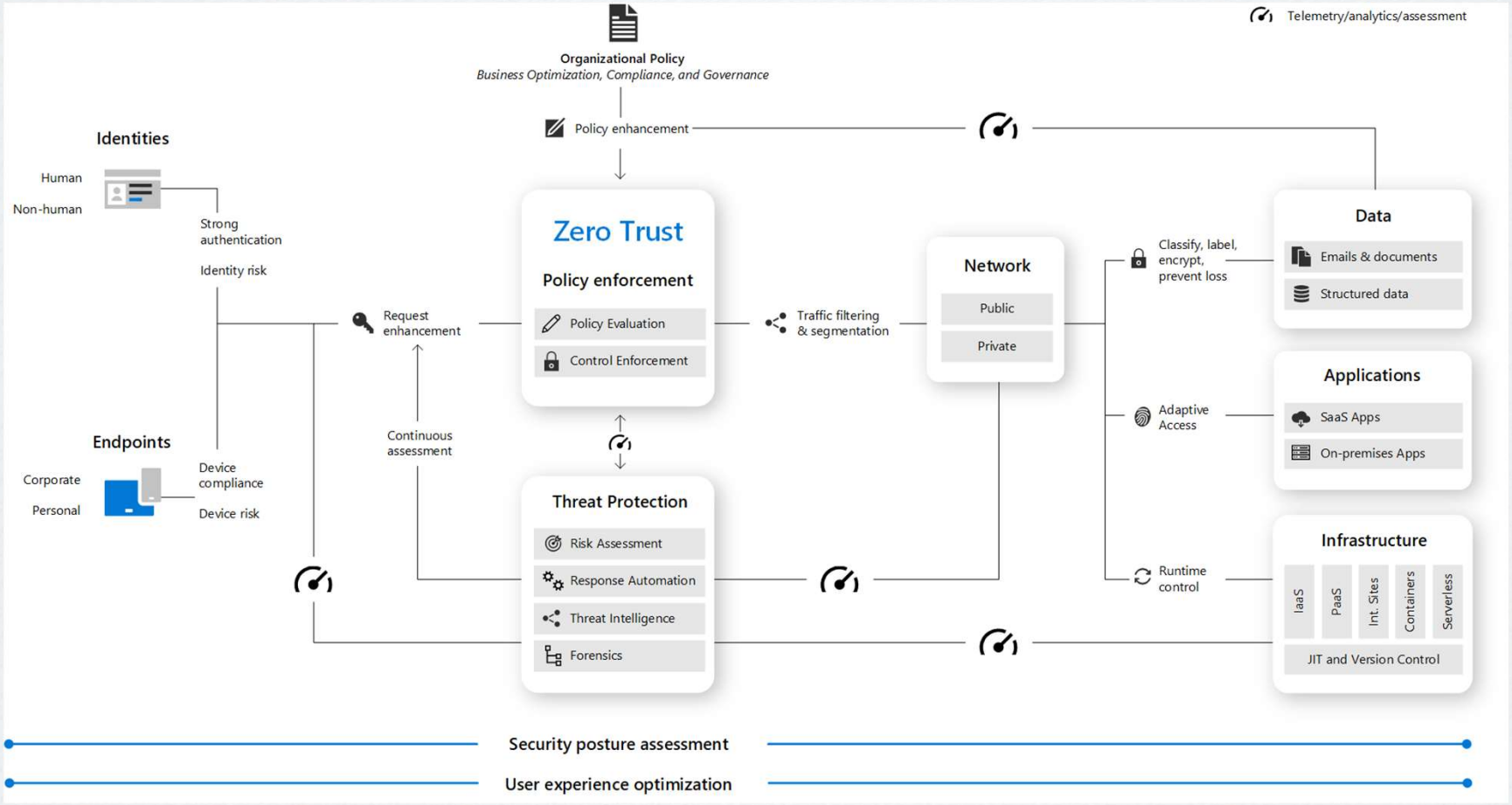
Learning

[Training | Microsoft Learn]

[Join Our Security Community - Microsoft Tech Community]

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Zero Trust architecture



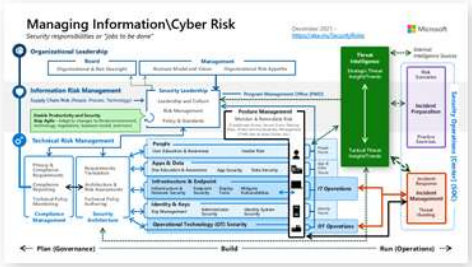
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

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?



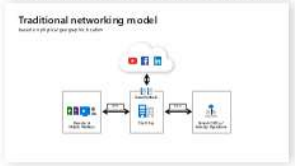
Zero Trust User Access
How to validate trust of user/devices for all resources?

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]

Future information

- Plan Defender for Servers data residency and workspaces | Microsoft Learn
- 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

Please rate my session

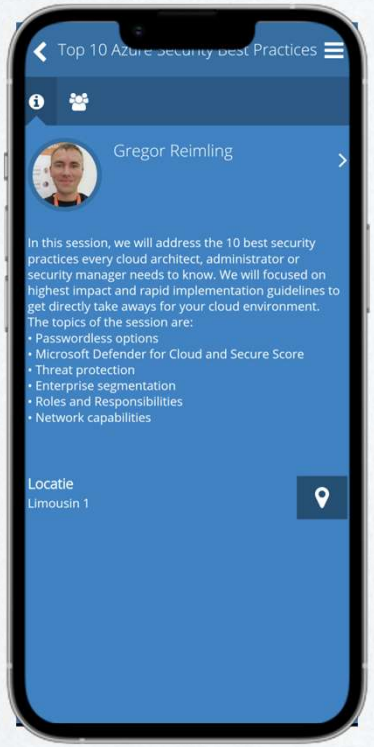
in the Yellenge app

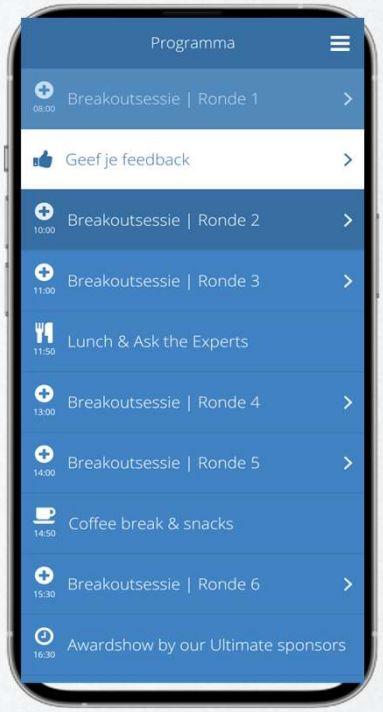
Yellenge

Event: **EXPERTS23**

Download on the App Store

ANDROID APP ON Google play





cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Thank you

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

Hobbies

Family, Community, Worldtraveler

Contact

@GregorReimling

@CloudInspires

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC