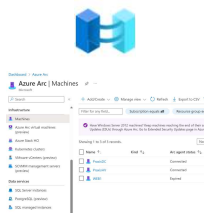


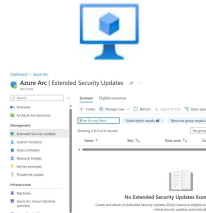


# Multicloud Servermanagement with Azure Arc

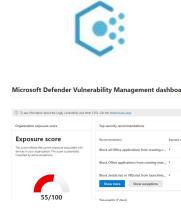
by Gregor Reimling  
MVP for Azure | MVP for Security



27.1.2024, Azure Saturday Hamburg

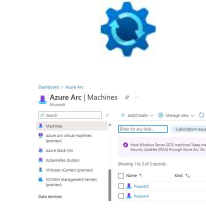


**FEITIAN**  
WE BUILD SECURITY

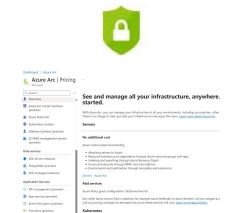


glueck kanja

q.beyond



VISORIAN



#CommunityRocks



# Sponsors



# About "Gregor Reimling"



## Focus

Azure Governance, Security and IaaS

## Certifications

Cloud Security Architect, MVP for MS Azure

## From

Cologne, Germany

## Hobbies

Family, Community, Worldtraveler

## My Blog

<https://www.reimling.eu>



[cloudinspires.me](https://cloudinspires.me)

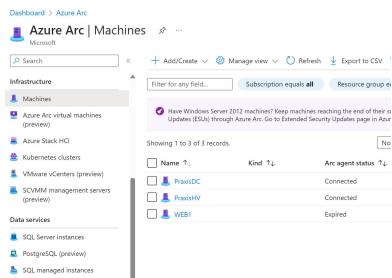
## Contact



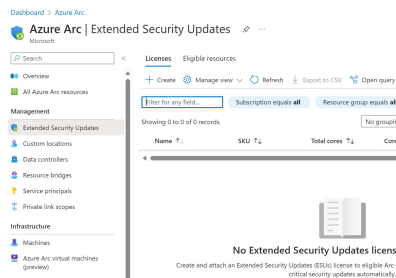
@GregorReimling

Gregor Reimling

# Agenda



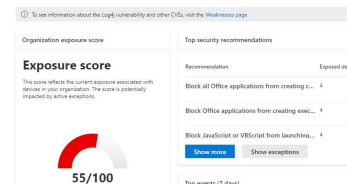
Overview about  
Azure Arc



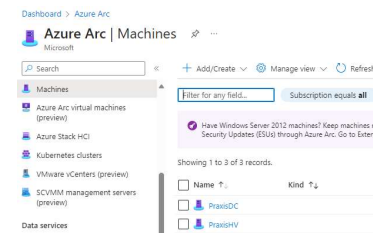
Server Management



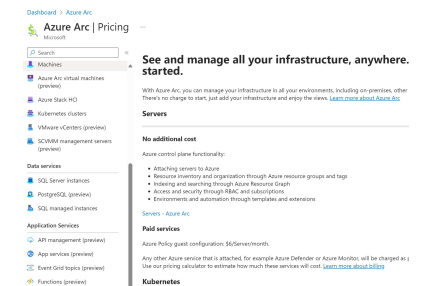
## Microsoft Defender Vulnerability Management dashboard



Azure Automate  
Machine Configuration

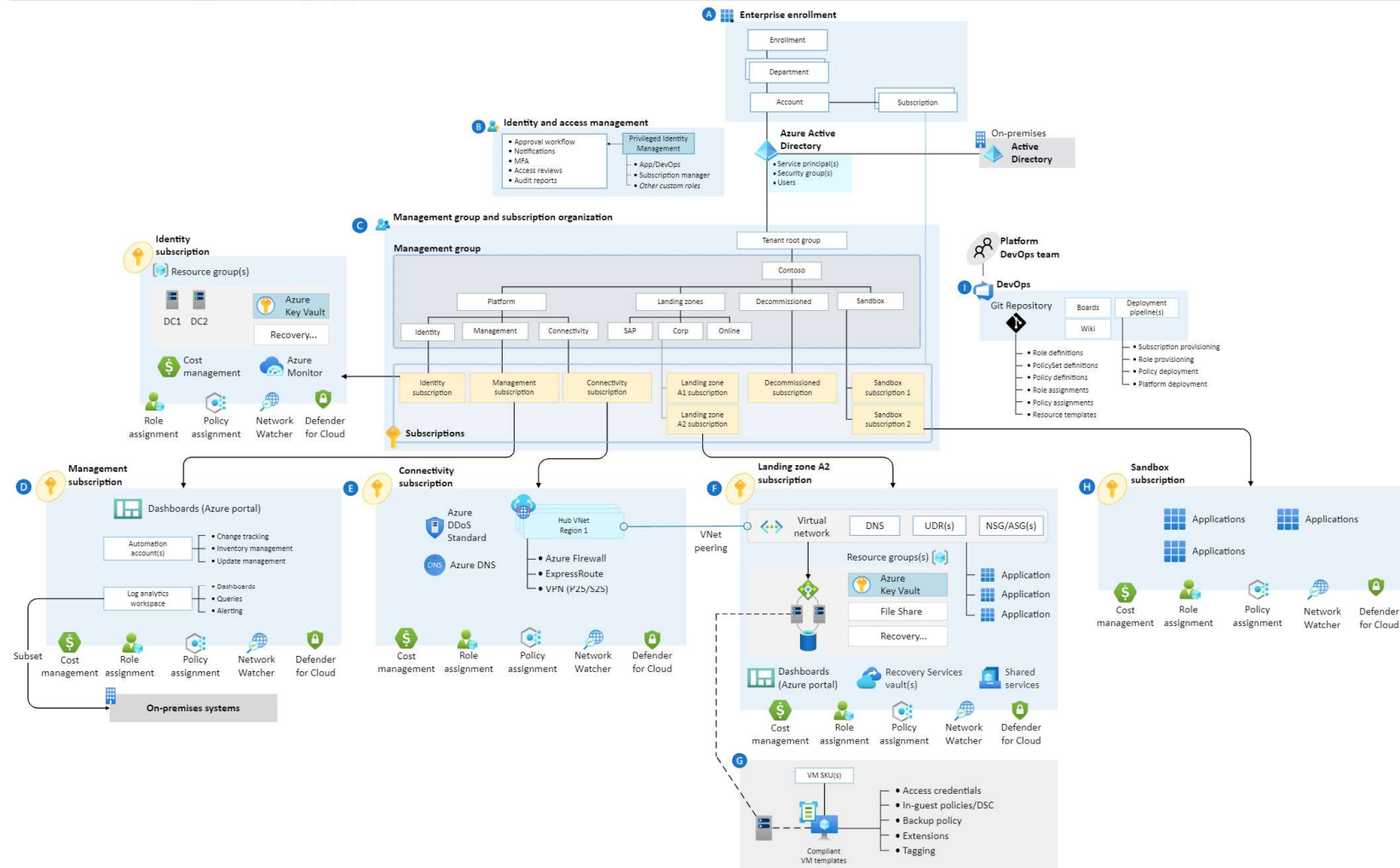


Update Management  
Center

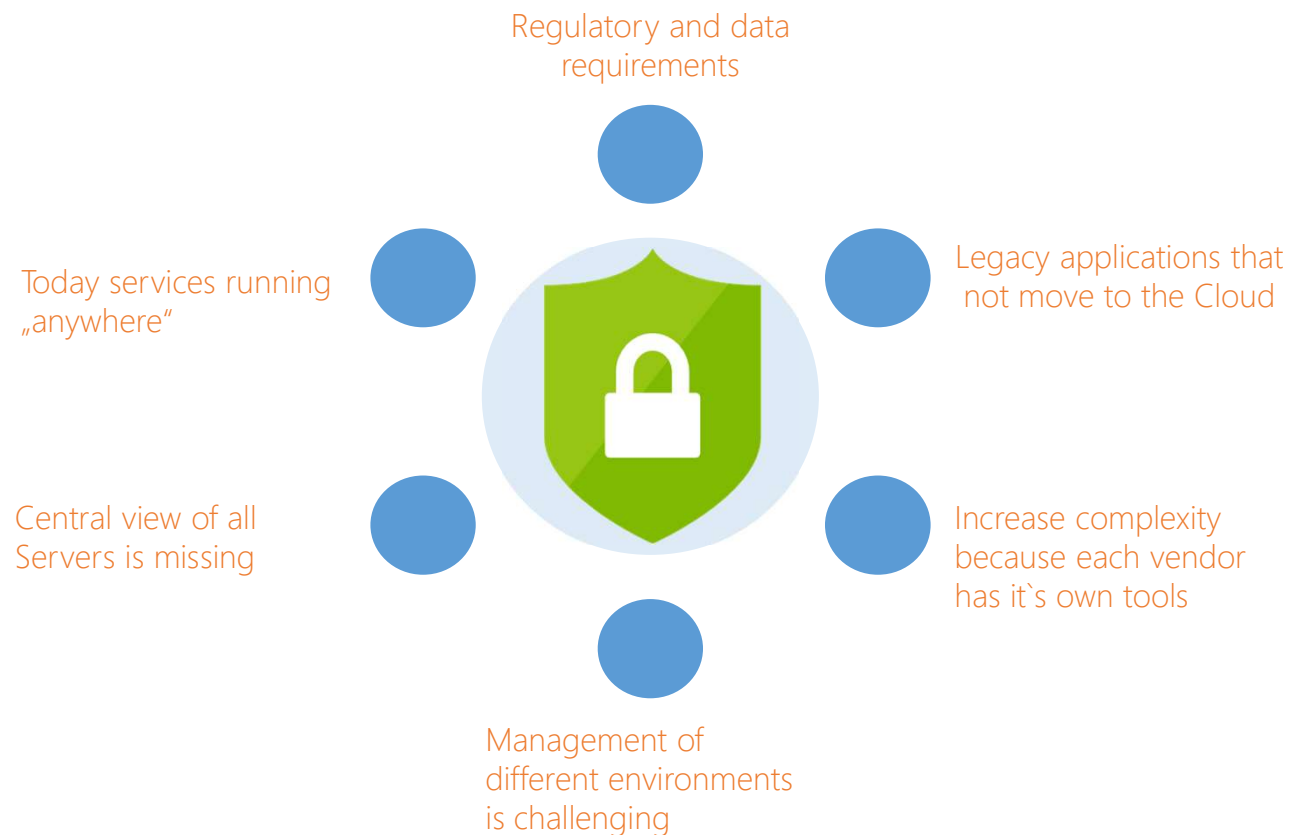


Defender for Server

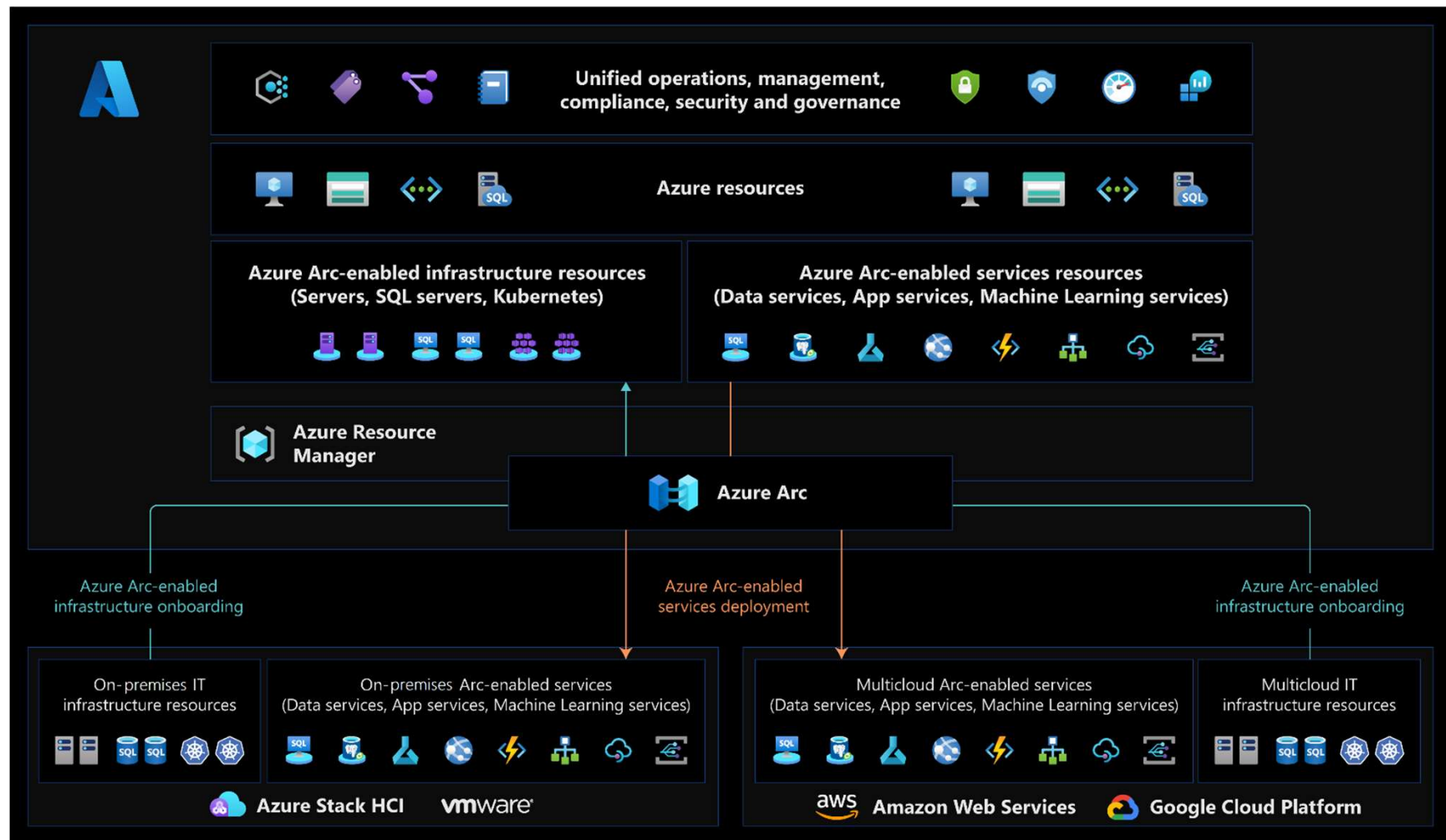
# Enterprise Scale



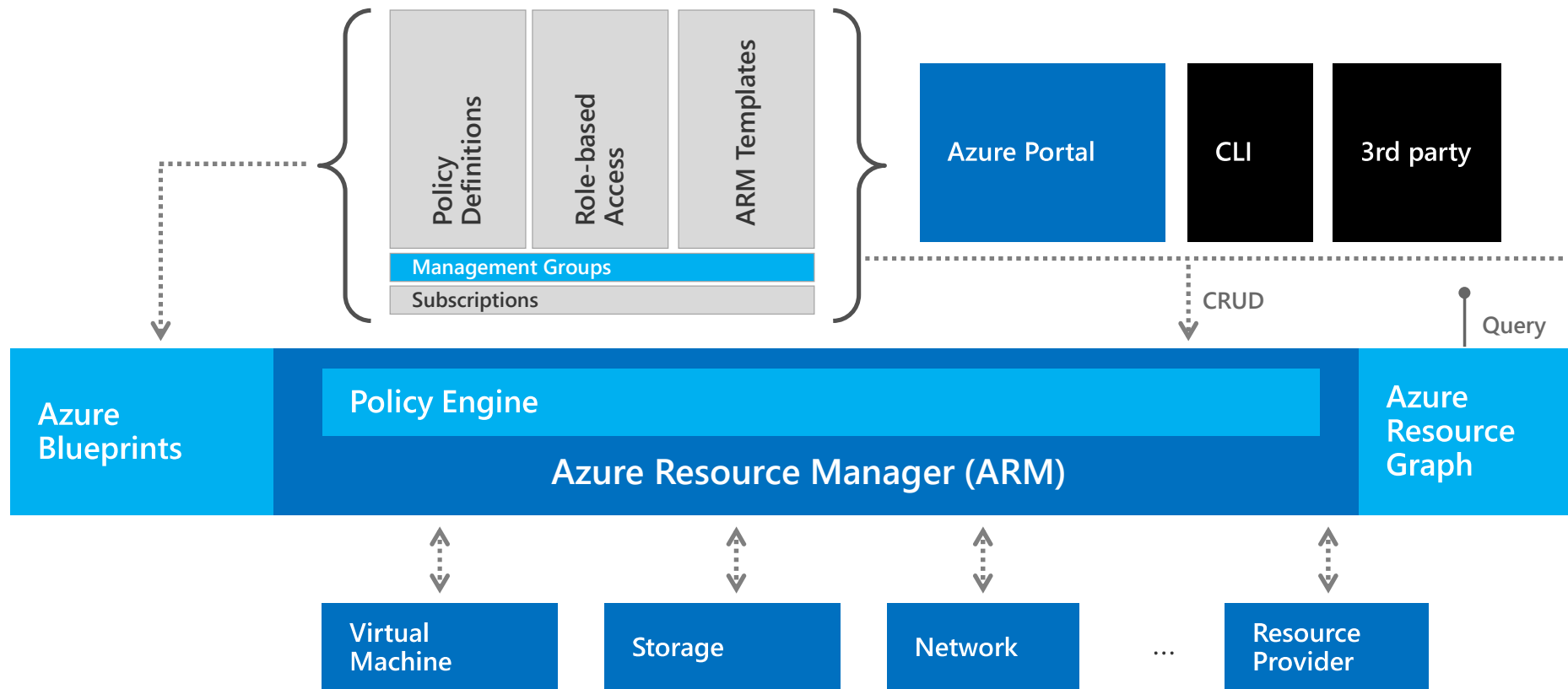
# Reasons for Hybrid Infrastructures





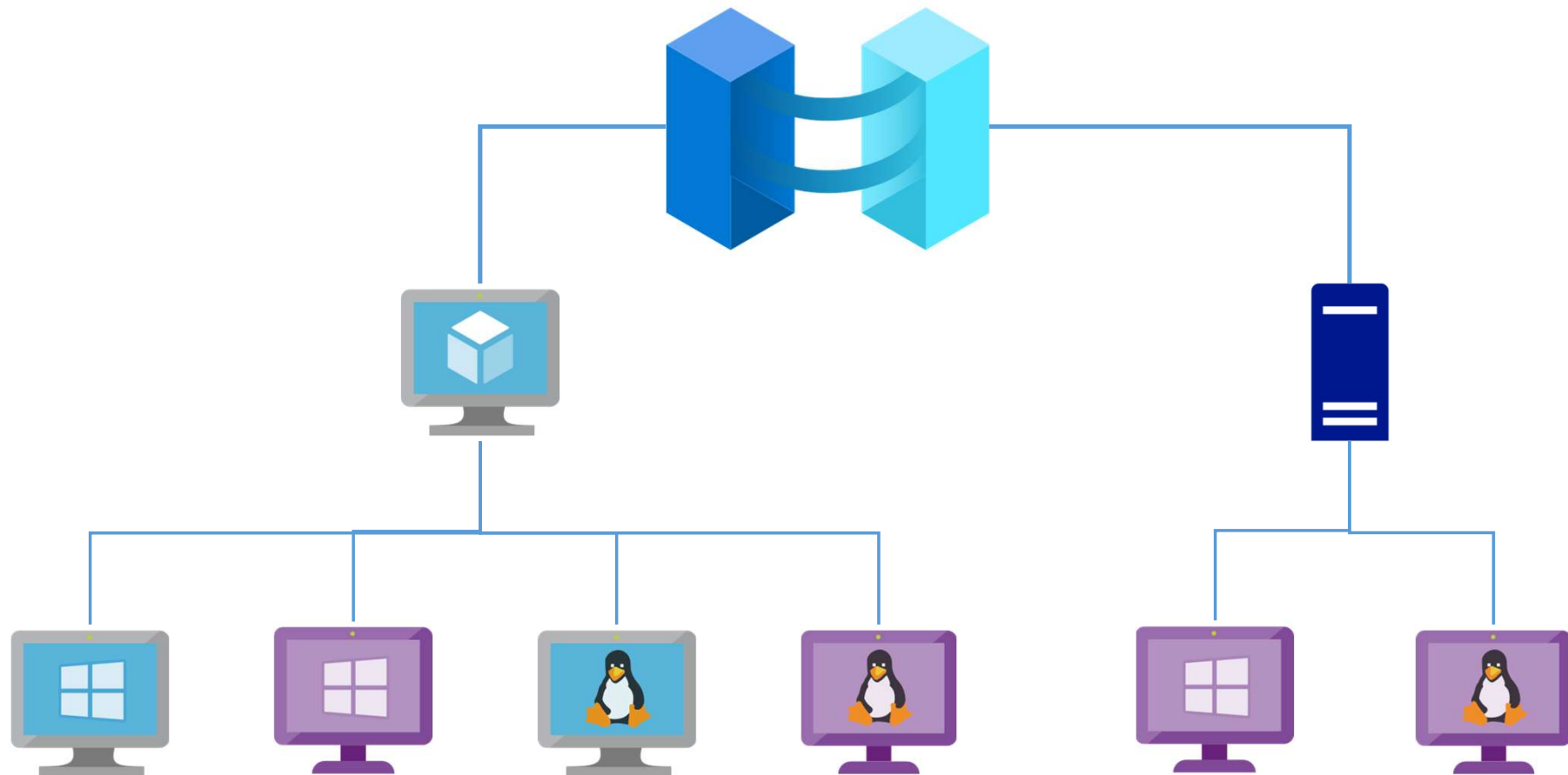


# Azure Governance Architecture





# This session



# Supported Environments and OS



## Environments

- VMware (including Azure VMware)
- Azure Stack HCI
- GCP, AWS, etc.



## Windows

- Windows Server 2008 R2 SP1 and higher (including Core)
- Windows IoT Enterprise



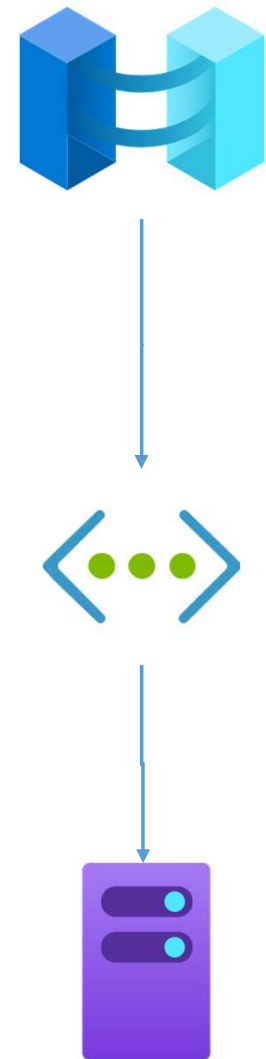
## Linux

- Ubuntu 16.04, 18.04, 20.04 and 22.04
- Debian 10 and 11
- CentOS Linux 7 and 8
- Rocky Linux 8
- SLES 12 and 15
- RHEL 7 and 8
- Amazon Linux 2
- Oracle Linux 7 and 8

# Prerequisites

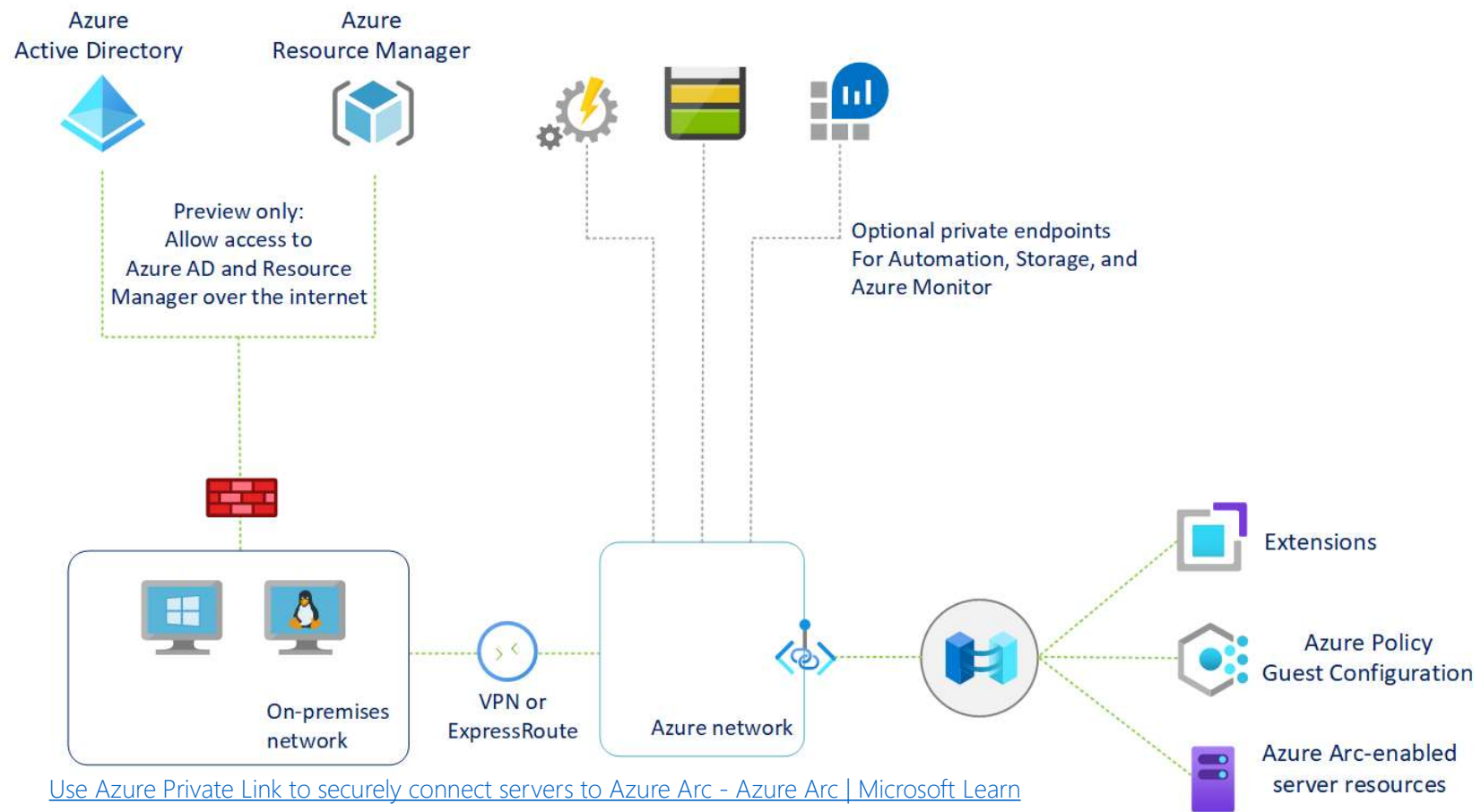
- NET Framework 4.6
- Windows PowerShell 4 (included in WS2012R2 and higher)
- Azure RBAC
  - Onboarding: Azure Connected Machine Onboarding
  - Read, Modify, Delete: Azure Connected Machine Resource Admin
- Resource Providers
  - Microsoft.HybridCompute
  - Microsoft.GuestConfiguration
  - Microsoft.HybridConnectivity
- Outbound via TCP 443 (Proxy server is supported)
- Private Link support

13



## Connecting to Azure Arc

# Private Link



# Connecting VMs

```
PS C:\Users\Administrator> try {
    $env:SUBSCRIPTION_ID = "009c17ca--4905999fba2d";
    $env:RESOURCE_GROUP = "arc_rg";
    $env:TENANT_ID = "e4f80c4f--3141bca1ced3";
    $env:LOCATION = "westeurope";
    $env:AUTH_TYPE = "token";
    $env:CORRELATION_ID = "95256887-01a2-4c82-948e-e457830cda97";
    $env:CLOUD = "AzureCloud";
    [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor 3072;
    # Download the installation package
    Invoke-WebRequest -UseBasicParsing -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$env:TEMP\install_windows_azcmagent.ps1";
    # Install the hybrid agent
    & "$env:TEMP\install_windows_azcmagent.ps1";
    if ($LASTEXITCODE -ne 0) { exit 1; }
    # Run connect command
    & "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "$env:RESOURCE_GROUP" --tenant-id "$env:TENANT_ID" --
location "$env:LOCATION" --subscription-id "$env:SUBSCRIPTION_ID" --cloud "$env:CLOUD" --tags
"Datacenter=Ohligs, City=Solingen, StateOrDistrict=NRW, CountryOrRegion=Germany, Service=Arc, Environment=Prod" --correlation-id "$env:CORRELATION_ID";}
catch {$logBody =
@{subscriptionId="$env:SUBSCRIPTION_ID";resourceGroup="$env:RESOURCE_GROUP";tenantId="$env:TENANT_ID";location="$env:LOCATION";correlationId="$env:CORRE
LATION_ID";authType="$env:AUTH_TYPE";messageType=$_.FullyQualifiedErrorId;message="$_"}};
    Invoke-WebRequest -UseBasicParsing -Uri "https://gbl.his.arc.azure.com/log" -Method "PUT" -Body ($logBody | ConvertTo-Json) | out-null;
    Write-Host -ForegroundColor red $_.Exception;}
VERBOSE: Installing Azure Connected Machine Agent
VERBOSE: .NET Framework version: 4.6.1586
VERBOSE: Downloading agent package from https://aka.ms/AzureConnectedMachineAgent to C:\Users\ADMINI~1\AppData\Local\Temp\AzureConnectedMachineAgent.msi
VERBOSE: Installing agent package
```

Installation of azcmagent completed successfully

time="2022-11-11T22:16:46+01:00" level=info msg="The computer is connected in Azure. This may take a few minutes."

time="2022-11-11T22:17:59+01:00" level=info msg="Log in using the pop-up browser to authenticate yourself."

27.1.2024, Azure Saturday Hamburg

**FEITIAN**  
WE BUILD SECURITY

glueck kanja

q.beyond

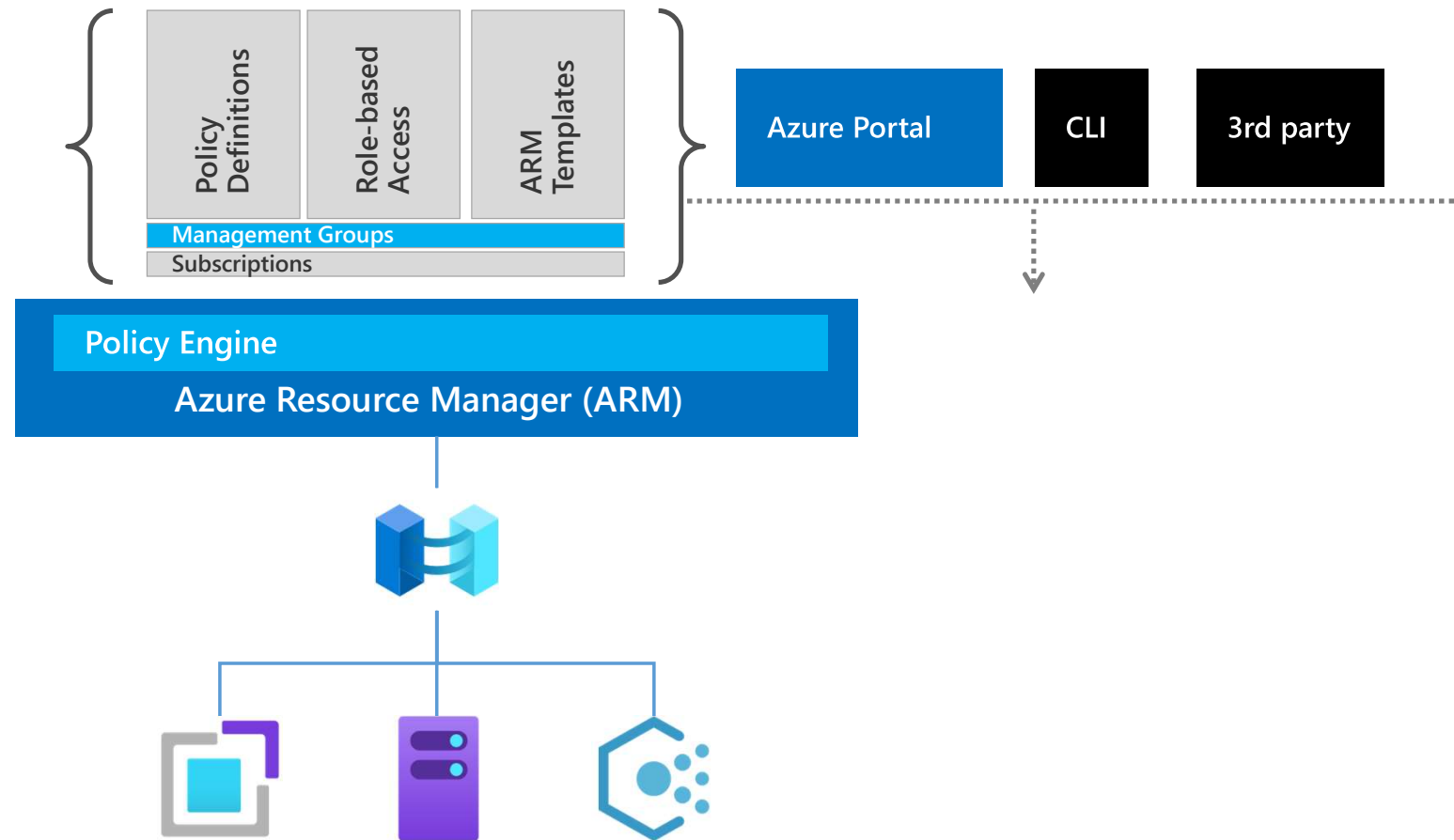
VISORIAN

#CommunityRocks





# Azure Architecture



# Connected Machine Agent

Azcmagent tool configure  
the Azure Connected  
Machine agent

Updates coming via  
Windows Update  
(configure is mandatory)

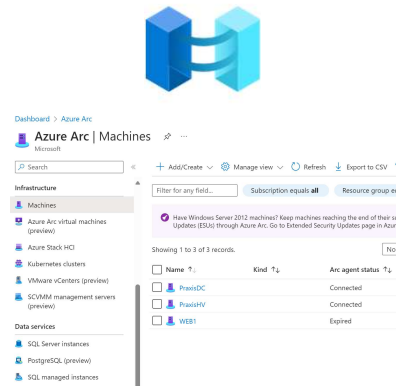
Server Renaming does not  
rename the Azure  
resource name (because  
is immutable)

Delete and re-create is  
needed for Server  
renaming

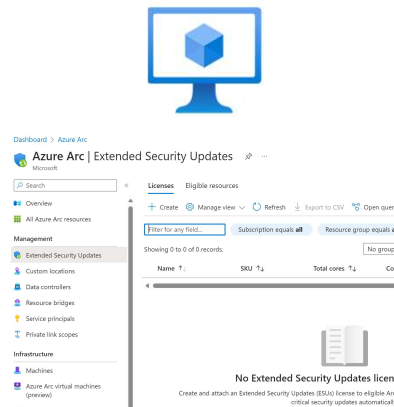
Remove any VM-extension

Use azcmagent to  
disconnect

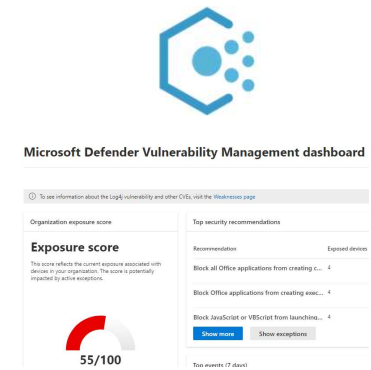
# Demo Azure Arc



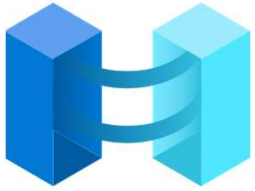
Overview about  
Azure Arc



Server Management



Azure Automanage  
Machine Configuration



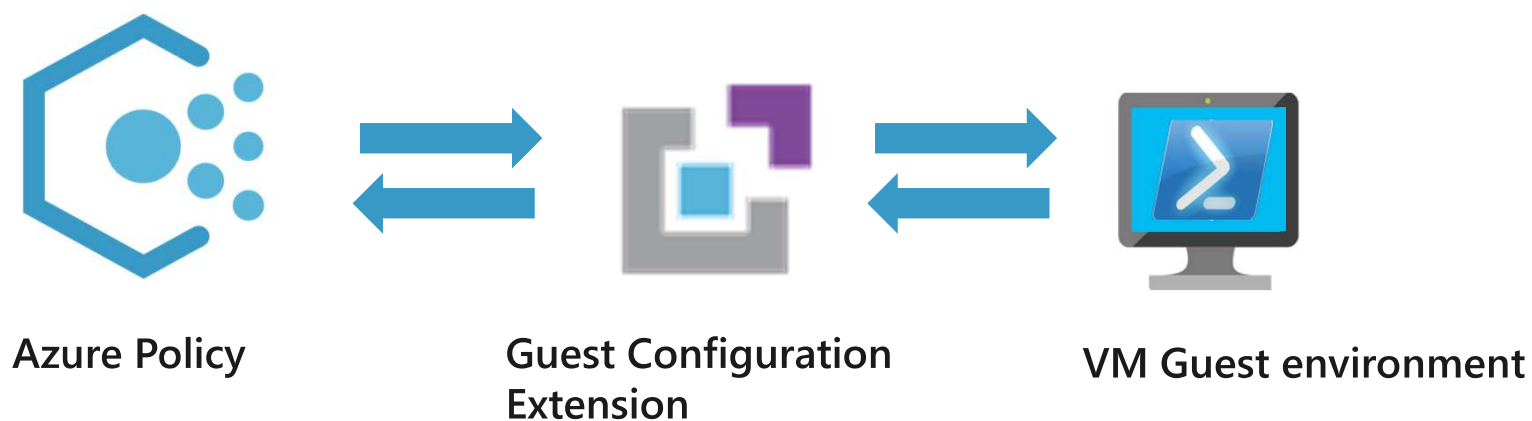
Azure Policy Guest Configuration  
Renamed to

Azure Automanage  
Machine Configuration

[Coming soon: guest configuration renames to machine configuration -](#)

[Microsoft Community Hub](#)

# How VM guest policy works



# Guest Configuration





[Dashboard](#) >

## Guest Assignments ...

Build Clouds

[+ Create](#) [⚙️ Manage view](#) [↺ Refresh](#) [↓ Export to CSV](#) [🔗 Open query](#) | [🏷️ Assign tags](#) [🗑️ Delete](#)

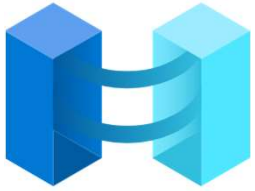
[Subscription equals all](#) [Resource group equals all](#) [Location equals all](#) [+🔍 Add filter](#) [No grouping](#)

<input type="checkbox"/> Name ↑↓	Machine ↑↓	Type ↑↓	Status ↑↓	Resource
<input type="checkbox"/>  AuditSecureProtocol (W... WEB1		Microsoft.HybridCompute	NonCompliant	<a href="#">arc_rg</a>
<input type="checkbox"/>  AzureWindowsBaseline ... WEB1		Microsoft.HybridCompute	NonCompliant	<a href="#">arc_rg</a>
<input type="checkbox"/>  WindowsDefenderExplo... WEB1		Microsoft.HybridCompute	Compliant	<a href="#">arc_rg</a>
<input type="checkbox"/>  WindowsLogAnalyticsA... WEB1		Microsoft.HybridCompute	Compliant	<a href="#">arc_rg</a>



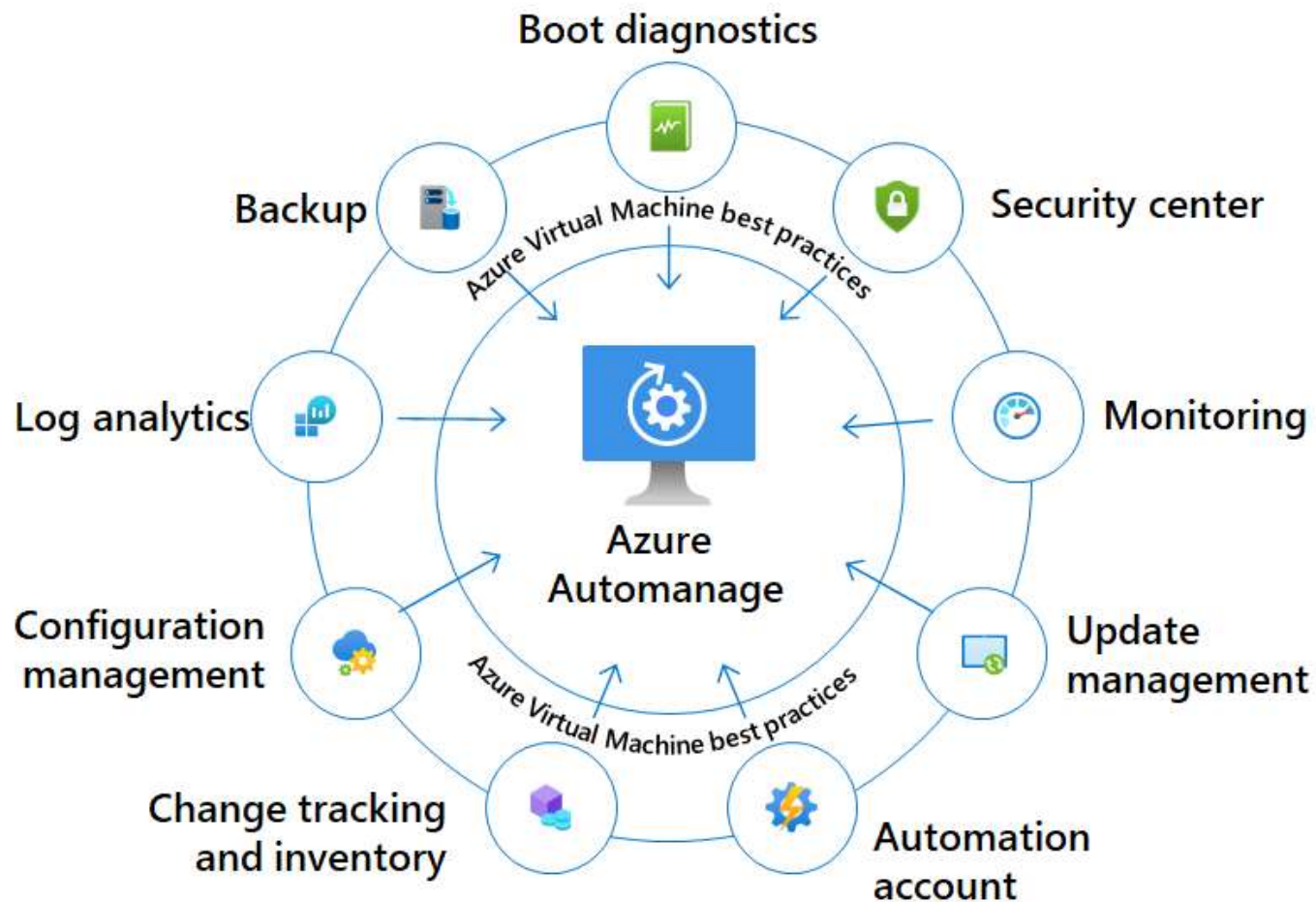
# Azure Automanage Machine Configuration

- Guest configuration extend Azure Policy to Server
- Perform audit and configuration inside Server
- Need Resource Provider Microsoft.GuestConfiguration
- Checks for changes every 5 minutes
- Installs security baselines for Windows and Linux
- Configured in audit-only mode
- Non-compliant devices are displayed but not reset
- Reset possible through advanced configuration



# Azure Automanage

# Azure Automanage – Your VM Service provider



# Azure Automanage



Automates best practices configuration for all VMs



Access to all VMs via Azure Arc (Multicloud enabled)



Fully customizable via user-defined profiles

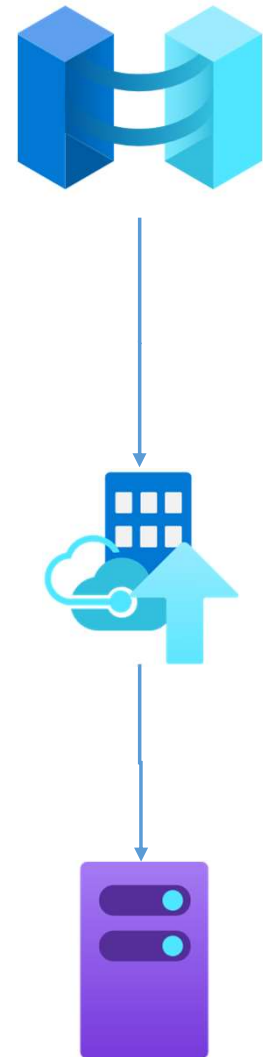


For Windows and Linux VMs

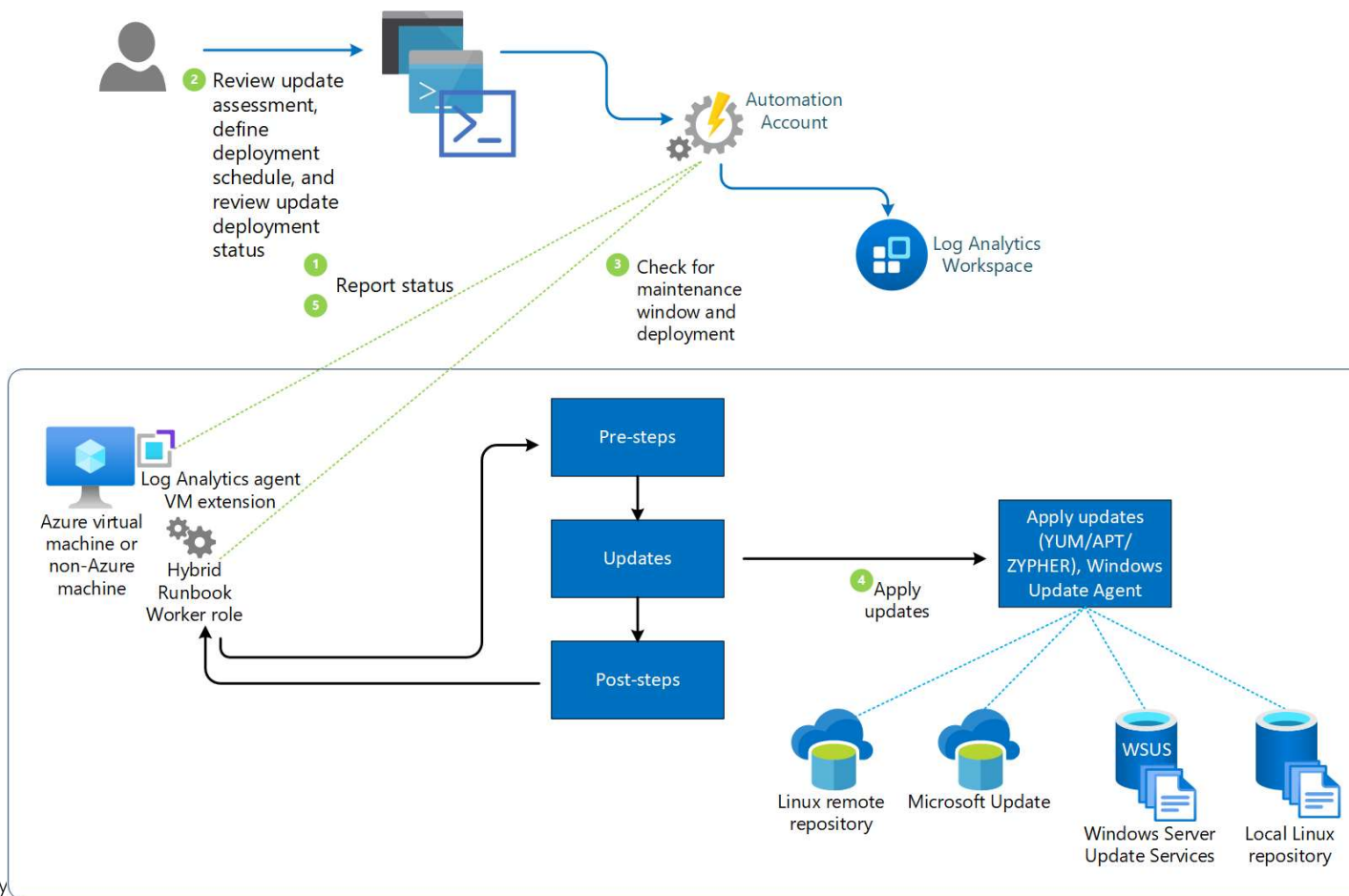


Available free of charge

# Azure Update Center



# Azure Automation Update Management (v1)





# Why Azure Update Center v2?



V2 is complete new

No dependencies to MMA or Azure Automation



Fully support for Azure Policy



Integration in Enterprise Scale

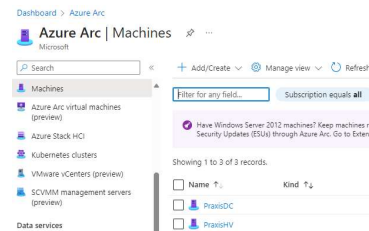


Server visibility in Azure guaranteed



Update Manager will charged by 5\$ per Server/month beginning of January (only for Arc Machines)

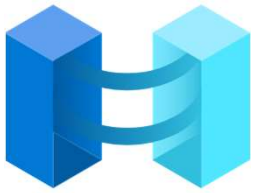
# Demo Azure Update Manager



Azure Update  
Manager

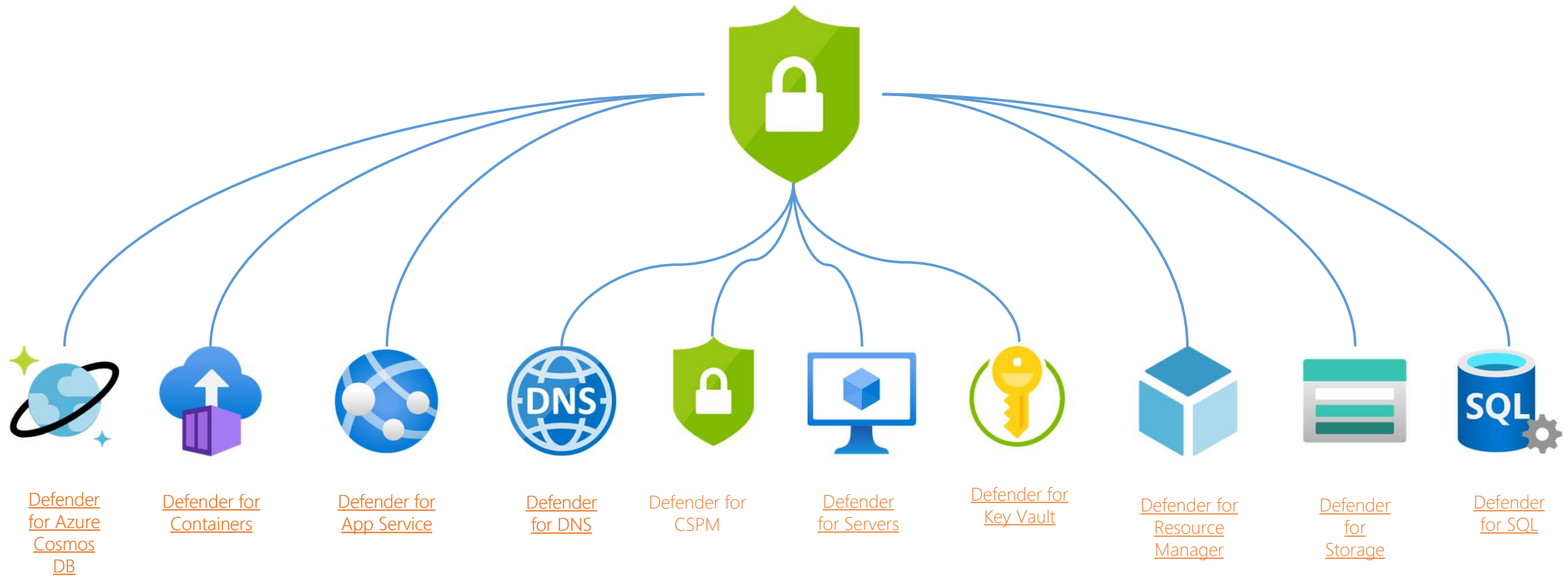


Azure Update Manager will begin billing on 1  
February 2024 for Arc-enabled servers

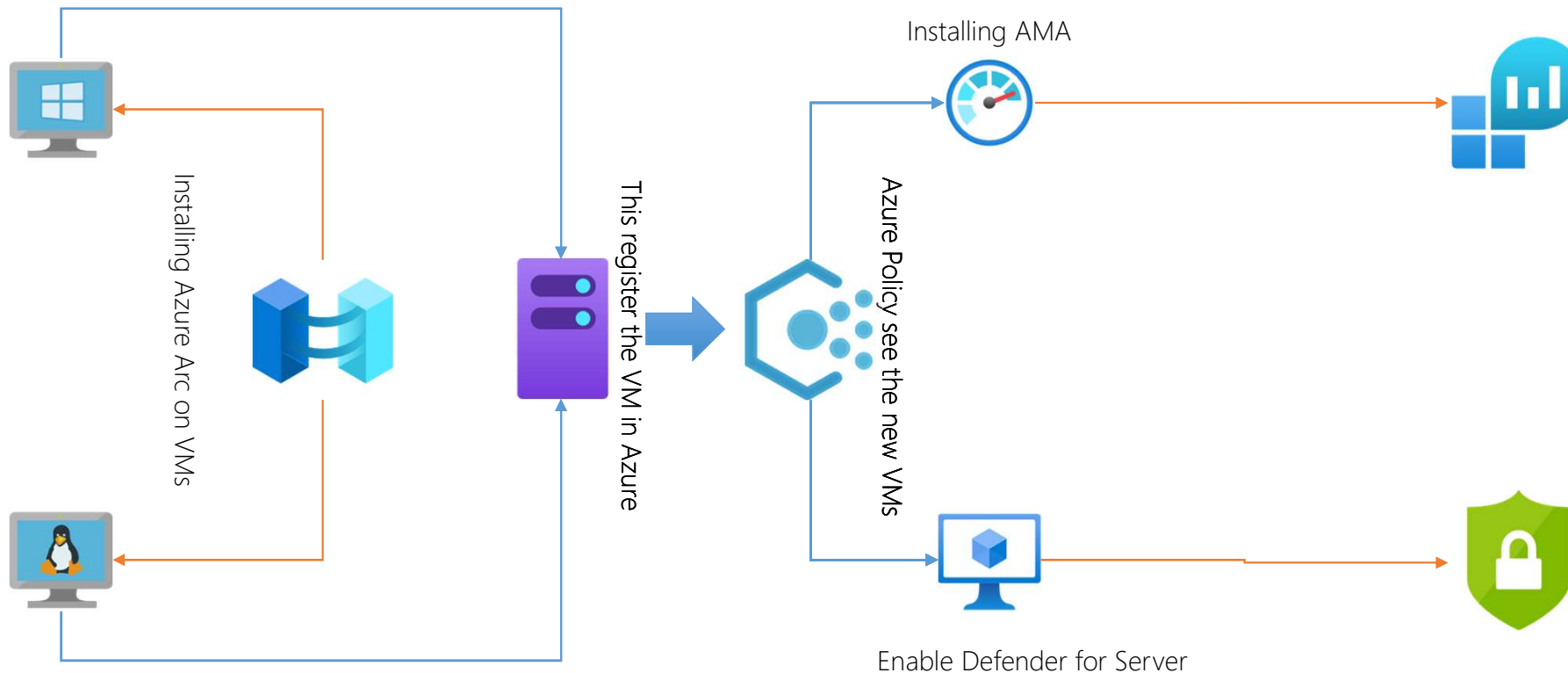


# Defender for Cloud

# Microsoft Defender for Cloud



# 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

# Auto-provisioning configuration

## 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

- 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



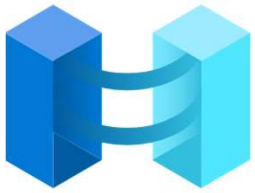
# Hybrid Server Onboarding

## 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



# How To Start



# Azure Arc jumpstart



## Azure Arc Jumpstart

**Overview**

- [Jumpstart Scenarios](#)
- [Jumpstart ArcBox](#)
- [Jumpstart HCIBox](#)
- [Jumpstart Release Notes](#)
- [Scenario Write-up Guidelines](#)
- [Jumpstart FAQ](#)
- [Open-Source Commitment](#)
- [Code of Conduct](#)
- [Contributing](#)
- [Security](#)


Overview

### Azure Arc Jumpstart

The Azure Arc Jumpstart is designed to provide a “zero to hero” experience so you can start working with Azure Arc right away!

The Jumpstart provides step-by-step guides for independent Azure Arc scenarios that incorporate as much automation as possible, detailed screenshots and code samples, and a rich and comprehensive experience while getting started with the Azure Arc platform.

Our goal is for you to have a working Azure Arc environment spun-up in no time so you can focus on the core values of the platform, regardless of where your infrastructure may be, either on-premises or in the cloud.



38

## [Overview](#) | [Azure Arc Jumpstart](#)

# Azure Arc Community Monthly Meetup

## Microsoft Azure Arc Community Monthly Meetup

### Overview

Once a month, the various Azure Hybrid Cloud product groups at Microsoft will hold a call to showcase new features, talk through important topics and engage in a Q&A regarding Azure Arc. The foundational goals of the call are highlighted below:

- Provide the Azure Arc community with product updates
- Host a short talk and/or demo on Azure Hybrid Cloud technologies and products technologies
- Collect feedback from the community on issues, blockers, use cases, and questions related to Azure Hybrid Cloud technologies and products

### Contributors 3



likamrat Lior Kamrat



microsoftopensource Microsoft Open ...



csand-msft Chris Sanders

[GitHub - microsoft/azure\\_arc\\_community: Public repository for hosting the Azure Arc Community content](#)

# Summary and Best Practices



# Links

- [Introduction to Azure Arc - Training | Microsoft Learn](#)
- [Managing the Azure Arc-enabled servers agent - Azure Arc | Microsoft Learn](#)
- [Overview of the Azure Connected Machine agent - Azure Arc | Microsoft Learn](#)
- [Archive for What's new with Azure Arc-enabled servers agent - Azure Arc | Microsoft Learn](#)
- [GitHub - microsoft/azure\\_arc\\_community: Public repository for hosting the Azure Arc Community content](#)
- [Azure Automanage | Microsoft Learn](#)
- [Update management center \(preview\) overview | Microsoft Learn](#)
- [The new Azure Update Center is GA Part 1 – three big reasons to migrate to Update Center](#)
- [Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn](#)
- [Join Our Security Community - Microsoft Tech Community](#)

# Azure Arc – Person of Interests



Lior Kamrat

Principal Product Manager -  
Azure Arc Platform

[Lior Kamrat | LinkedIn](#)



Thomas Maurer

Senior PM and Chief Evangelist  
Azure Hybrid at Microsoft

[Thomas Maurer | LinkedIn](#)

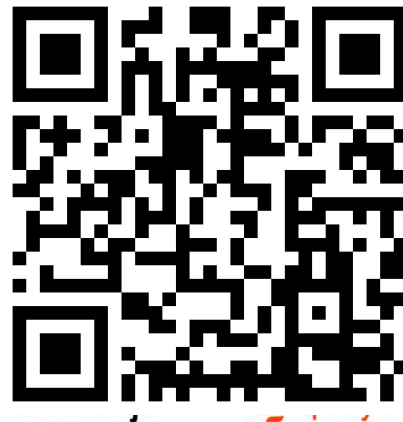


Thank You



## Blog

- <https://www.Reimling.eu>



## Contact



- @GregorReimling
- Gregor Reimling



# Agenda

---

- Point 1
- Point 2
  - Subpoint 1
  - Subpoint 2
- Point 3

# Jane Doe

MCT, Azure Expert, COO

 @janedoe4343

 /in/janedoe

 janecodescode

 janescodeblog.org

 janescompany4343.org



# One

27.1.2024, Azure Saturday Hamburg



glueck kanja

 q.beyond

 VISORIAN

#CommunityRocks



# Content

---

- First
- Second
  - First
  - Second
- Third

# Vielen Dank für's Zuhören!

---