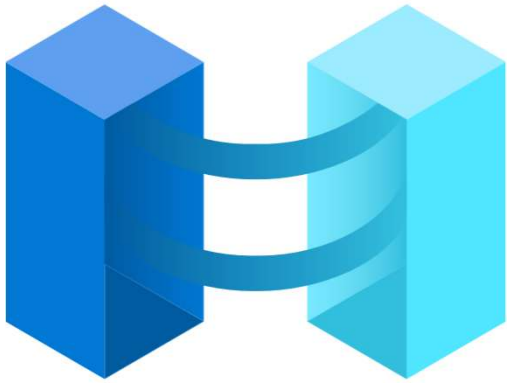
Secure, Govern, Automate: Der moderne Operation-Stack mit Azure Arc

Gregor Reimling



Azure Meetup Düsseldorf

Gregor Reimling (he/him)

th1

Chief Azure Technologist @ adesso SE, Germany

Gregor is awarded with the Microsoft MVP for Microsoft Azure and Security. He works as Chief Azure Technologist for adesso SE and is technical lead for Azure . His main areas are Microsoft Azure, Enterprise scale architectures, Cloud Security, Governance, Hybrid and Migration.

gregor@reimling.eu

reimling.eu

@GregorReimling

/in/GregorReimling

youtube.com/@GregorReimling

github.com/GregorReimling

Microsoft MVP Most Valuable Professional

Azure & Security

Azure Meetup BONN

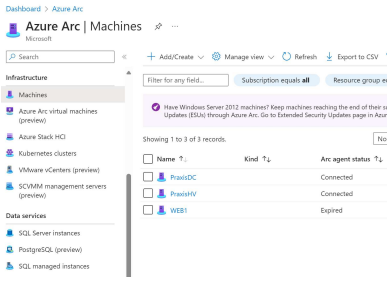
Cloud Inspires Podcast

Stories and people behind Cloud Transformation

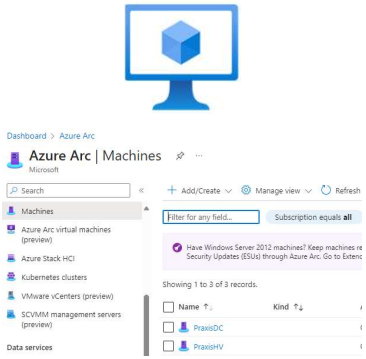
Slide 2

th1 Sicher, dass du deine Pronomen nicht anpassen möchtest? =)
thorben.forke@adesso.de, 2025-02-20T00:03:28.494

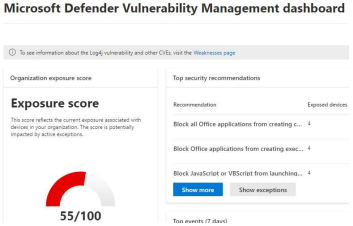
Agenda



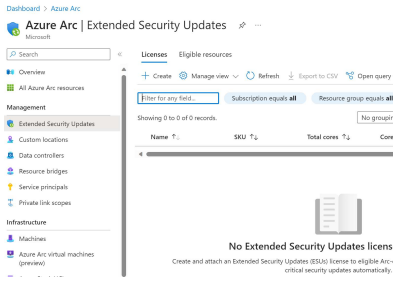
Overview about Azure Arc



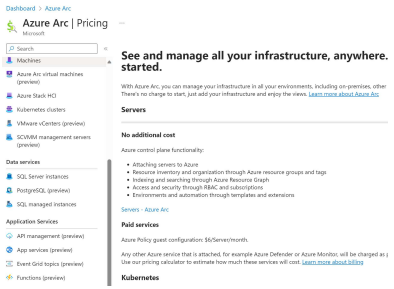
Server Management



Azure Automanage Machine Configuration

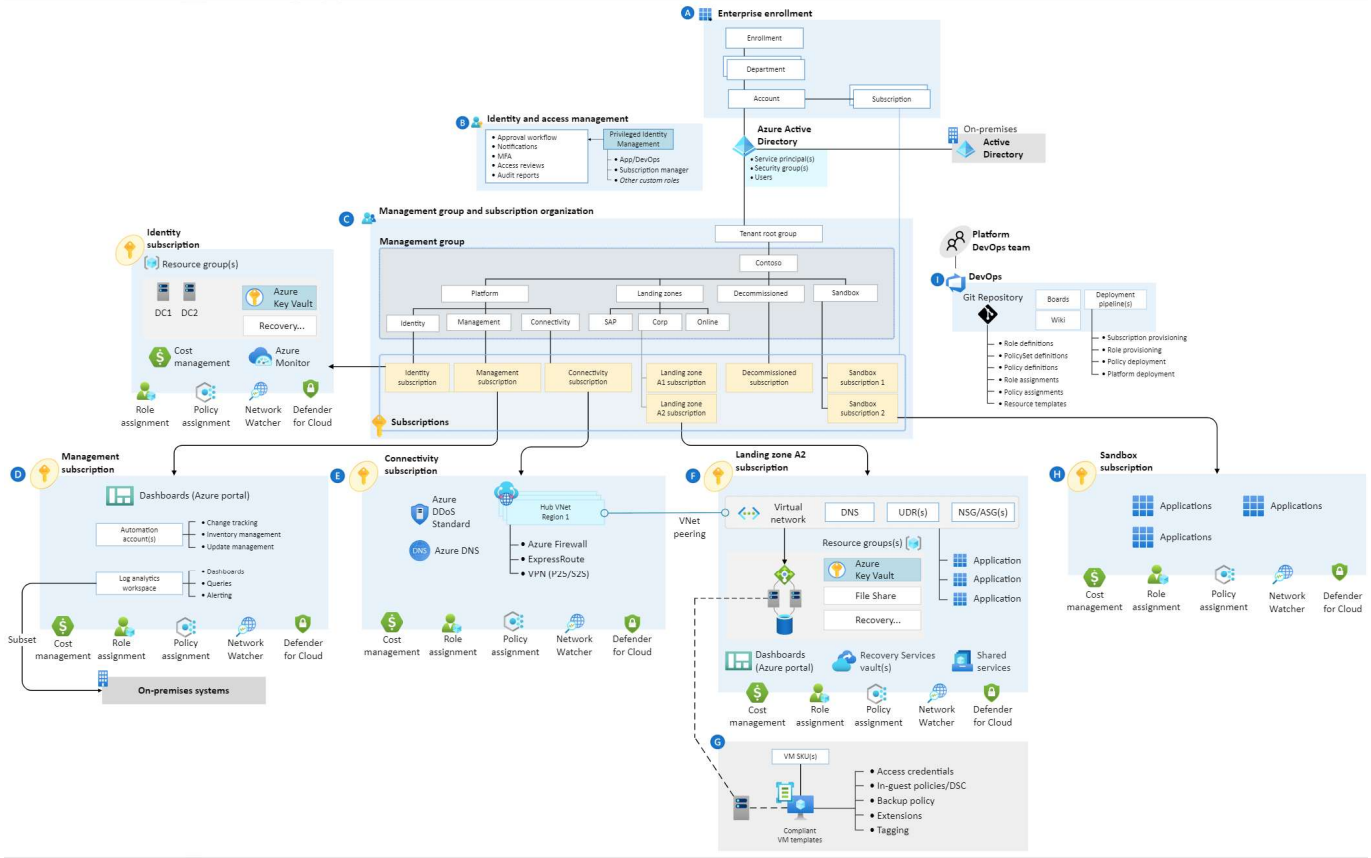


Update Management Center

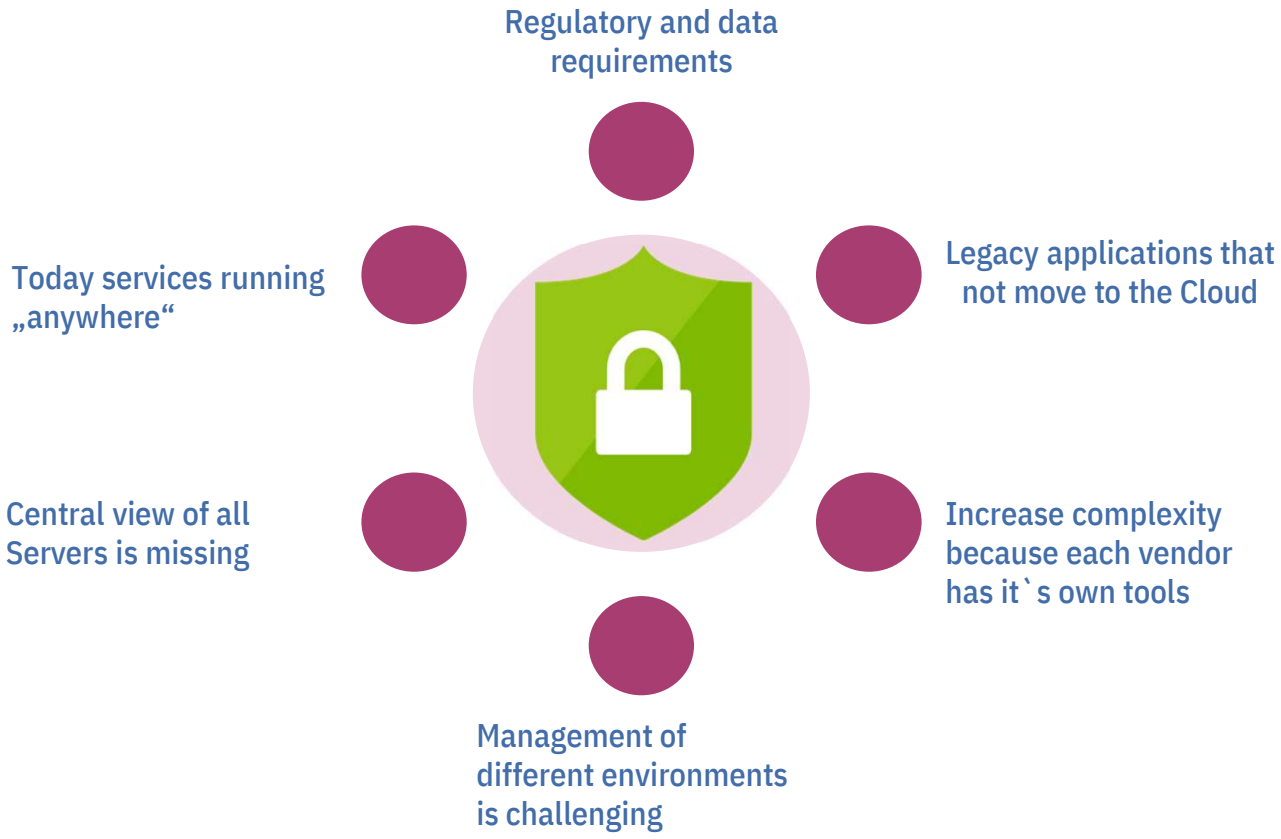


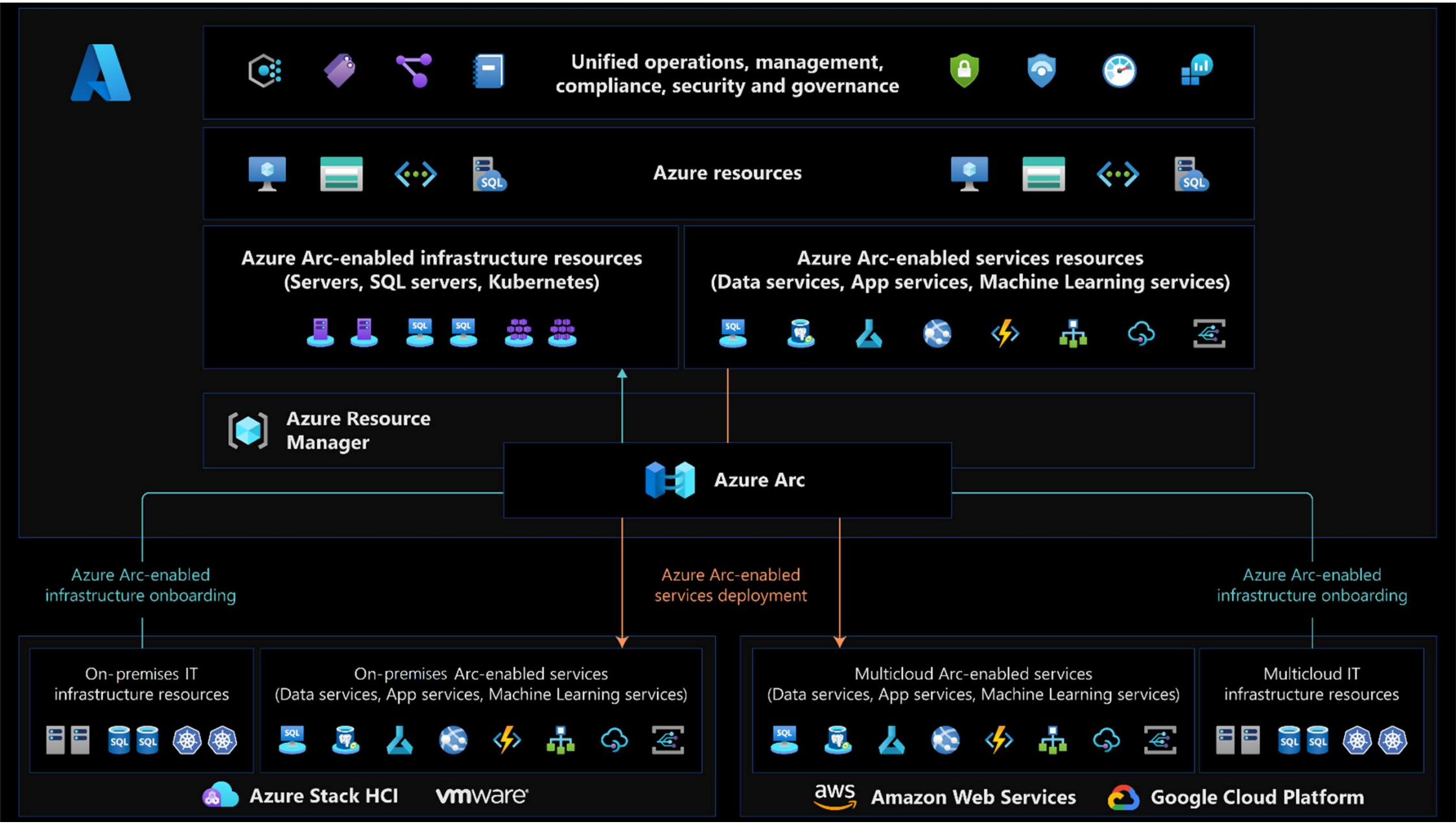
Defender for Server

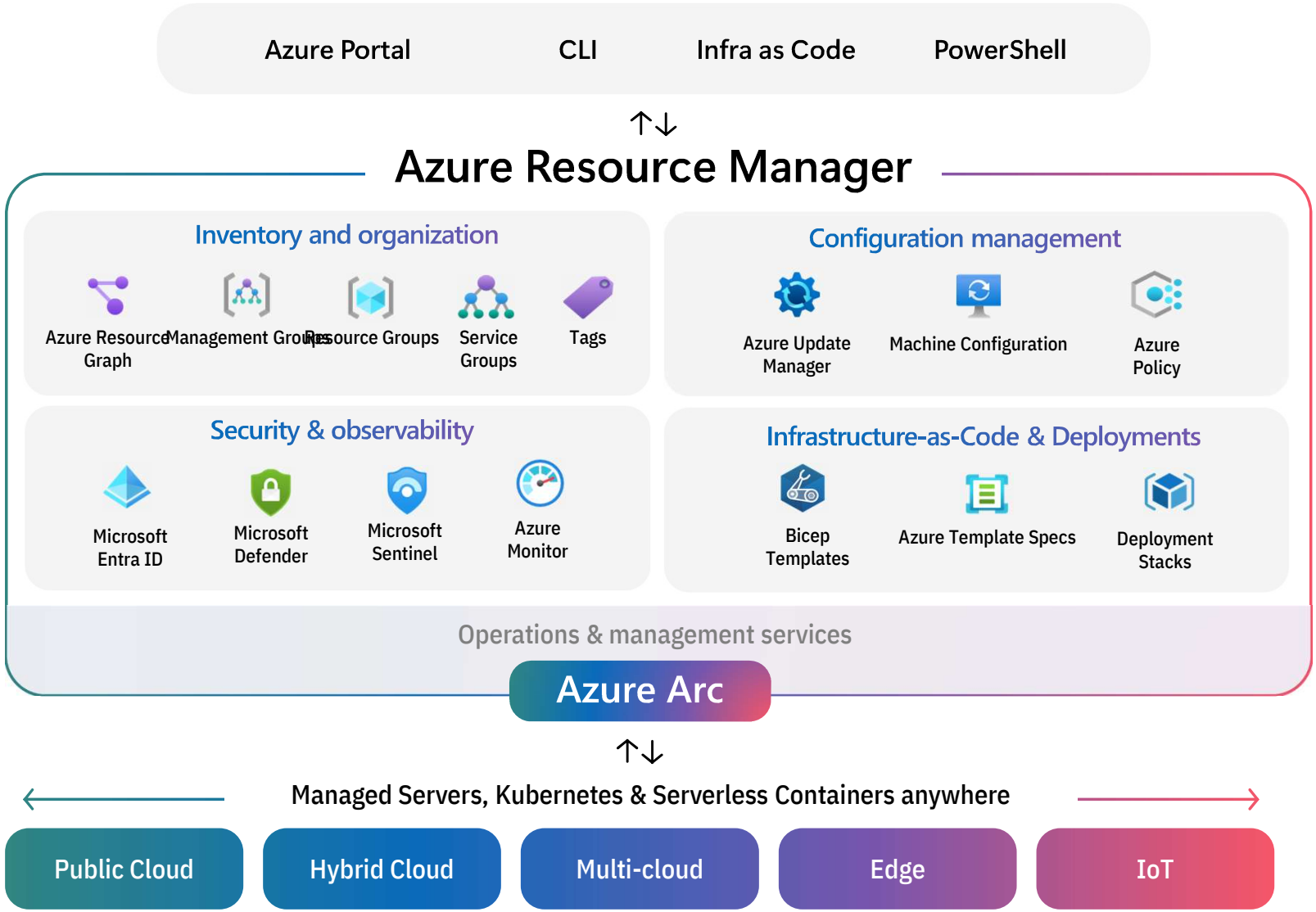
Enterprise Scale



Reasons for Hybrid Infrastructures



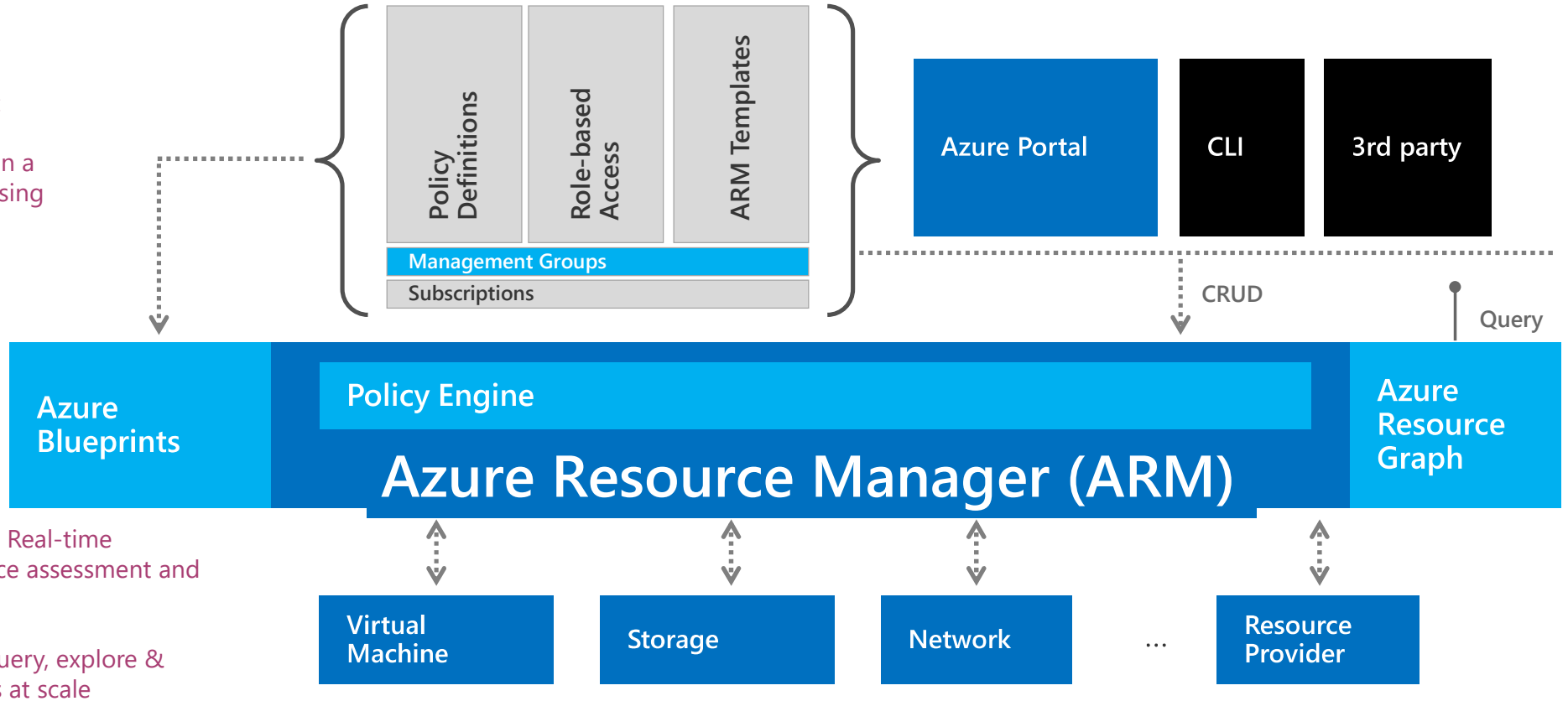

Unified operations, management, compliance, security and governance
Azure resources
Azure Arc-enabled infrastructure resources (Servers, SQL servers, Kubernetes)
Azure Arc-enabled services resources (Data services, App services, Machine Learning services)
Azure Resource Manager
Azure Arc
Azure Arc-enabled infrastructure onboarding
Azure Arc-enabled services deployment
Azure Arc-enabled infrastructure onboarding
On-premises IT infrastructure resources
On-premises Arc-enabled services (Data services, App services, Machine Learning services)
Multicloud Arc-enabled services (Data services, App services, Machine Learning services)
Multicloud IT infrastructure resources
Azure Stack HCI
vmware
aws
Amazon Web Services
Google Cloud Platform


Azure Portal
CLI
Infra as Code
PowerShell
Azure Resource Manager
Inventory and organization
Azure Resource Graph
Management Groups
Resource Groups
Service Groups
Tags
Configuration management
Azure Update Manager
Machine Configuration
Azure Policy
Security & observability
Microsoft Entra ID
Microsoft Defender
Microsoft Sentinel
Azure Monitor
Infrastructure-as-Code & Deployments
Bicep Templates
Azure Template Specs
Deployment Stacks
Operations & management services
Azure Arc
Managed Servers, Kubernetes & Serverless Containers anywhere
Public Cloud
Hybrid Cloud
Multi-cloud
Edge
IoT

Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility

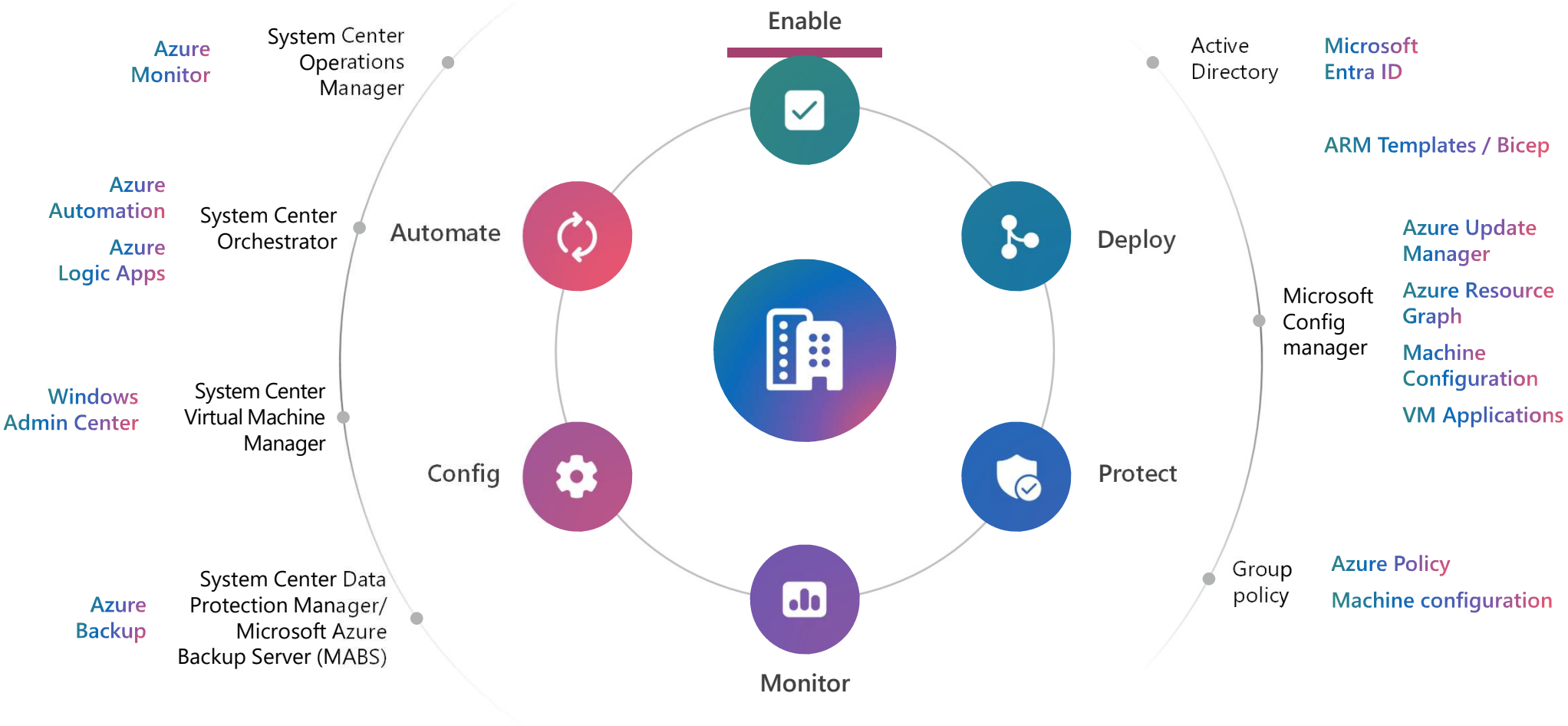
1. Environment Factory: Deploy and update cloud environments in a repeatable manner using composable artifacts



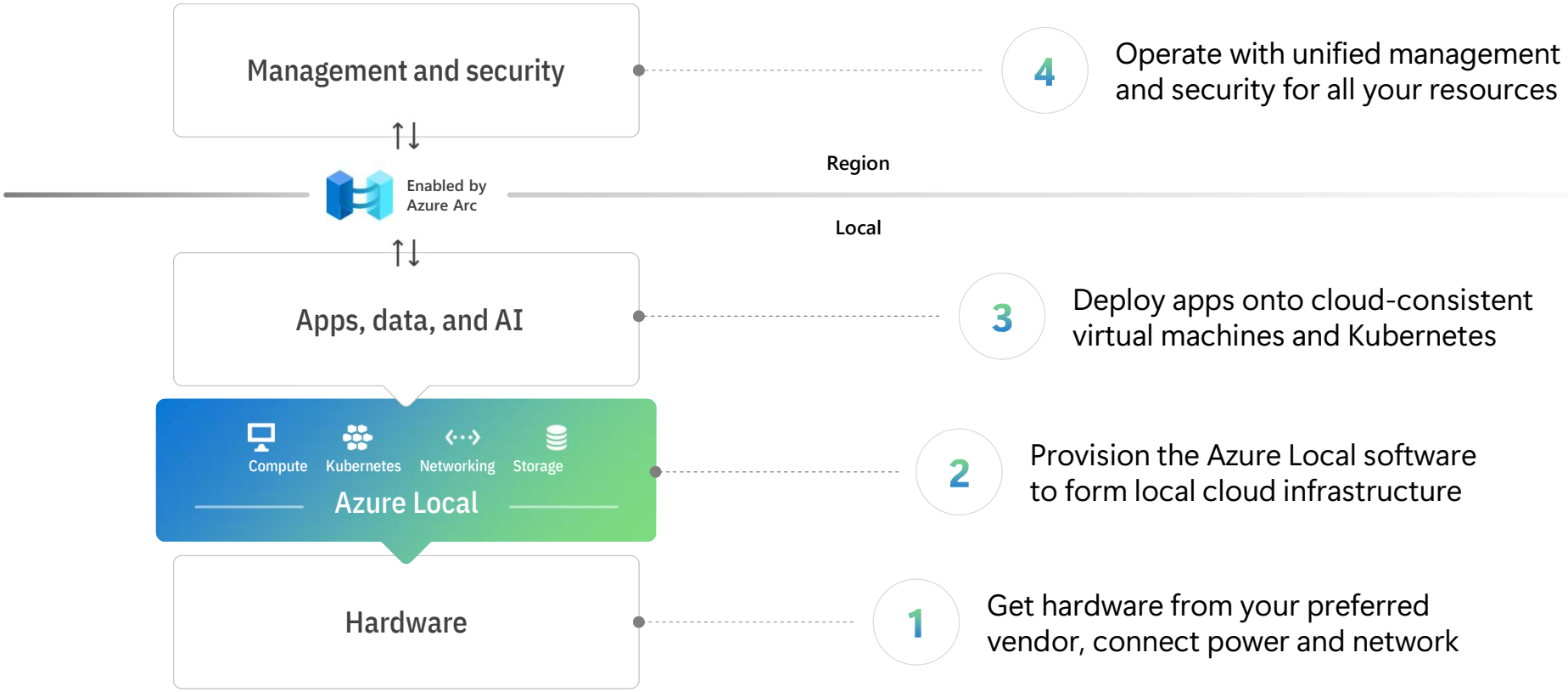
2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

3. Resource Visibility: Query, explore & analyze cloud resources at scale

Azure's strategy for managing hybrid environments



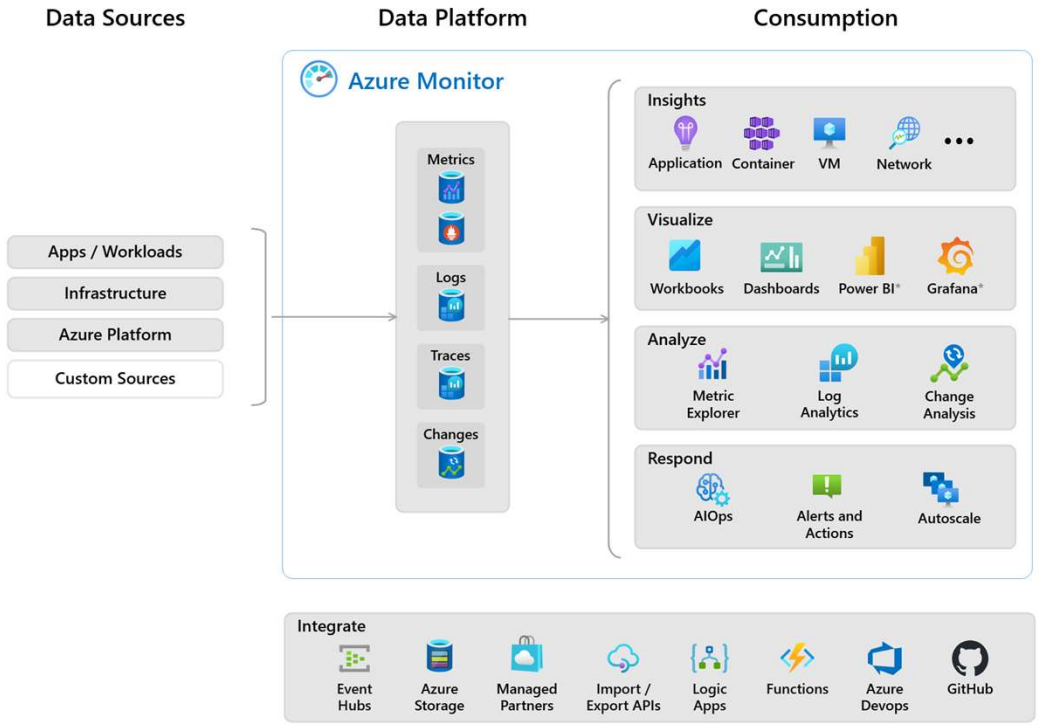
How Azure Local works (connected)



Monitor anywhere with Azure Monitor enabled by Azure Arc

Consistent monitoring across your hybrid and multi-cloud compute

- Detect & diagnose issues across apps and dependencies with application insights
- Correlate issues at infra level with insights for VMs, containers, storage, network, etc.
- Operationalize at scale with smart alerts and automated actions
- Drill down with Log Analytics for troubleshooting & deeper diagnostics
- Create visualizations with workbooks, Azure Monitor dashboards with Grafana, and Azure Managed Grafana



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

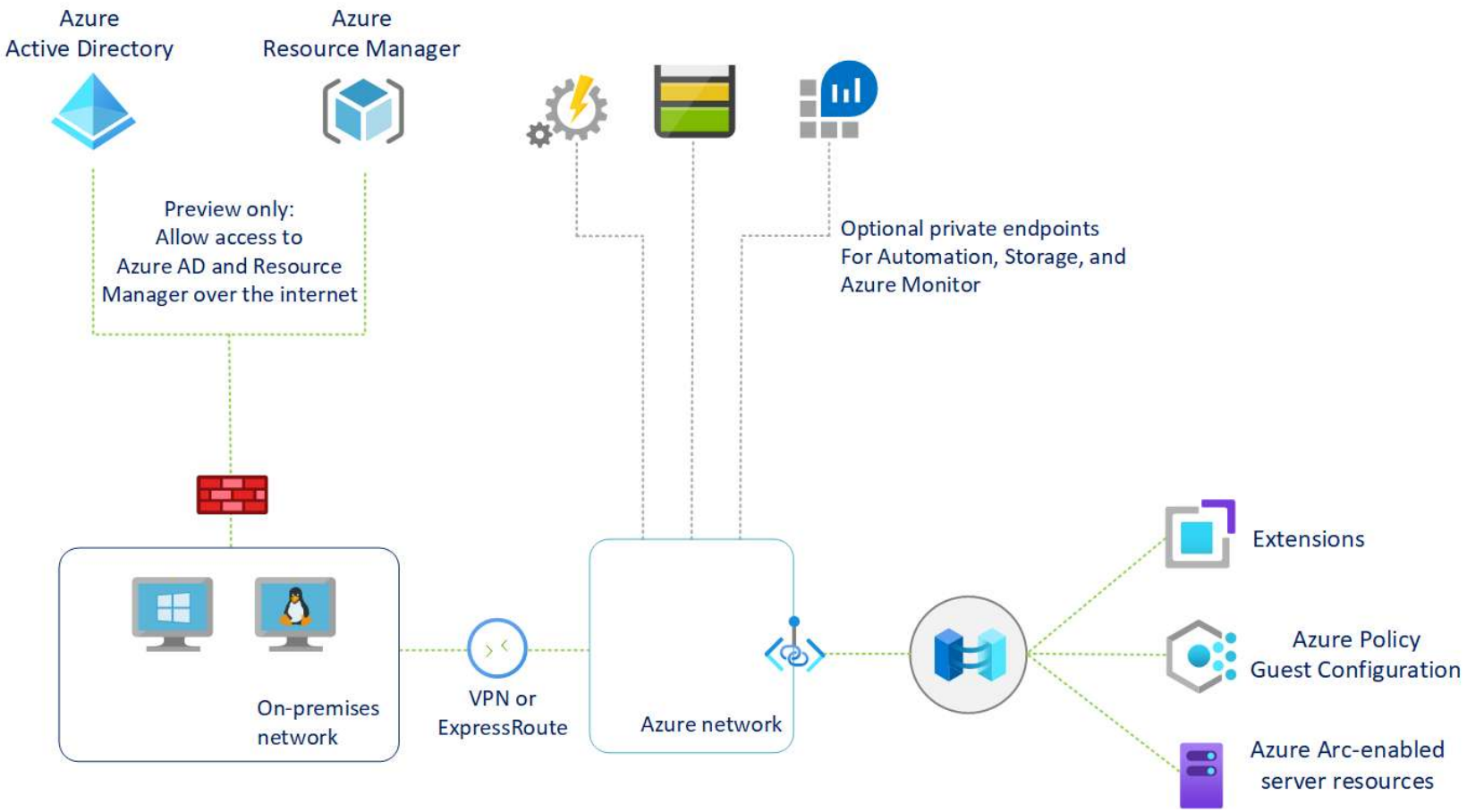
Linux

- 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 Ressource Admin**
- Resource Providers
  - **Microsoft.HybridCompute**
  - **Microsoft.GuestConfiguration**
  - **Microsoft.HybridConnectivity**
- Outbound via TCP 443 (Proxy server is supported)
- Private Link support

Private Link



Use Azure Private Link to securely connect servers to Azure Arc - Azure Arc | Microsoft Learn

Connecting VMs

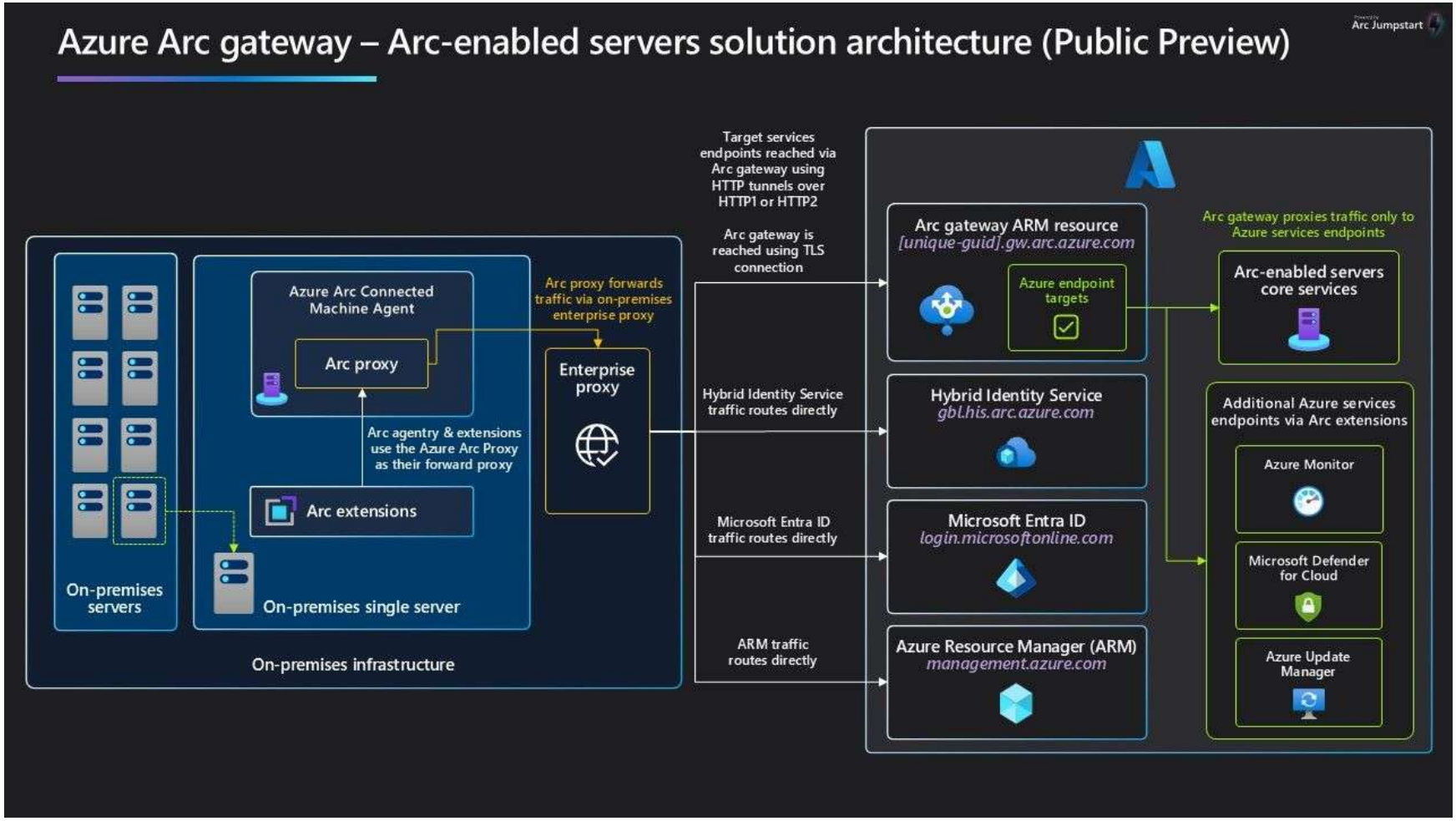
```
PS C:\Users\Administrator> try {
    $env:SUBSCRIPTION_ID = "009c17ca--4905999fba2d";
    $env:RESOURCE_GROUP = "arc_rg";
    $env:TENANT_ID = "e4f80c4f--3141bca1ced3";
    $env:LOCATION = "westeurope";
    $env:AUTH_TYPE = "token";
    $env:CORRELATION_ID = "95256887-01a2-4c82-948e-e457830cda97";
    $env:CLOUD = "AzureCloud";
    [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor 3072;
    # Download the installation package
    Invoke-WebRequest -UseBasicParsing -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$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="$env:CORRELATION_ID";authType="$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."
```

Azure Meetup
Düsseldorf

Why Azure Arc Gateway

- Azure Arc Gateway provides a single endpoint for all inbound traffic from Arc-enabled resources
- **Endpoints required without Arc gateway = 17**
  - **Using Extensions can grow up this numbers up to 150+ endpoints**
  - **Each extension has his own**
- **Endpoints required without Arc gateway = 8**
- **Arc Gateway has two components**
  - **Arc Gateway – Common Frontend for Arc traffic. Gateway is served on a specific domain**
  - **Arc Proxy – Component that routes all Arc traffic to it´s destination in Azure**

Azure Arc Gateway



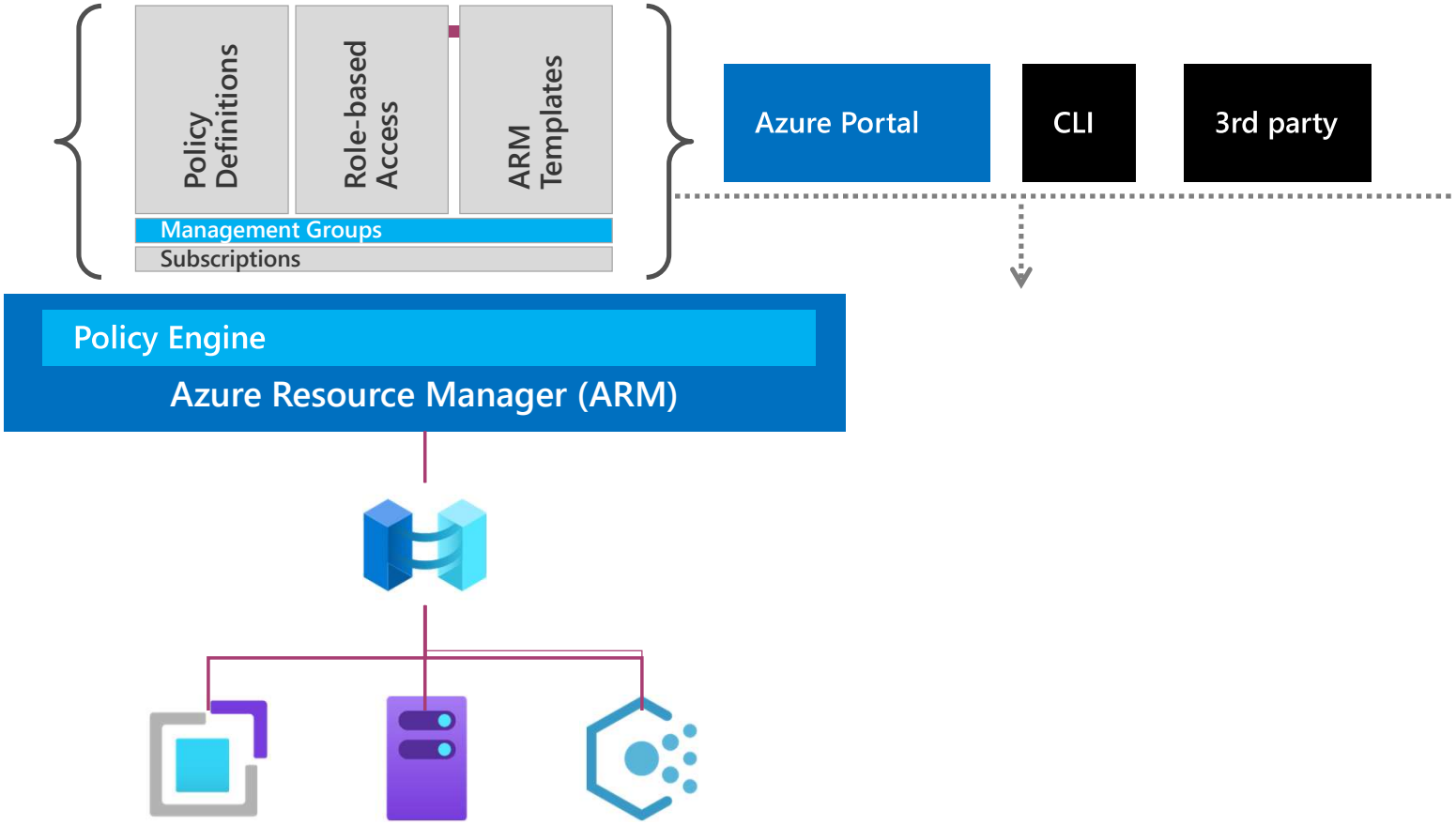
Azure Architecture

providing control over the cloud environment, without sacrificing developer agility

1. Environment Factory:
   Deploy and update
   cloud environments in a
   repeatable manner using
   composable artifacts

2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

3. Resource Visibility: Query, explore & analyze cloud resources at scale



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 ressource name (because is immutable)

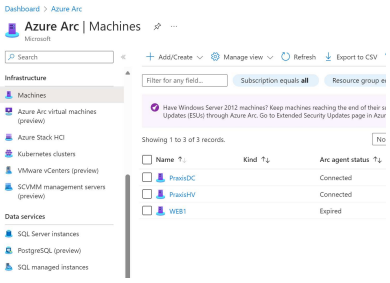
Delete and re-create is needed for Server renaming

Remove any VM-extension

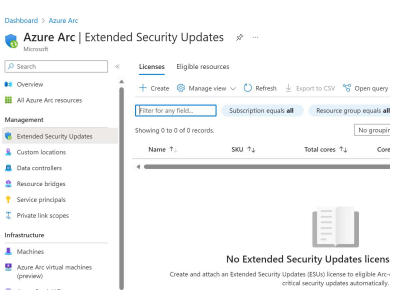
Use azcmagent to disconnect

Windows Server doesn't check for updates in Microsoft Update by default.
! Configure Windows Update client to check for other Microsoft products !

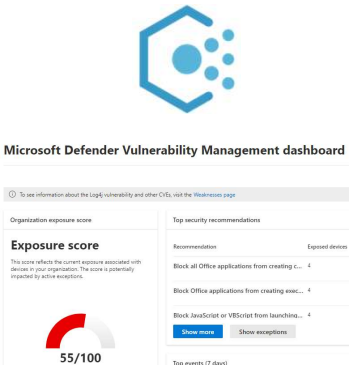
Demo Azure Arc



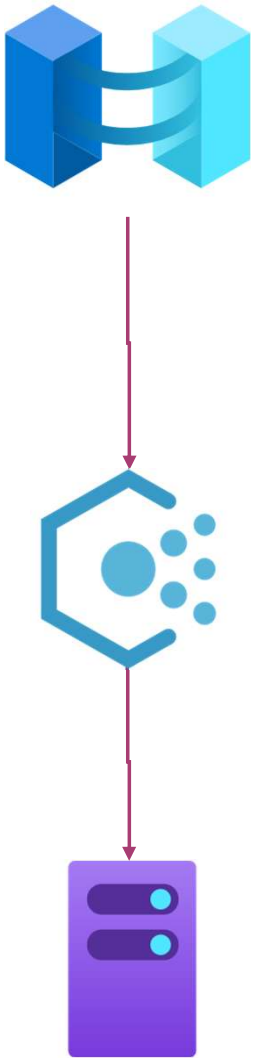
Overview about Azure Arc



Server Management



Azure Automanage Machine Configuration



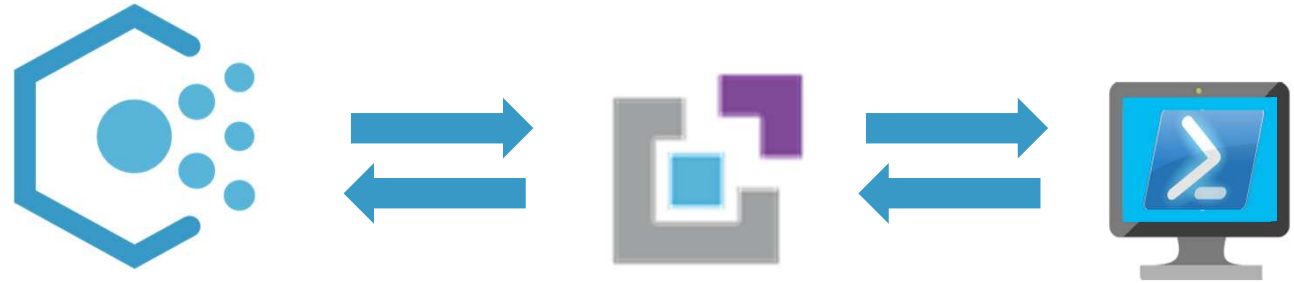
Azure Policy Guest Configuration

Renamed to

Azure Automanage Machine Configuration

Coming soon: guest configuration renames to machine configuration - Microsoft Community Hub

How VM guest policy works

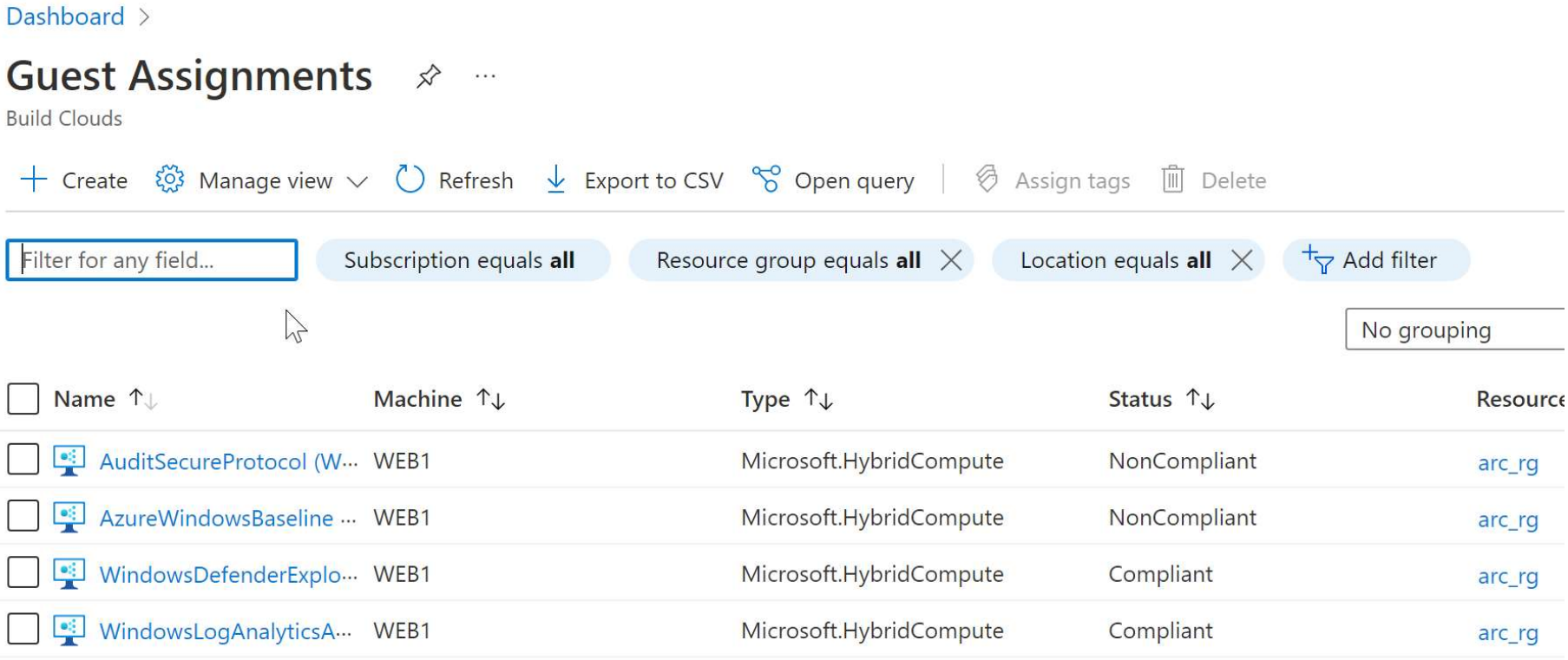


Azure Policy

Guest Configuration Extension

VM Guest environment

Guest Assignments



Azure Meetup
Düsseldorf

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 Update Manager

Patch Orchestration

Azure Managed – Safe Deployment

- Supported for Linux und Windows
- This mode activate automatic patching of the VM
- Assessment will be stored in Azure Resource Graph
- Support Patches by Availability

Customer Managed Schedules

- Only for Windows VMs
- Support no Patches by Availability
- Default Mode when nothing is configured

Windows automatic updates

- Configuration of the Windows VM would be used (Registry-/GPO-settings)

Manual updates

- Only for Windows VMs
- Support no Patches by Availability
- Mode only be used when 3rd party patch solution is in place

ImageDefault

- Only for virutal Linux VMs
- Default Mode when nothing is configured
- Support no Patches by Availability

Hotpatch

WS 2022 Datacenter: Azure Edition Server Core

Azure = GA

Azure Stack HCI = GA

Hotpatch activated by default

WS 2022 Datacenter: Azure Edition mit Desktop

Azure = GA

Azure Stack HCI = GA

Hotpatching for Azure Arc

Support for Windows Server 2025
(Standard and Enterprise is availablet)
Status for older OS Systems not knowing

[Hotpatch für Windows Server: Azure Edition | Microsoft Learn]
[Hotpatching: Improving server security and productivity | Windows Server Summit 2024]

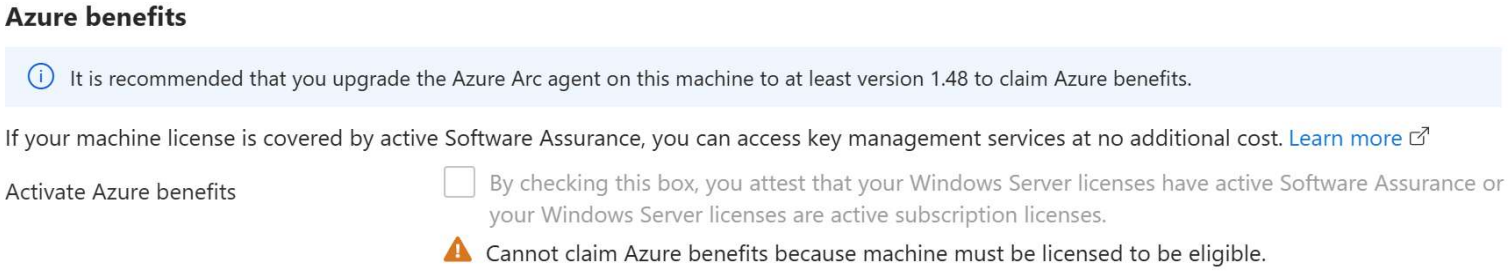
Price Overview

Service	Price
Azure	Free
Extended Security Updates (ESUs) via Arc	Free
Defender for Server P2 via Arc	Free
Azure Stack HCI clusters	Free
Azure Arc	**5$ (4,62€)**
Other enabled Defender Plans via Arc	0,16$ per Day (5$ per Month)

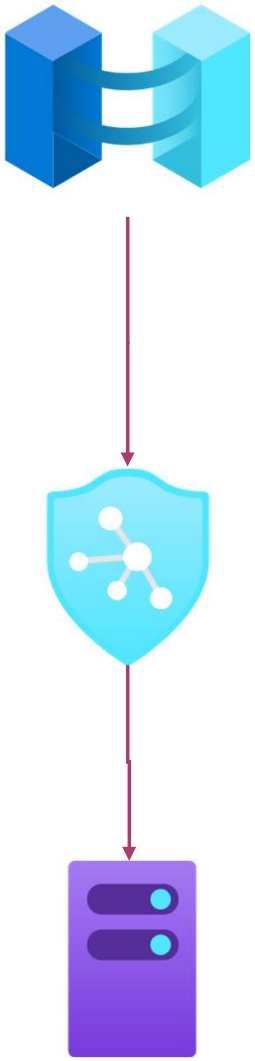
Azure Meetup
Düsseldorf

Price changes with Windows Software Assurance

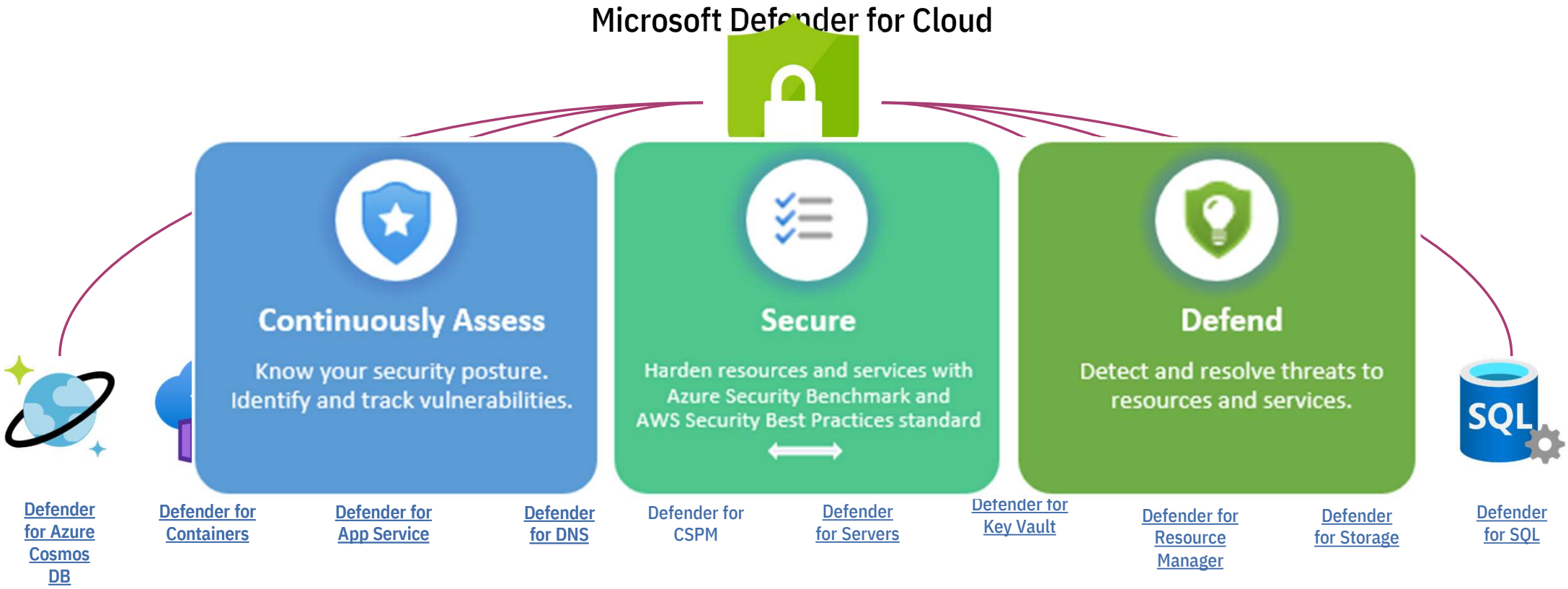
- Microsoft announced on Ignite 2024 that the following services are free to customers with activated Windows Server Software Assurance
  - Azure Update Manager
  - Azure Change Tracking and Inventory
  - Azure Machine Configuration
  - Windows Admin Center in Azure for Arc
  - Remote Support
  - Network HUD
  - Best Practices Assessment
  - Azure Site Recovery (Configuration Only)



Announcing General Availability: Windows Server Management enabled by Azure Arc | Microsoft Community Hub



Defender for Cloud


Microsoft Defender for Cloud
Continuously Assess
Know your security posture. Identify and track vulnerabilities.
Secure
Harden resources and services with Azure Security Benchmark and AWS Security Best Practices standard
Defend
Detect and resolve threats to resources and services.
SQL
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

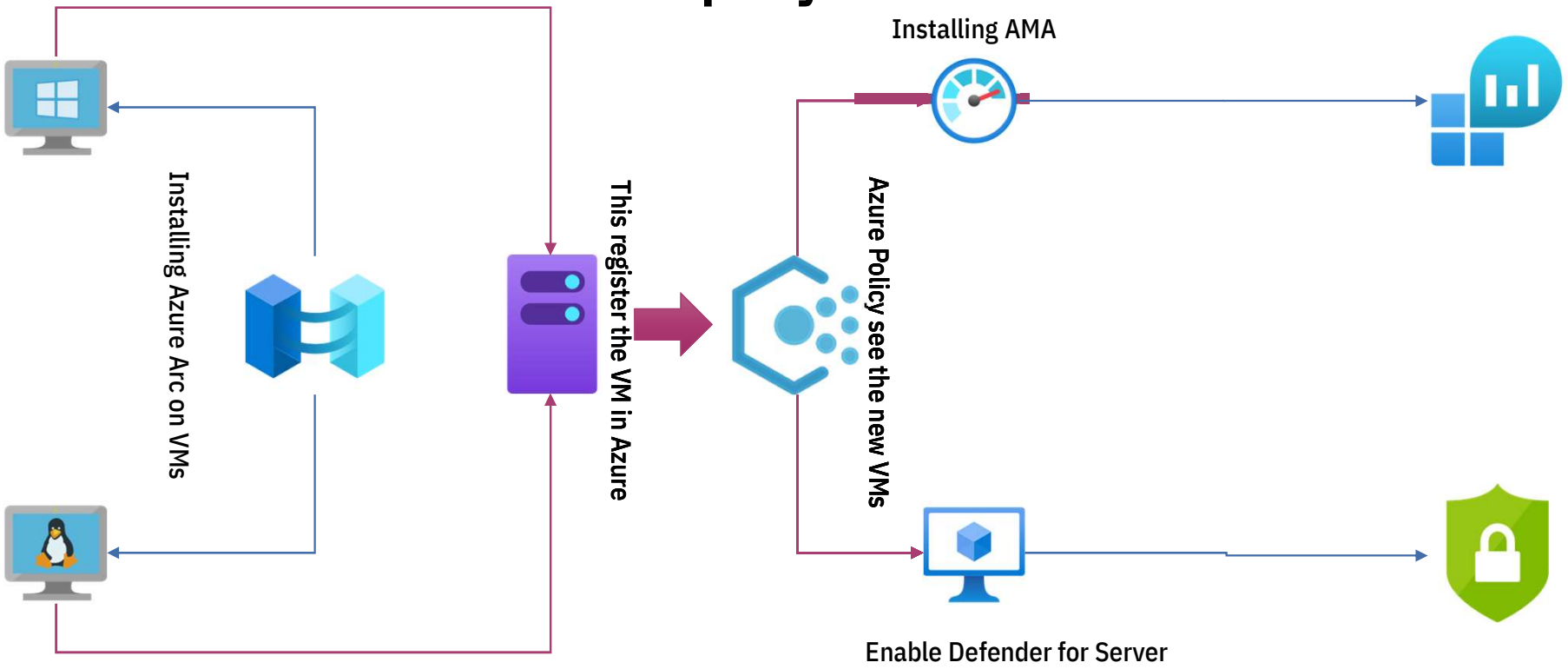
Activation of Defender for Servers

- 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

Defender for Server

	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**

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

What's new

Arc-enabled servers

- Arc server agent auto-upgrade
- Machine configuration – OS policy editor
- Customizable baselines
- Windows Server 2025 Recovery Environment configuration through policy

Arc-enabled Kubernetes

- Access any other resources in Azure securely with workload identity
- Offline access to secrets on edge workloads
- Managed ArgoCD Support

Multi-cloud management

- Google Cloud Platform support
- AWS S3 to Azure Storage mover

http://aka.ms/Ignite25/ArcBlog

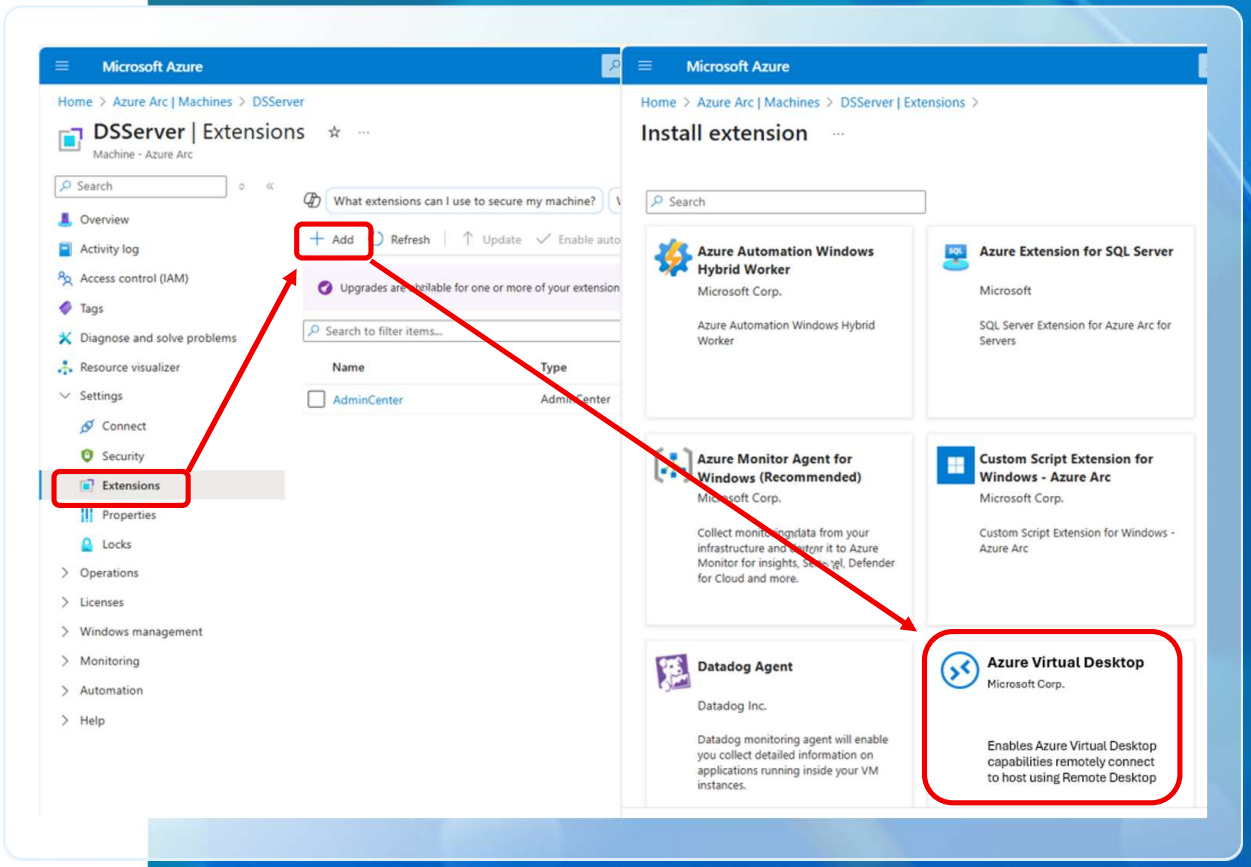
Azure Arc Azure Virtual Desktop extension deployment

Pre-requisites

- Admin creates host pool
- Admin creates VM using tools of their choice

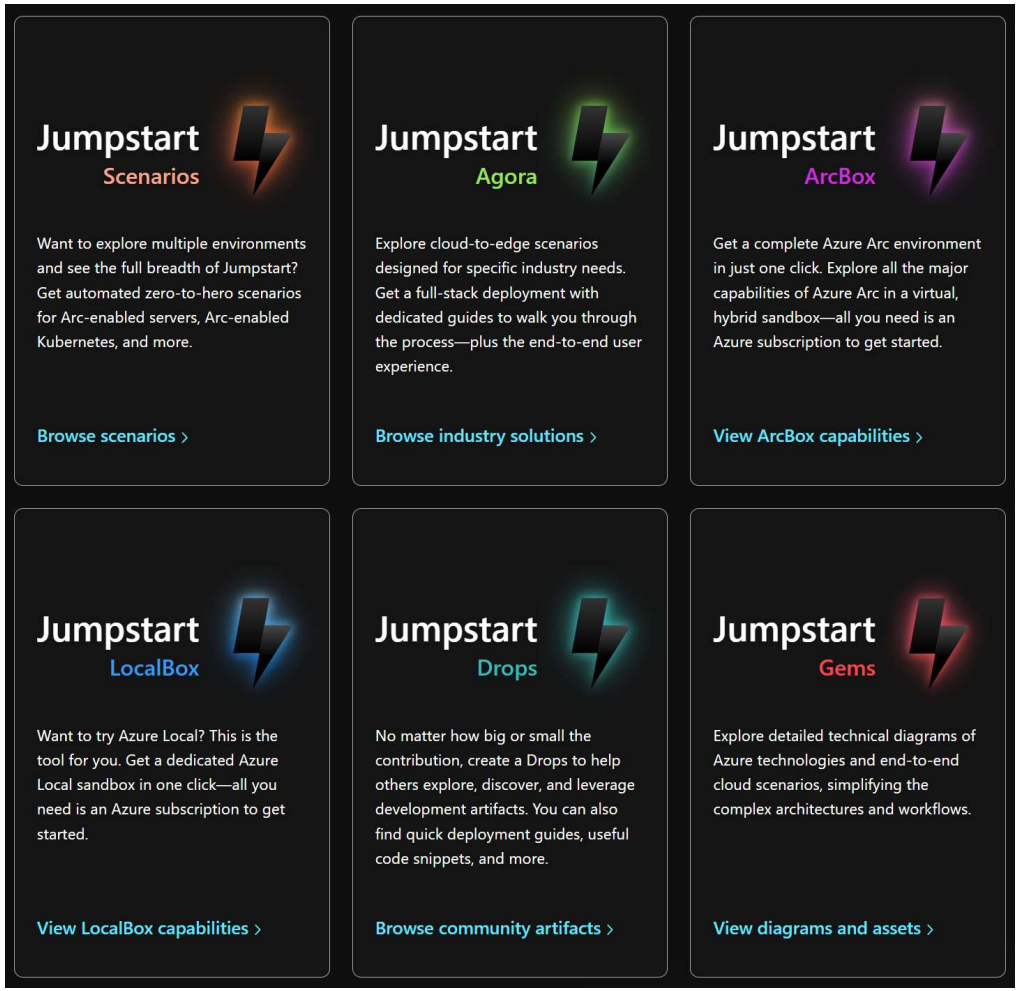
1. Install Azure Arc Connected Machine Agent
2. “Add” Azure Virtual Desktop Arc extension
   - Installs Azure Virtual Desktop agents
   - Installs Remote Desktop Session Host (RDSH role (Windows Server only)
   - Adds device to Azure Virtual Desktop host pool

Leverage Partner solutions for creating virtual machines (VM), lifecycle and power management



How To Start

Overview | Azure Arc Jumpstart



How to start

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

Azure Arc Community Monthly Meetup

GitHub - microsoft/azure_arc_community: Public repository for hosting the Azure Arc Community content

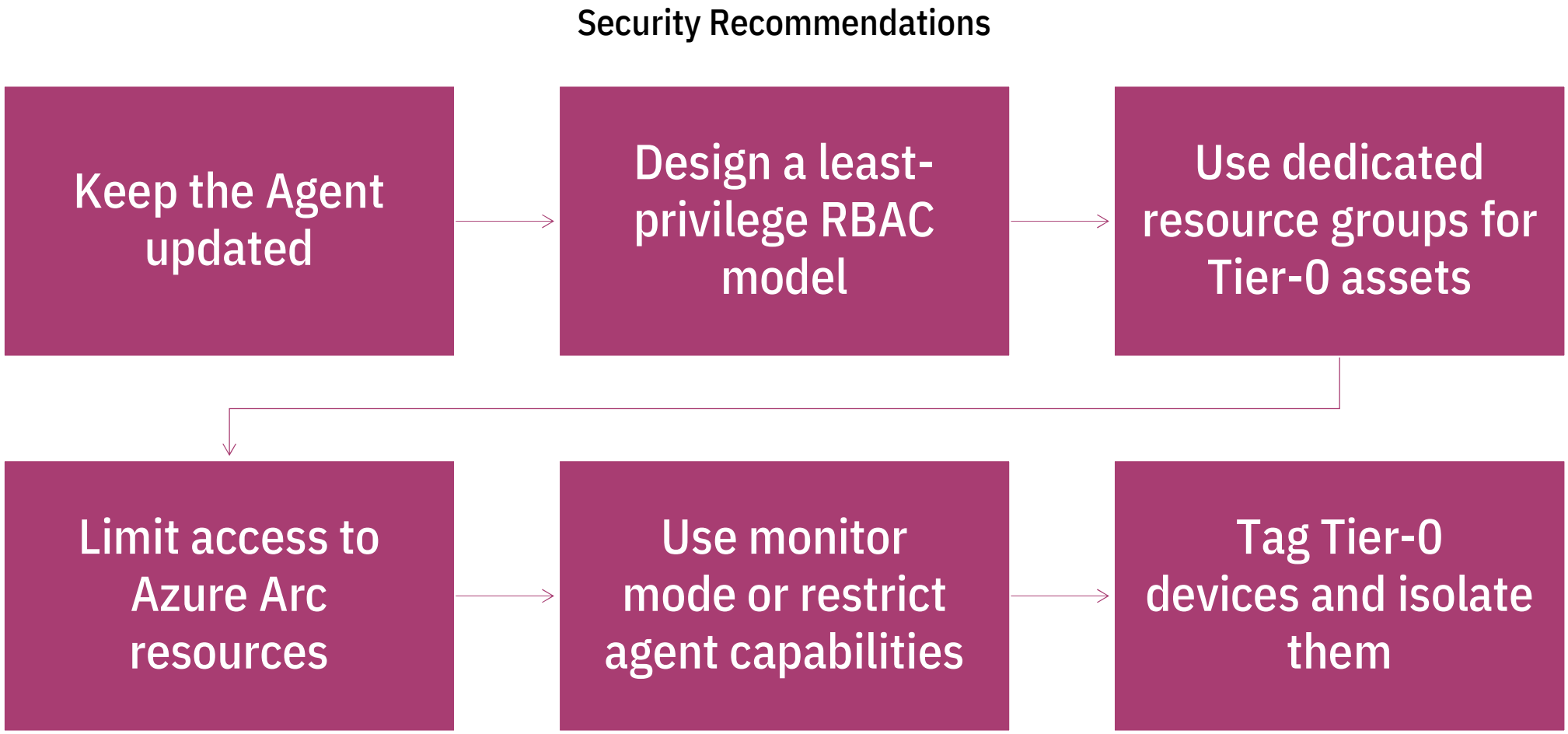
Contributors 3


likamrat Lior Kamrat


microsoftopensource Microsoft Open ...


csand-msft Chris Sanders

aka.ms/ArcCustomerSignup


Security Recommendations
Keep the Agent updated
Design a least-privilege RBAC model
Use dedicated resource groups for Tier-0 assets
Limit access to Azure Arc resources
Use monitor mode or restrict agent capabilities
Tag Tier-0 devices and isolate them

Summary and Best Practices

Links

- Arc Jumpstart Training – YouTube
- A Guide to Adaptive Cloud at Microsoft Ignite 2024 | Microsoft Community Hub
- Azure Arc Jumpstart
- PowerShell Gallery | jumpstart
- Azure Arc Jumpstart Drops
- Build a Business case with Azure Migrate - Azure Migrate | Microsoft Learn
- We have been waiting for SO LONG...Arc Gateway!
- Azure Arc Security recommendation by Jeffrey Apel | LinkedIn
- Connect to AWS with the multicloud connector in the Azure portal - Azure Arc | 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
- Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
- Pricing – Azure Arc | Microsoft Azure

Save the Date

s|three

Jetzt hafte ich

IT-Sicherheitsverantwortung 2026 – NIS2, Regulatorik und persönliche Haftung

Speakers

Alexander Busse
Interim CISO & KI-Engineer für Security Governance

Thomas Ullrich
Internationaler Management- & Cybersecurity-Advisor für Governance & Regulierung

Event

19. Februar 2026, 17:30 Uhr

Online & bei uns im Office
SThree Düsseldorf
Georg-Glock-Str. 12

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

Gregor Reimling (he/him)

th1

Chief Azure Technologist @ adesso SE, Germany

Gregor is awarded with the Microsoft MVP for Microsoft Azure and Security. He works as Chief Azure Technologist for adesso SE and is technical lead for Azure . His main areas are Microsoft Azure, Enterprise scale architectures, Cloud Security, Governance, Hybrid and Migration.

gregor@reimling.eu

reimling.eu

@GregorReimling

/in/GregorReimling

youtube.com/@GregorReimling

github.com/GregorReimling

Microsoft MVP Most Valuable Professional

Azure & Security

Azure Meetup BONN

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

th1 Sicher, dass du deine Pronomen nicht anpassen möchtest? =)
thorben.forke@adesso.de, 2025-02-20T00:03:28.494