



IT biztonsági megoldások hibrid/multi cloud környezetekre

Berecz Sándor
2023.09.05

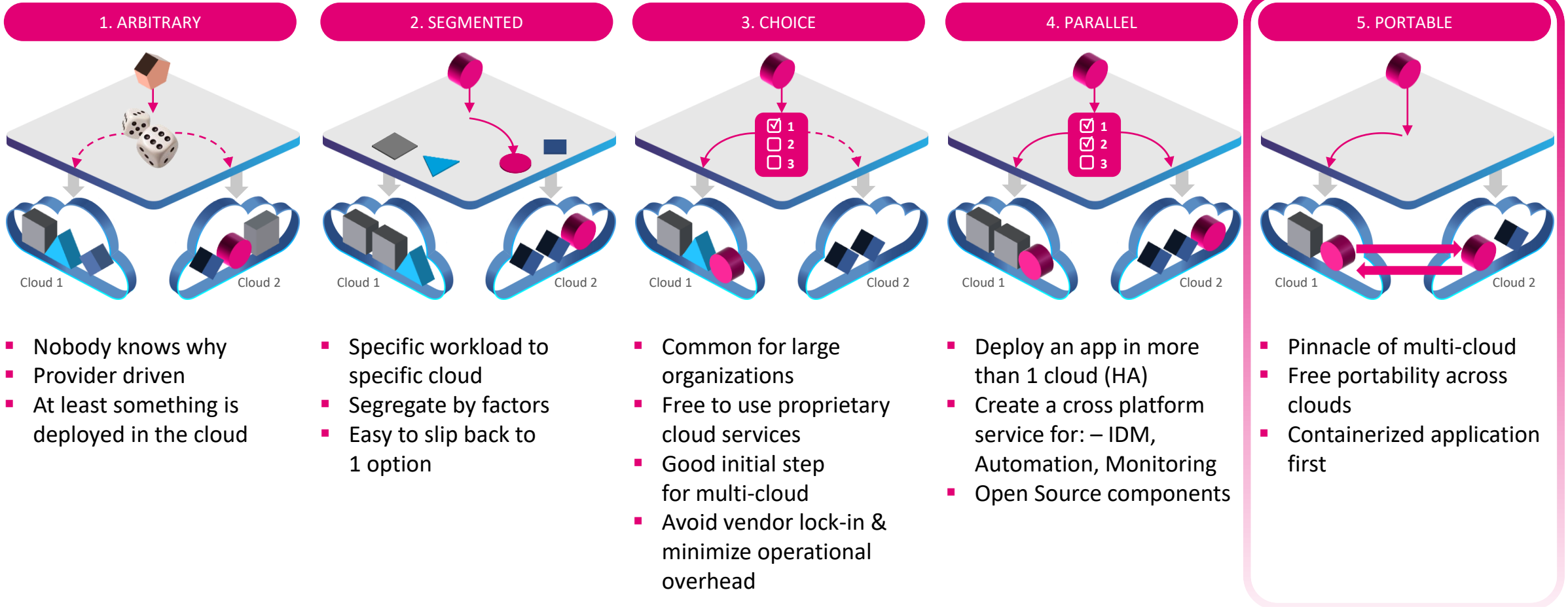


Next Gen
**HYBRID
DATA
CENTER**



Multi Cloud Decisions and options

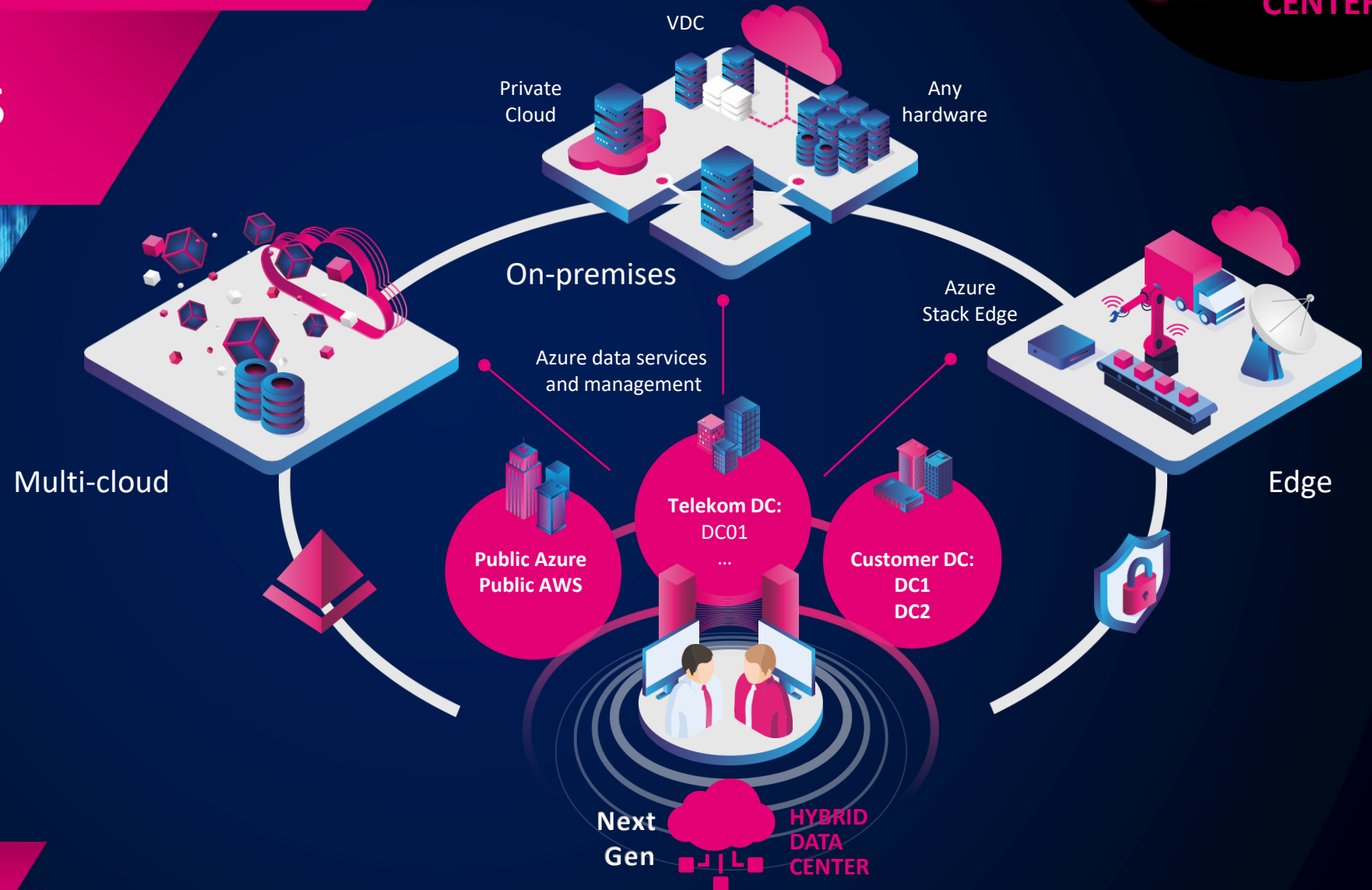
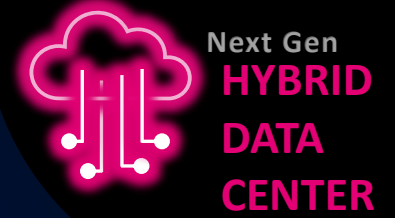
Multi-Cloud means different things to different people.



Next Gen
**HYBRID
DATA
CENTER**



Converged IaaS/PaaS offering for our customers



Challenges for multi-cloud and hybrid environments

Resource inventory

Security visibility

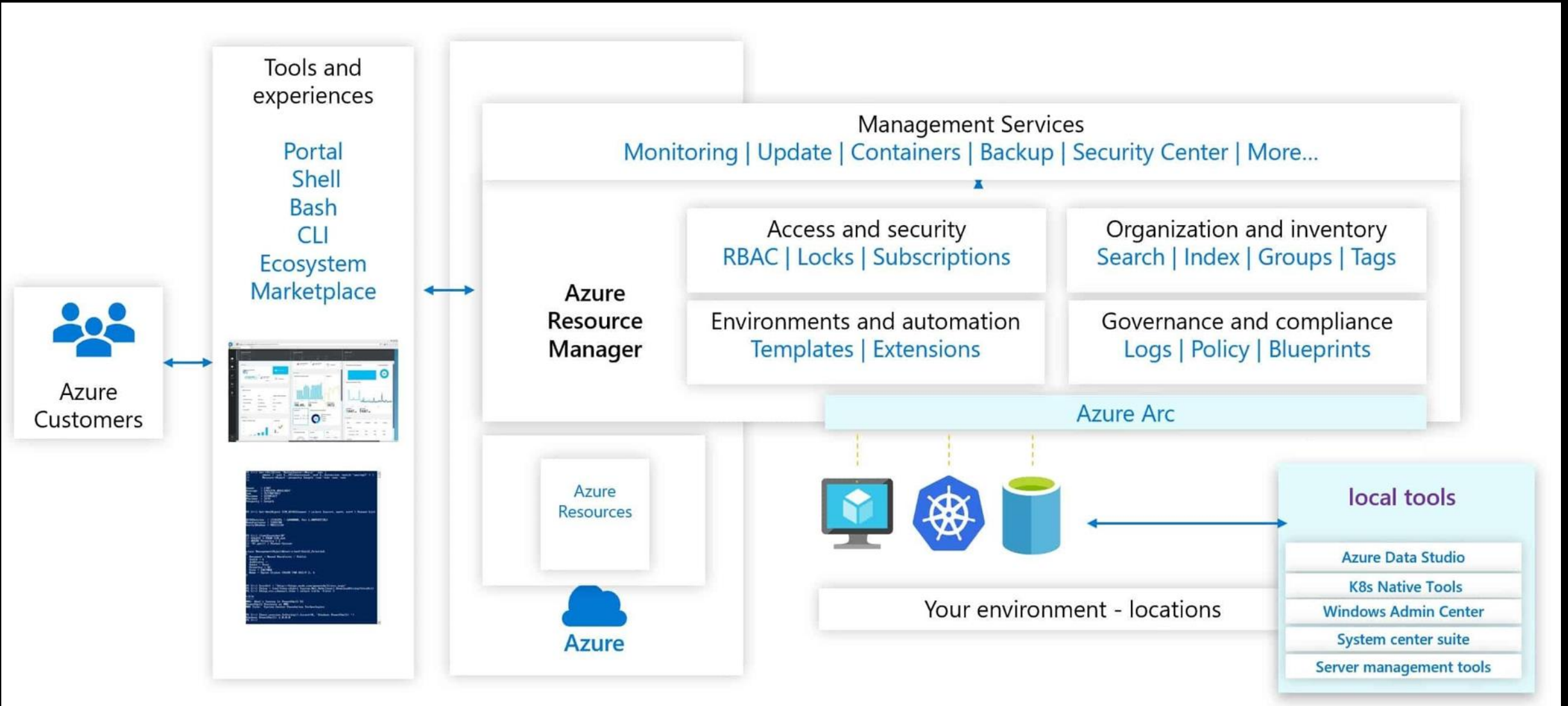
Access controls and permissions management

Vulnerability and Patch Management

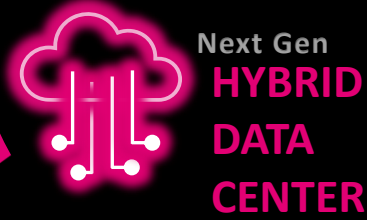
Data governance

Traditional security controls - Network, Data, IAM

Azure Arc Management Overview



Azure Arc and Azure resources in the Azure Portal



Microsoft Azure (Preview) Search resources, services, and docs (G+)

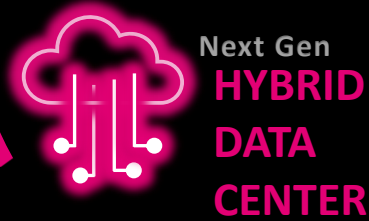
Home > All resources

Subscription == all Resource group == all Type == 4 selected Location == all

Showing 1 to 17 of 17 records. ☐ Show hidden types

Name	Type	Resource group	Location	Subscription
Kubernetes - Azure Arc				
Kubernetes service				
Server - Azure Arc				
☐ CloudLinux	Server - Azure Arc	ContosoRG	East US	Contoso
☐ CloudWin	Server - Azure Arc	ContosoRG	East US	Contoso
☐ OnPremLinux	Server - Azure Arc	ContosoRG	East US	Contoso
☐ OnPremWin	Server - Azure Arc	ContosoRG	East US	Contoso
Virtual machine				
☐ k8s-master-15210696-0	Virtual machine	TestAKE1211-2	East US	Wide World
☐ k8s-master-30122681-0	Virtual machine	WWISF3	East US	Wide World
☐ k8s-master-36673619-0	Virtual machine	WWISP3	East US	Wide World
☐ marcool001	Virtual machine	devtestmarcool2388179951000	North Europe	Wide World

Azure Arc Tagging



Microsoft Azure (Preview) Search resources, services, and docs (G+)

Home > All resources > OnPremLinux

All resources

Microsoft

+ Add Manage view ...

Filter for any field...

Name ↑↓

- ContosoK8s1
- ContosoK8s2
- TestArcCluster1211
- SanFrancisco-Warehouse
- Singapore-Warehouse
- CloudLinux
- CloudWin
- OnPremLinux**
- OnPremWin

OnPremLinux | Tags

Server - Azure Arc

Search (Ctrl+/) Delete all

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tags to resource groups. Tag names are case insensitive, but tag values are case sensitive. [Learn more about tags](#)

Name	Value
City	: Redmond
CountryOrRegion	: US
Datacenter	: Eastlake
StateOrDistrict	: WA
	:

OnPremLinux (Server - Azure Arc)

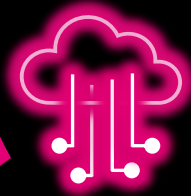
City : Redmond CountryOrRegion : US Datacenter : Eastlake StateOrDistrict : WA

No changes

Navigation Menu:

- Overview
- Activity log
- Access control (IAM)
- Tags**
- Diagnose and solve problems
- Settings
 - Security
 - Extensions
 - Properties
 - Locks
- Operations
 - Policies
 - Update management
 - Inventory
 - Change tracking
- Monitoring
 - Insights

Update Management



Next Gen
HYBRID
DATA
CENTER

Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > Azure Arc > WAC01

WAC01 | Update management

Server - Azure Arc

Search (Ctrl+/)

Manage multiple machines Schedule update deployment

Compliance ⓘ

Missing updates (3)

Update agent readiness ⓘ

Failed update deployments ⓘ

Learn more

Update Management for Windows

Manage machines

Provide feedback

0 Critical
1 Security
2 Others

0 out of 0 in the past thirty days

Ready (view)

Missing updates (3) Deployment schedules History

Filter by name

Classifications: All

Update name	Classification	Published date	Information link
2021-05 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems (KB5003171)	Security updates	5/11/2021	KB5003171
Windows Malicious Software Removal Tool x64 - v5.89 (KB890830)	Update rollups	5/11/2021	KB890830
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.339.480.0)	Definition updates	5/12/2021	KB2267602

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Security

Extensions

Properties

Locks

Operations

Policies

Update management

Inventory

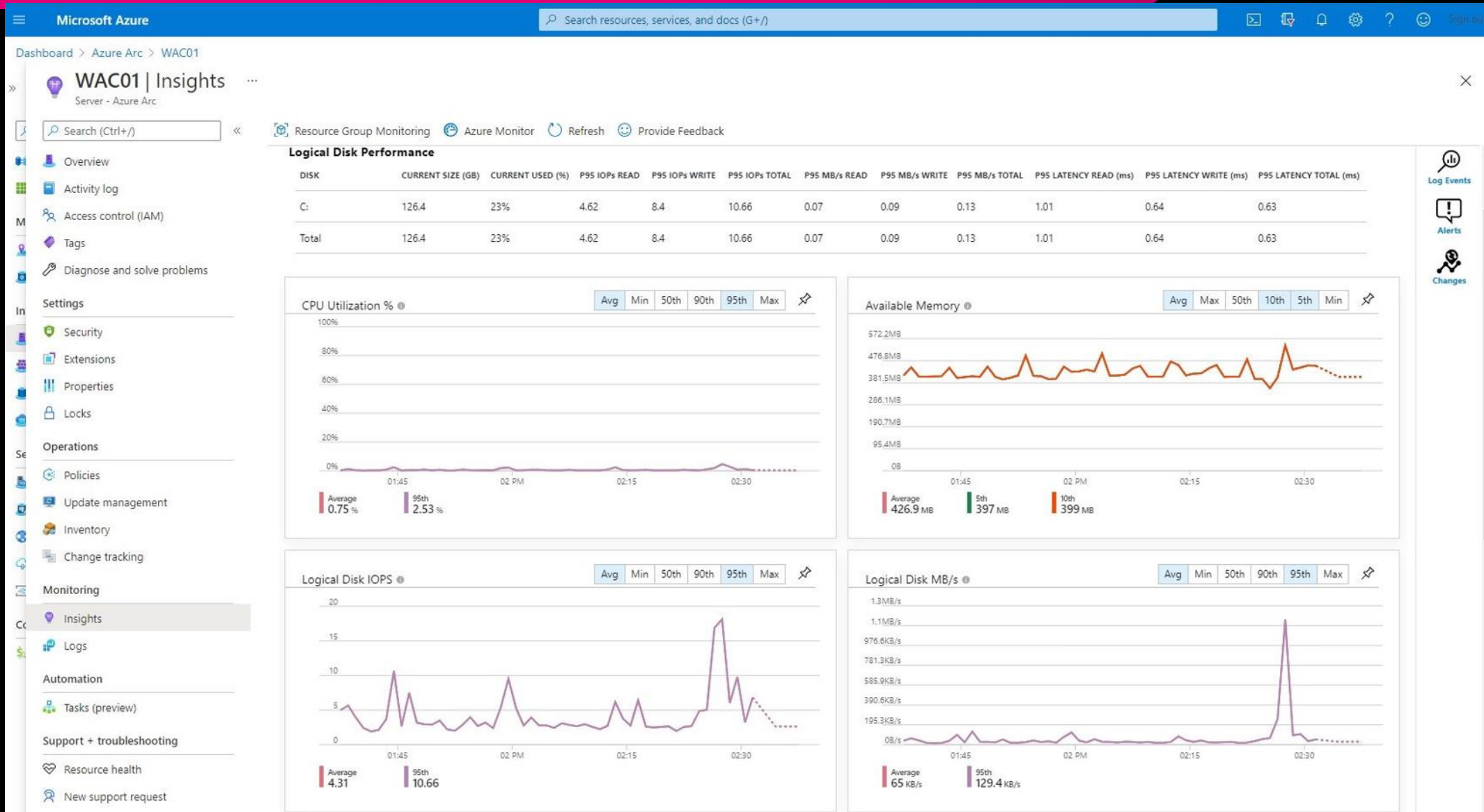
Change tracking

Monitoring

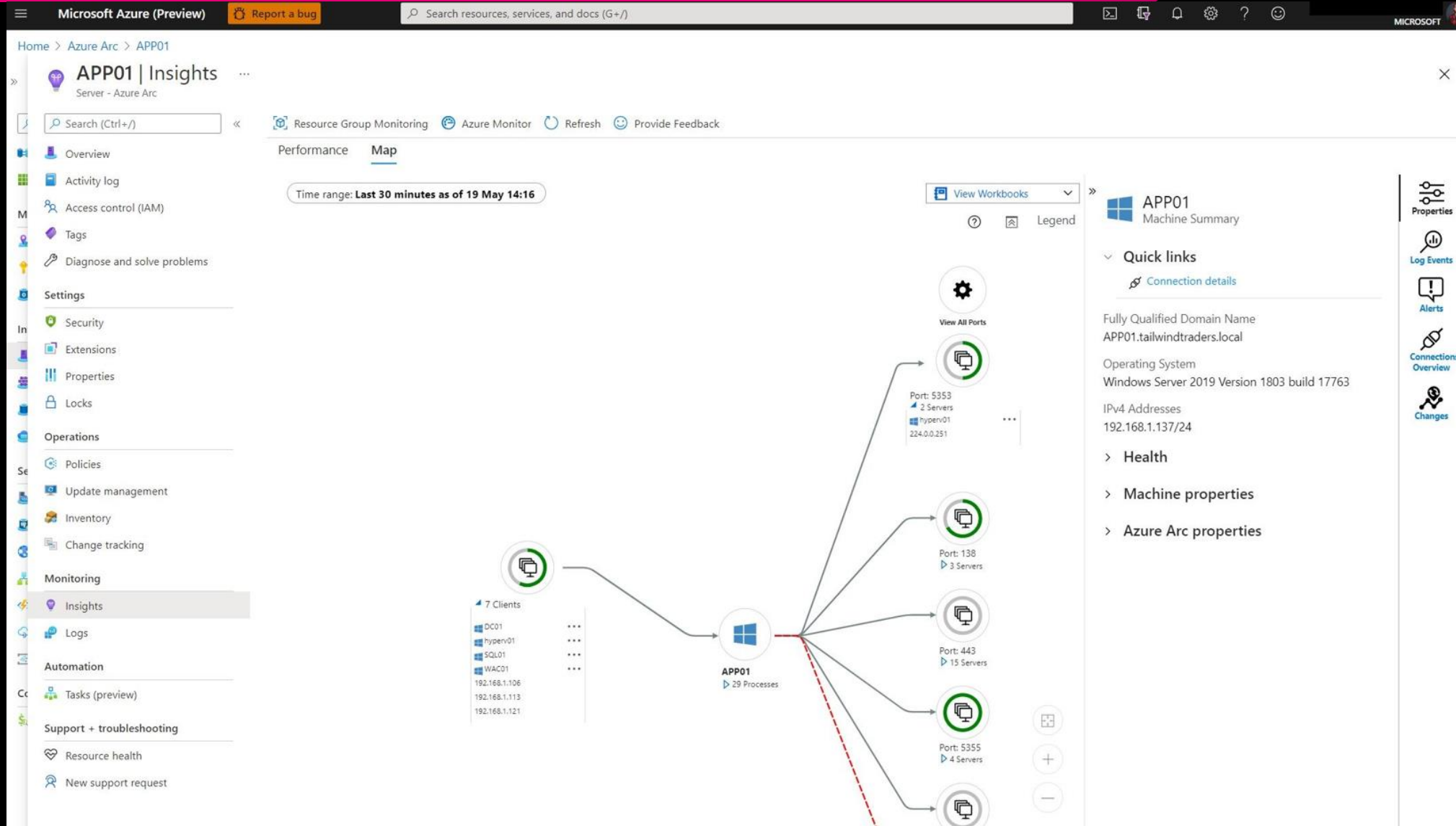
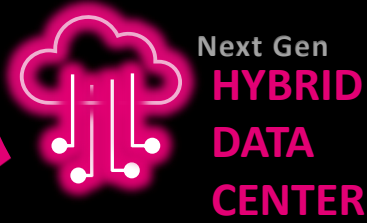
Insights

Logs

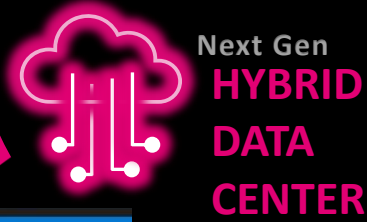
Monitoring



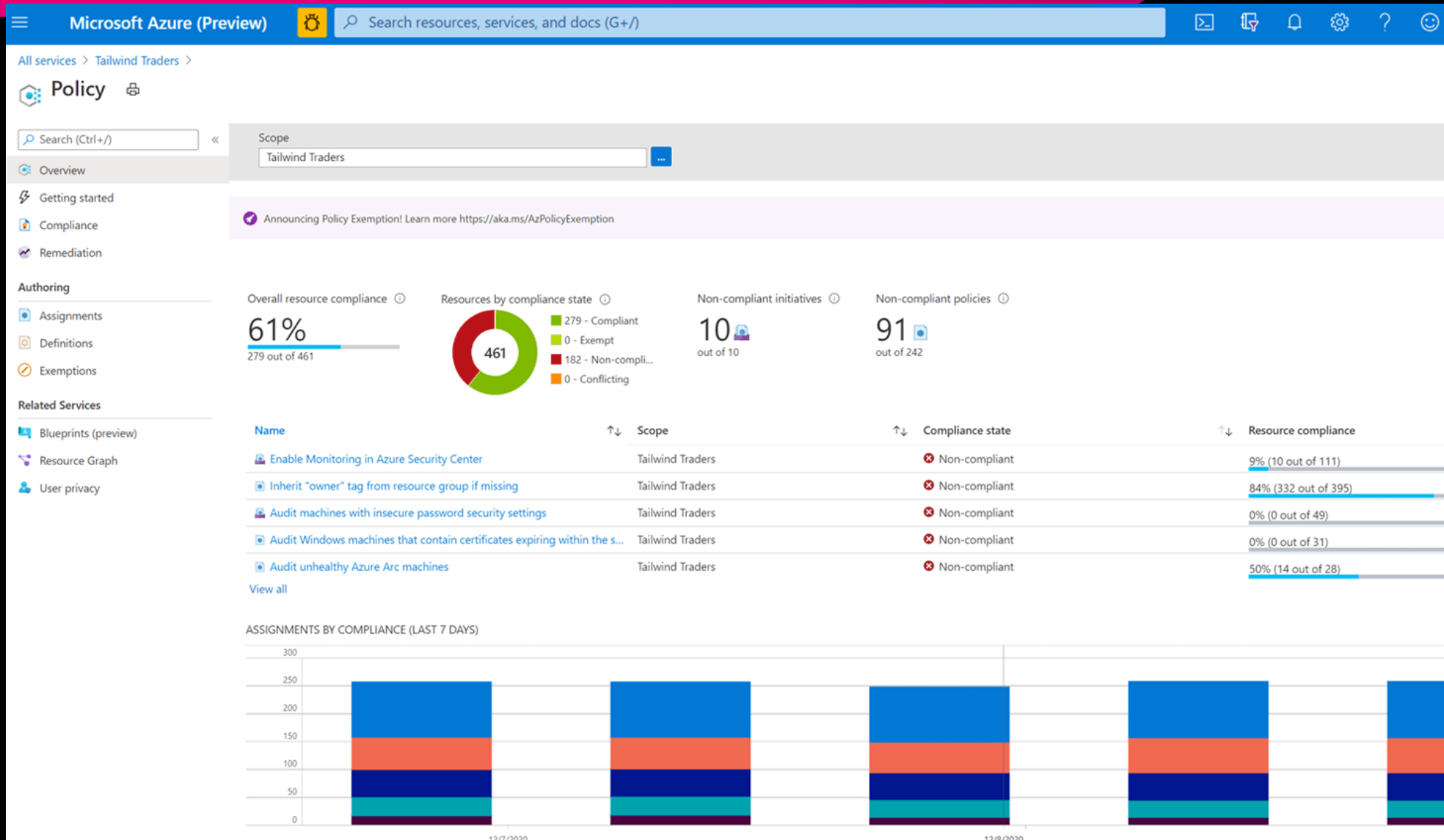
Azure Monitor Map



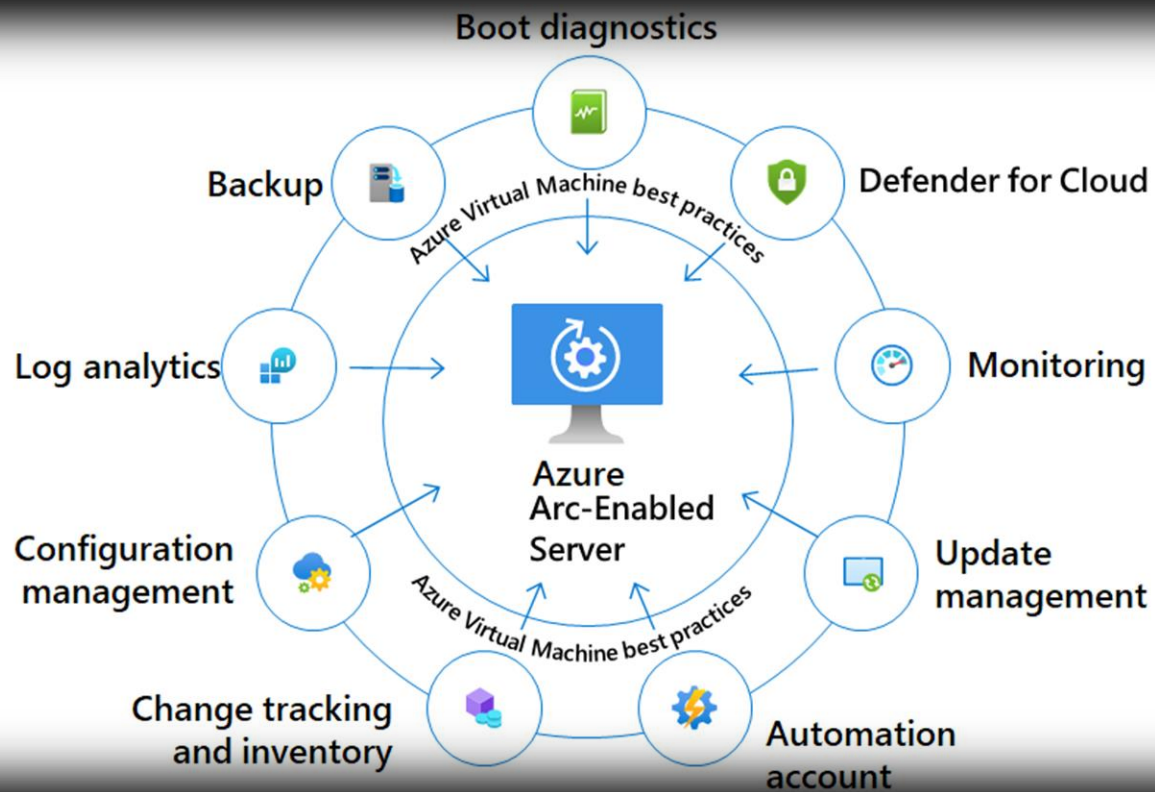
Next Gen
HYBRID
DATA
CENTER



Azure Policy



Toolset



- Intelligently onboards virtual machines/bare metal to select best practices Azure services
- Automatically configure each service per Azure best practices
- Support customization of best practice services
- Monitor for drift and corrects for it when detected
- Provide a simple experience (point, click, set, forget)

Microsoft Security Copilot

Microsoft Security Copilot

The first generative AI security product that empowers SOC analysts to defend their organizations at machine speed and scale

Classified as Microsoft Confidential



Microsoft Security Copilot

💠 Tell me about my latest incidents.

💠 Are any of my machines affected?

💠 Summarize this incident in PowerPoint.

💠 Which alerts are being triggered the most?

💠 What is log4shell?

💠 How can I improve my security posture?

How can I improve my security posture

Jan 10, 12:38 PM

Here are three evidence-based recommendations to improve your security posture:

1. **Use Microsoft Intune ASR rules to prevent common attack techniques:** This will help protect your devices from common attack techniques. Currently, 438,174 out of 758,659 devices are impacted. Learn more about ASR rules [here](#).
2. **Use Microsoft Intune to enforce the latest Defender security baseline:** This will ensure that your devices are up-to-date with the latest security settings. Currently, 438,174 out of 758,659 devices are impacted. Learn more about the Defender security baseline [here](#).
3. **Use Microsoft Intune Endpoint Privilege Management to reduce exposure by enabling standard users and limiting local admin accounts:** This will help minimize the attack surface by reducing the number of local admin accounts. Currently, 438,174 out of 758,659 devices are impacted. Learn more about Endpoint Privilege Management [here](#).

✓ Sources

Microsoft Intune

✓ Confirm

🎯 Off-target

📄 Report

📌 Pin

Let's go into real Hybrid

- *Bring the power of cloud-native resource management to your on-premises datacenters*
- *Deliver robust and innovative Azure Cloud Management Services to any location*

- Modernization (increase of functionalities) of existing Datacenter services
- NO CAPEX investment needed
- Best of both worlds – Public and Private cloud benefits offered end to end
- Overcoming data residence issue in regulated and public sectors



Exercising governance with Azure Policies



Leveraging the power of cloud automation



Gaining deep insight with Log Analytics



Leverage cloud native management



Securing your workloads



Protecting your data with Azure Backup



Datacenter
(Hosting + Connectivity)



Futurezone 3.0 for Next Gen Hybrid DC Demo



Next Gen
**HYBRID
DATA
CENTER**

Thank you!



LIFE IS FOR SHARING.

cloudsolutions@telekom.hu