TD SYNNEX

BENVENUTI!!!

skybackbone engenio

25 ottobre 2024

Presentazione Gruppo

Mauro Tronchin
Azure Meetup Veneto

Il gruppo nasce con l'obiettivo di creare una community per la condivisione di informazioni ed esperienze su **Microsoft Azure** e **365**.

Si rivolge a professionisti del settore IT ma anche ad appassionati di tecnologia, studenti e imprenditori interessati ad approfondire le **soluzioni cloud** e **ibride messe** a disposizione da **Microsoft**.

azuremeetup VENETO

meetup

Microsoft

TD SYNNEX

skybackbone engenio

Sessioni tecniche in **presenza** ed eventi dedicati al mondo Azure e M365

Sessioni tecniche **online** con argomenti proposti dal gruppo

| Cosa facciamo |

azuremeetup VENETO

meetup

Microsoft

TD SYNNEX

skybackbone engenio

azureontrack VENETO

YouTube

| Cosa facciamo |

azuremeetup VENETO

meetup

Microsoft

TD SYNNEX

skybackbone engenio

| Cosa facciamo |

azuremeetup VENETO

meetup

Microsoft

TD SYNNEX

skybackbone engenio

Prossimi Speaker:

Zeno Testoni
6 novembre 2024

Giuliano Latini
Dicembre 2024

| Cosa facciamo |

Agenda

14:45-15:15 - **Luigi Pandolfino** (Azure Meetup Veneto): Le novità di Windows Server 2025

15:15-16:00 - **Marco Moioli** (Microsoft): Hybrid Cloud con Azure Arc

16:00-16:15 - Coffee Break

16:15-17:00 - **Giuseppe Nale**, **Piero Malfona** (SkyBackBone): Il patch management senza WSUS

17:00-17:45 - **Thomas Forte**, **Vito Trentadue** (TDSYNNEX): Proteggi le tue identità con Microsoft Entra

17:45-18:15 - **Davide Cenedese** (Azure Meetup Veneto): Governance delle risorse Azure

18:15-18:30 - Chiusura e ringraziamenti

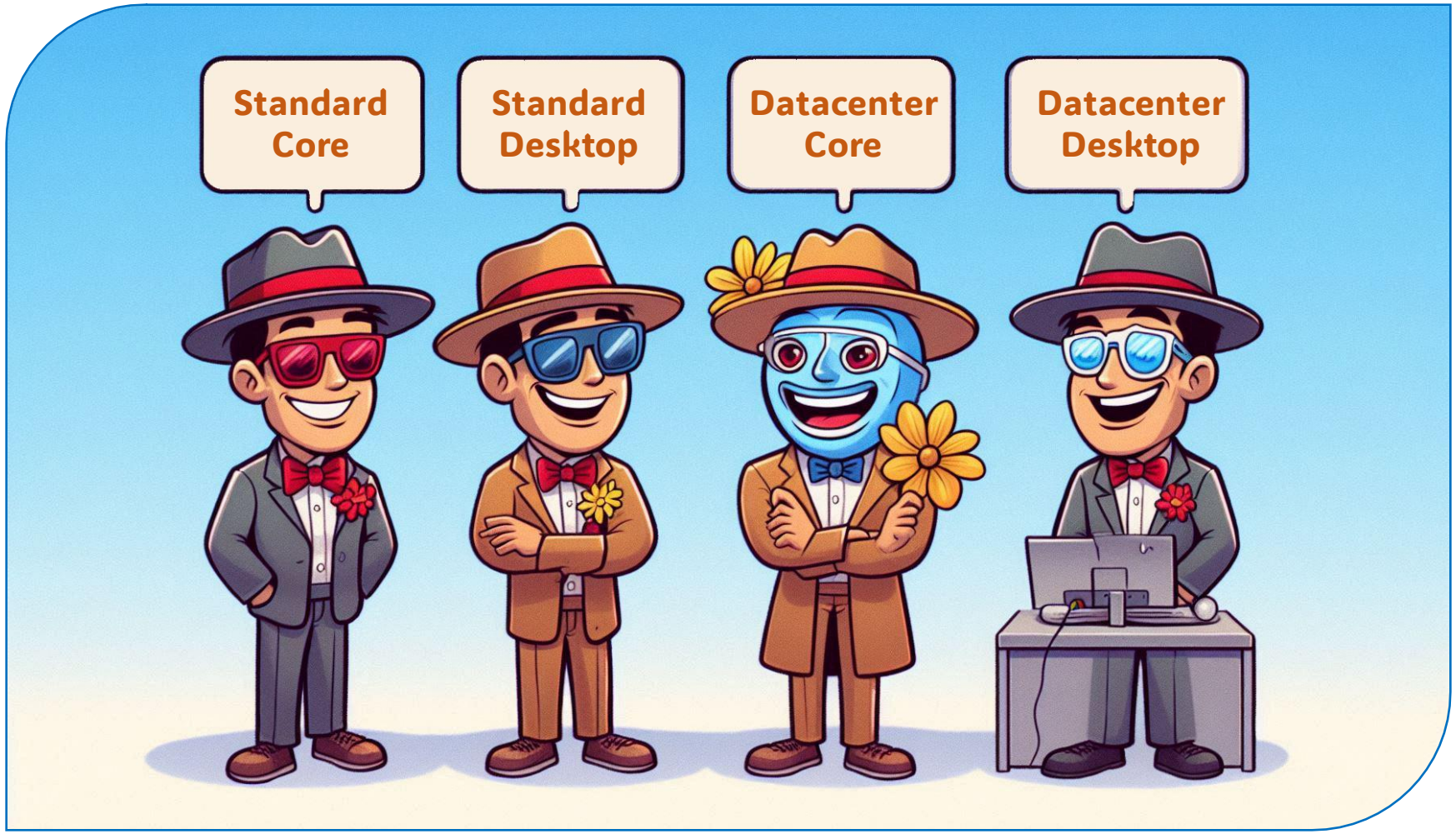
18:30-19:30 - Preparazione gara e competizione

19:30-19:45 - Premiazione

25 ottobre 2024

Le novità di Windows Server 2025

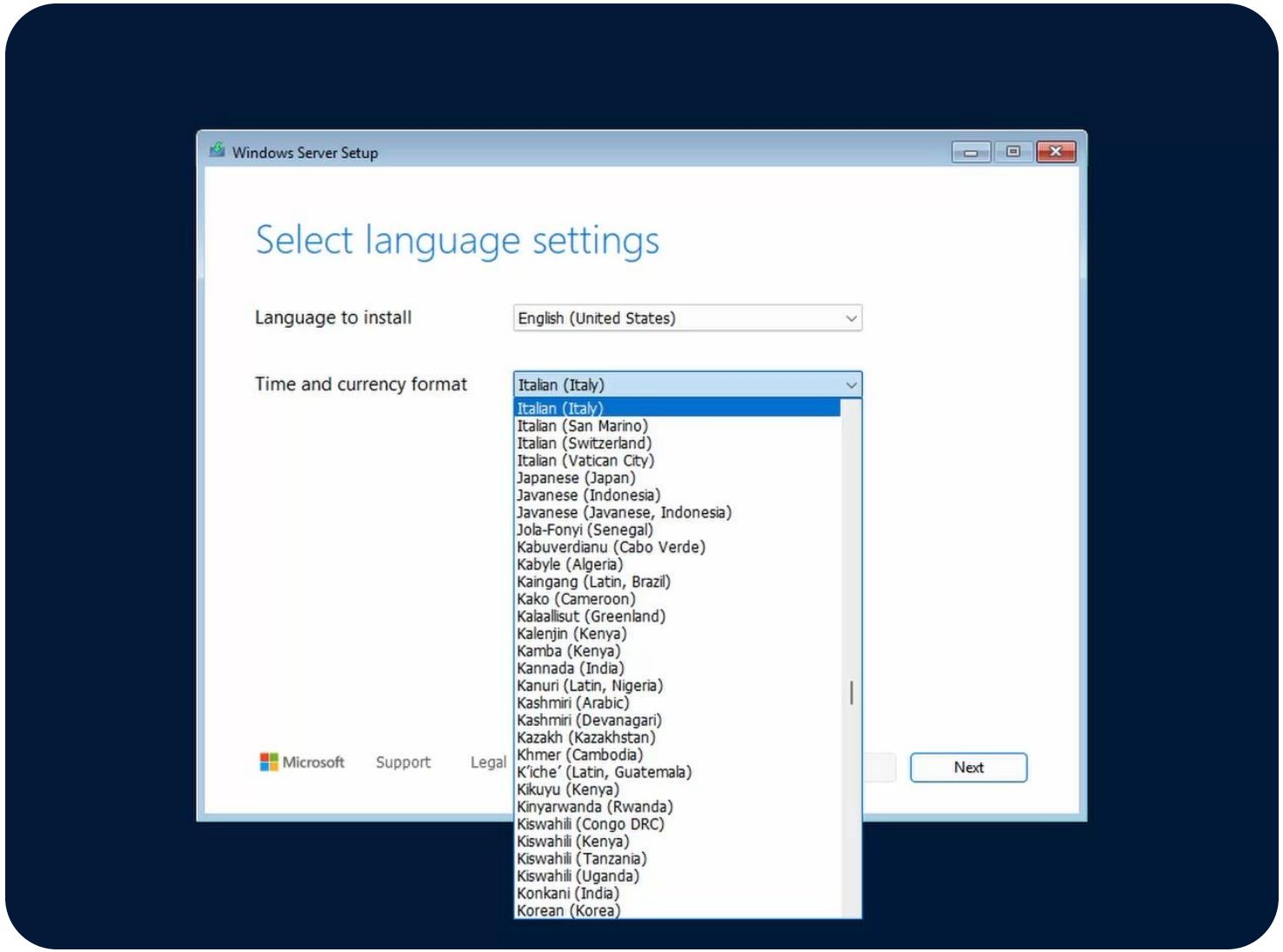
Luigi Pandolfino
Coordinatore Azure Meetup Veneto



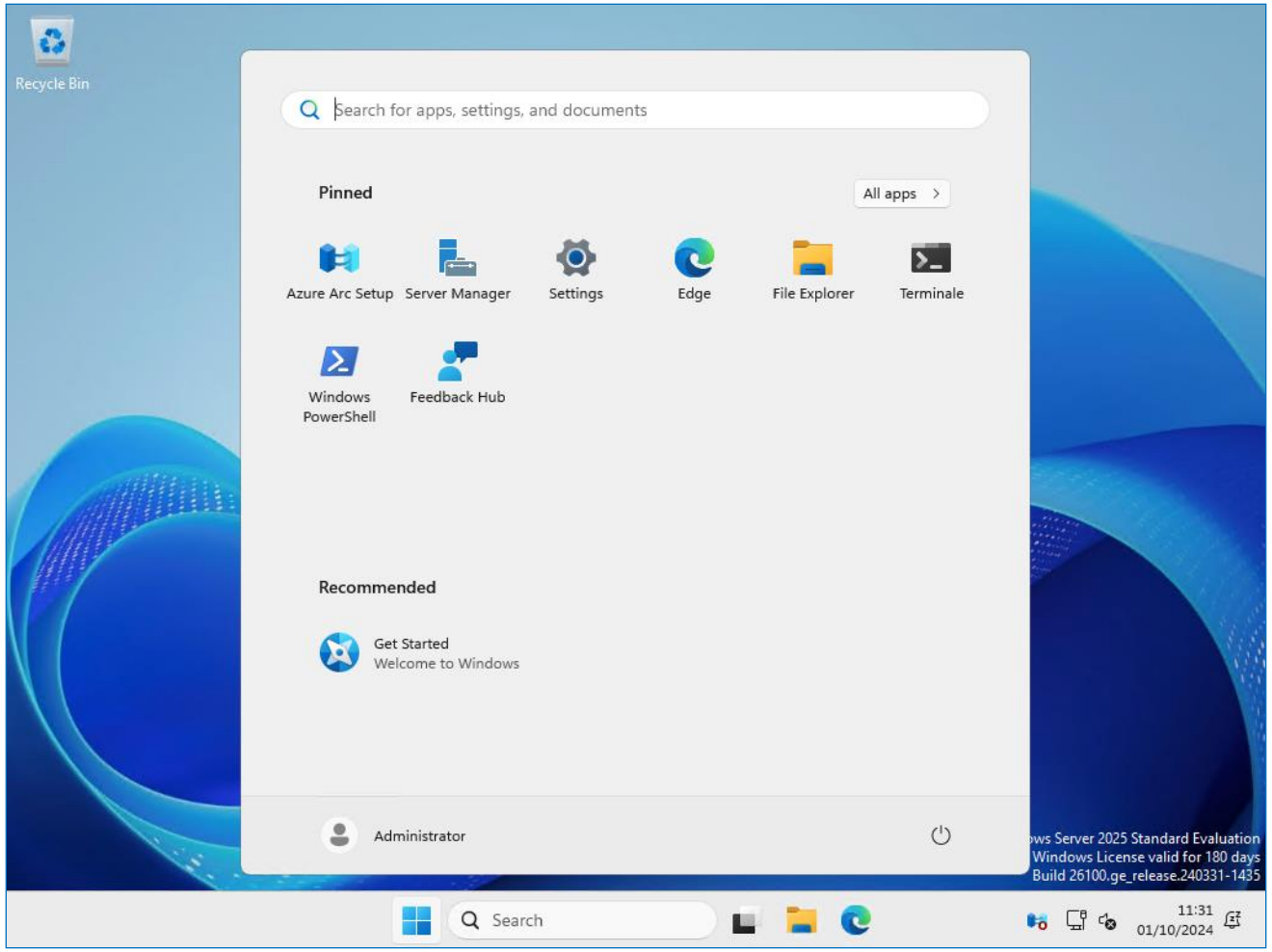
Server Core: la versione raccomandata, include i componenti essenziali di Windows e può essere gestito da remoto con Windows Admin Center e PowerShell.

Server Desktop Experience: la versione completa che include anche l'interfaccia grafica.

Stesse edizioni di Windows Server 2022: Windows Server Standard, Windows Server Datacenter, Windows Server Azure Edition.

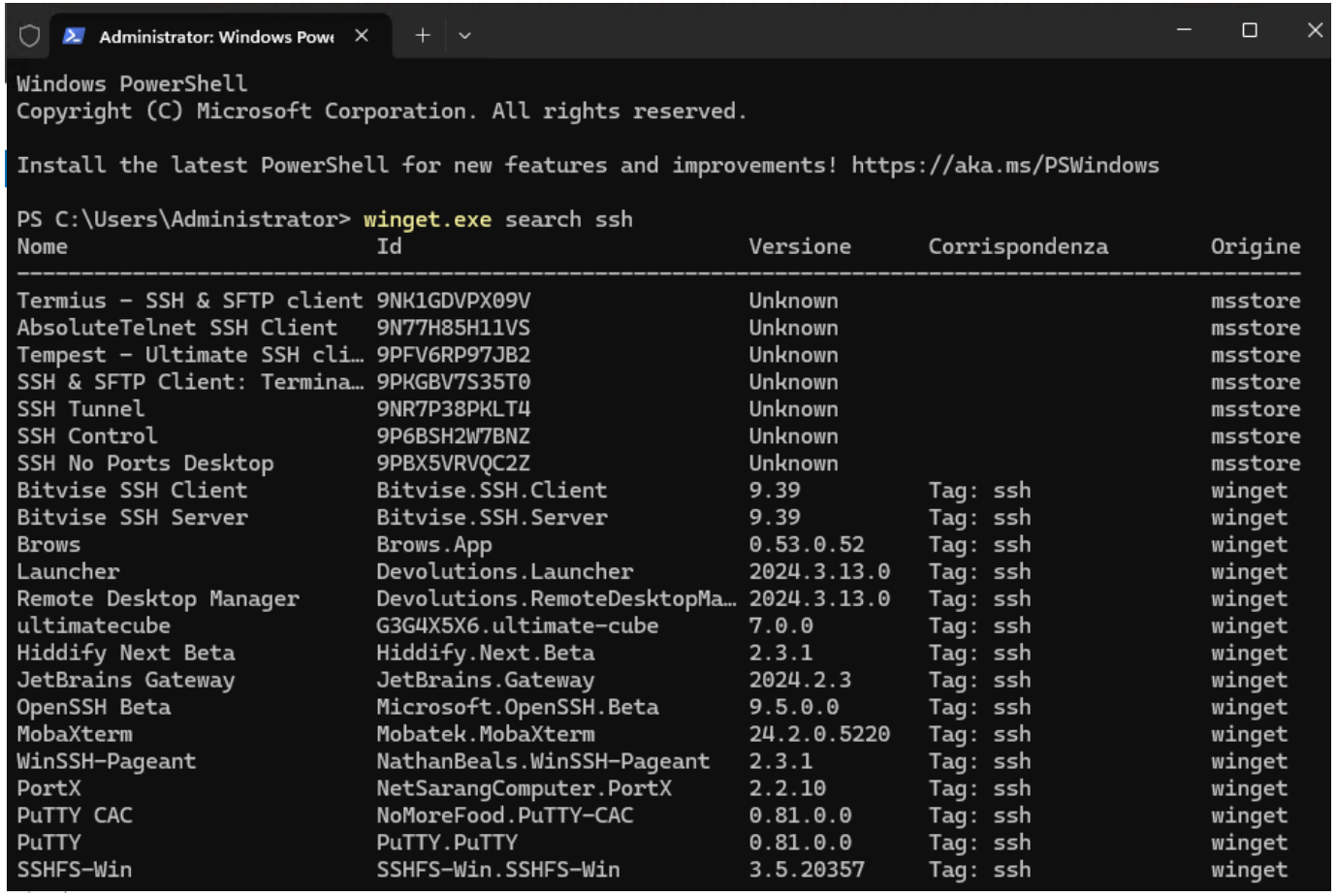


| Installazione e versioni |



Requirements	Description
Processor	1.4 GHz 64-bit processor Compatible with x64 instruction set Supports NX and DEP, CMPXCHG16b, LAHF/SAHF, and PrefetchW
Memory/RAM	512 MB (2 GB for Server with Desktop Experience installation option) ECC (Error Correcting Code) type or similar technology, for physical host deployments
Disk Space	Minimum 32 GB (Windows Server 2025 using the Server Core installation option)
Network Requirements	An Ethernet adapter capable of at least 1 gigabit per second throughput Compliant with the PCI Express architecture specification
Additional	UEFI 2.3.1c-based system and firmware that supports secure boot Trusted Platform Module Graphics device and monitor capable of Super VGA (1024 x 768) or higher-resolution

| Requisiti Hardware e nuova GUI |



WIFI

Il servizio Wireless LAN è installato per impostazione predefinita

Bluetooth

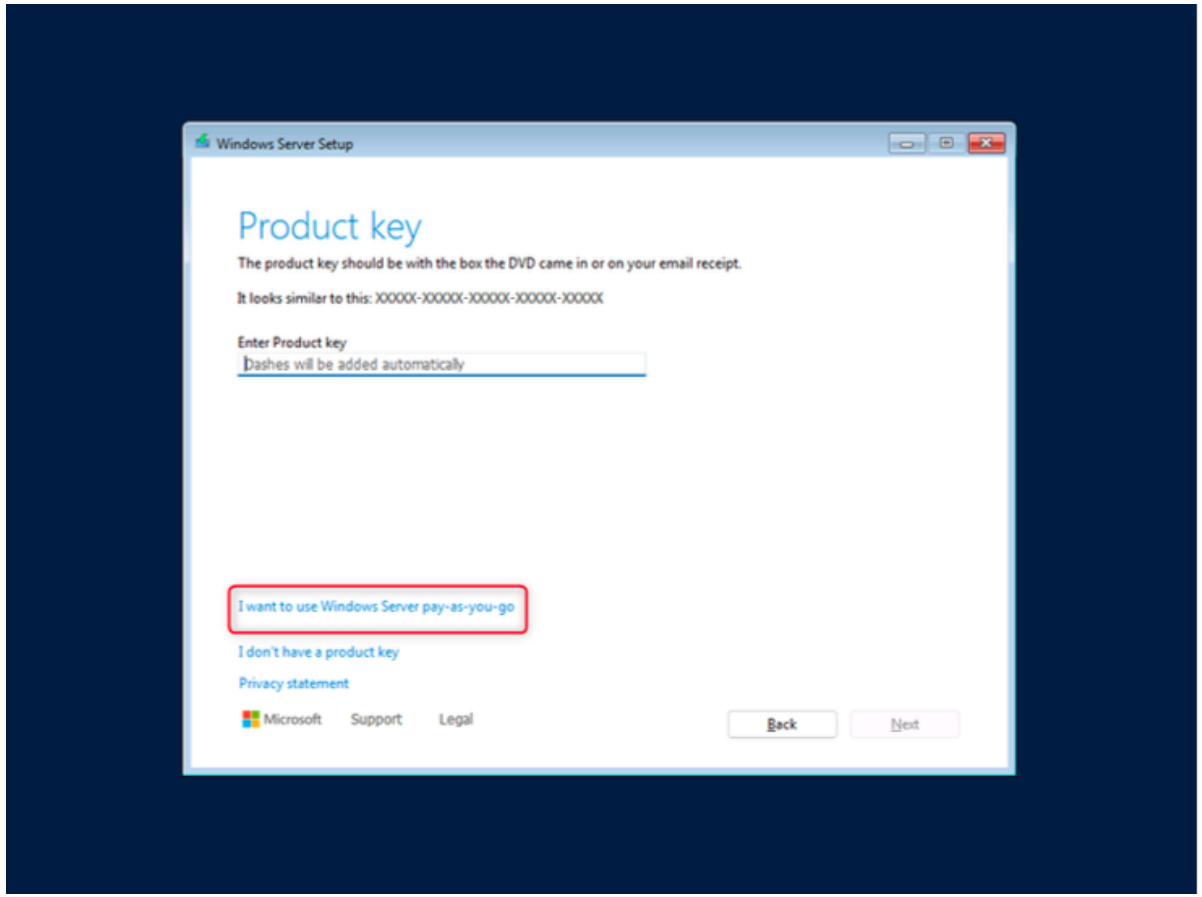
Ora possibile connettere mouse, tastiere, cuffie, dispositivi audio

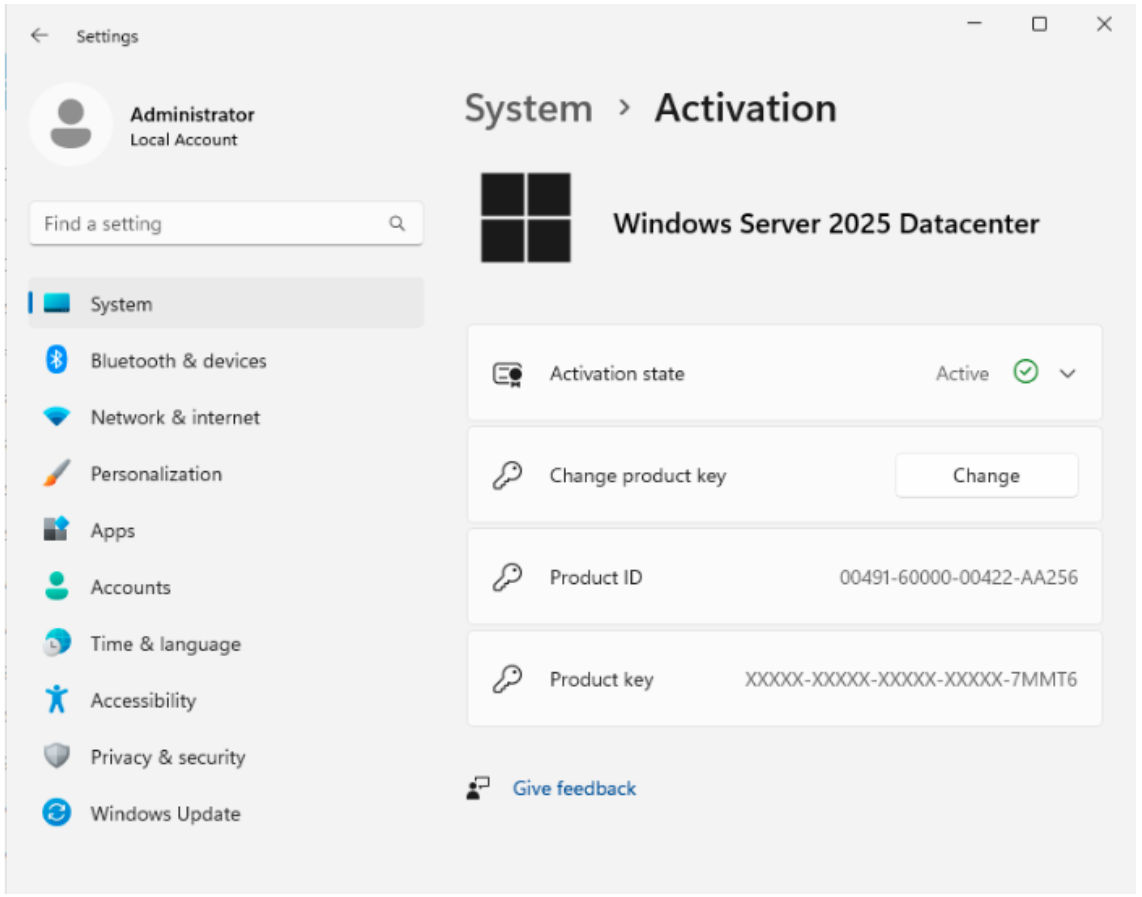
OpenSSH

Offre la possibilità di collegarsi e gestire via SSH i server

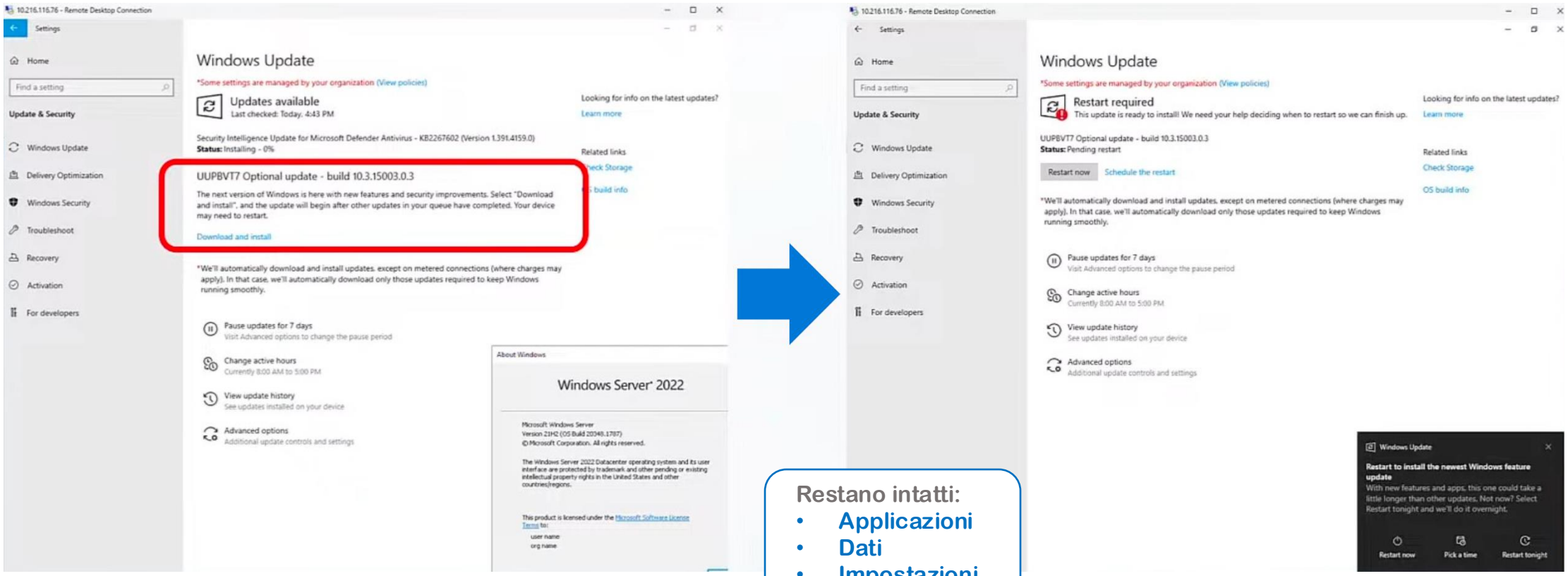
WinGET

Permette installazioni di software tramite terminale semplificando l'amministrazione





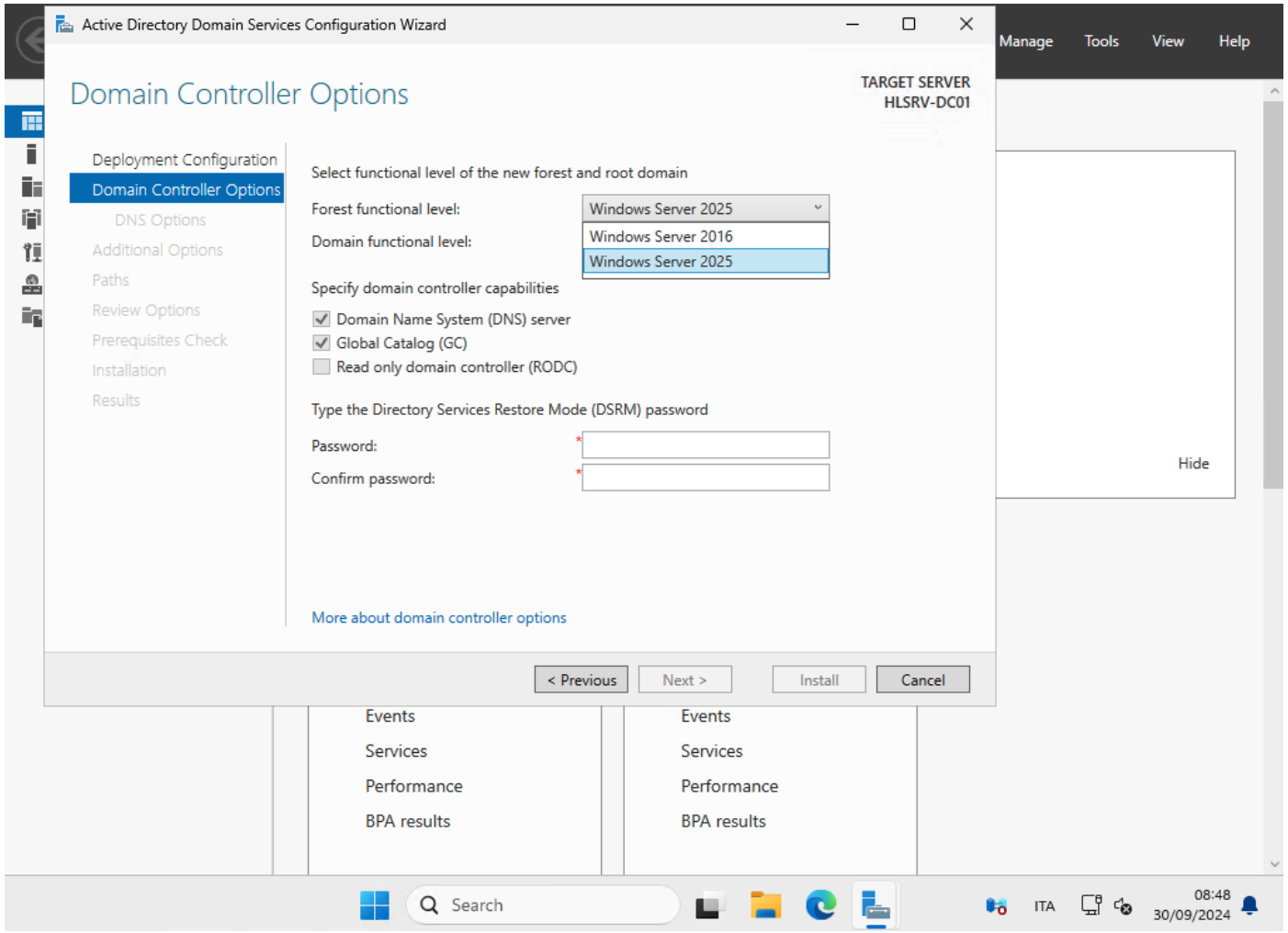
| Licensing basato su Subscription |



Restano intatti:

- Applicazioni
- Dati
- Impostazioni

| Upgrade in-place senza Downtime |



Livelli funzionali Active Directory

Forest functional level: Windows Server 2025
Domain functional level: Windows Server 2025

Microsoft non aggiungerà livelli intermedi per 2019 e 2022

Funzionalità deprecate

NTLM con passaggio a Kerberos
TLS 1.0 e 1.1 disabilitati di default
VBScript in favore di **PowerShell**
WSUS

Funzionalità rimosse

Server SMTP
WordPad
PowerShell 2.0 in favore di 5.0+
Console IIS 6.0

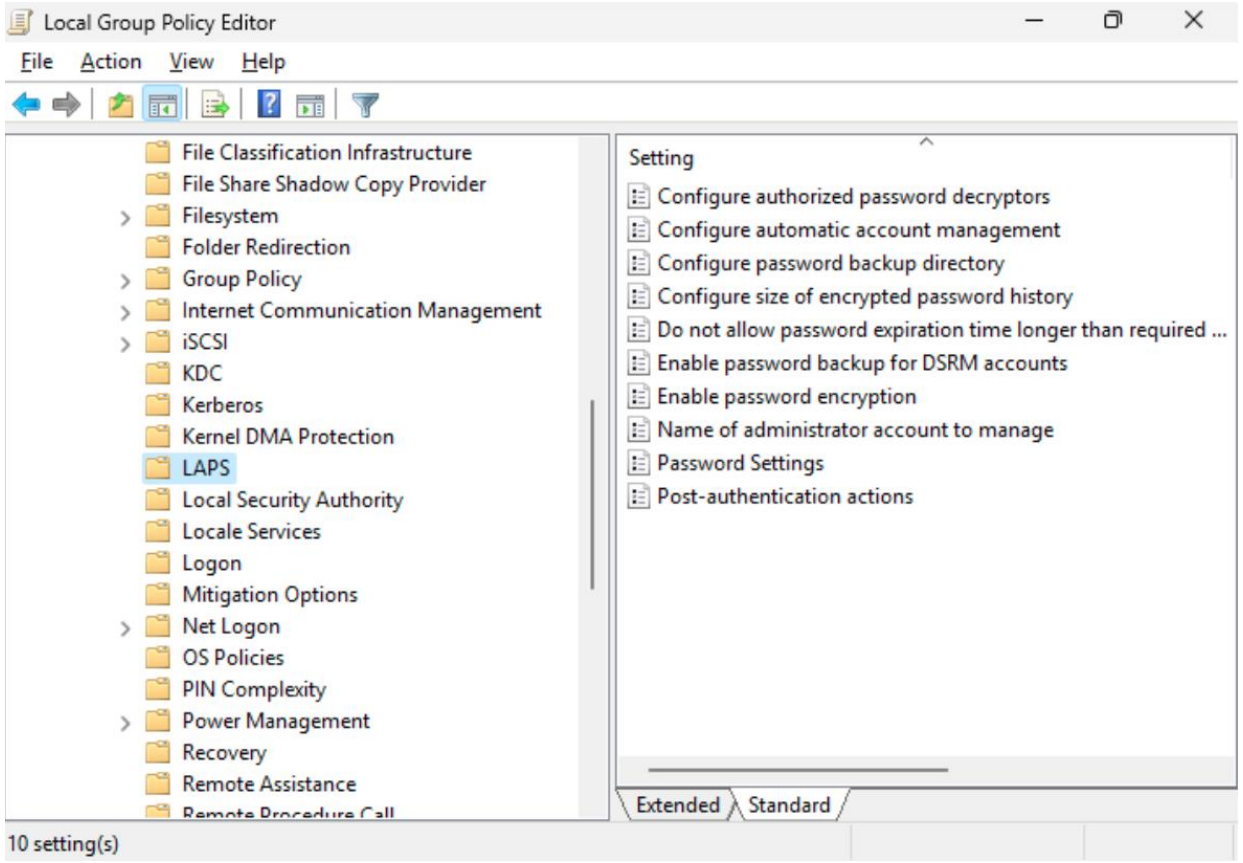
Funzionalità Aggiornate

Supporto TLS 1.3 per LDAP
Kerberos con migliore encryption
Active Directory 32k database page size

https://learn.microsoft.com/it-it/windows-server/get-started/removed-deprecated-features-windows-server-2025

Windows Local Administrator Password Solution

Gestione automatica degli account
Rilevamento del rollback dell'immagine
Funzionalità Passphrase
Miglioramento leggibilità dizionario delle password



E’ una funzionalità di **Windows Server 2025** che protegge i sistemi dalle vulnerabilità grazie alla possibilità di fare patching **senza dover riavviare**.

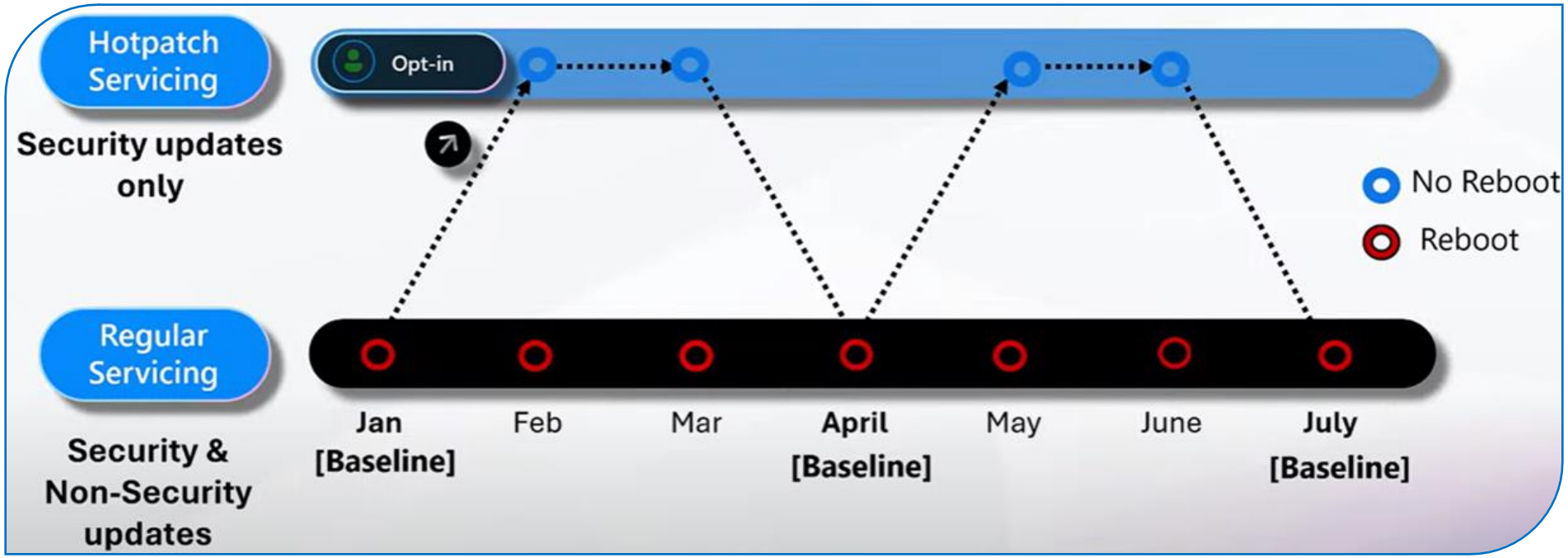
Hot-patch applica le patch **direttamente al codice in memoria nei processi attivi**, senza la necessità di riavviare il processo stesso.

Velocizzazione processi di sicurezza

Miglioramento produttività

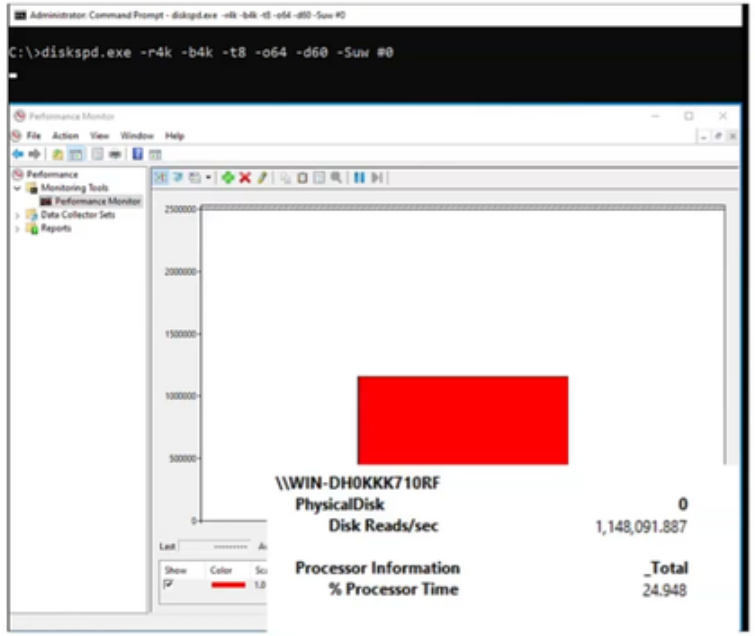
Riduzione Costi

Ciclo di rilascio trimestrale



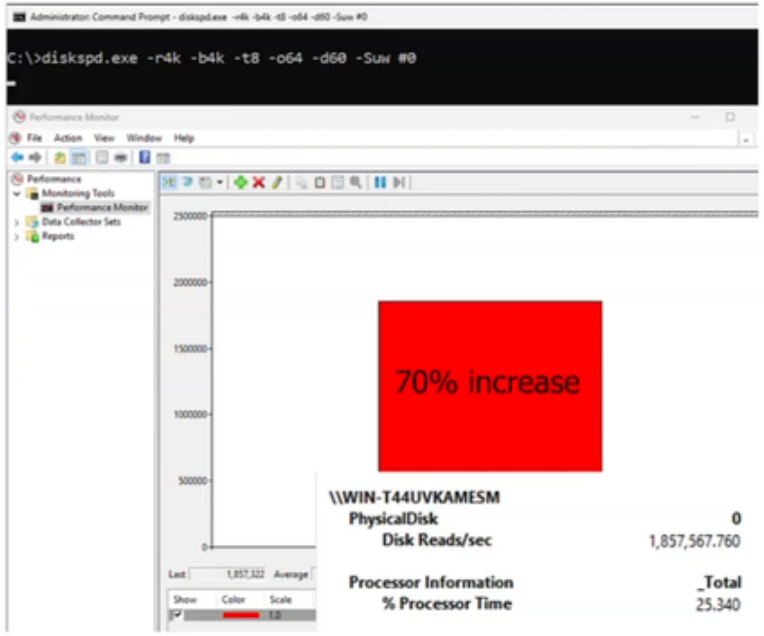
Gli aggiornamenti cumulativi che richiedono un riavvio sono pianificati **4 volte** all'anno
Mediamente un **67% in meno di reboot**
Le correzioni **zero-day** possono richiedere un riavvio

70% more IOPs on NVMe SSDs



Windows Server 2022

1.1M IOPs



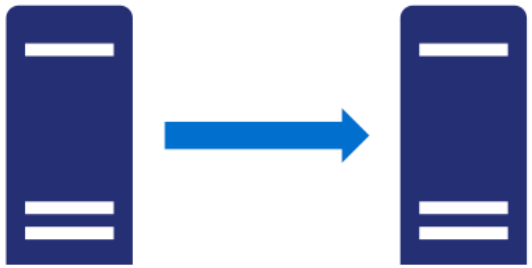
Windows Server 2025

1.86M IOPs

Importanti ottimizzazioni:

- Riduzione utilizzo CPU
- Uso migliore delle code
- Cache ottimizzata

Storage Spaces Direct più performante con soluzioni all-flash basate su **NVMe**



Storage Replica

Prestazioni superiori con Enhanced Log

Storage Replica Compression disponibile per tutte le edizioni di Windows Server

ReFS

Maggiore ottimizzazione per deduplica e compressione

Ottimizzato anche per hot-data come le Virtual Machine

Fino al 60% di spazio risparmiato nei File Server e 90% per VHD, ISO e Backup

Storage Spaces

Thin Provisioning

Supporto Stretch Cluster

Alla base dei servizi di virtualizzazione di:

- Azure
- Azure Stack
- Windows Server
- Windows Client
- Container con Hyper-V isolation

Maximums for virtual machines

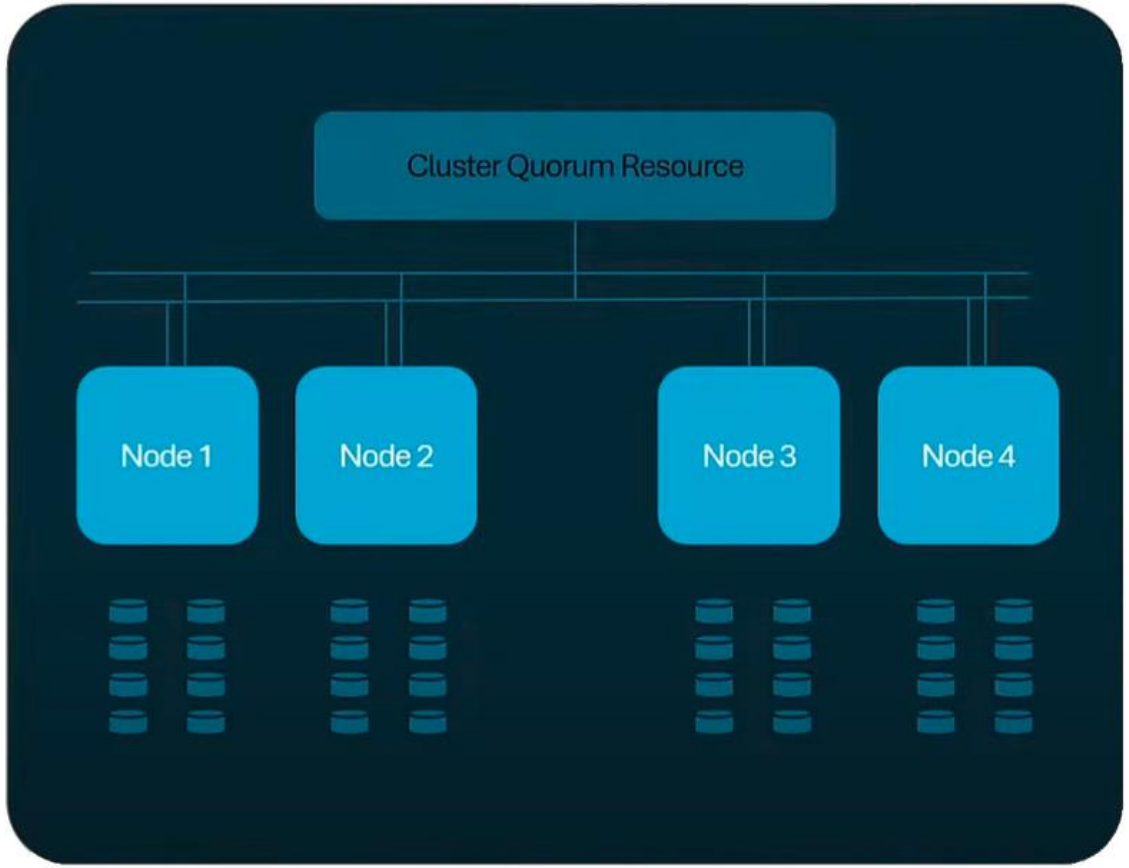
- 240 TB RAM for generation 2 VM
- 1 TB RAM for generation 1 VM
- 2048 vCPU for generation 2 VM
- 64 vCPU for generation 1 VM

Maximums for Hyper-V hosts

- 4 PB for hosts that support 5-level paging
- 256 TB for hosts that support 4-level paging
- 2048 logical processors per host

Failover Clustering

- Aggiornamenti Cluster-aware
- Workgroup Cluster (Certificate-based VM Live Migration)
- VM Live Migration con GPU-P
- Miglioramento delle performance di Storage Replica nelle configurazioni stretch cluster con Storage Spaces Direct



GPU Partitioning (GPU-P)

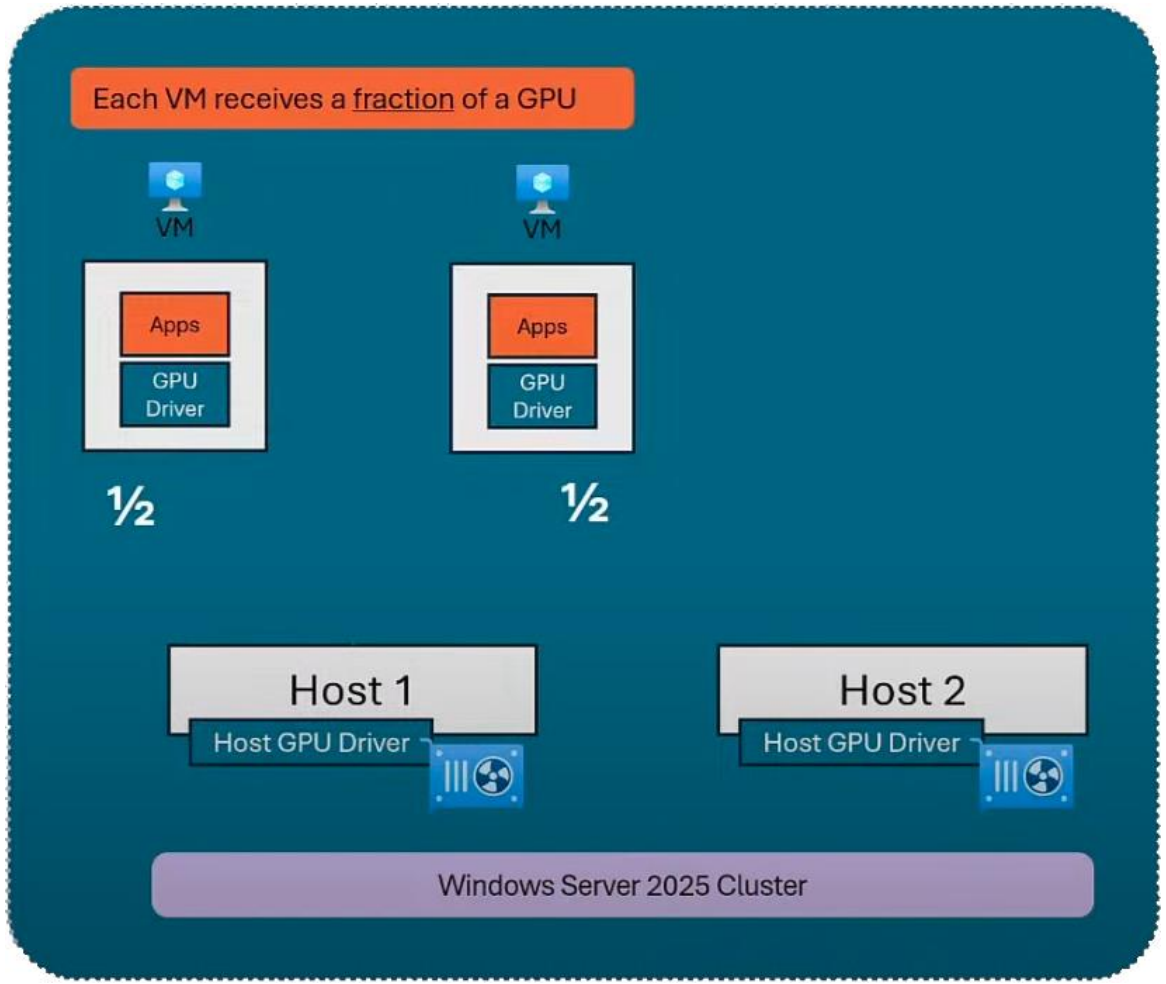
La possibilità di condividere GPU tra più VM:

- Creare GPU partition
- Assegnare ogni partizione a una VM
- Gestire tramite WAC o PS

Supporto per Live Migration e Failover Cluster

Attualmente supportano GPU-P:

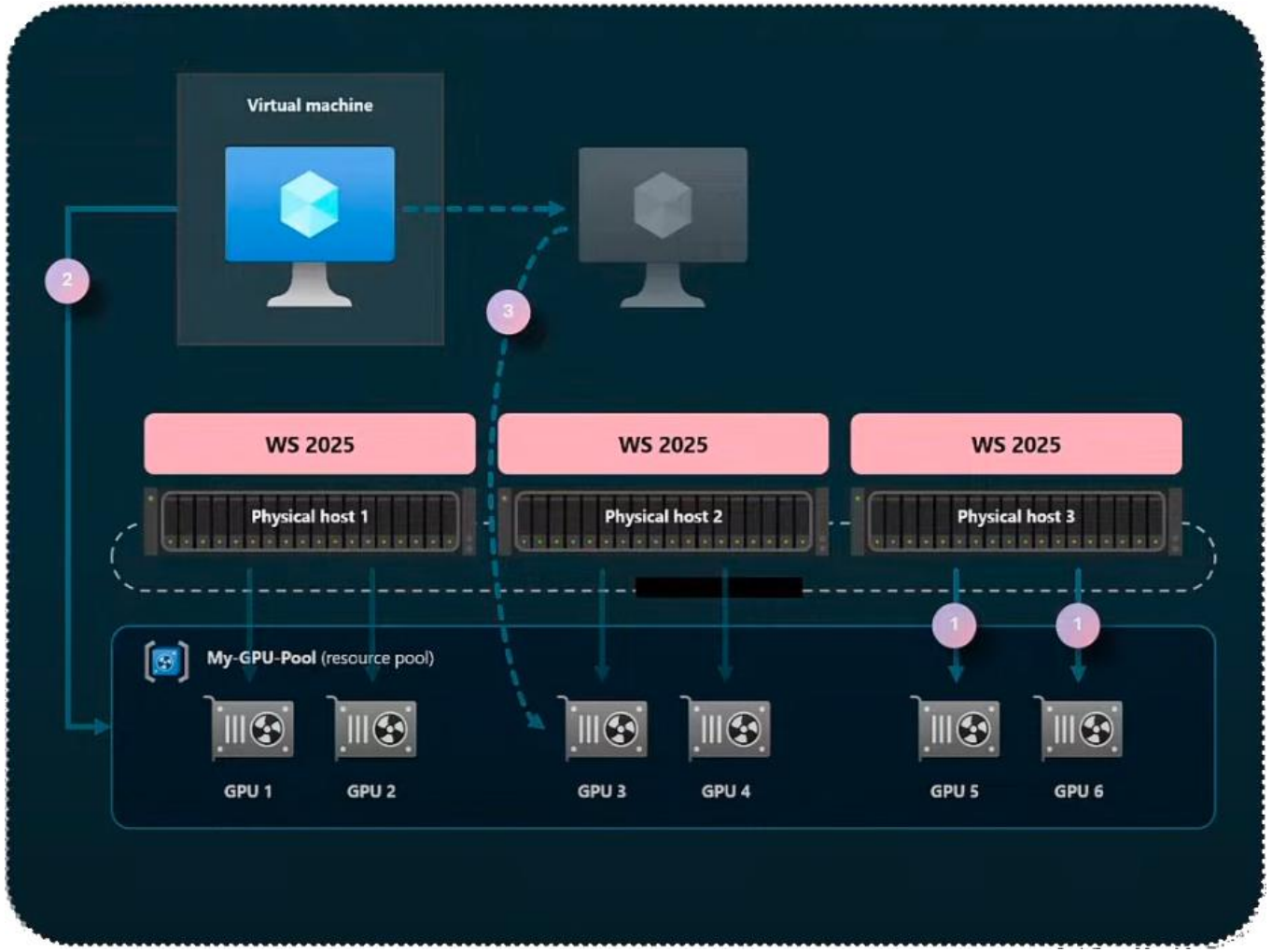
NVIDIA A2, A10, A16, A40
NVIDIA L2, L4, L40, L40S



GPU Pool

Tramite **Discrete Device Assignment (DDA)** abbiamo la possibilità di **dedicare una o più GPU fisica** a una macchina virtuale.

Live migration di VM non è al momento supportata, ma le macchine possono essere **riavviate automaticamente** in caso di necessità e posizionate dove le **risorse GPU** sono **disponibili**.

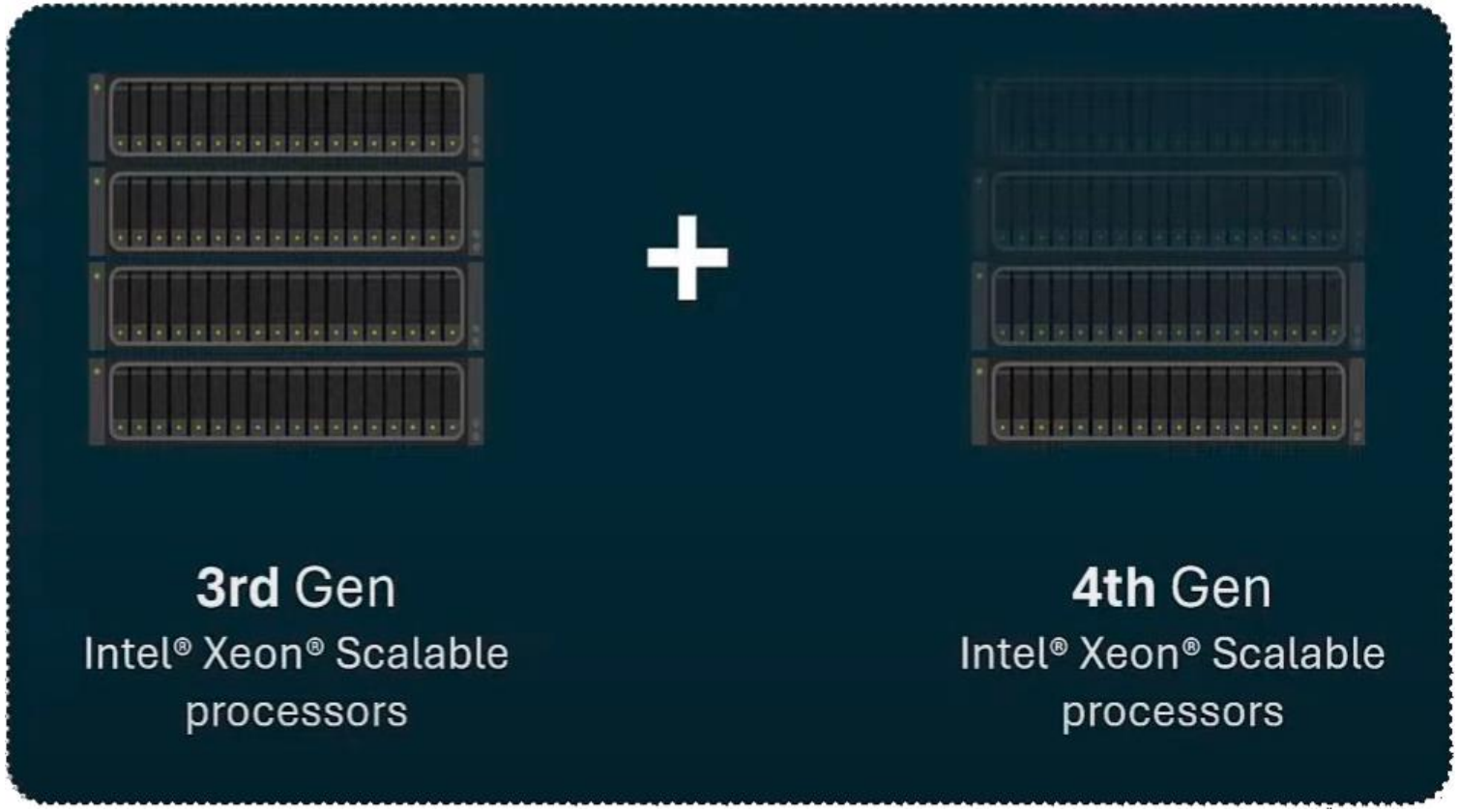


Dynamic Processor Compatibility

Migliorato in Windows Server 2025: permette Live Migration tra server con processori di famiglie differenti (capability sets)

Ogni VM riceve dinamicamente il numero massimo di set di istruzioni disponibili su tutti i server del cluster

Non permette la migrazione tra Vendor diversi (Intel-to-AMD)

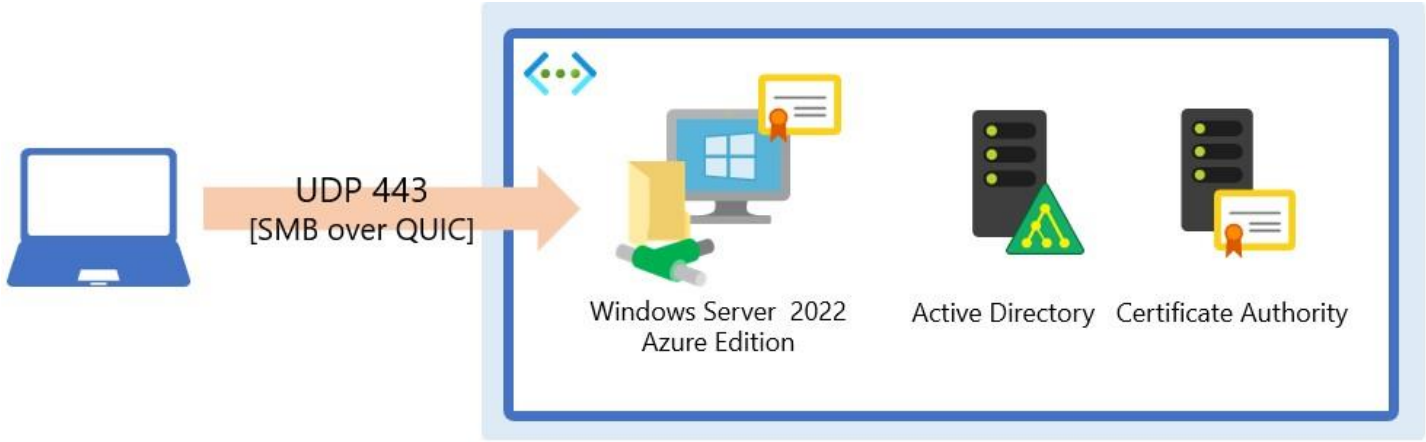


SMB over QUIC

Funzionalità ereditata da **Windows Server 2022 Azure Edition** che consente di accedere ai file server Windows **tramite Internet**.

La comunicazione è crittografata sulla porta **UDP 443**, quindi può essere utilizzata in sicurezza.

Disponibile in tutte le edizioni: Standard, Datacenter, Azure Edition



WSUS Deprecation

"We have no current plans of removing WSUS from in-market versions of Windows Server (including Windows Server 2025).
Microsoft will continue to ensure that existing WSUS features work.
However, we do not plan to invest in new features going forward"

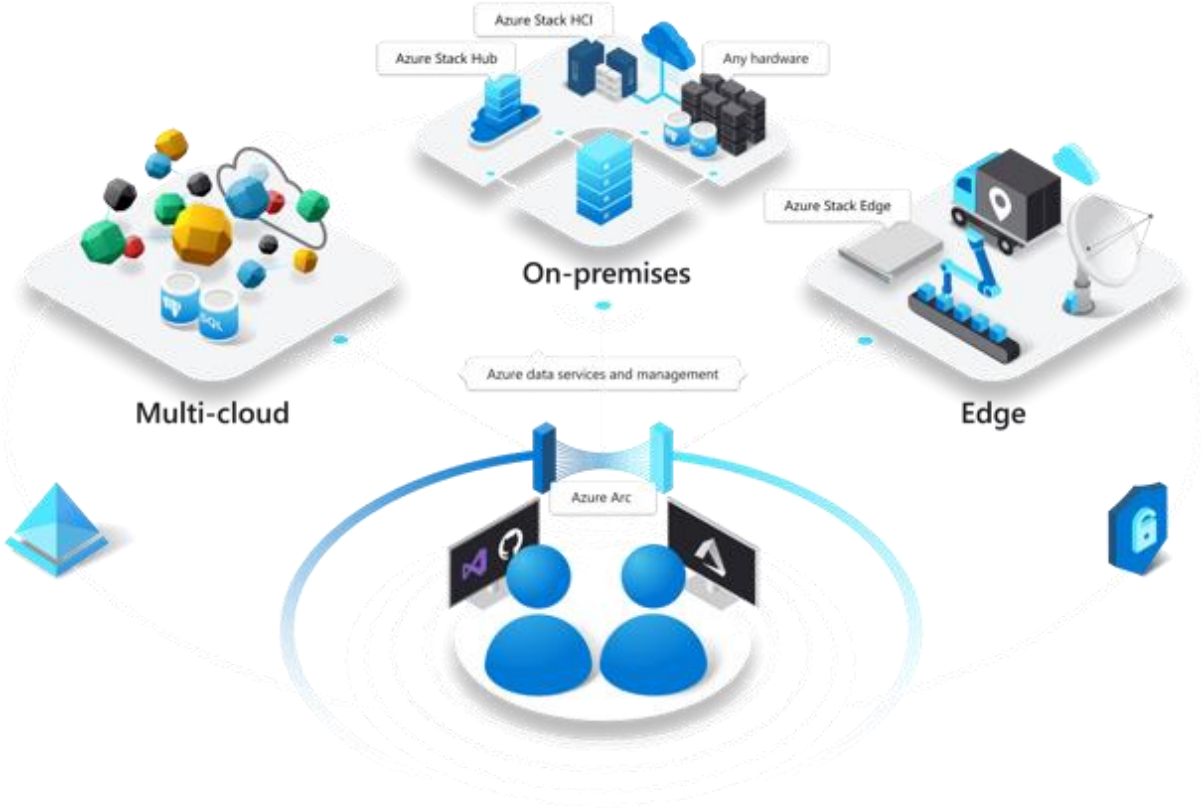
"While the WSUS role remains available in Windows Server 2025, we recommend organizations transition to cloud tools, including Windows Autopatch and Microsoft Intune for client update management and Azure Update Manager for server update management"

| …ma WSUS?? |

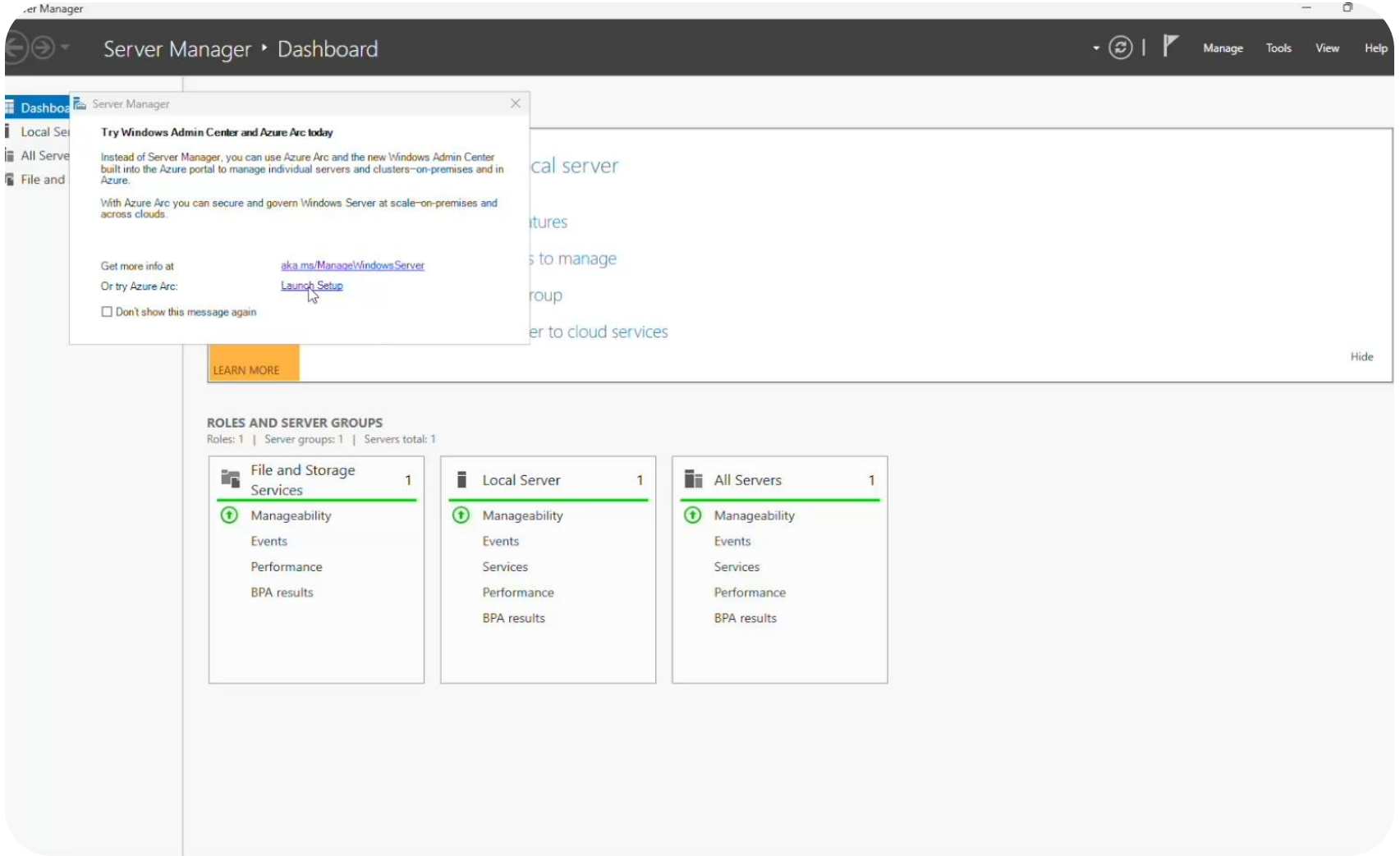
Azure Arc

Piattaforma di **governance** di risorse locali e multi-cloud:

- Server (Windows o Linux)
- Cluster Kubernetes
- Servizi dati Azure
- SQL Server esterni ad Azure
- Virtual Machine (VMware o Azure Stack HCI)



| Integrazione con Azure Arc |

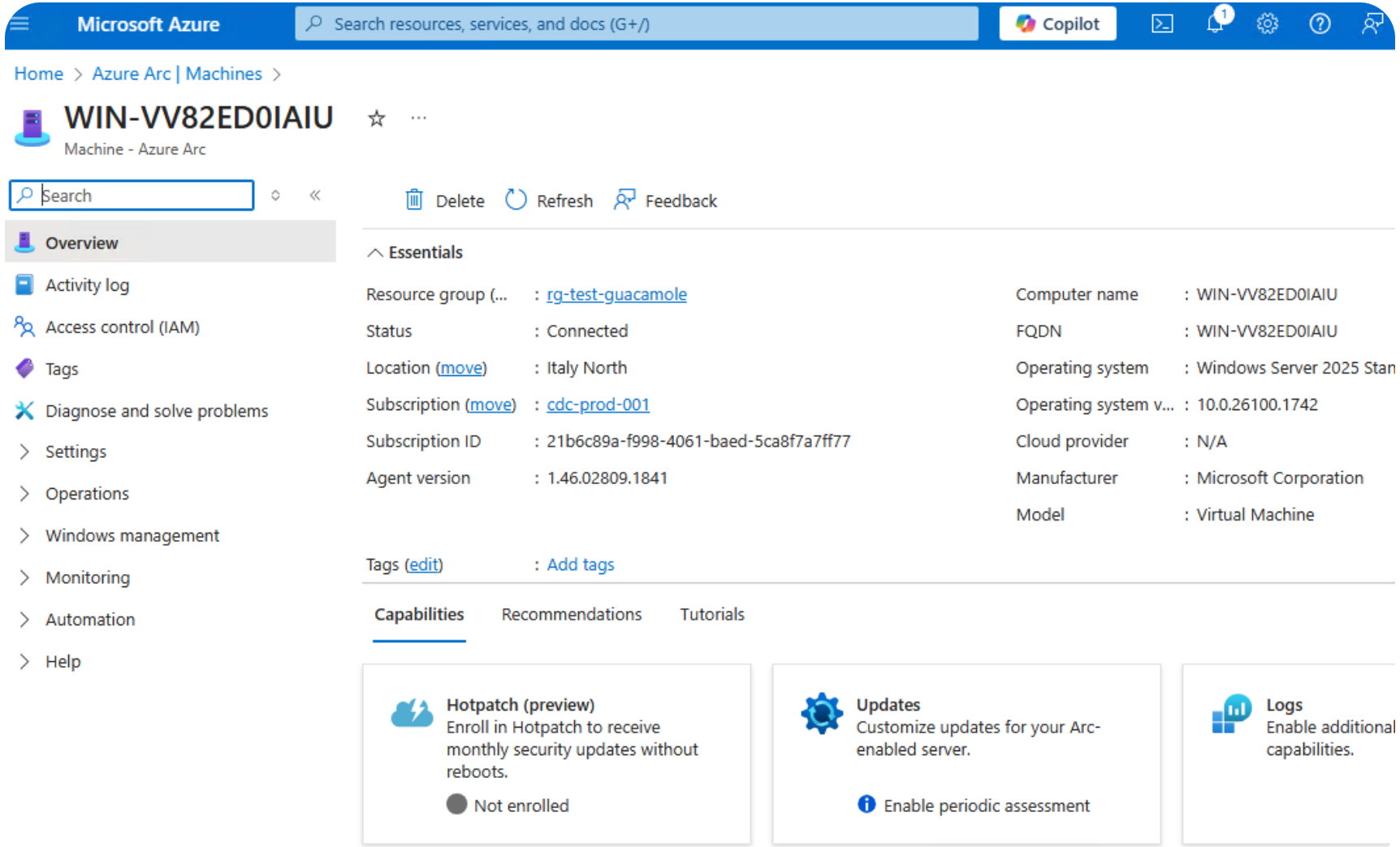


”Get Hybrid with Azure Arc”

Windows Server 2025 si avvantaggia di una più stretta integrazione con i servizi di **Azure**, in particolare tramite **Azure Arc**.

Estendere le potenzialità di Azure ai data center on-premises rende più semplice la gestione di ambienti **ibridi** e **multicloud**.

| Integrazione con Azure Arc |



”Get Hybrid with Azure Arc”

Windows Server 2025 si avvantaggia di una più stretta integrazione con i servizi di Azure, in particolare tramite Azure Arc.

Estendere le potenzialità di Azure ai data center on-premises rende più semplice la gestione di ambienti ibridi e multicloud.

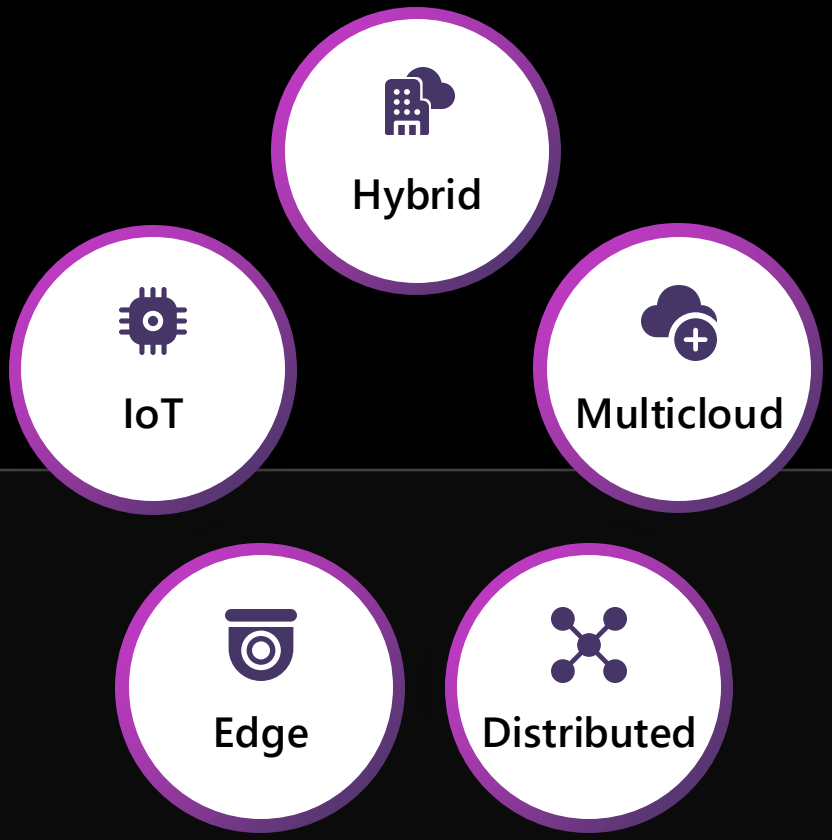
| Integrazione con Azure Arc |

Microsoft

Azure Arc

Hybrid Cloud con Azure Arc

Marco Moioli
Cloud Solution Architect - Microsoft
25 Ottobre 2024

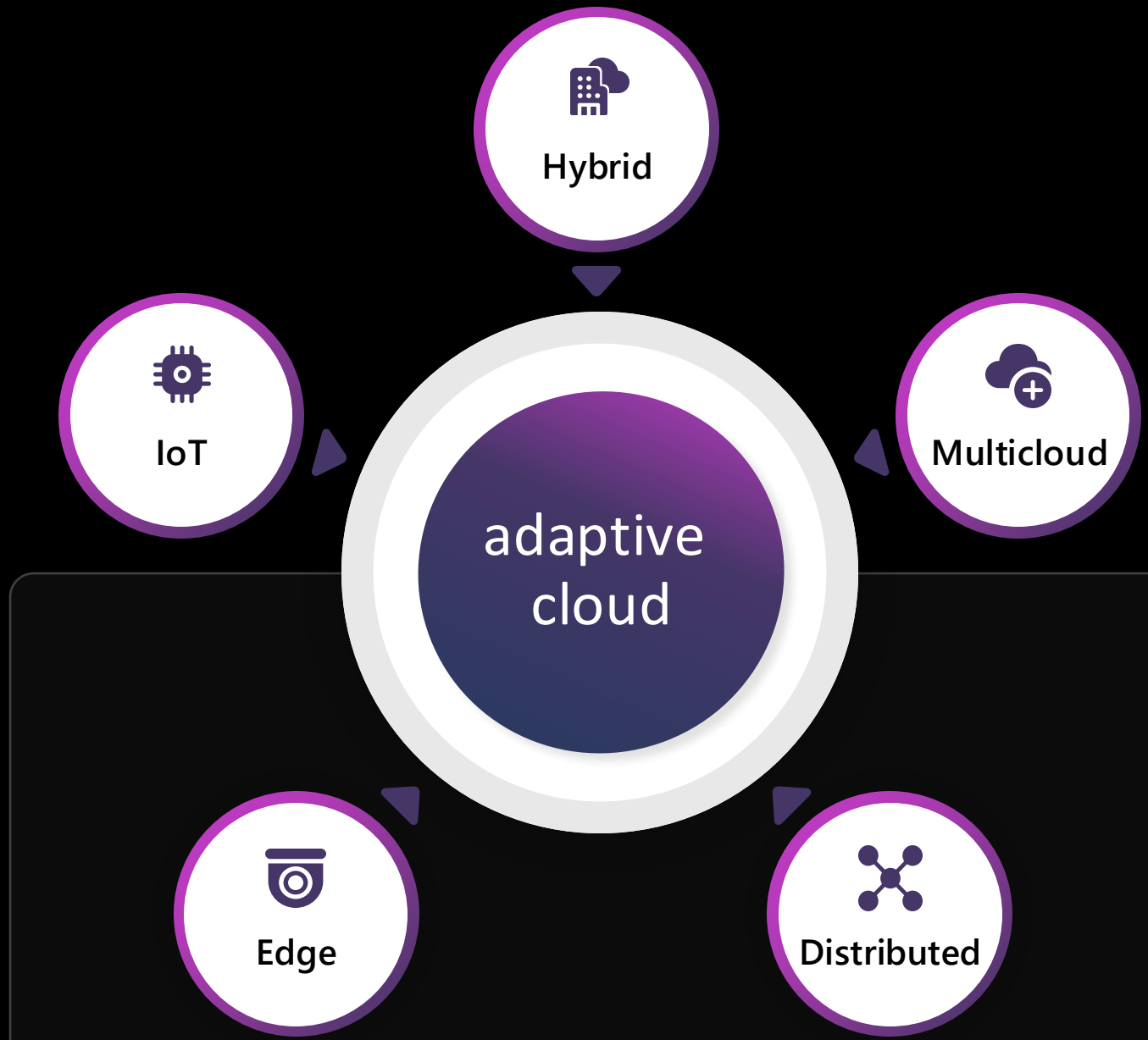


Common customer challenges

Sprawling systems

Information and process silos

Increased technical debt



Advancing hybrid cloud to adaptive cloud

Thrive in dynamic environments by unifying teams, sites, and systems across hybrid, multicloud, edge, and IoT.

Adaptive Cloud

f Operate with AI-enhanced central management

Microsoft Copilot for Azure

Azure Monitor

Microsoft Defender for Cloud

b Rapidly develop and scale applications across boundaries

Visual Studio

GitHub

Azure Kubernetes Service

d Cultivate data and insights across physical operations

IoT Operations

Microsoft Fabric

Machine Learning

Microsoft Azure

Windows Server

SQL

SUSE

Red Hat

vmware

Google Cloud

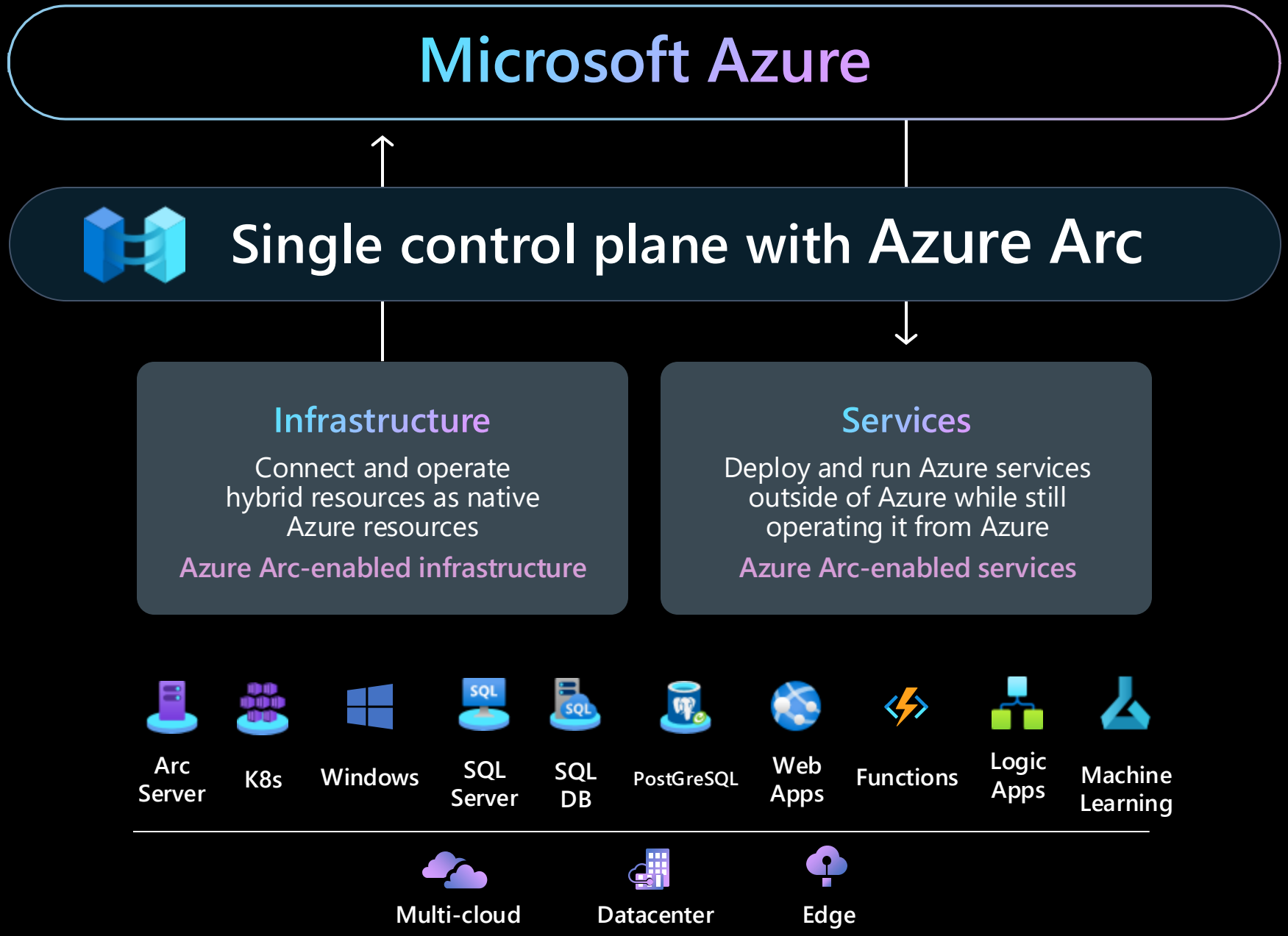
aws

ORACLE

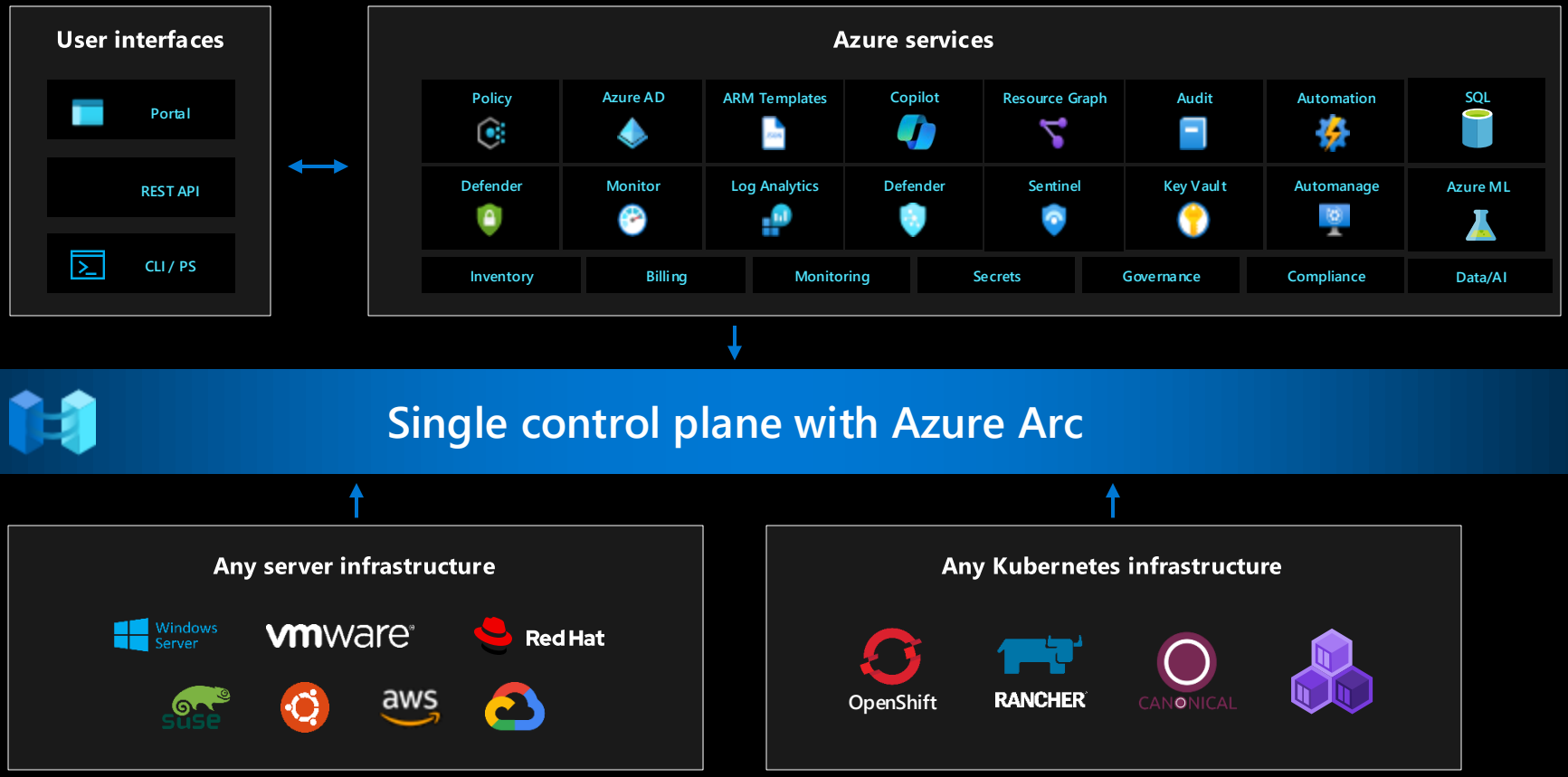
Enabled by Azure Arc

Customer aspirations

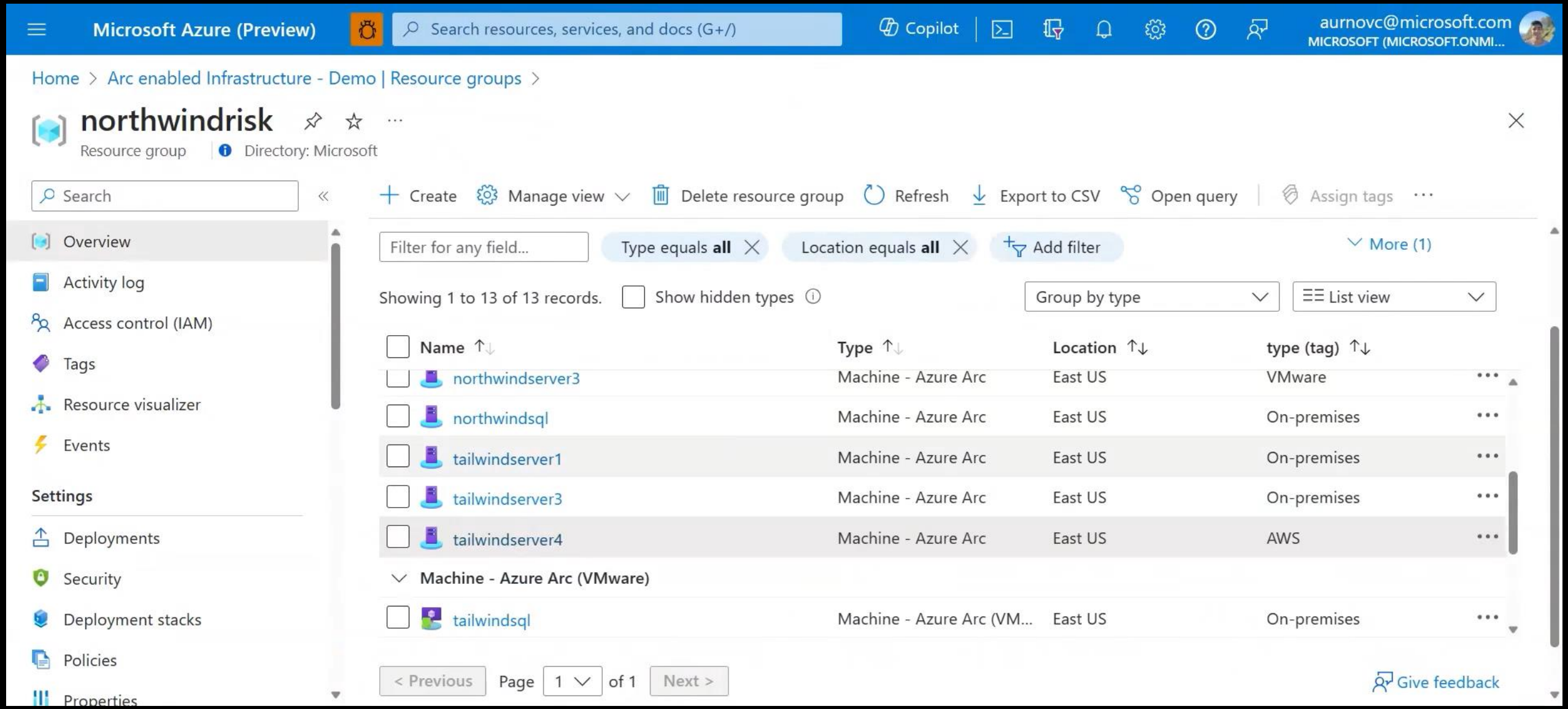
- Deliver products as a service
- Transform data into new products
- Accelerate application development
- Secure and govern distributed digital estate
- Modernize facilities and assets
- Manage multicloud, datacenter and edge modalities in a single control plane


Microsoft Azure
Single control plane with Azure Arc
Infrastructure
Connect and operate hybrid resources as native Azure resources
Azure Arc-enabled infrastructure
Services
Deploy and run Azure services outside of Azure while still operating it from Azure
Azure Arc-enabled services
Arc Server
K8s
Windows
SQL Server
SQL DB
PostGreSQL
Web Apps
Functions
Logic Apps
Machine Learning
Multi-cloud
Datacenter
Edge

Azure Arc: extending Azure management & security to any infrastructure



Manage your private, public and edge environment in a consistent way


Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
Copilot
aurnovc@microsoft.com
MICROSOFT (MICROSOFT.ONMI...
Home > Arc enabled Infrastructure - Demo | Resource groups >
northwindrisk
Resource group
Directory: Microsoft
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Type equals all
Location equals all
Add filter
More (1)
Showing 1 to 13 of 13 records.
Show hidden types
Group by type
List view
Name
Type
Location
type (tag)
northwindserver3 Machine - Azure Arc East US VMware
northwindsql Machine - Azure Arc East US On-premises
tailwindserver1 Machine - Azure Arc East US On-premises
tailwindserver3 Machine - Azure Arc East US On-premises
tailwindserver4 Machine - Azure Arc East US AWS
Machine - Azure Arc (VMware)
tailwindsql Machine - Azure Arc (VM... East US On-premises
< Previous
Page 1 of 1
Next >
Give feedback

Innovate anywhere with Azure

Azure Arc

Secure and govern your infrastructure and apps

Build apps once, deploy and manage them anywhere

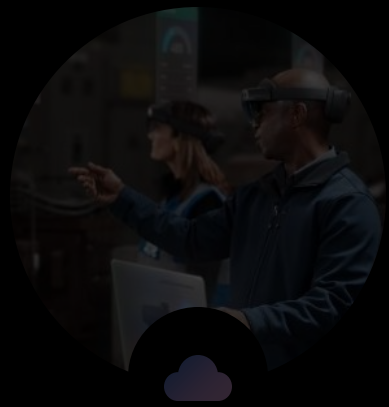
Run Azure data, app, and AI/ML services from cloud to edge

Innovate anywhere with Azure

Azure Arc

Secure and govern your infrastructure and apps

Build apps once, deploy and manage them anywhere



Run Azure data, app, and AI/ML services from cloud to edge

Secure and govern across environments

Customer needed

Simplified operations & management across thousands of remote sites with heterogenous assets

To leverage cloud-based threat detection, response, and analytics

To catalog and govern IT inventory with policy and role-based access control

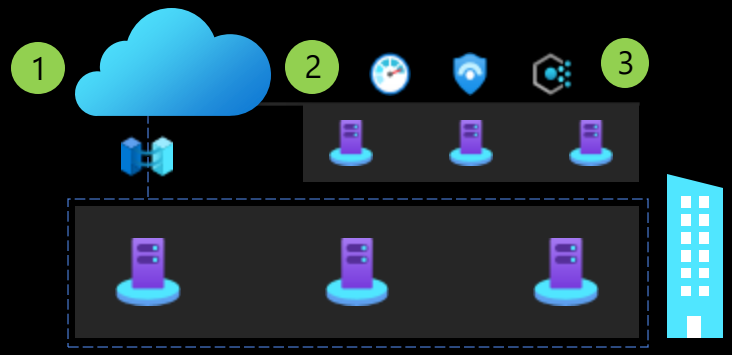
Business continuity with observability across the stack and automated recovery from failures

GREGGS

bp

ING

How



1. Migrate WS/SQL/Linux to Azure regions
2. Arc-enable remaining WS/SQL/Linux in Datacenters and at the edge
3. Integrate operations, management, and security across all environments

Microsoft Offerings

Enabled by Azure Arc

- Azure Resource Manager
- Microsoft Defender for Cloud
- Microsoft Sentinel
- Azure Policy
- Azure Monitor
- Microsoft Purview
- Azure Automanage
- Azure Update Manager
- Microsoft Copilot in Azure

Azure Arc-enabled servers

Bring Azure capabilities to your on-premises and multicloud servers with Azure Arc

Reach

Windows and Linux

VM and bare metal

At scale searchable inventory

Configure

Consistent VM extensions

Centralized agent management—monitoring, security, update management

Govern

Built-in Azure policies

Compliance across environments

Audit and enforce OS settings

Secure

Entra ID Managed Identity

Server security baselines

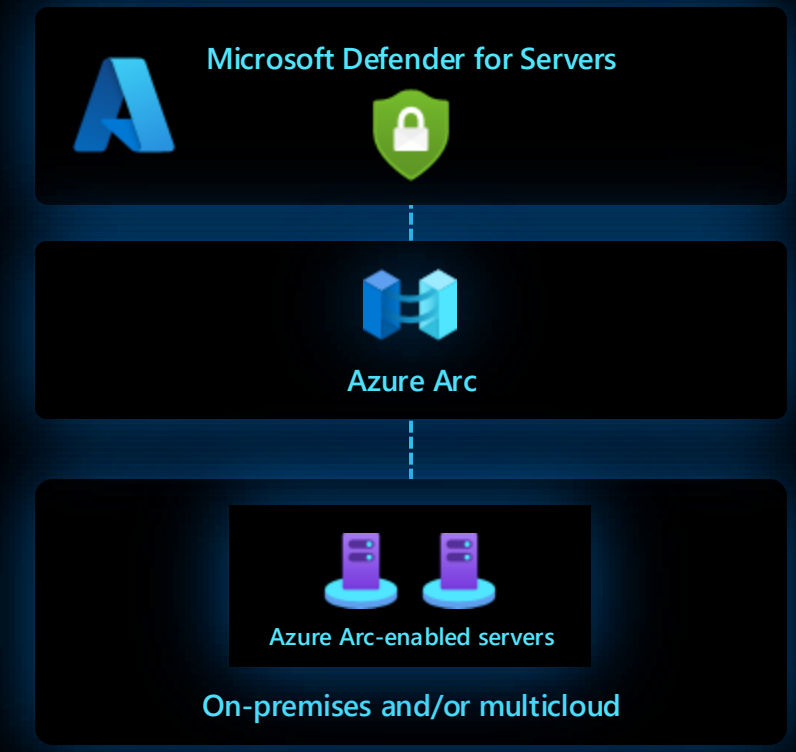
Role-Based Access control

Any infrastructure, familiar tools

Deploy defender for servers anywhere

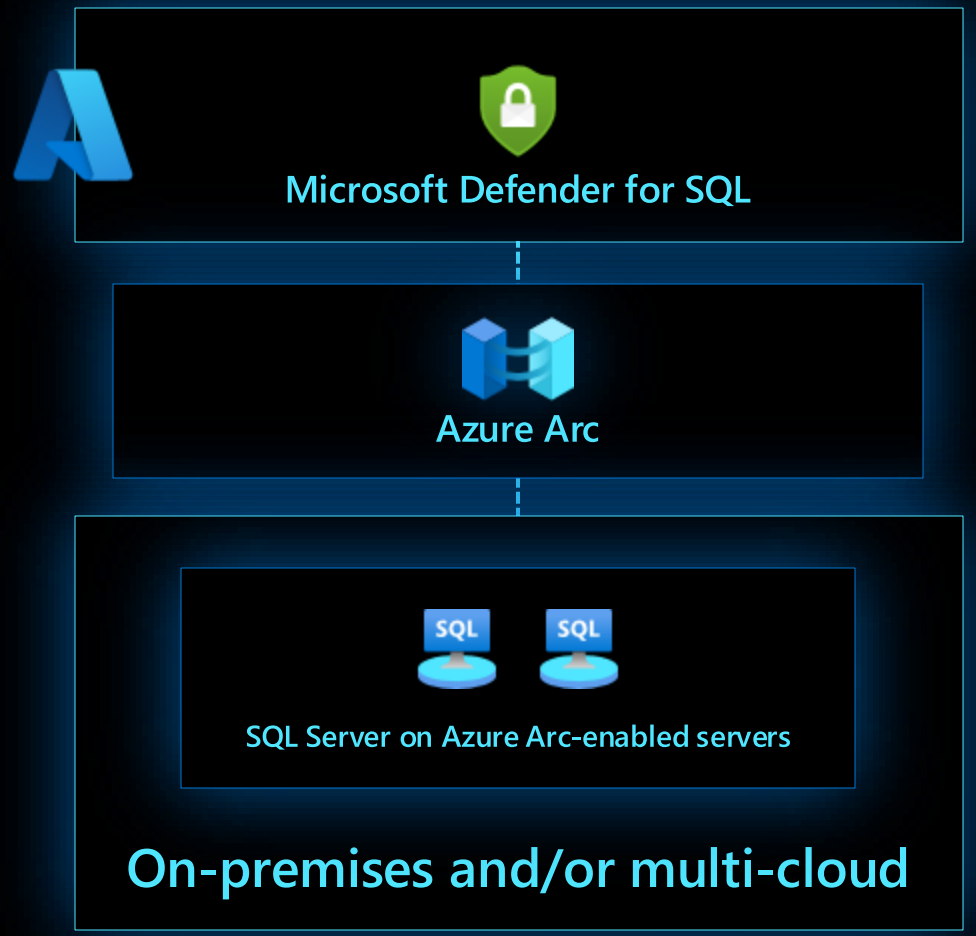
Secure hybrid and multicloud environments

- Reduce risk with contextual security posture management
- Get compliance benchmarks mapped to industry standards
- Vulnerability assessment built-in with flexibility to use tools, like Qualys, offering integrated vulnerability scanning for your connected machines
- Use Just-in-Time VM access to control access to commonly attacked management ports
- Block malware with adaptive application controls
- Set guardrails with Azure Policy integration, server owners can view and remediate to meet their compliance



Deploy Defender for databases (SQL) anywhere

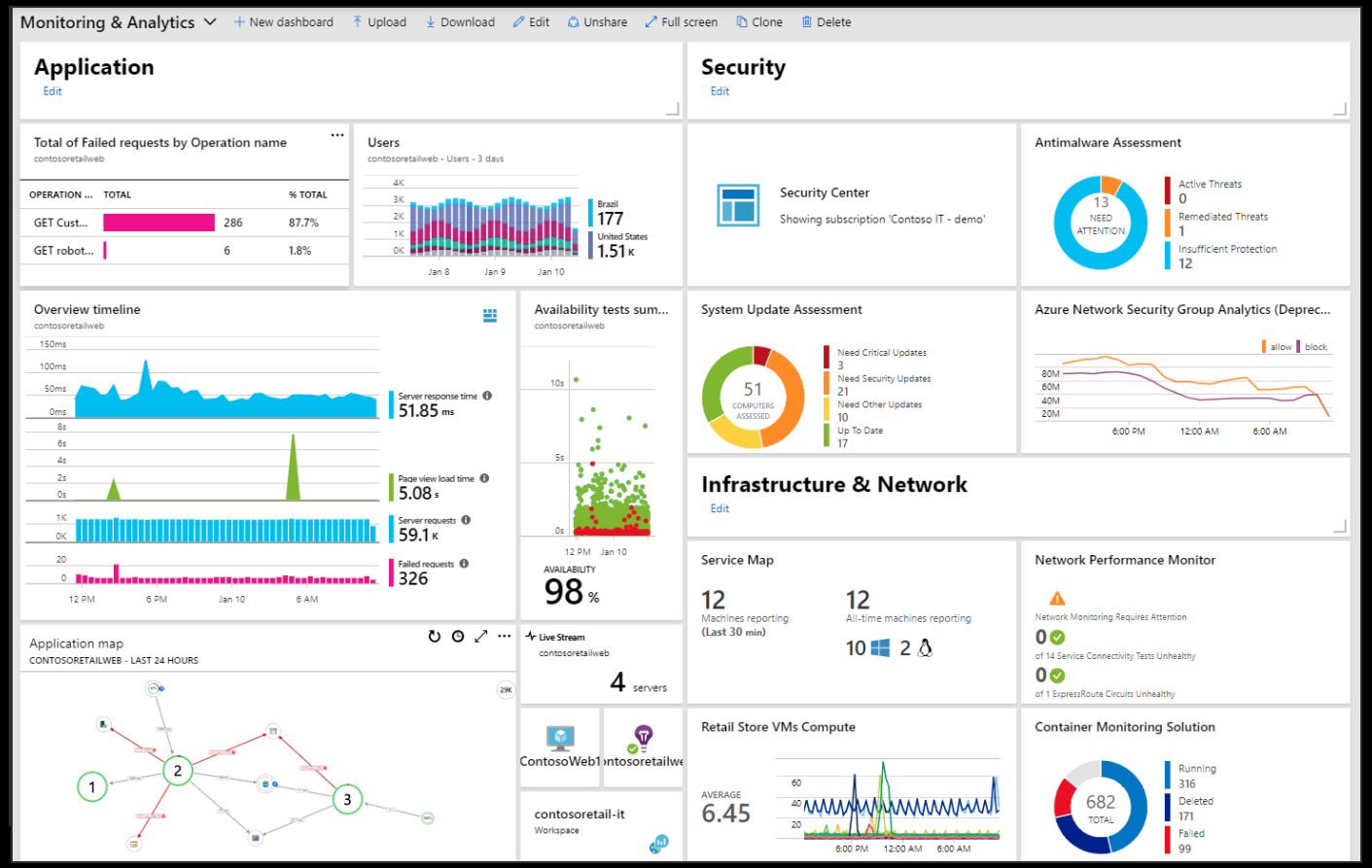
- Monitor and remediate potential vulnerabilities for SQL Servers in Azure, on-premises or in other clouds
- Discover, track, and remediate potential database vulnerabilities with assessment scans.
- Monitor for threats such as SQL injection, brute-force attacks, and privilege abuse with advanced threat protections



Azure Monitor anywhere enabled by Azure Arc

Consistent monitoring across your hybrid and multi-cloud compute

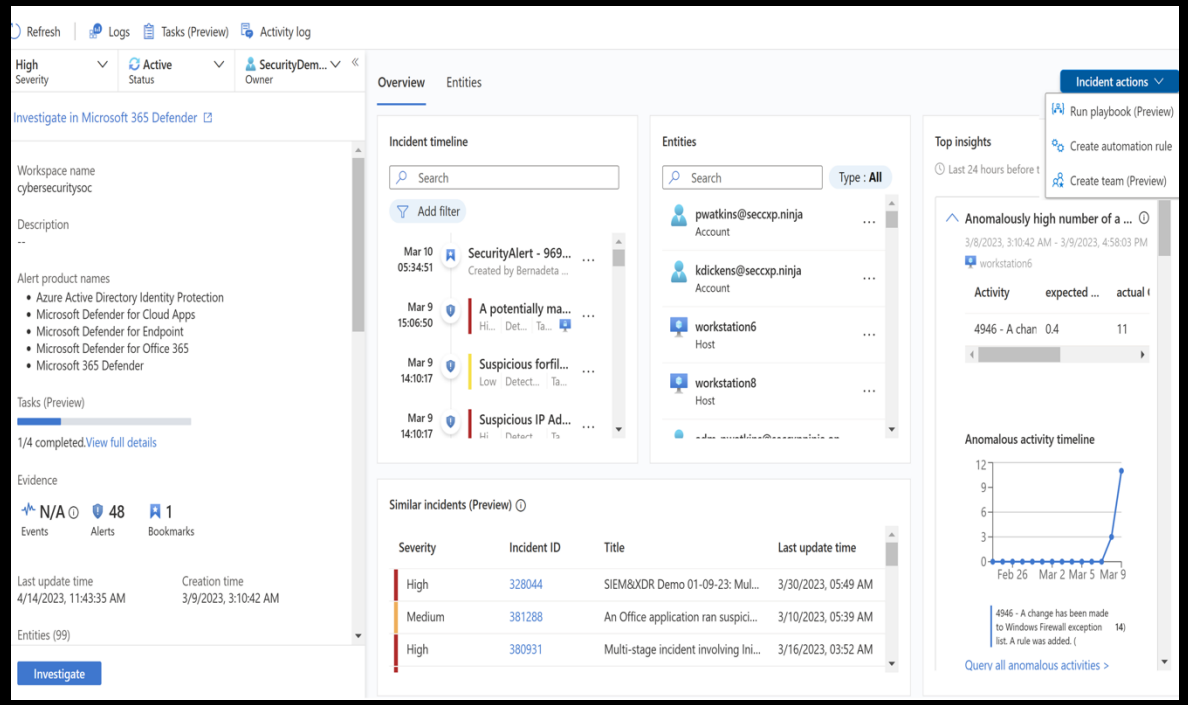
- Detect and diagnose issues across apps and dependencies with application insights
- Correlate issues at infra level with insights for VMs, containers, network, etc.
- Operationalize at scale with smart alerts and automated actions
- Drill down with Log Analytics for troubleshooting & deeper diagnostics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



Microsoft Sentinel, powered by AI, enabled by Azure Arc

Stay ahead of evolving attacks with a comprehensive solution to detect, investigate and respond to incidents

- Build-in enhanced UEBA, automation (SOAR), hunting capabilities, and threat intelligence (TI) to expedite investigation and response
- Industry's first unified experience for SIEM and XDR, with built in GenAI and Threat Intelligence
- Quick response to issues through collaboration with built-in case management for SOC teams
- Stay ahead of threats with built-in threat intelligence with the latest insights from Microsoft Defender Threat Intelligence (MDTI) and Microsoft threat research



Reduce mean time to respond (MTTR) by 80%[1]

Commissioned study-The Total Economic Impact™ of Microsoft Azure Sentinel, conducted by Forrester Consulting, 2020

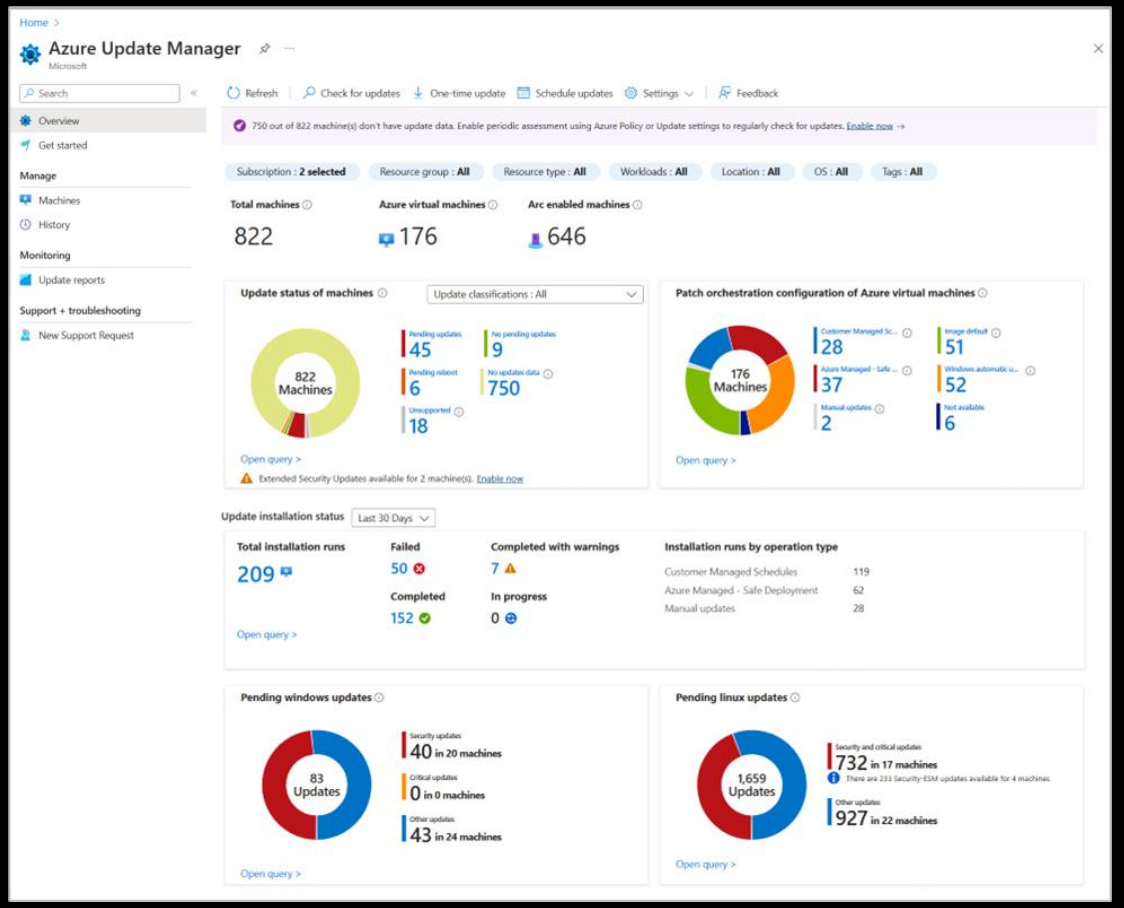
Comprehensive patching with Azure Update Manager

Update and patch your Windows and Linux servers running anywhere with Azure Update Manager enabled by Azure Arc

→ **Streamlined patch management**
Oversee update compliance for your entire fleet of machines in Azure (Azure VMs), on-premises, and multicloud environments

→ **Centralized control with RBAC**
Inherit Azure RBAC configured on the machines to control who can perform update operations and edit schedules. Seamless access management to Azure resources with Azure roles and identity

→ **Intelligent automation and scheduling**
Automate and orchestrate securely with customized, defined maintenance schedules, hot-patching, and auto-patch to reduce reboots and optimize during VM downtimes



ESUs enabled by Azure Arc

Flexible PAYGO monthly billing and savings

Monthly billing model centralized in Azure to run end-of-support operating systems

Visibility and reliability

Ensure consistent Windows Server 2012/R2 and SQL Server 2012 performance with high availability and visibility over your entire data and server estate. Keyless delivery

Security and compliance

Seamlessly extend Azure security and governance to your environment and stay compliant with supported software

Microsoft Defender for Cloud

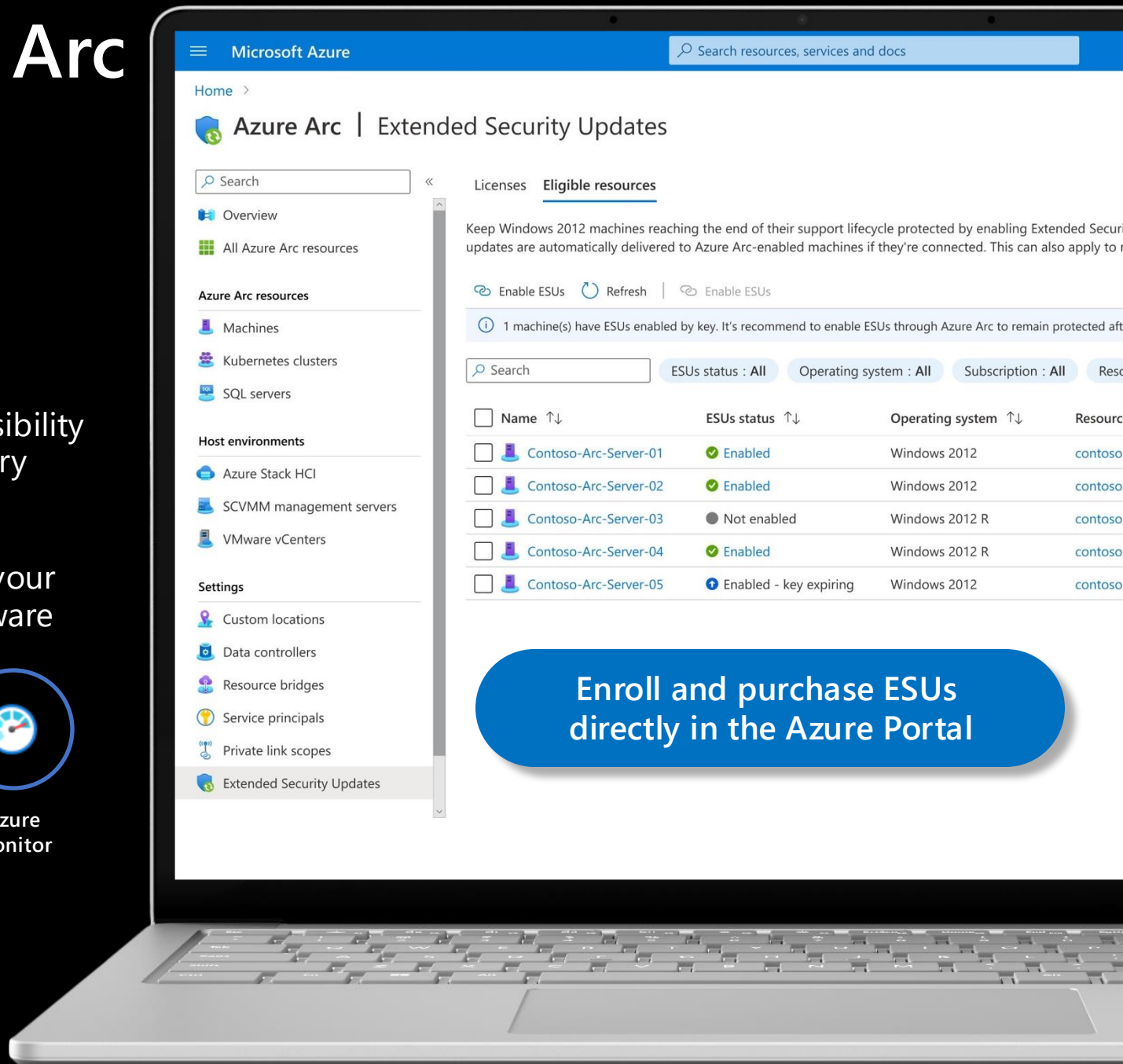
Azure Update Manager

Microsoft Sentinel

Azure Policy

Azure Monitor

For Windows Server 2012/2012 R2,
SQL Server 2012 and SQL Server 2014 (July 2024)



VMware vSphere and System Center VMM

GENERALLY AVAILABLE

Purpose built for VMware vSphere

Bring Azure capabilities your environments with Azure Arc

At-scale management for your VMware vSphere & SCVMM VMs in Azure

Connect at scale

Connect an entire environment managed by vCenter or System Center Virtual Machine Manager at scale

Automatic inventory discovery

Automatic up to date inventory synced from vCenter & SCVMM to Azure and available via Azure Resource Graph

Install Arc Agent at scale

Install Arc agent at scale using portal, CLI, or running the script yourself

Secure, govern and monitor

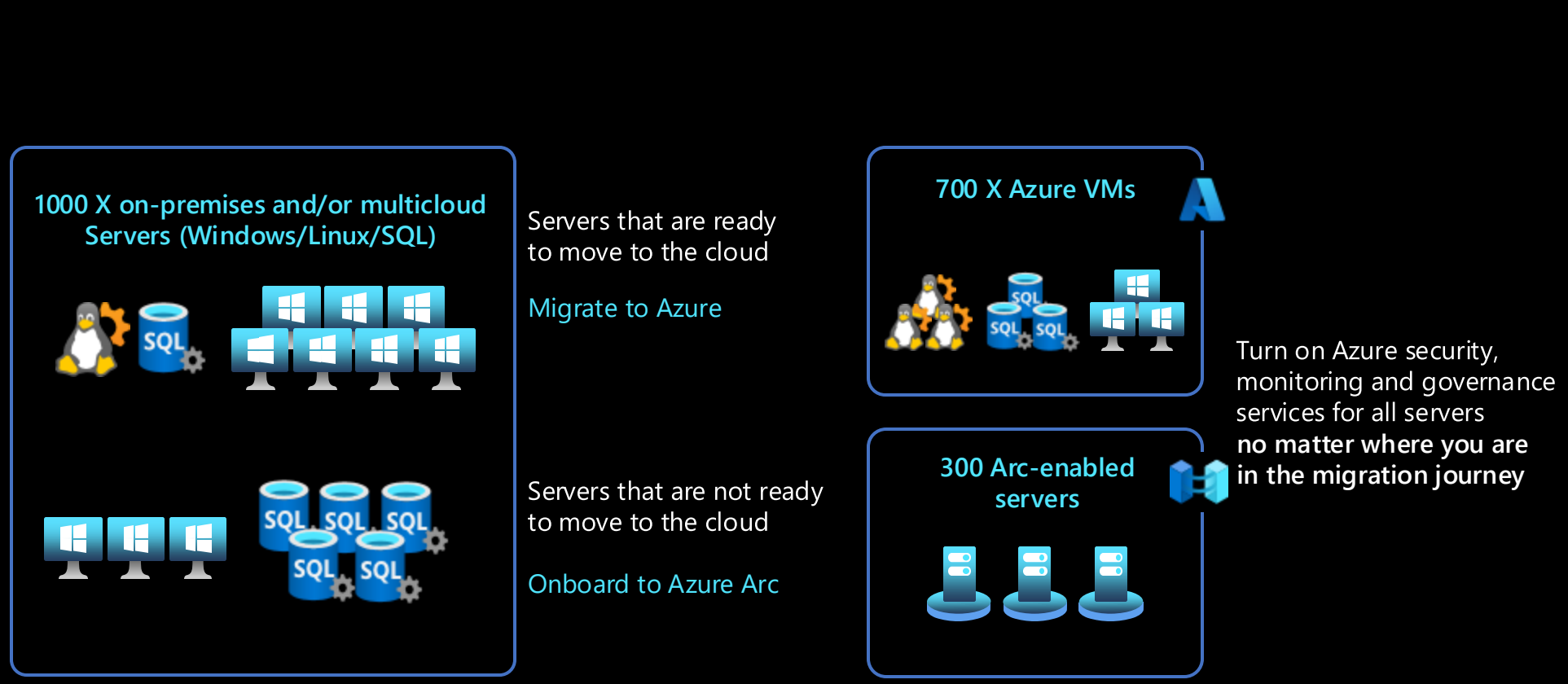
Perform governance, monitoring and security at scale using Azure Monitor, Microsoft Defender, Azure Policy, Azure Update Manager, and more

VMware vSphere and System Center environments hosted anywhere

Unified experience with Arc-enabled Servers

Migrate and Modernize to Azure on your own terms

Azure Arc helps you consistently secure and govern infrastructure across environments as you migrate and modernize

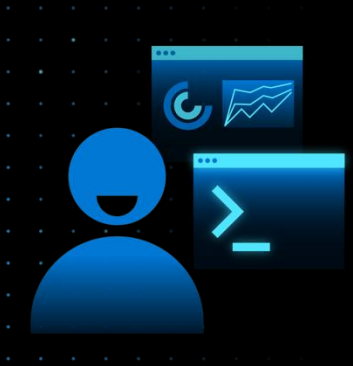


Azure Stack HCI

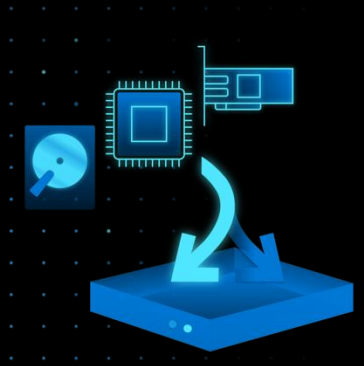
Modern subscription for flexible, familiar hyperconverged infrastructure

Azure hybrid by design

Enterprise scale and price performance



Familiar management and operations



Choice of deployment options

When to use Azure Stack HCI

Distributed compute anywhere for low latency with central cloud management

Affordably run intelligent edge and remote branch office solutions

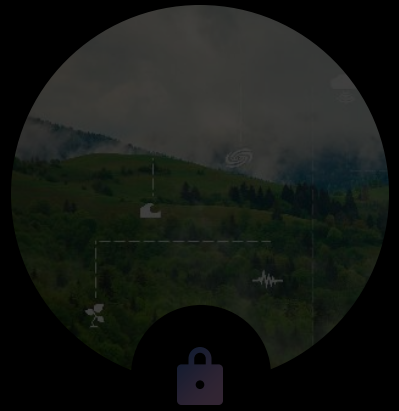
Industry-best performance for SQL Server databases

Deploy cloud native apps and Azure Arc enabled services through tight integration with AKS on-prem

Best in class virtual desktop experience with Azure Virtual Desktop for Azure Stack HCI

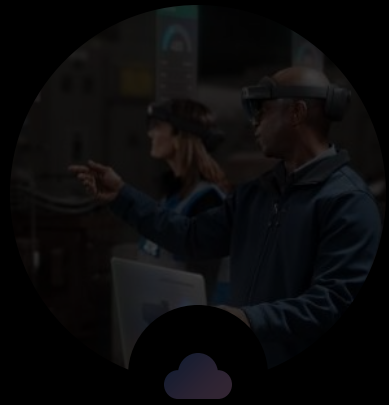
Innovate anywhere with Azure

Azure Arc



Secure and govern your infrastructure and apps

Build apps once, deploy and manage them anywhere



Run Azure data, app, and AI/ML services from cloud to edge

Deliver cloud agility anywhere and modernize applications from cloud to edge using Kubernetes

Customer need to

Run Azure services on-premises for low-latency, compliance and distributed computing needs

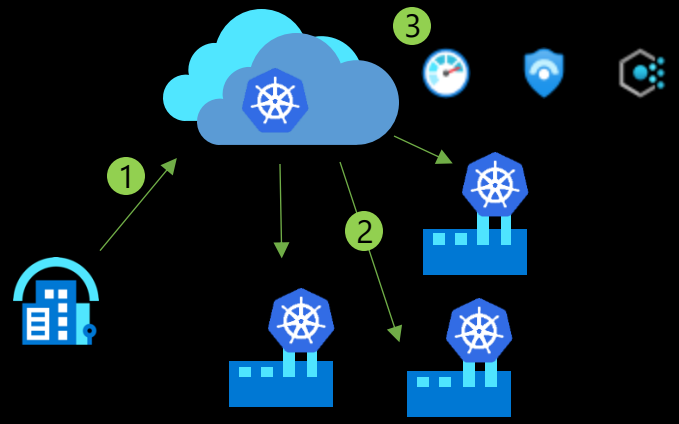
Build cloud-native Kubernetes applications and deploy in your enterprise and at the edge

Ops-as-Code: Automate repeatable configuration and deployment tasks

Deploy to new or existing infrastructure – Windows Server, VMware and more

Entain Millennium bcp uniper

How



1. Dev/Test Kubernetes apps in Azure regions
2. Continuously deploy and update production apps on Arc-enabled K8s at the edge
3. Operate, manage, and secure with the same tools

Microsoft Offerings

Enabled by Azure Arc

- AKS on Azure Stack HCI, Windows Server, Windows IoT
- At-scale Kubernetes management (CNCF)
- GitOps pipelines
- Flux
- Azure monitoring and security for containers
- Open Service Mesh
- Azure Container Apps - preview
- Azure Application Services – preview

Build apps once, deploy and manage them **anywhere with Azure Arc**

Build and modernize to cloud-native apps on any Kubernetes

Bring cloud data management to any infrastructure

Consistent GitOps and policy driven deployment on any Kubernetes

Integrate Azure Security, governance and monitoring into your DevOps toolkit

Azure Arc-enabled Kubernetes

Azure Arc-enabled SQL Managed Instance

Azure Arc-enabled PostgreSQL

Azure Stack HCI

vmware

aws

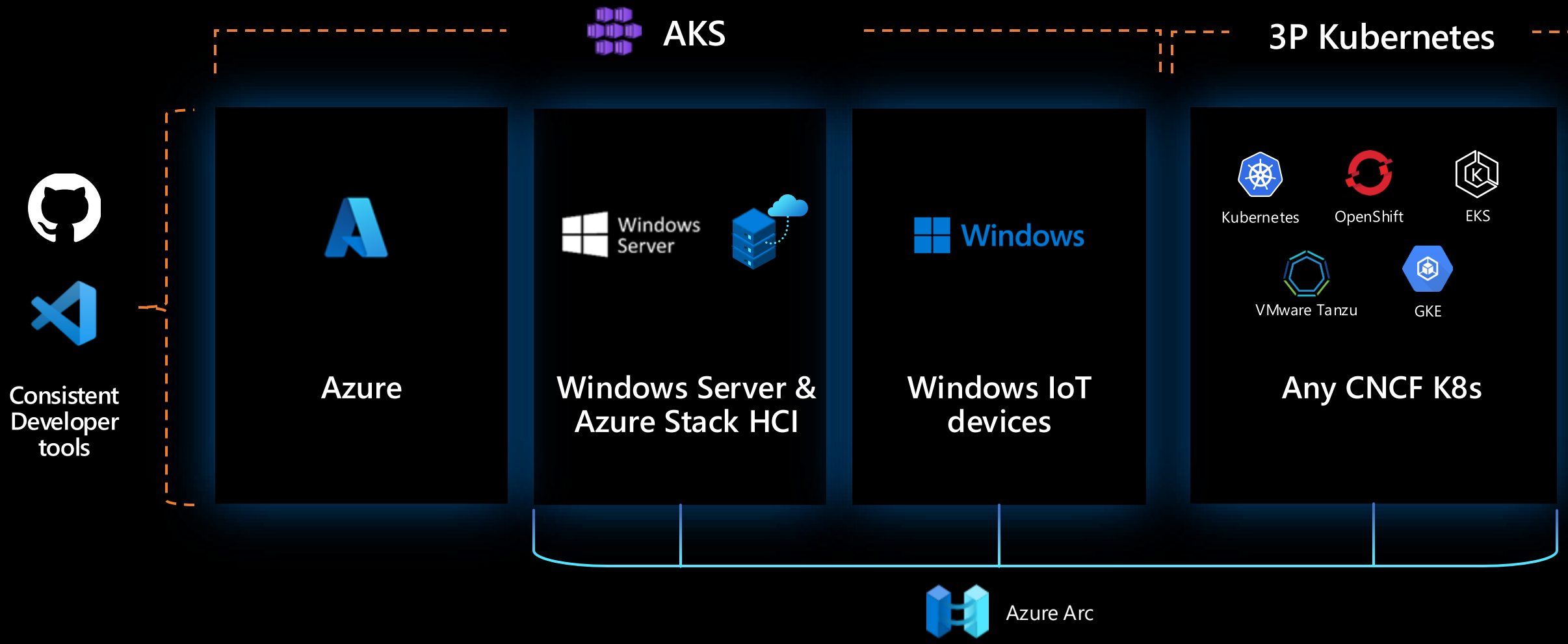
Azure IoT

On-premises, multicloud, and edge

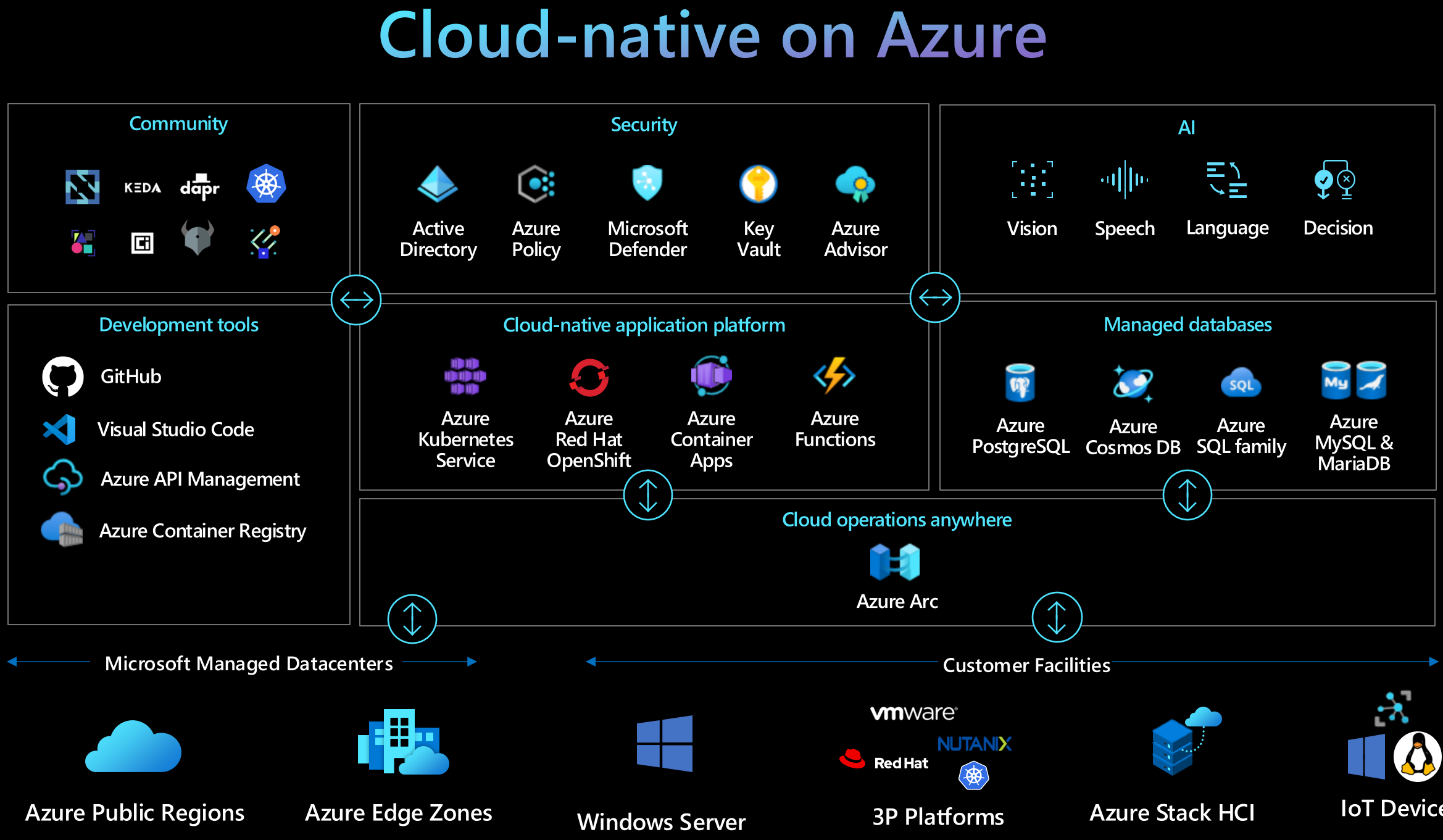
Managed Kubernetes from cloud to edge

GENERALLY AVAILABLE

Flexible deployment options on the infrastructure of your choice



Cloud-native on Azure



Azure Arc-enabled Kubernetes

GENERALLY AVAILABLE

Connect, manage, and operate Kubernetes clusters and applications running anywhere

AKS on Azure Stack HCI or Windows Server

Multiple 3P Kubernetes flavors supported

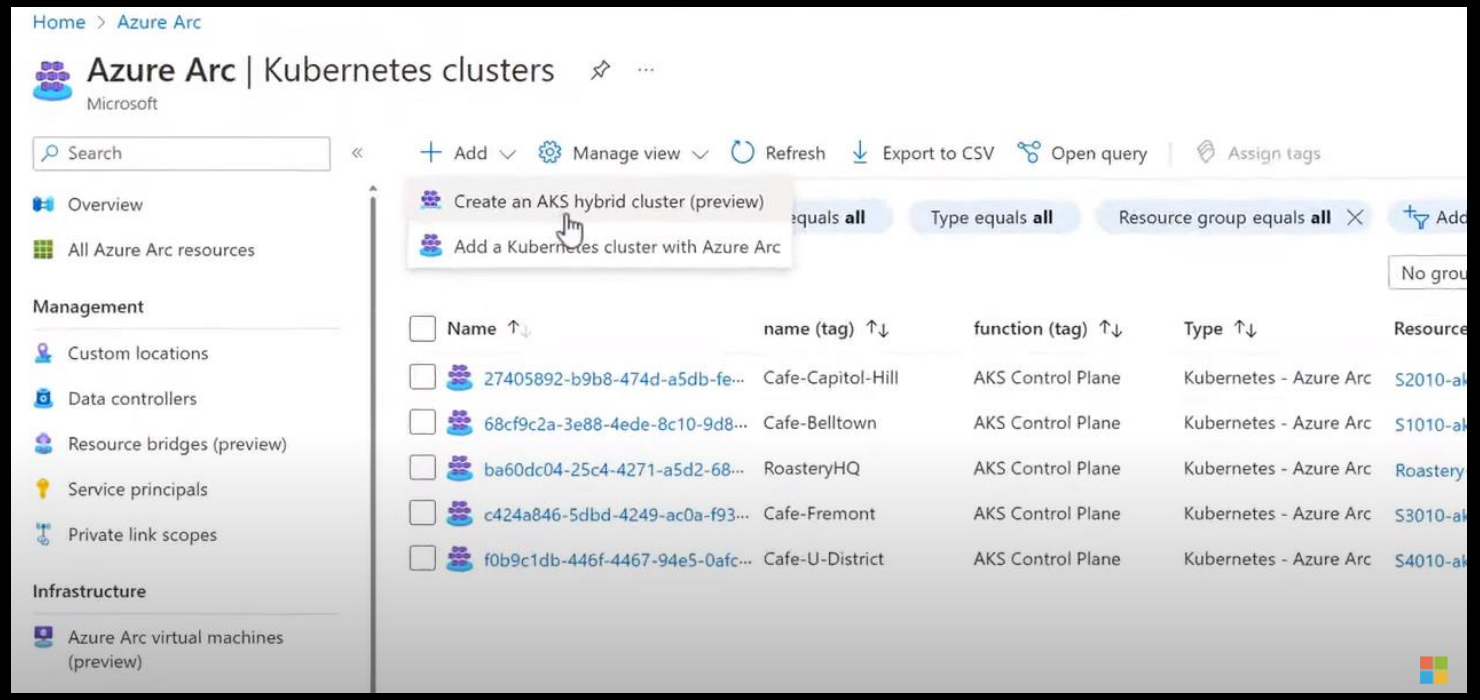
Deploy apps and configurations at-scale with GitOps

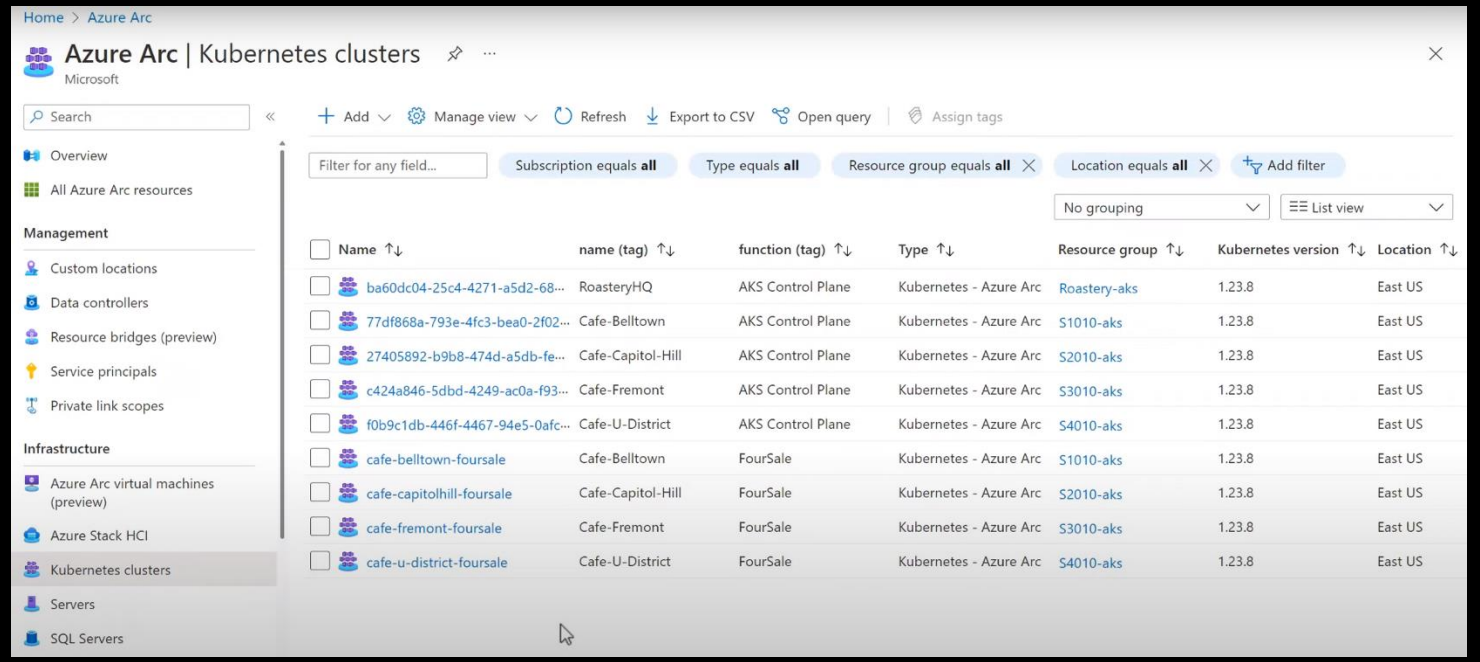
Secure, govern and monitor all your clusters, from Azure

AKS Kubernetes OpenShift EKS GKE VMware Tanzu NUTANIX PLATFORM9 CANONICAL

RANCHER WNDRVR kublr MIRANTIS

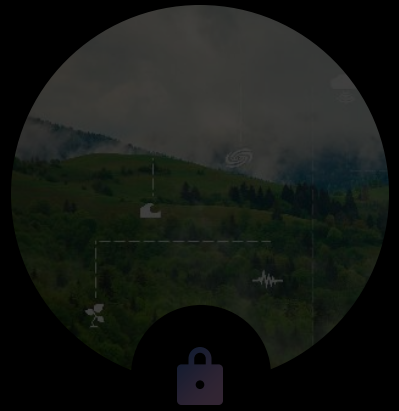
Create Kubernetes clusters and manage them from the Azure Portal





Innovate anywhere with Azure

Azure Arc



Secure and govern your infrastructure and apps

Build apps once, deploy and manage them anywhere

Run Azure data, app, and AI/ML services from cloud to edge

Transform physical operations with cloud and AI

Customer needed

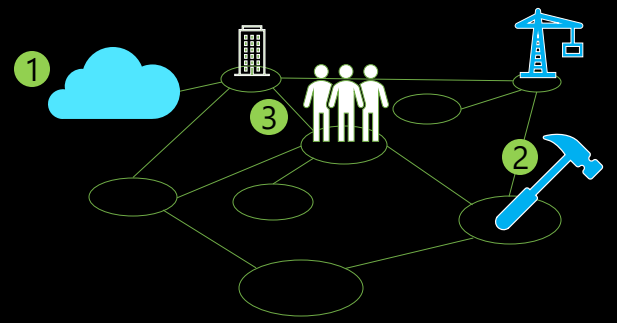
Data connections from physical operations to the cloud, to harness AI and insights

Automated and improve site workflows centrally, from the cloud across multiple locations

Reliable edge solutions that could operate with intermittent connectivity

Distributed compute at the edge for low latency with central cloud management

How



1. Model & describe physical processes in Azure
2. Collect data, create context, derive insights where needed
3. Make decisions and take actions. Repeat.

Microsoft Offerings

Enabled by Azure Arc

- SQL MI
- Azure SQL MI Business Critical
- PostgreSQL – preview
- Azure Machine Learning
- Azure IoT Hub
- Azure Digital Twins
- Azure Stack HCI
- Windows IoT

JOHN DEERE

CARNIVAL CORPORATION & PLC

Run Azure data, app, and ML services

Configuration management | Observability | Governance | Security

- Microsoft Copilot for Azure
- Microsoft Defender for Cloud
- Azure Monitor
- Microsoft Sentinel
- Azure Policy
- Azure Update Manager
- Configuration Management
- Inventory Management

Azure Services across your infrastructure

Windows Server | SQL | Azure Stack HCI | vmware | aws | ORACLE | Azure IoT | suse

Datacenter, multicloud, and edge

Bring cloud manageability to SQL Server anywhere

Manage, govern, and protect your SQL Server from Azure

Manage all SQL estate with better observability

Single view of all SQL Servers deployed on-premises, in Azure and other clouds

Capture key performance metrics and realize faster time-to-value with **monitoring**

Gain proactive & actionable insights with automated **best practices assessment**

Enhance business continuity

Manage **Availability Groups** inventory and track real-time health status

View Always-on **Failover Cluster Instances** and protect with Defender

Automated backups and point-in-time restore for seamless application of policy

Govern and protect all SQL estate using Azure

Protect your on-premises & multicloud data using **Microsoft Defender** for Cloud

Enhance security using **Extended Security Updates** as a service & **auto patching**

Central insights and governance across all SQL Servers with Microsoft Purview

Azure billing enabled by Azure Arc for SQL Server anywhere, with simplified onboarding

Management Capabilities Comparison

✗ Not supported ✓ Supported ✓ Future support

	Customer Infrastructure or 3P Clouds		Azure
Built-in capabilities	**SQL Server**	**Arc Enabled SQL Server**	**SQL Server Azure VM**
Pay-as-you-go billing	✗	✓	✓
Azure AD auth	✗	✓	✓
Best practices assessment	✗	✓	✓
Inventory management	✗	✓	✓
Auto patching	✗	✓	✓
Auto backup	✗	✓	✓
Monitoring	✗	✓	✓
Defender for SQL Server	✓	✓	✓
TDE with Azure Key Vault	✗	✓	✓
HA/DR inventory management	✗	✓	✓
License usage management	✗	✓	✓
Cluster aware patching and upgrades	✗	✓	✓
Purview premium	✗	✓	✓
Point-in-time restore	✗	✓	✓
Backup long-term retention to Azure	✗	✓	✓

*Some information regarding product roadmap may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

bwsqlserver2022

Server - Azure Arc

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Connect (preview)
Windows Admin Center (preview)
Security
Extensions
Properties
Locks

Operations
Policies
Machine Configuration
Automanage
Updates
Inventory
Change tracking

Monitoring

Delete Refresh

Essentials

JSON View

Resource group (move)	: bwvmsrg	Computer name	: bwsqlserver2022
Status	: Connected	FQDN	: bwsqlserver2022
Location (move)	: East US	Operating system	: Windows Server 2022 Datacenter
Subscription (move)	: Microsoft Azure Sponsorship	Operating system version	: 10.0.20348.1487
Subscription ID	: e1775f9f-a286-474d-b6f0-29c42ac74554	Cloud provider	: N/A
Agent version	: 1.25.02203.713	Manufacturer	: Microsoft Corporation
		Model	: Virtual Machine

Tags (edit) : Click here to add tags

Capabilities | Recommendations | Tutorials

Updates
Customize updates for your Arc-enabled server.

Logs
Enable additional monitoring capabilities.

Monitoring insights
Enable additional monitoring capabilities.

Policies
View compliance by assigning guest configuration policies to your machine.
Not configured

Change tracking and inventory
Enable consistent control and compliance of this machine with Change tracking and inventory.

Security
Continuously monitor for potential security vulnerabilities and recommendations.

Windows Admin Center (preview)
Manage your operating system from anywhere — without needing a VPN

Azure Arc-enabled data services

Bring cloud data management to any infrastructure

GENERALLY AVAILABLE — Azure Arc-enabled SQL Managed Instance – Business Critical

PREVIEW — Azure Arc-enabled PostgreSQL

Supports all connectivity modes

Always up to date

Automated updates
No downtime, evergreen

Multi-layer security

Comprehensive encryption
Azure RBAC & Policy

Elastic scale

Scale up and down
Pay for what you use

Simplified DevOps

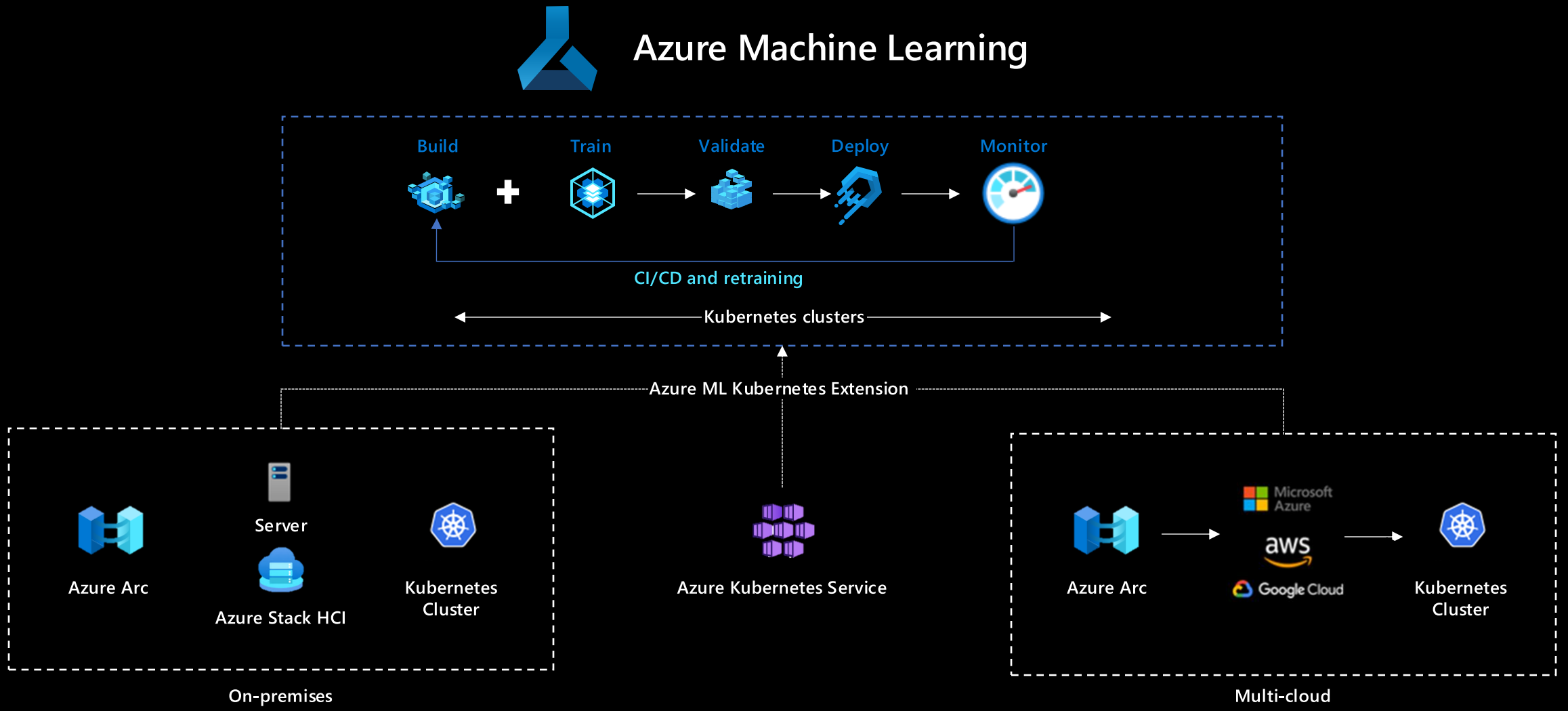
Deploy in seconds
Built in HA/DR

Any infrastructure

Azure Arc-enabled machine learning

GENERALLY AVAILABLE

Bring fully operationalized machine learning to on-premises and multicloud



Azure Arc-enabled Servers pricing

Azure Arc is free to install. Basic management services like inventory, tagging, server organization, RBAC, and querying with Azure Resource Graph are free. Paid services are:

Microsoft Defender for Cloud $5/server/month (Plan 1) or $15/server/month (Plan 2)

Free for the first 30 days, with 500MB/server included data. $0.02/server/hr.

Azure Monitor $2.30/GB [pay-as-you-go]

Billed for log analytics, tests, metrics, alerts, and notifications. 5GB per billing account/month is included

Microsoft Sentinel $2/GB-ingested [pay-as-you-go]

Billed for volume of data ingested for analysis in Microsoft Sentinel, stored in the Azure Monitor Log Analytics workspace

Azure Update Manager $5/server/month [pay-as-you-go]

Charged at a daily prorated value of $0.16/server/day. Only charged for days when Arc servers are connected and managed

Azure Policy Guest Configuration $6/server/month

Policies assigned by Defender for Cloud, ESUs, or on Azure Stack HCI resources are exempt

New cloud billing model for SQL Server (pay-as-you-go*)

Better cost efficiency when paying only for what you use

SQL Server pay-as-you-go licensing enabled by Azure Arc
(per core per month/hour)

Pricing	Monthly rate	Hourly rate
Standard Edition	$73	$0.100
Enterprise Edition	$274	$0.375

Optimize asset capitalization

- Organizations that focus on EBITDA and capitalized expenses prefer to purchase their licenses
- Customers that bill on a cost-plus or other expense-based chargeback model will prefer the Pay-As-You-Go model

Optimize upfront costs

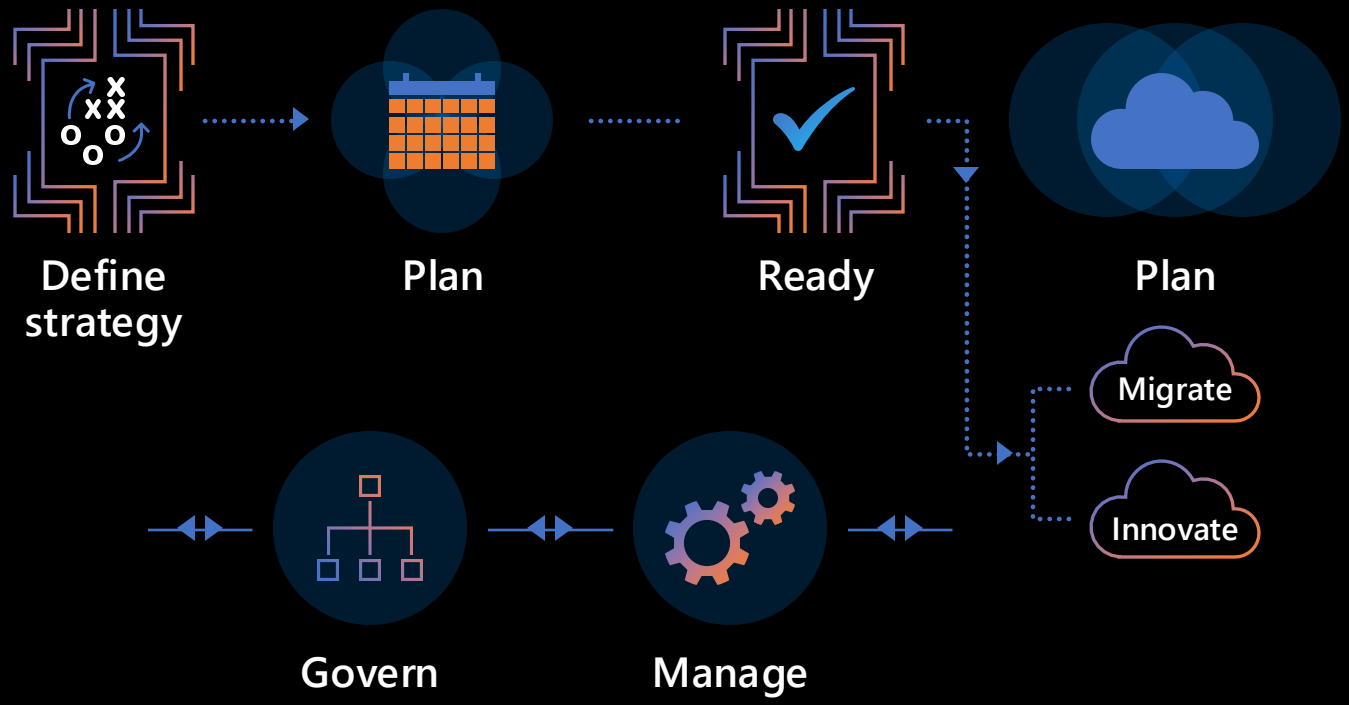
- Pay-As-You-Go doesn't have any upfront costs and is billed monthly but in the long term it may have a higher TCO

Optimize for periodic consumption

- Reduced IP cost of periodic workloads such as of ERP, payroll, giving campaigns and others
- Scale down the entire VM or stop SQL Server instance

Available on SQL Server 2014, 2016, 2017, 2019, and 2022 * Traditional Licensing Options are still available. More here.

Complete guidance for an adaptive cloud approach



Microsoft Cloud Adoption Framework for Azure | Microsoft Azure

Start with the cloud adoption framework to guide your cloud journey and build on it using the hybrid adoption scenario guidance

Build skills across your team with Microsoft Learn

Accelerate deployment with Reference Architectures

Optimise workloads with Azure Well-Architected

Apply best practices to rapidly onboard

Review technical documentation on featured products

Next steps

Install Azure Arc

Gain visibility into your entire on-premises and multicloud estate for a single pane of glass

Manage and secure

Get started using Microsoft Defender for Cloud, Azure Monitor, Copilot, and more

Azure Migrate and Modernize

Utilize the Azure Migrate and Modernize program to deploy Arc at scale and securely move to the cloud with proven best practices and incentives to accelerate

Learn more

Azure Arc Jumpstart:
https://aka.ms/AzureArcJumpstart

Technical documentation:
https://aka.ms/AzureArcDocs

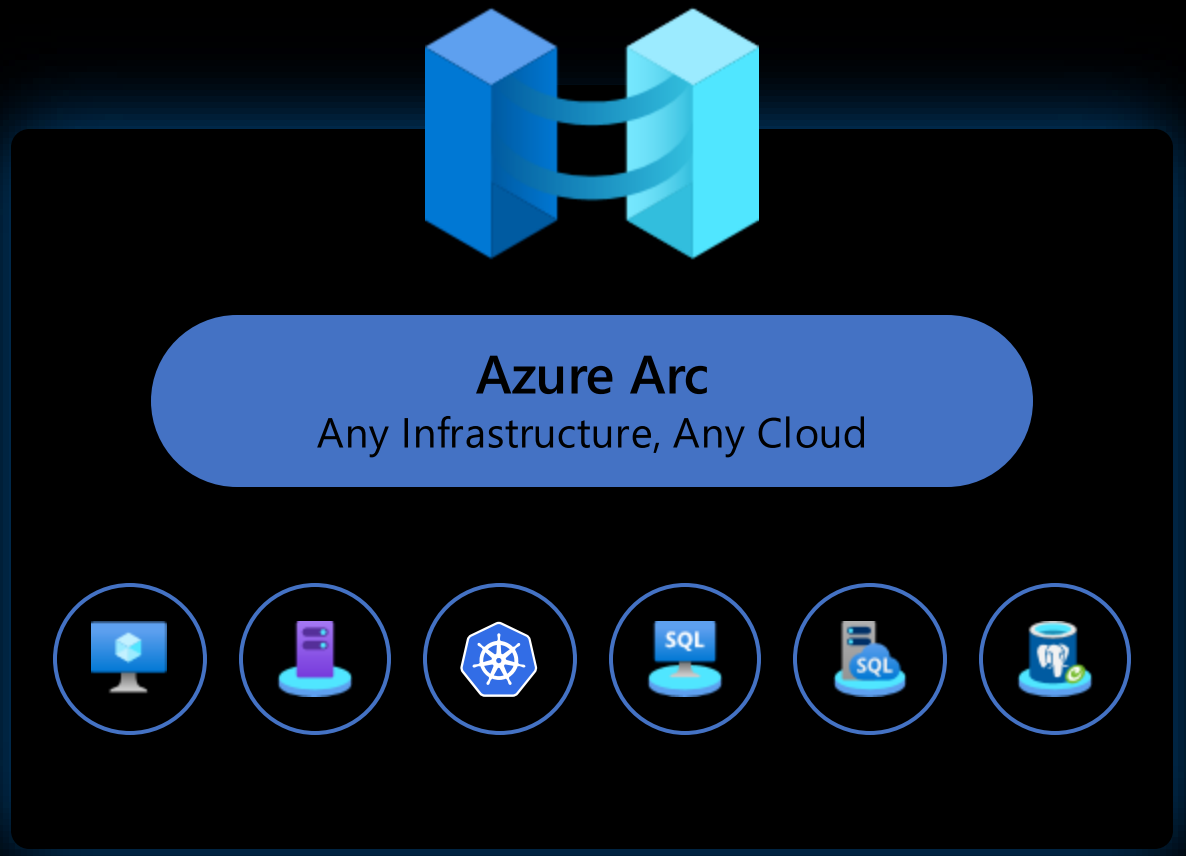
Azure Arc Learning Path:
https://aka.ms/AzureArcLearn

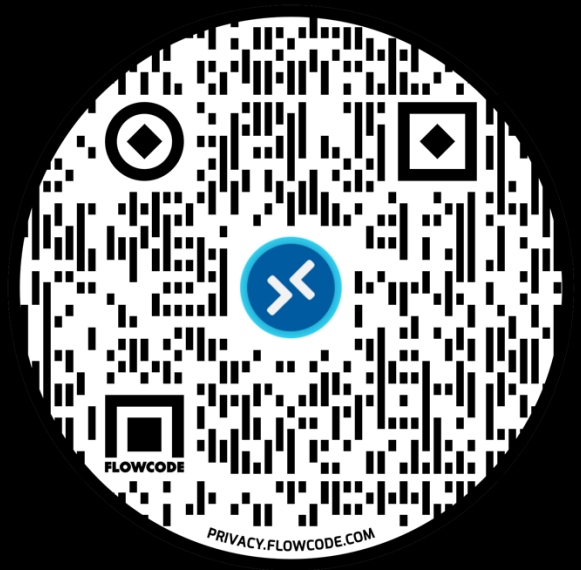
Azure Arc Learning Companion:
https://aka.ms/pathways

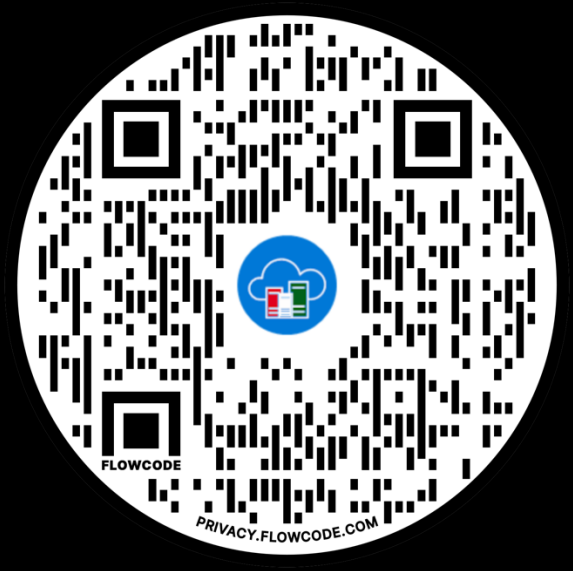
Azure Arc ESU Docs:
https://aka.ms/arcesudocs

Azure Arc Total Economic Impact Report:
https://aka.ms/arcforresterstudy

SQL Arc:
https://aka.ms/ArcSQL







Azure Virtual Desktop
& Windows 365 Italian User Group

Intune Italian User Group

Microsoft Security Italian User Group

Thank you

TD SYNNEX | skybackbone engenio

Presentazione aziendale

skybackbone engenio

Sommario

Chi siamo ?

Fondata nel 2011 a Modena, da un team con **esperienza pluri-decennale**, siamo una **Società di Consulenza** nella **gestione dei Sistemi Informativi Aziendali** con particolare **focus sulla Cyber Security** e sulle applicazioni ERP in Cloud.

Cosa facciamo ?

Forniamo **servizi innovativi con l'obiettivo di ottimizzare ed automatizzare tutti i processi di gestione del** sistema **ICT** di un'azienda.

| Cloud | | Servizi Automatici | | Servizi Gestiti | | Security |

Patch Management

Security Management | Cloud | **Backup** Management

Performance Management

TD SYNNEX | skybackbone engenio

Managed Services

Il futuro è a portata di mano.

Il **futuro** **è gestito**.

eREACT servizio di **Patch Management**

eREACT - Patch Management

Windows | Linux | SQL Server

Perché le Aziende non applicano le Patch?

1) E se poi qualcosa va storto? Mancanza di piano per tornare velocemente a «Prima dell'Attività».

eREACT — Snapshot/Cloni/Backup automatizzati, con successiva pulizia

2) Downtime... Riavvio dei Server, dei servizi, delle applicazioni. Per quanto tempo saranno fermi i miei sistemi?

eREACT — Riavvio orchestrato = minimo fermo possibile

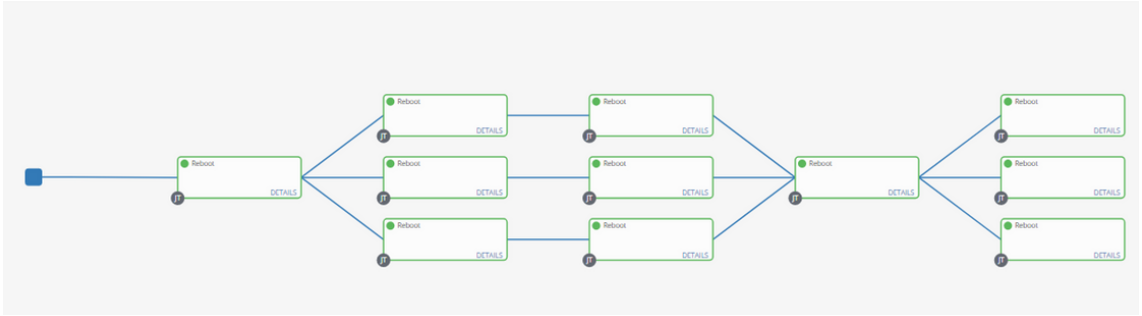
eREACT – cosa può fare?

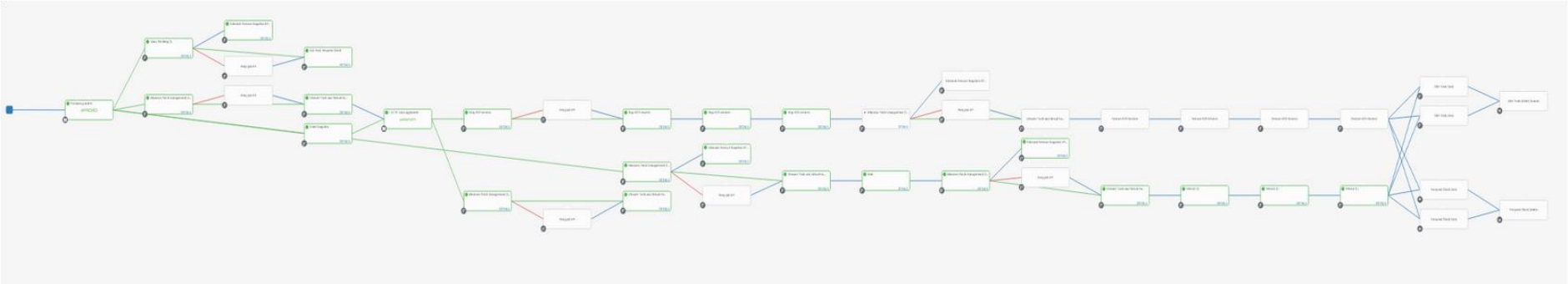
eReact si adatta «sartorialmente» alle infrastrutture e alle dipendenze specifiche di ogni cliente.
Riavvio ordinato: Database, Application Server, Gateway, DMZ, Bilanciatori …

1
- Crea/Rimuovi Snapshot
- Attiva Backup su richiesta
- Aggiorna Windows/Linux/SQL
- Avvia/Arresta Servizi
- Spegni/Accendi Server
- Riavvia/Reset

2
- Switch Cluster
- Aggiorna VMware Tools
- Check URL
- Check Process
- Gestisci Attività Pianificate

eREACT - esempi di Workflow

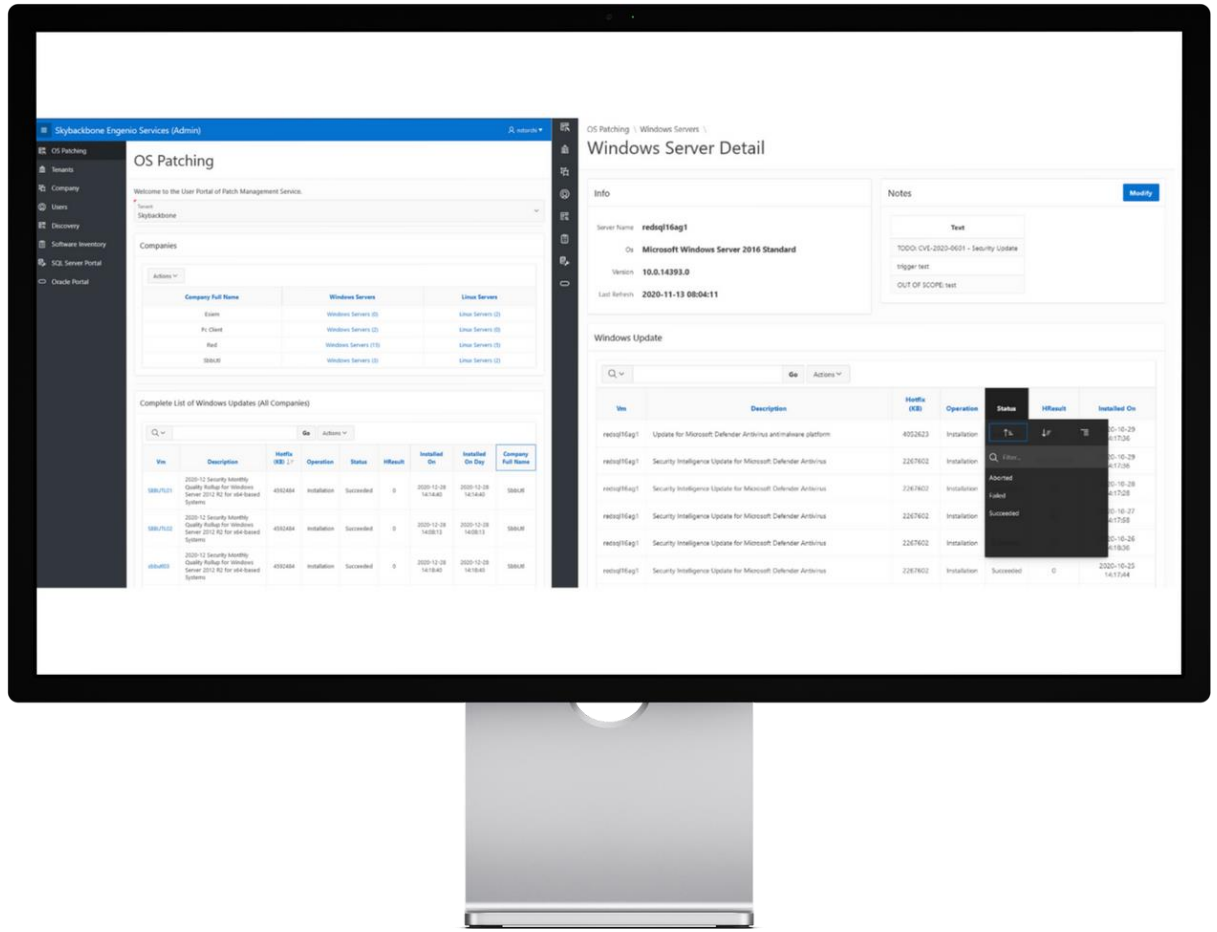




eREACT - Portale Web

Dati aggregati o in dettaglio

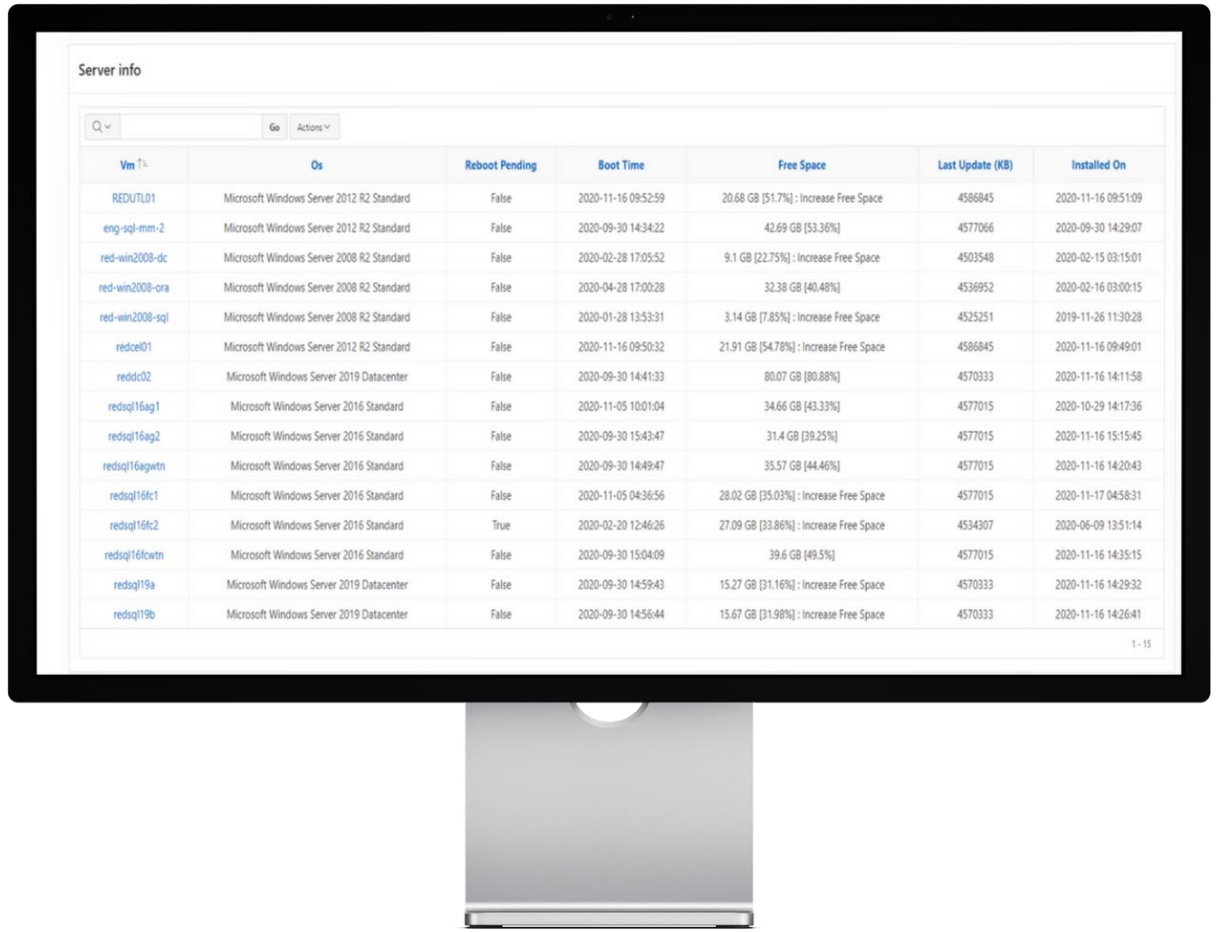
Divisione per ambiente produttivo



eREACT - Portale Web

Divisione per sistema operativo

Report interattivi e scaricabili



Dashboard
19097 HOSTS

Perchè scegliere eREACT ?

Dashboard
14391 HOSTS

| Servizio Gestito |

| Integrazione Sistemi |

| Agentless |

VMware, Azure, Hyper-V, Nutanix AHV (gestione delle snapshot, backup, cloni)

| Servizio personalizzato |

| Automatico |

| Reports self-service Portal |

eVA servizio di **Vulnerability Assessment**

Le vulnerabilità vanno gestite.

Ogni settimana vengono individuate più di 2000 vulnerabilità e ogni giorno una 0 day (Vulnerabilità zero-day) viene scoperta.
L'approccio "only patch" oltre ad essere difficilmente attuabile **è diventato inefficace** e le **aziende** sono **continuamente esposte** a nuovi rischi.

| 65 giorni |

Normale tempistica per applicare le patch.

| 7 mesi |

Per scoprire un nuovo data breach.

| 80% dei data breach |

Derivano da un patch management insufficiente.

Cosa fa eVA.

Solo attraverso un **monitoraggio costante** delle **vulnerabilità** si **riduce** notevolmente la **superficie** di **attacco** dell'infrastruttura IT e quindi la possibilità che si verifichi **un incidente cyber**.

eVA è il servizio gestito da Skybackbone che **scansiona** periodicamente le **infrastrutture**, permettendo di **identificare e trattare le vulnerabilità prima** che vengano sfruttate dagli hacker.

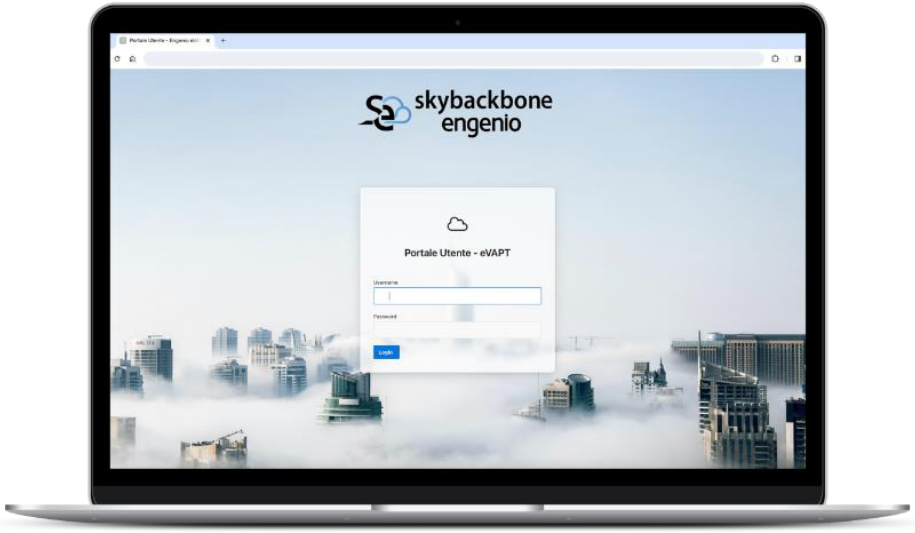
| Sorveglianza |

Costante

| Infrastruttura IT |

Sicura

Punti chiave di eVA.

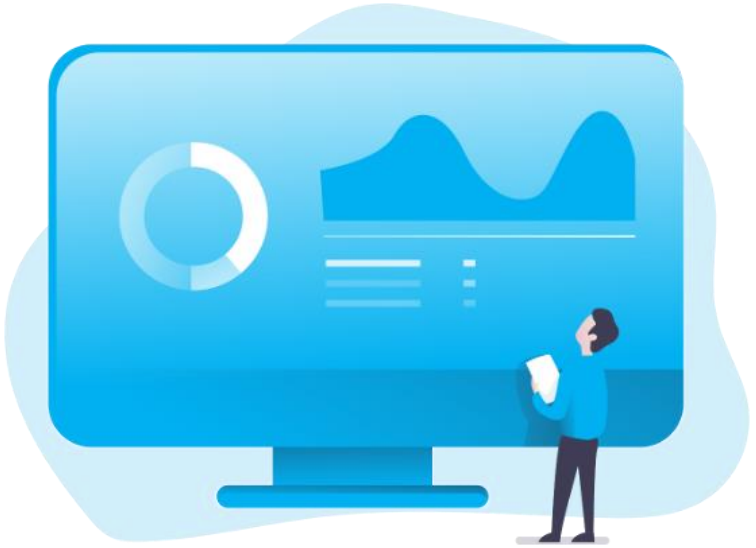


| Periodic Reports | | Remediation Tips | | No System Impact |

| Cyber Team Dedicated |

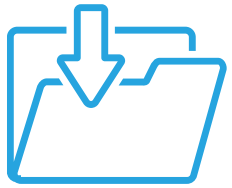
Semplifica attività complesse di analisi **automatizzandole** e dona alla tua azienda le **competenze di un team cyber**.

eSIEM+ servizio di **Log Management**



Gestione dei Log: estrarre il massimo valore

E tu cosa fai con i log che raccogli?



Vuoi solamente **conservarli** ?

oppure

Vuoi **ricavare informazioni** utili ?

Una volta **estratti** i **log**, sei **pronto** per **procedere**.

Cosa fa eSIEM+

All in **one** solutions.

Machine
Learning

Vulnerability
Scanning

Threat
Defense

Logging
Analytics

Monitoring

Alarms

Soluzione Cloud Completa per il Log Management.

Più di **300 applicazioni supportate**...ma il numero è costantemente in crescita!

Sistemi Operativi Supportati
Windows, Linux, Solaris, AIX, AS400

Database Supportati
SQL Server, Oracle, Postgres, MySQL, DB2, Cassandra, MongoDB

Web Server
Apache HTTPD, NGINX, Microsoft IIS

Application Server
Tomcat, Jboss, Weblogic

Hypervisor / Orchestrator
VMWare, Xen, Docker, Kubernetes, Oracle VM

Apparati Networking
Fortigate, Cisco, F5, CheckPoint

Suite di Sicurezza
QRADAR, TrendMicro, McAfee

Storage
NetApp FAS, Hadoop

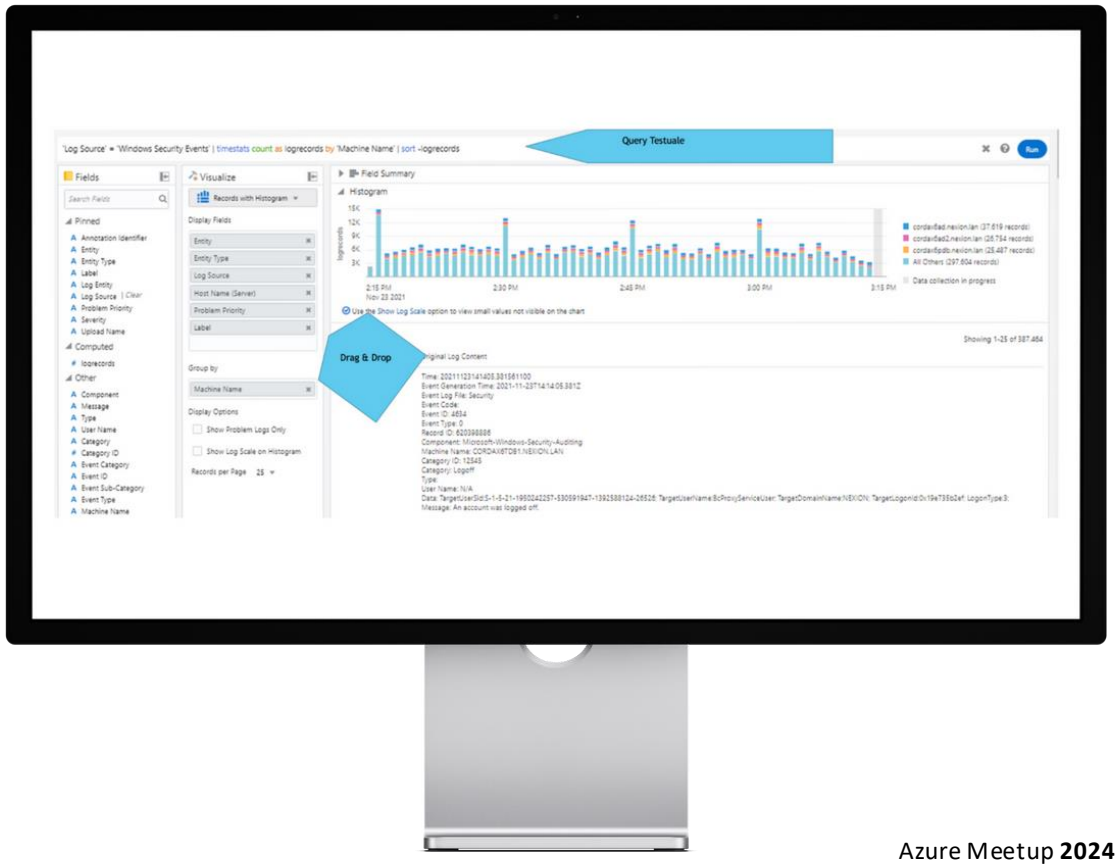
Software Gestionali
SAP, PeopleSoft

Front End per Ricerche ed Analisi.

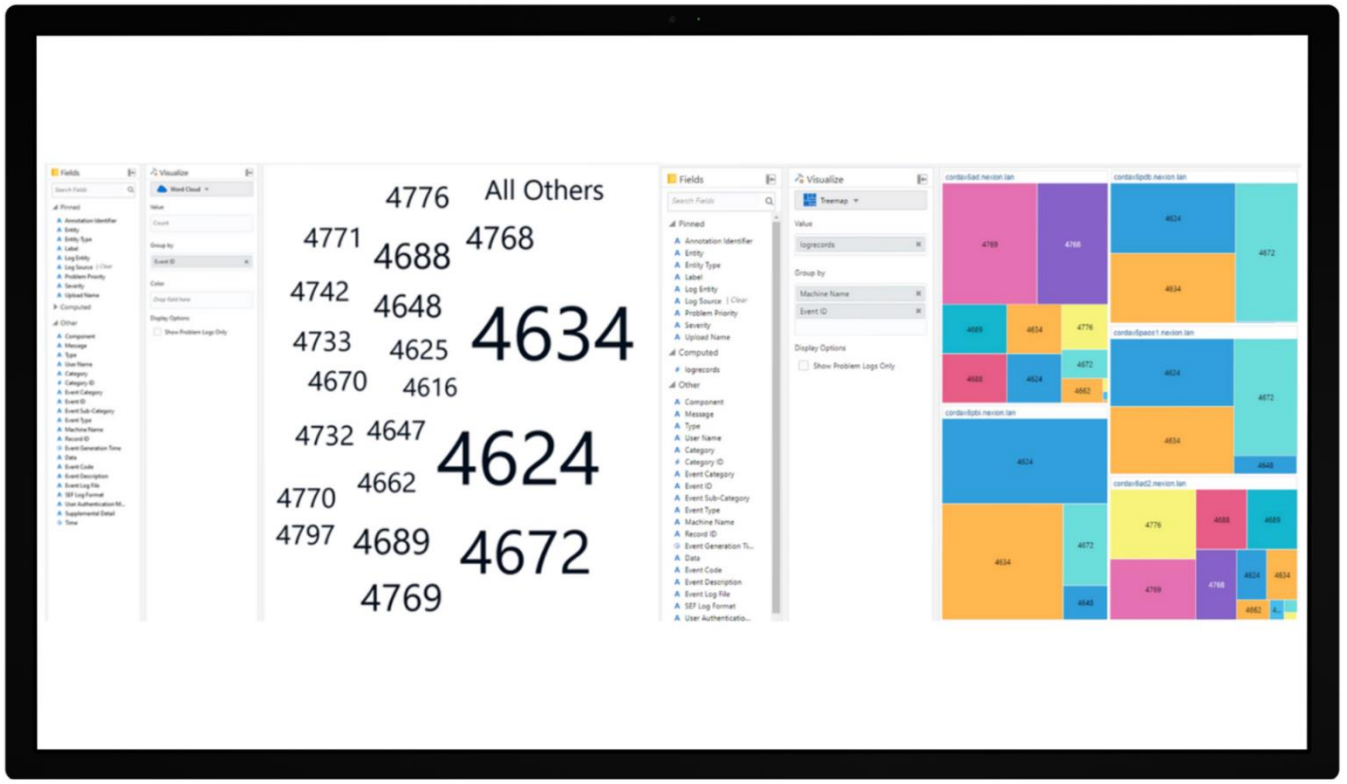
Pagina Web su cui fare Query semplici e complesse:

(A) query semplici utilizzando Drag & Drop degli Elementi

(B) query complesse raffinando il Testo della Query



Front End per Ricerche ed Analisi.



TD SYNNEX | skybackbone engenio

GRAZIE

Dal **Team** di skybackbone engenio

Contatti.

+39 059 868 0754

marketing@skybackbone.it

www.engenio.it

TD SYNNEX

Proteggi le Tue Identità con Microsoft Entra: *Innovazione e Sicurezza*

Vito Trentadue *– Pre-Sale & Cloud Solution Architect Microsoft & Microsoft Certified Trainer – TD SYNNEX*

About me

TD SYNNEX

- **Vito Trentadue**
- **Pre-Sale & Cloud Solution Architect Microsoft**
- **Microsoft Certified Trainer**
- **Focus su Azure AVD, Infrastruttura**
- **Altri focus, AI, Copilot, Fabric**

Profilo LinkedIn

Agenda

TD SYNNEX

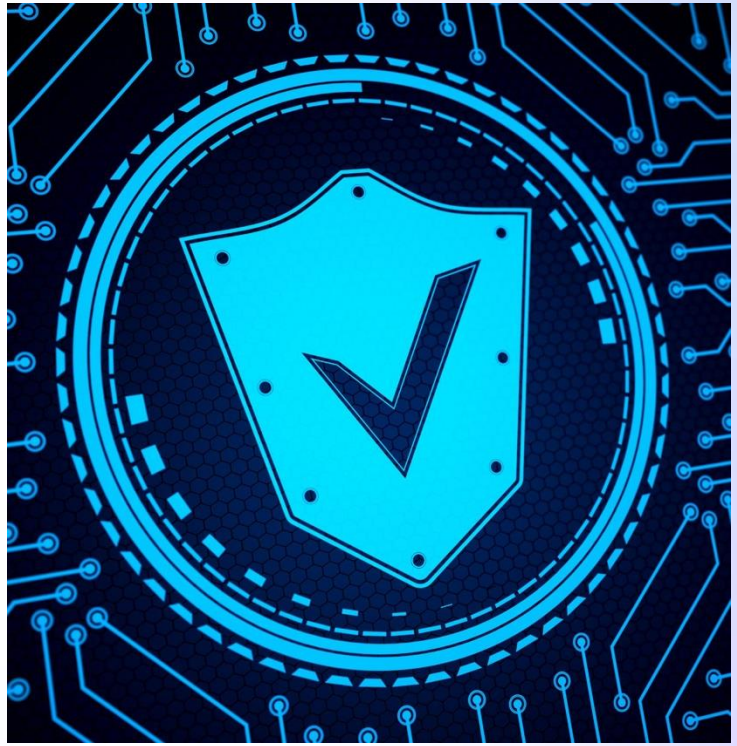
- Microsoft Entra – Prodotti Free
- Microsoft Entra – Prodotti SMB
- Microsoft Entra Plans
- Microsoft Secure Future Initiative
- Defender for Cloud App

Microsoft Entra – Security Default

Cosa sono i Security Default:
Servono a semplificare la protezione dell'organizzazione da attacchi correlati all'identità, ad esempio password spraying, riproduzione e phishing comuni negli ambienti attuali.

A chi sono destinate queste impostazioni?

- Alle organizzazioni che vogliono aumentare la propria postura di sicurezza ma non sanno come o da dove iniziare.
- Alle organizzazioni che usano il livello gratuito delle licenze Microsoft Entra ID.



Microsoft Entra – Security Default

TD SYNNEX

Feature	Description
Multifactor Authentication (MFA)	Requires all users to register for MFA and perform MFA when necessary.
Blocking Legacy Authentication	Prevents the use of older, less secure authentication protocols.
Protecting Privileged Activities	Ensures that privileged activities, such as access to the Azure portal, are protected by MFA.
Automatic Enablement	Security defaults are automatically enabled for new tenants created on or after October 22, 2019.
Administrator Requirements	Administrators are required to perform MFA.
User Registration	Users must register for MFA within 14 days of security defaults being enabled.
Revoking Active Tokens	Administrators should revoke all existing tokens to require all users to register for MFA.
Disabling Security Defaults	Security defaults can be disabled if other security protections, such as Conditional Access, are in place.
Fraud Alert	Allows users to report fraudulent verification requests. This feature will be removed on March 1, 2025, and replaced by the "Report suspicious activity" feature.
Identity Protection	Configures reports and alerts to protect identities.

Microsoft Entra – Altri strumenti free

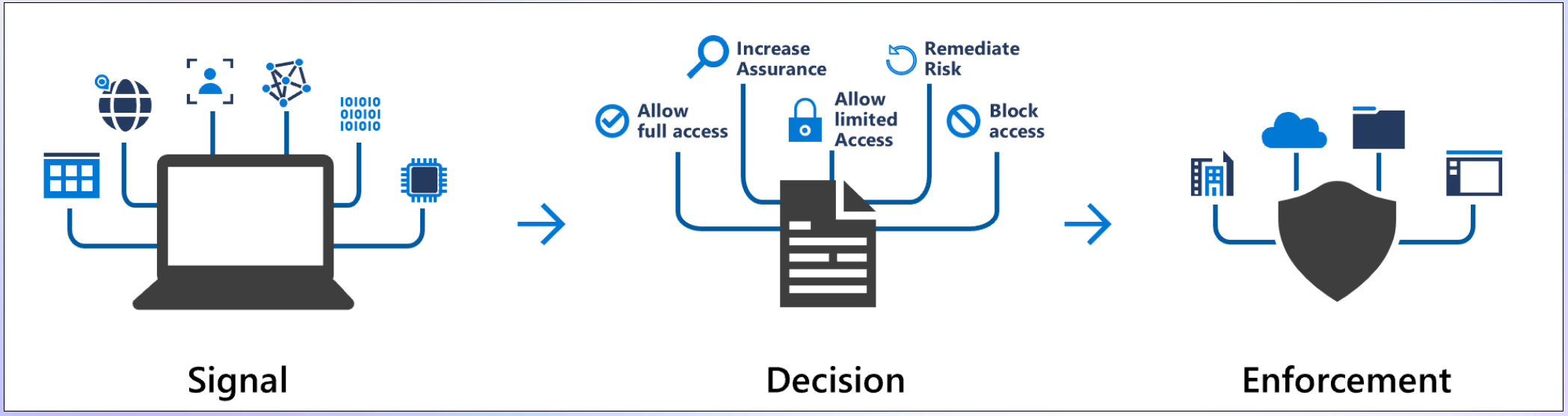
- **Microsoft Entra Audit log**
- **Microsoft Entra Sign-in log**
- **Azure Activity Log**
- **Office 365 Audit Log**
  - **SharePoint activity**
  - Exchange admin activity
  - Teams
- **Alerts** from Microsoft Defender for Cloud, Microsoft 365 Defender, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint and Microsoft Defender for Cloud Apps

Microsoft Entra – Conditional Access

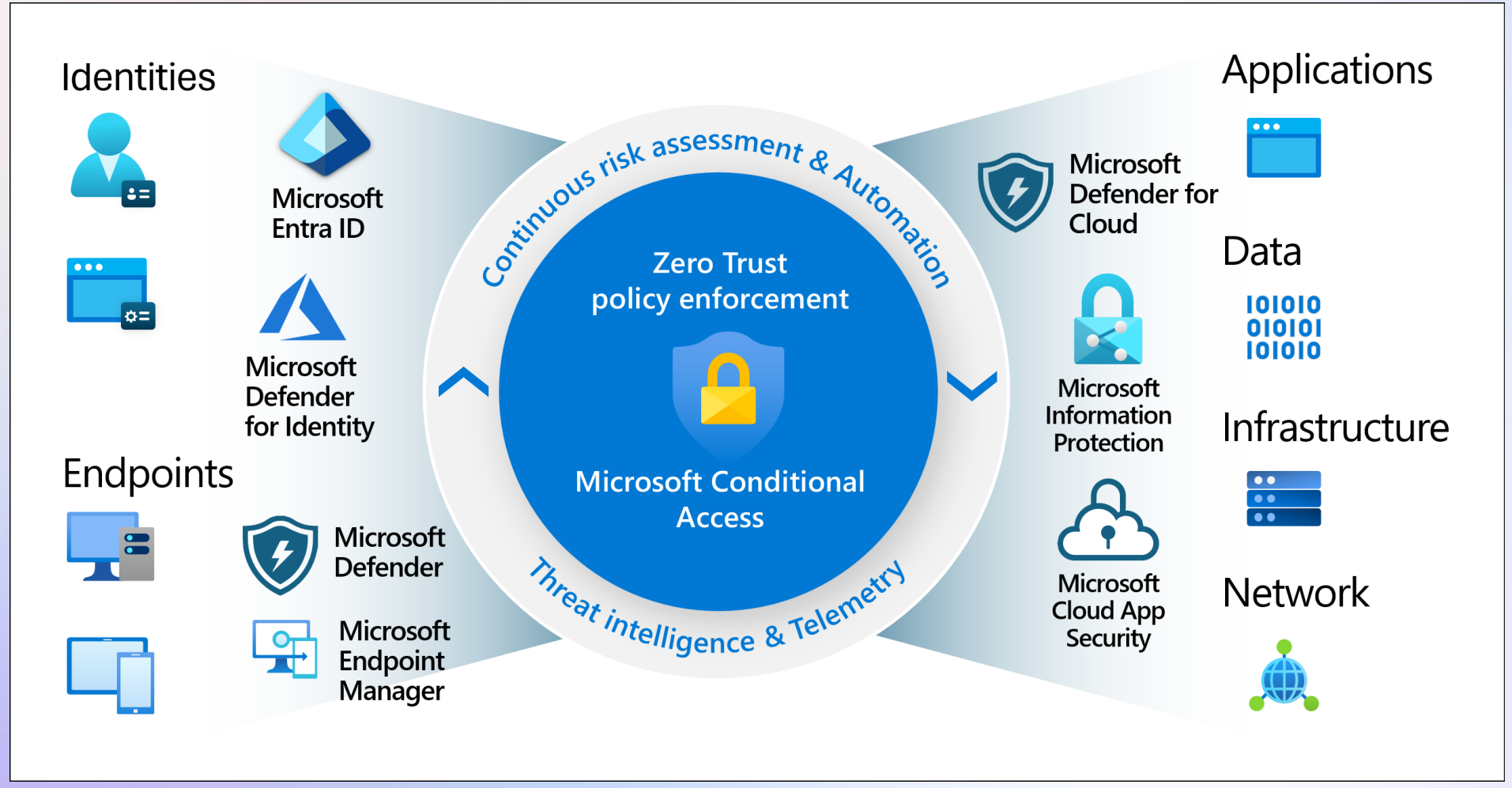
TD SYNNEX

Cos'è

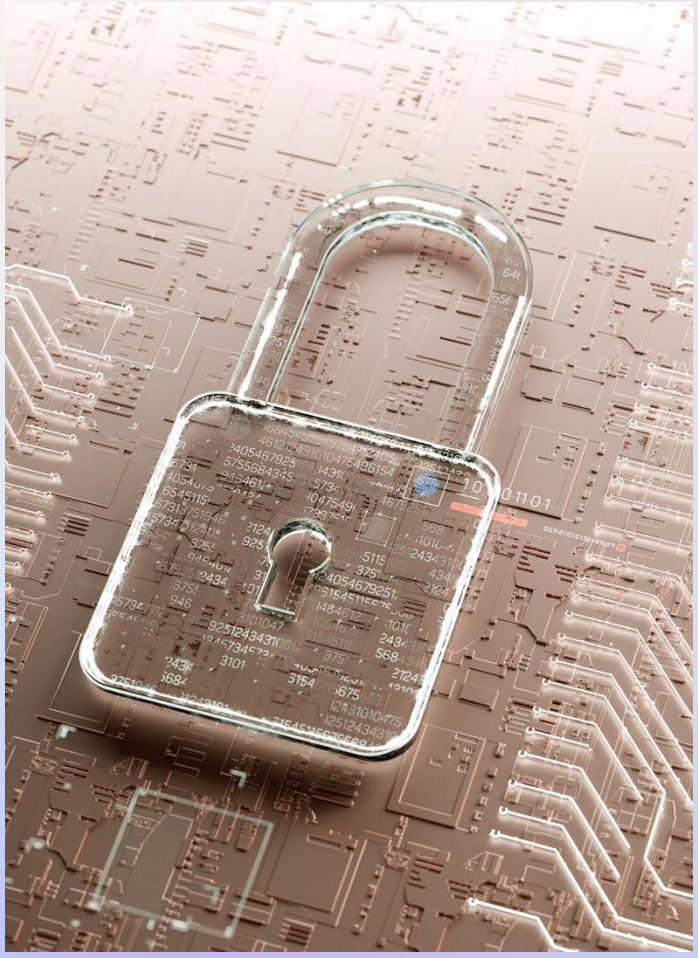
L'accesso condizionale di Microsoft Entra riunisce i segnali per prendere decisioni e imporre i criteri dell'organizzazione



Microsoft Entra – Conditional Access



Microsoft Entra – Conditional Access



Decisioni comuni:

- Blocca accesso
  - ➢ Decisione più restrittiva
- Concedere l'accesso
  - ➢ Decisione meno restrittiva, può comunque richiedere una o più delle opzioni seguenti:
    - ✓ Richiedere l'autenticazione a più fattori
    - ✓ Richiedere un livello di autenticazione
    - ✓ Richiedere che il dispositivo sia contrassegnato come conforme
    - ✓ Richiedere un dispositivo aggiunto a Microsoft Entra ibrido
    - ✓ Richiedi app client approvata
    - ✓ Richiedere criteri di protezione dell'app
    - ✓ Richiedere la modifica della password
    - ✓ Richiedere le condizioni per l'utilizzo

Microsoft Entra – Plan Comparison

Feature	Microsoft Entra ID Free - Security defaults (enabled for all users)	Microsoft Entra ID Free - Global Administrators only	Office 365	Microsoft Entra ID P1	Microsoft Entra ID P2
Protect Microsoft Entra tenant admin accounts with MFA	✅	✅ (*Microsoft Entra Global Administrator* accounts only)	✅	✅	✅
Mobile app as a second factor	✅	✅	✅	✅	✅
Phone call as a second factor			✅	✅	✅
SMS as a second factor		✅	✅	✅	✅
Admin control over verification methods		✅	✅	✅	✅
Fraud alert				✅	✅
MFA Reports				✅	✅
Custom greetings for phone calls				✅	✅
Custom caller ID for phone calls				✅	✅
Trusted IPs				✅	✅
Remember MFA for trusted devices		✅	✅	✅	✅
MFA for on-premises applications				✅	✅
Conditional Access				✅	✅
Risk-based Conditional Access					✅
Self-service password reset (SSPR)	✅	✅	✅	✅	✅
SSPR with writeback				✅	✅

Microsoft Entra – Microsoft Secure Future Initiative

TD SYNNEX

Secure by design

Security comes first when designing any product or service.

Secure by default

Security protections are enabled and enforced by default, require no extra effort, and aren't optional.

Secure operations

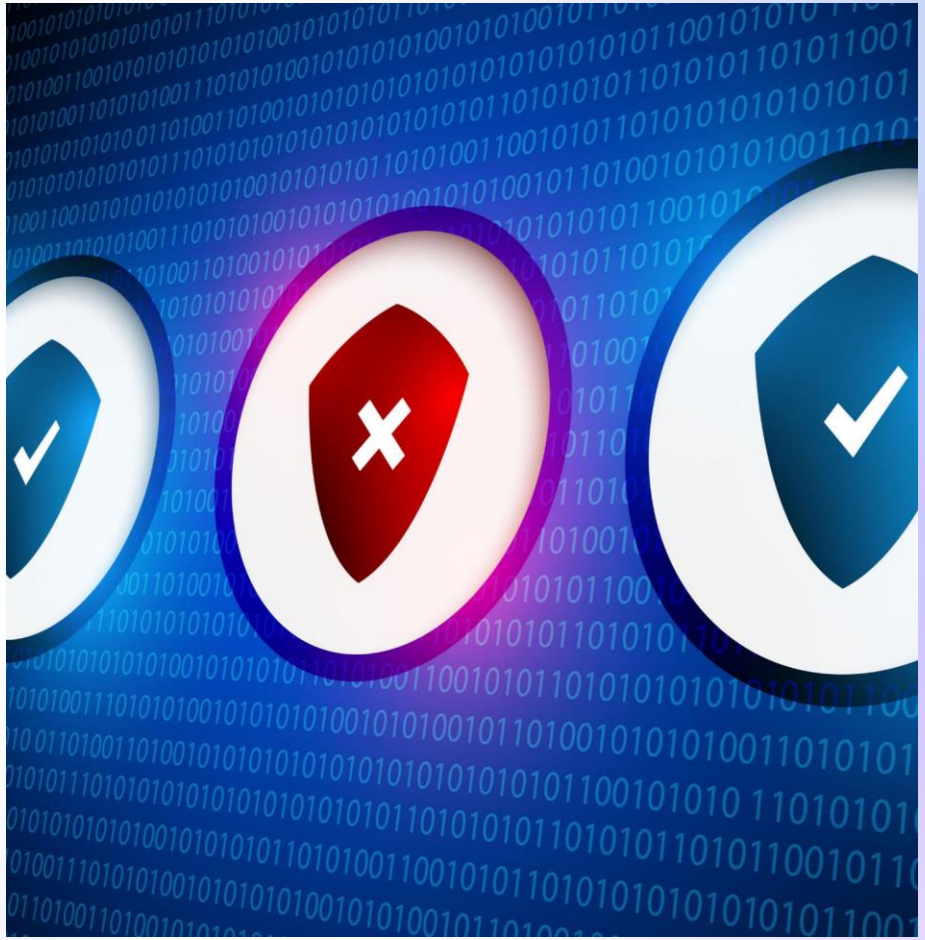
Security controls and monitoring will be continuously improved to meet current and future threats.

Microsoft Entra – Microsoft Secure Future Initiative

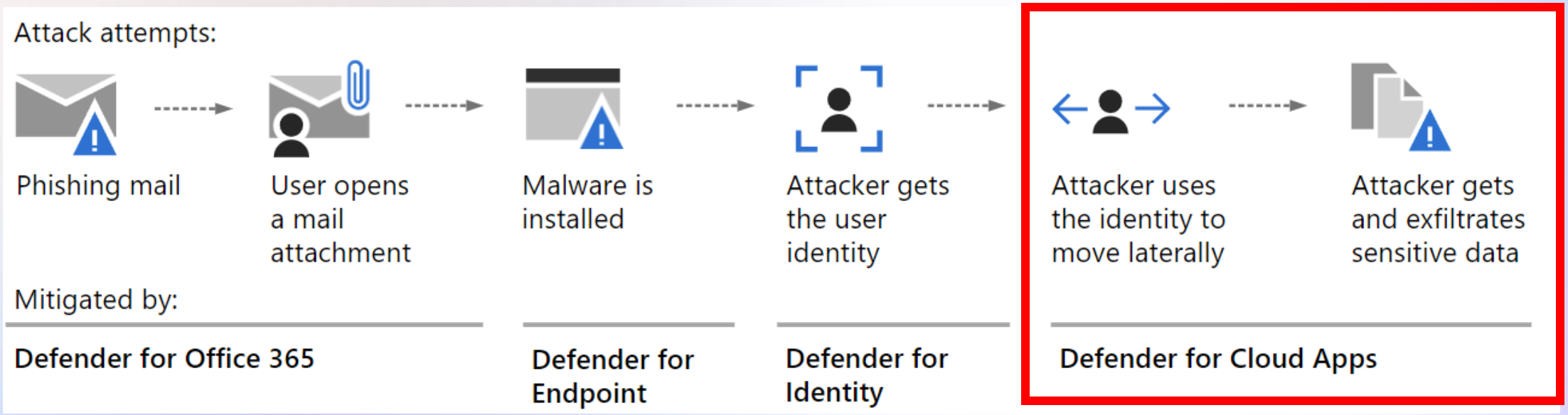
TD SYNNEX

Fasi temporali

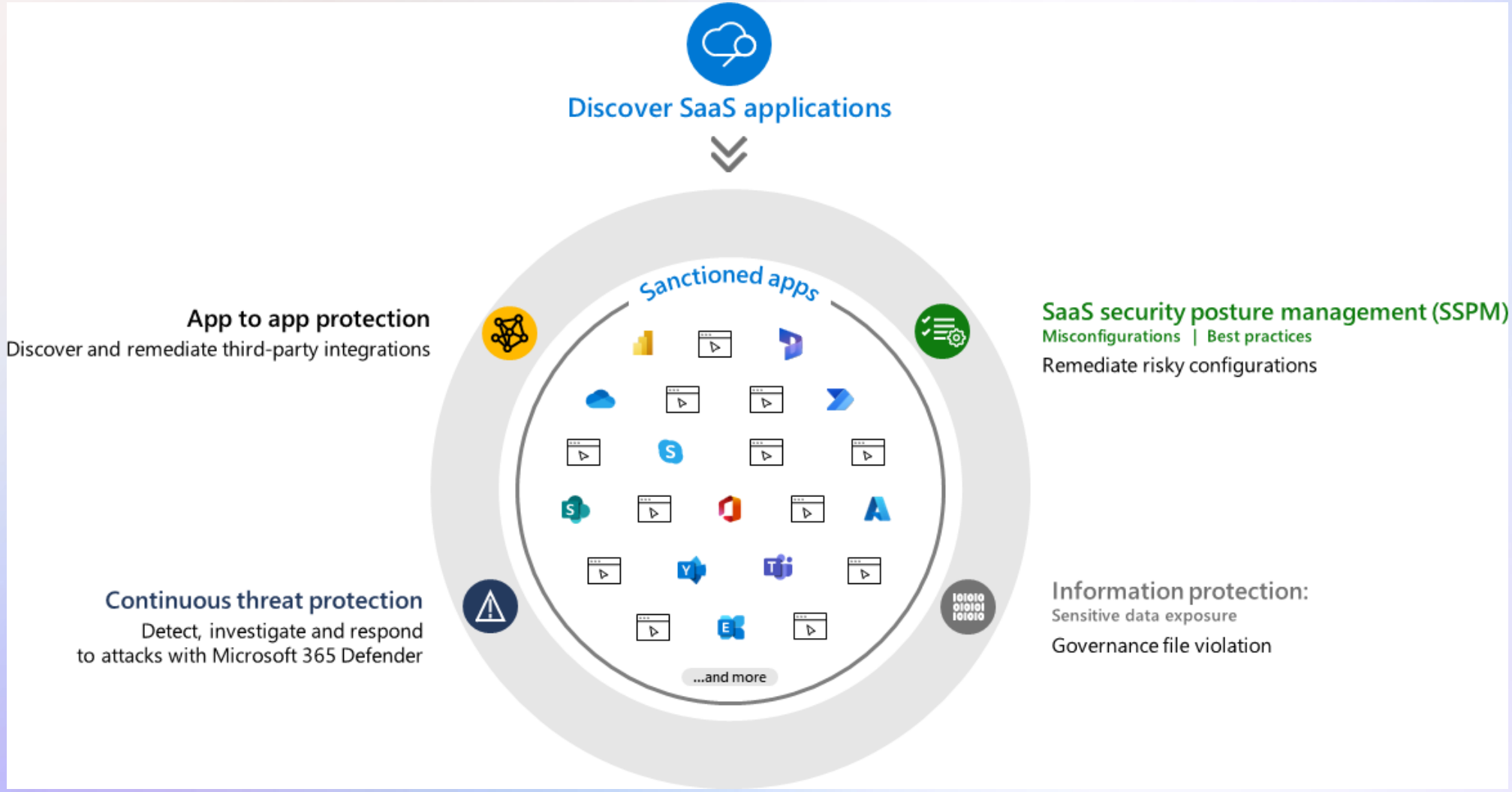
1. Security Default attivi di default nei nuovi tenant
2. Security Default forzati
3. Policy di Accesso Condizionale genarate da Microsoft
4. Obbligo di MFA per accesso ai portali Azure/Entra/Intune
5. Disattivazione delle sottoscrizioni di Azure non utilizzate
6. Obbligo di MFA per accesso ad Azure tramite Powershell/CLI/mobile app/Infrastructure as Code tools (ARM, Bicep, Terraform,…)



Microsoft Entra – Defender for Cloud Apps



Microsoft Entra – Defender for Cloud Apps



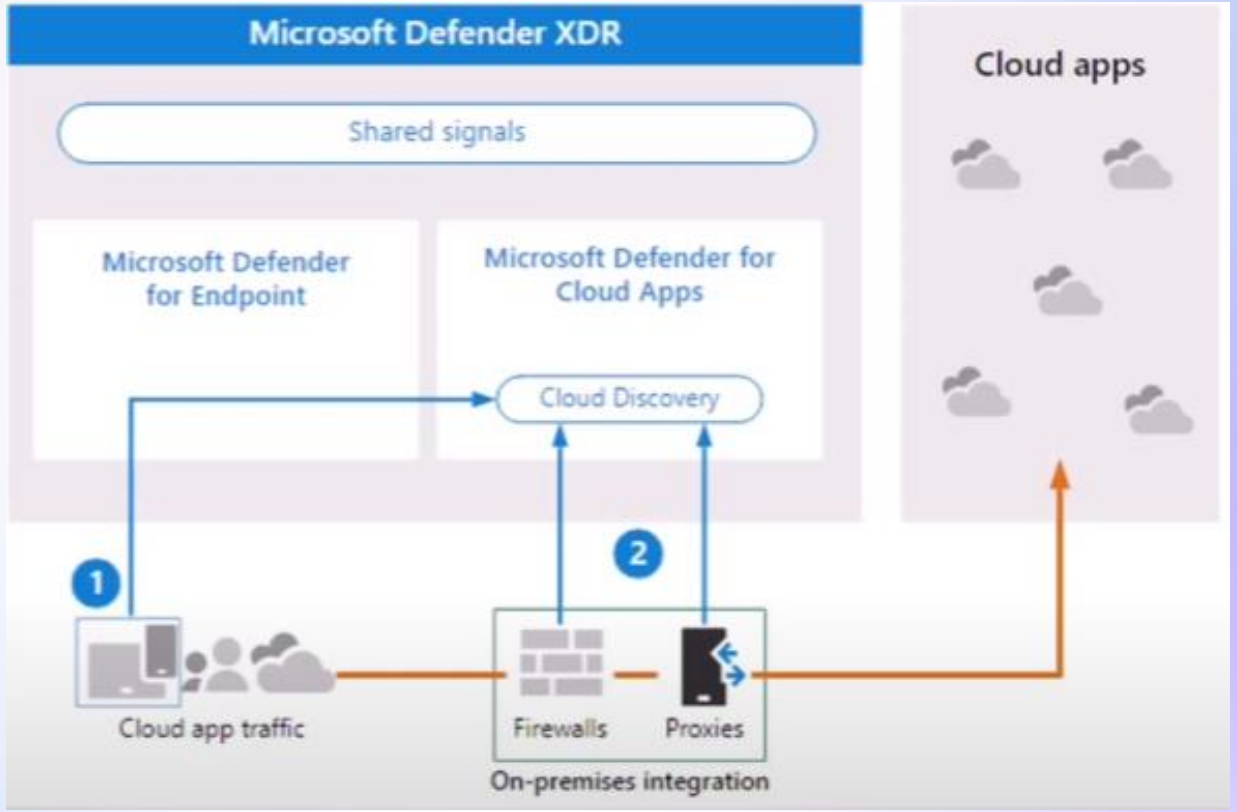
Microsoft Entra – Defender for Cloud Apps

TD SYNNEX

Discover SaaS Applications

Cloud Discovery analizza i log del traffico rispetto al catalogo delle app di Microsoft Defender per il cloud di oltre 31.000 app cloud. Le app vengono classificate e classificate in base a più di 90 fattori di rischio per offrire visibilità continuativa sull'uso del cloud, shadow IT e sul rischio che Shadow IT pone nell'organizzazione.

Dopo aver esaminato l'elenco delle app individuate nell'ambiente in uso, è possibile proteggere l'ambiente approvando le app sicure (approvate) o vietando le app indesiderate (non approvate) nei modi seguenti.

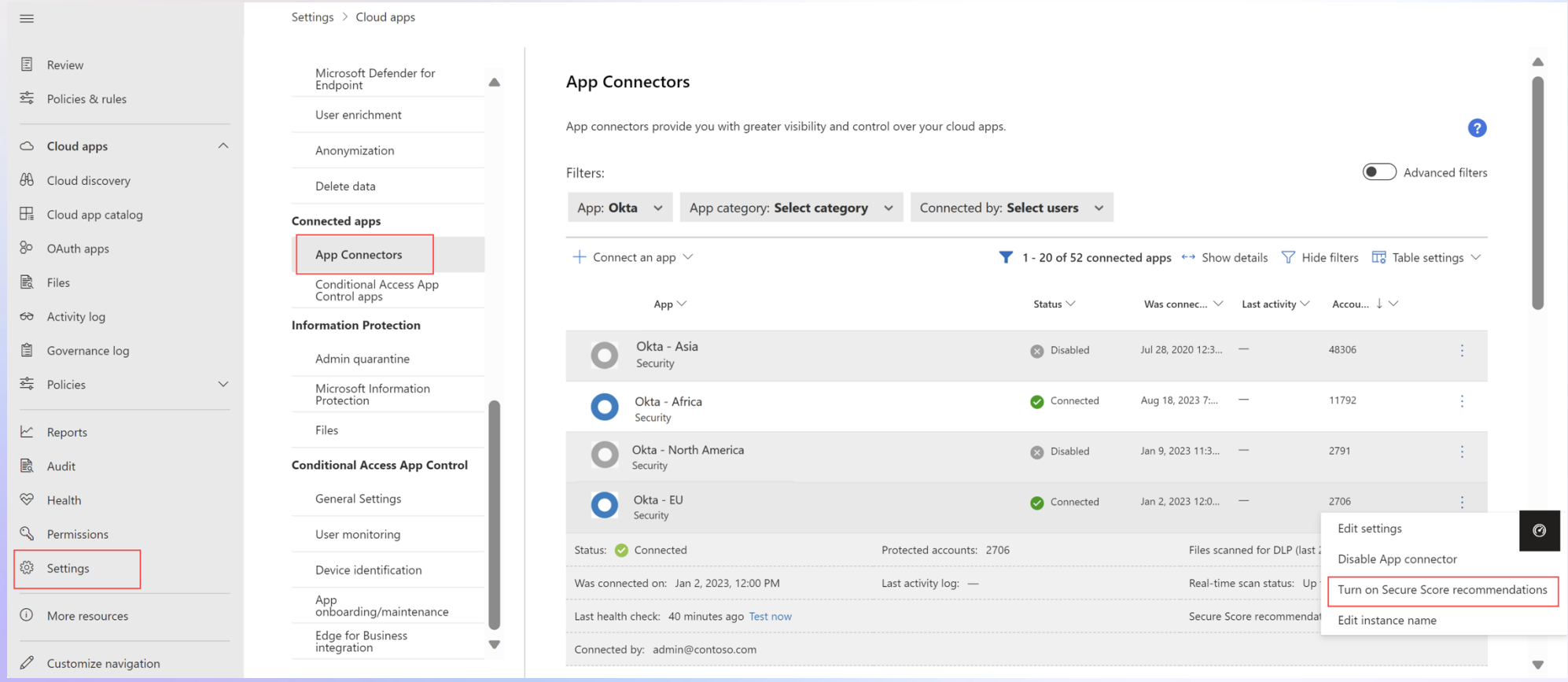


Microsoft Entra – Defender for Cloud Apps

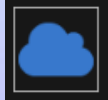
TD SYNNEX

SaaS security posture (SSPM)

Gli ambienti dell'applicazione SaaS possono essere configurati in un comportamento rischioso. Microsoft Defender per il cloud App offre valutazioni della configurazione della sicurezza dei rischi per le applicazioni SaaS per evitare possibili rischi. Queste raccomandazioni vengono visualizzate tramite Microsoft Secure Score dopo aver creato un connettore per un'applicazione



Microsoft Entra – Defender for Cloud Apps

Icona tipo di criterio	Tipo di criterio	Categoria	Usare
	Criteri attività	Rilevamento di minacce	I criteri di attività consentono di applicare un'ampia gamma di processi automatizzati usando le API del provider di app. Questi criteri consentono di monitorare attività specifiche eseguite da vari utenti o di seguire frequenze inaspettatamente elevate di un determinato tipo di attività. Ulteriori informazioni
	Criteri di rilevamento anomalie	Rilevamento di minacce	I criteri di rilevamento anomalie consentono di rilevare attività insolite nel cloud. Il rilevamento si basa sui fattori di rischio impostati per avvisare l'utente quando si verifica un evento diverso dalla baseline dell'organizzazione o dall'attività regolare dell'utente. Ulteriori informazioni
	Criteri per le applicazioni OAuth	Rilevamento di minacce	I criteri delle app OAuth consentono di analizzare le autorizzazioni richieste da ogni app OAuth e approvarla o revocarla automaticamente. Si tratta di criteri predefiniti inclusi in app Defender per il cloud e che non possono essere creati. Ulteriori informazioni
	Criteri di rilevamento malware	Rilevamento di minacce	I criteri di rilevamento malware consentono di identificare i file dannosi nell'archiviazione cloud e di approvarlo o revocarlo automaticamente. Si tratta di un criterio predefinito fornito con app Defender per il cloud e non può essere creato. Ulteriori informazioni
	Criteri file	Protezione delle informazioni	I criteri file consentono di analizzare le app cloud per identificare file o tipi di file specifici (condivisi, condivisi con domini esterni) e dati (informazioni proprietarie, informazioni personali, informazioni relative alle carte di credito e altri tipi di dati). Consentono anche di applicare azioni di governance ai file (le azioni di governance sono specifiche delle app cloud). Ulteriori informazioni
	Criteri di accesso	Accesso condizionale	I criteri di accesso consentono il monitoraggio in tempo reale e il controllo degli accessi degli utenti alle app cloud. Ulteriori informazioni
	Criteri della sessione	Accesso condizionale	I criteri di accesso consentono il monitoraggio in tempo reale e il controllo delle attività degli utenti alle app cloud. Ulteriori informazioni
	Criteri di individuazione delle app	Ombreggiatura IT	Come già menzionato, i criteri di individuazione delle app consentono di impostare avvisi di notifica quando vengono rilevate nuove app all'interno dell'organizzazione. Ulteriori informazioni
	Criteri di rilevamento anomalie di Cloud Discovery	Ombreggiatura IT	I criteri di rilevamento anomalie di Cloud Discovery esaminano i log usati per l'individuazione delle app cloud e la ricerca di occorrenze insolite. Ad esempio, quando un utente che non ha mai usato Dropbox prima carica improvvisamente 600 GB in Dropbox o quando sono presenti molte più transazioni del solito in una determinata app. Ulteriori informazioni

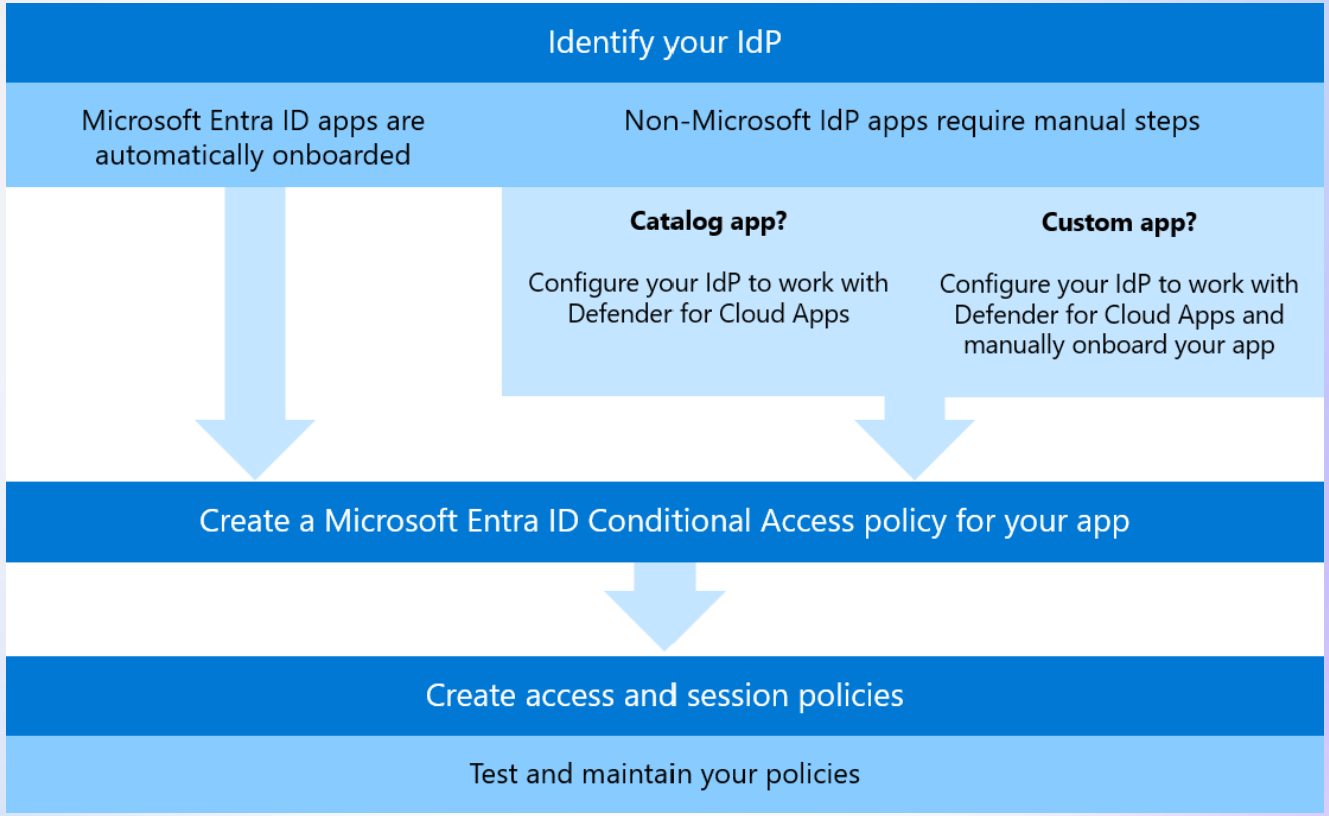
Microsoft Entra – Defender for Cloud Apps

TD SYNNEX

Conditional Access App Control

Non è sufficiente sapere cosa è successo nell'ambiente cloud dopo il fatto. È necessario arrestare le violazioni e le perdite in tempo reale. È anche necessario impedire ai dipendenti di mettere intenzionalmente o accidentalmente a rischio i dati e l'organizzazione.

Si vuole supportare gli utenti dell'organizzazione mentre usano le migliori app cloud disponibili e portare i propri dispositivi per funzionare. Tuttavia, sono necessari anche strumenti per proteggere l'organizzazione da perdite di dati e furti in tempo reale. Microsoft Defender per il cloud App si integra con qualsiasi provider di identità (IdP) per offrire questa protezione con criteri di accesso e sessione.



azuremeetup VENETO

meetup

Microsoft

25 ottobre 2024

Davide Cenedese
System Architect

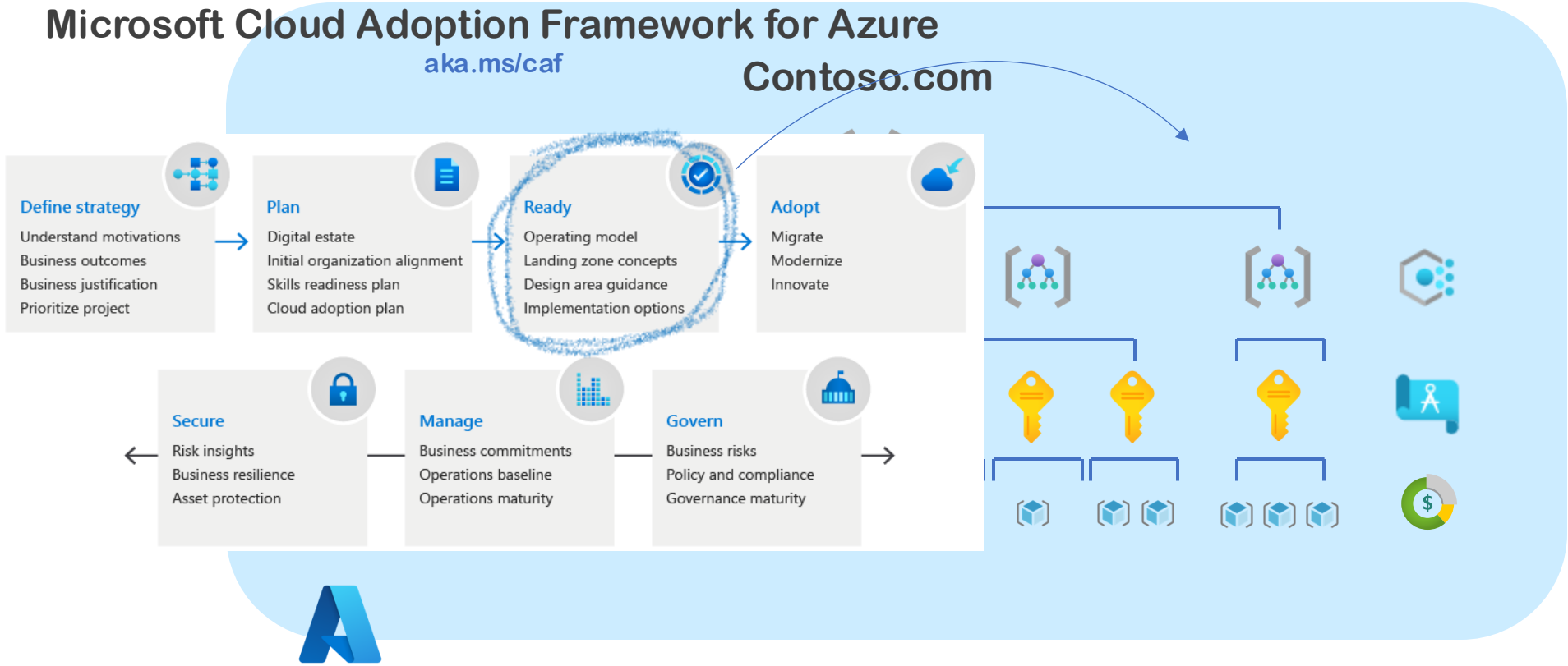
Governance delle risorse Azure

Linee guida per mitigare i rischi e favorire la produttività

- Standard e procedure aziendali e normative
- Sicurezza
- Budget
- Efficienza operativa e continuità di servizio

Microsoft Cloud Adoption Framework for Azure

aka.ms/caf



Soluzioni di governance

- Compliant
- Monitorato
- Sicuro

Gestione dei costi

Stabilità della soluzione

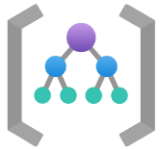
azuremeetup VENETO

meetup

Microsoft

TD SYNNEX

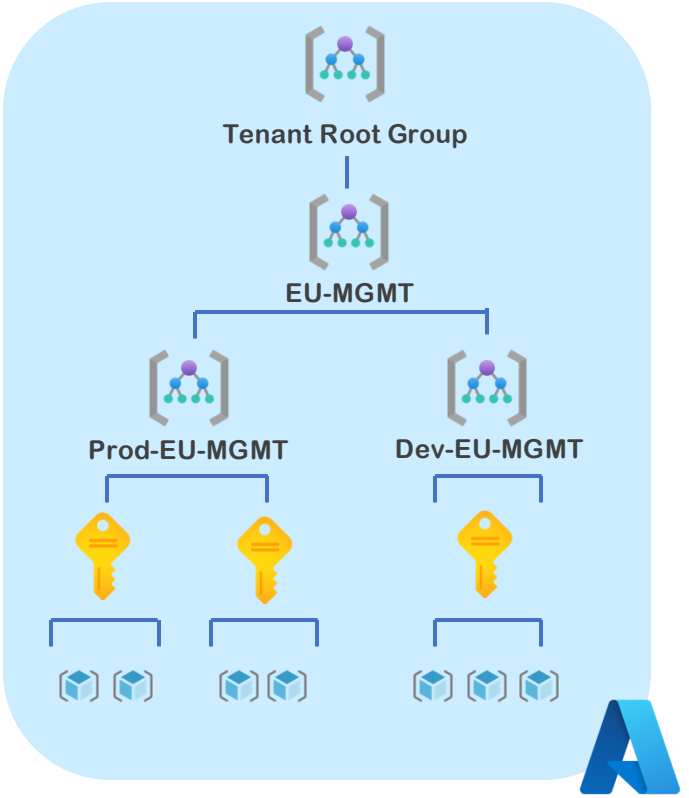
skybackbone engenio



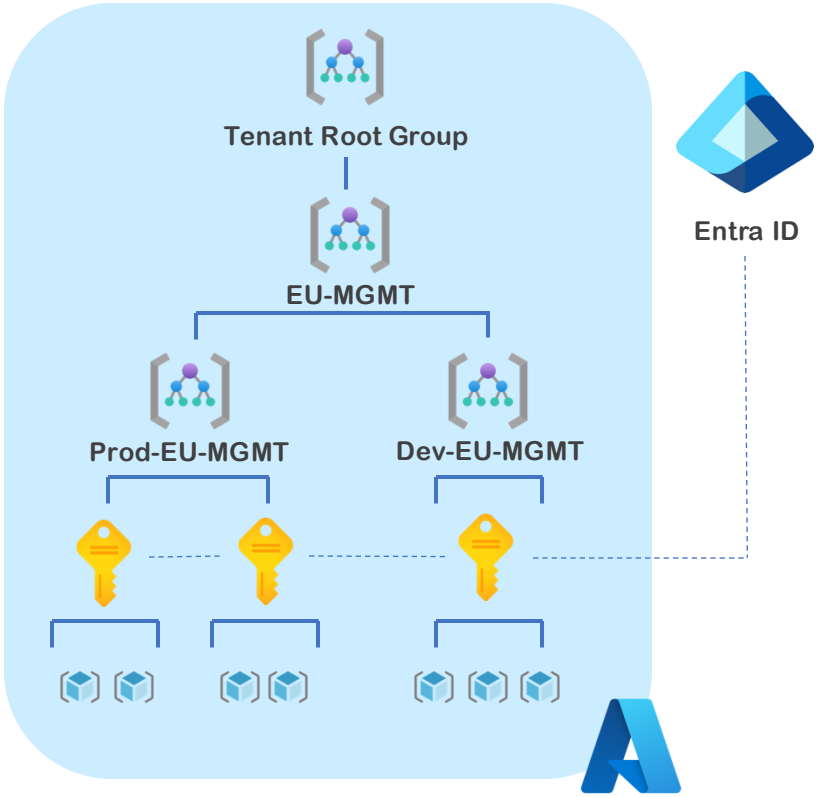
Management groups

Subscriptions

Resource groups



- Role-based Access Control (RBAC)
- Attribute-based Access Control (ABAC)
- Resource Locks
  - Read-only
  - Do not delete
- Tags



Azure Policy

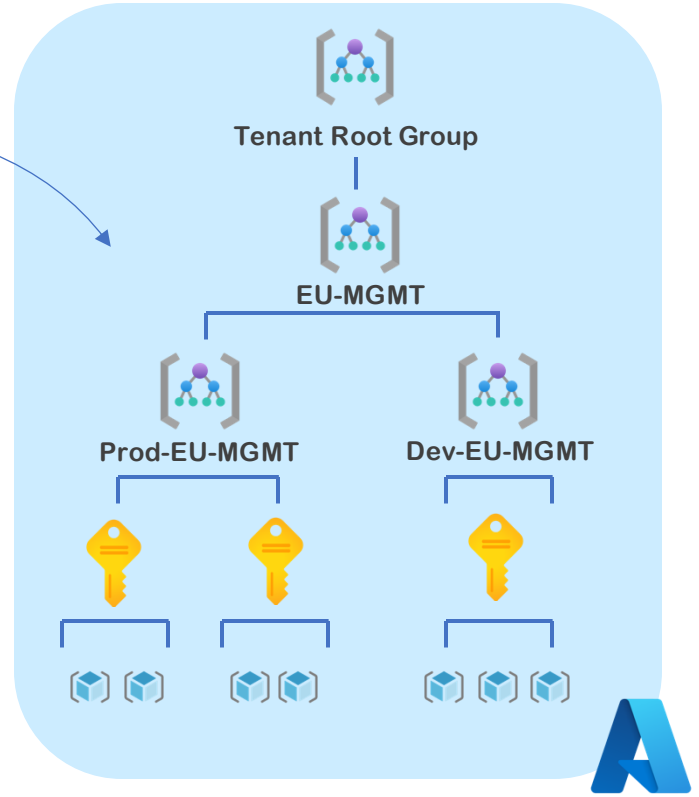
Regole IF - THEN

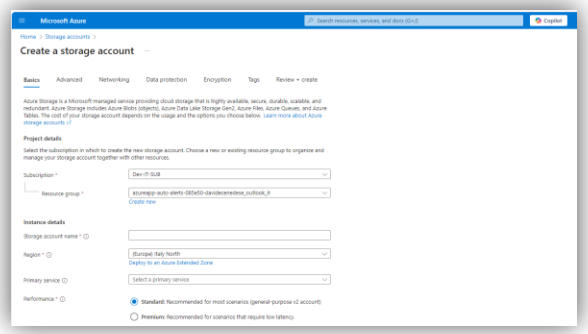
Operazioni consentite e negate

Forzare la compliance

Audit

Scope





Azure portal

```
davide [ ~ ]$ az storage account create
-n mystorageaccount -g MyResourceGroup
-l westus --sku Standard_LRS
```

Azure CLI

```
PS /home/davide> New-AzStorageAccount
-ResourceGroupName MyResourceGroup
-Name mystorageaccount -Location westus
-Location westus -SkuName Standard_GRS
-MinimumTlsVersion TLS1_2
```

Azure PowerShell

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.1",
  "parameters": {
    "StorageAccountName": {
      "type": "string",
      "metadata": {
        "description": "The name of the Azure Storage Account where the templates are stored."
      }
    },
    "ContainerName": {
      "type": "string",
      "metadata": {
        "description": "The Container inside the Storage Account."
      }
    },
    "SasToken": {
      "type": "string",
      "metadata": {
        "description": "The Shared Access Signature for the Storage Account."
      }
    }
  },
```

ARM templates

```
@minLength(3)
@maxLength(11)
param storagePrefix string

@allowed([
  'Standard_LRS'
  'Standard_GRS'
  'Standard_RAGRS'
  'Standard_ZRS'
  'Premium_LRS'
  'Premium_ZRS'
  'Standard_GZRS'
  'Standard_RAGZRS'
])
param storageSKU string = 'Standard_LRS'

param location string
```

Bicep templates

| Infrastructure as Code |

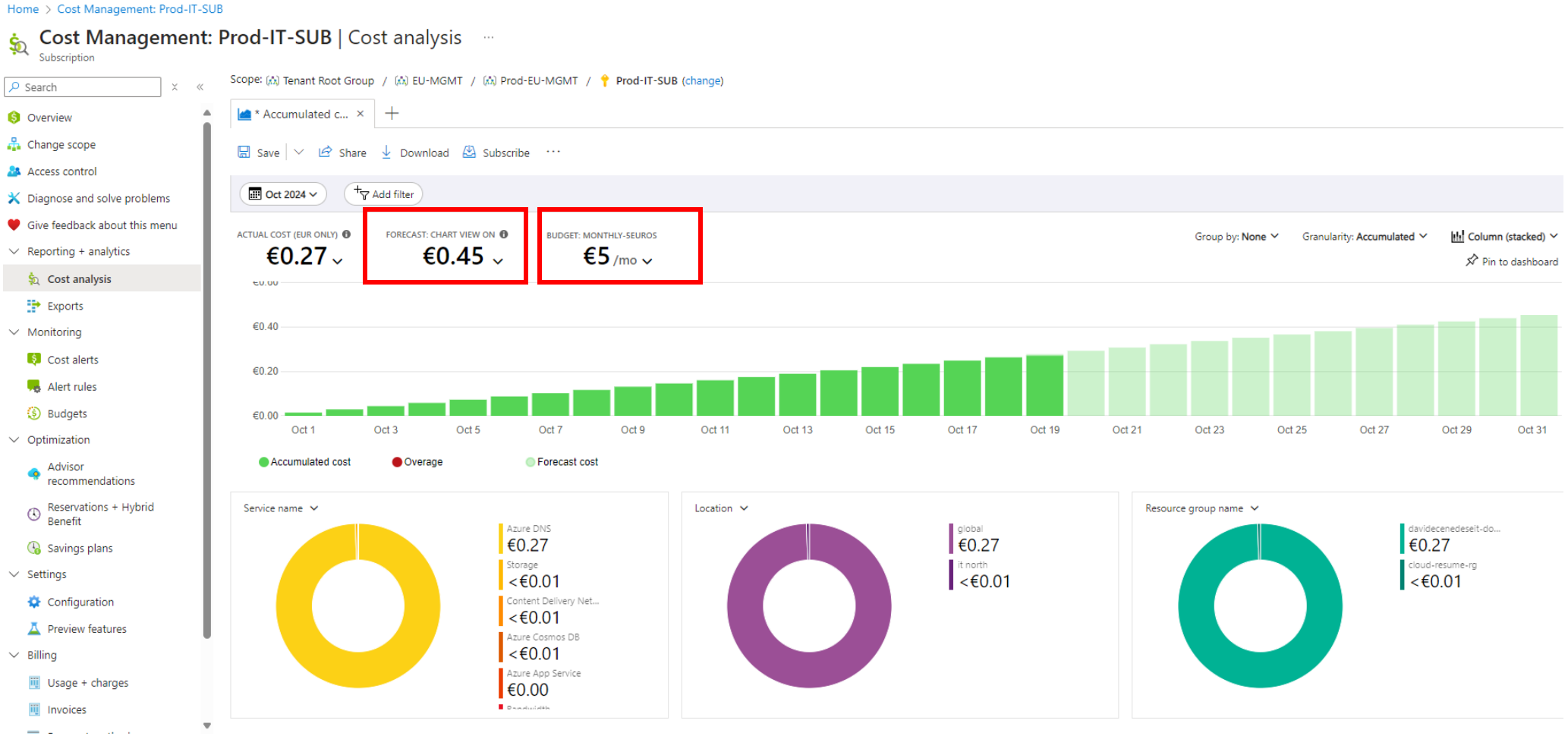
Template Specs

- Template ARM o Bicep
- Versioning
- Access control

Deployment stacks

Collezione di risorse gestite

- Deny assignments
- Gestione via CLI o PS



| Cost Management |

meetup Microsoft

TD SYNNEX skybackbone engenio

thank you