



#GlobalAzureTorino



TORINO

# Workloads are ready for Take-Off: Secure your migration journey with Azure Migrate

• Luca Torresi  
Zeno Testoni



INTR3

TD SYNNEX

PA EXPERTISE  
RETELIT GROUP

# Luca Torresi

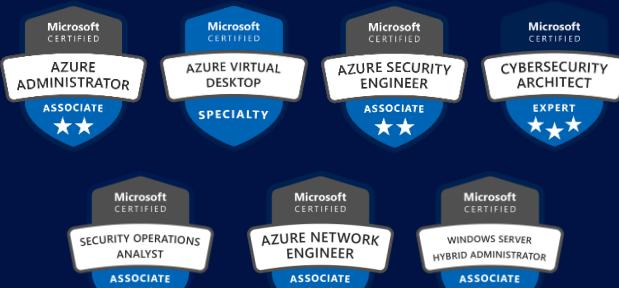
- ICT Consultant da 9 anni
- Cloud Engineer @ SoftJam Spa
- Mi occupo di: Microsoft Azure, Microsoft 365 e Security
- Contatti:



Linkedin: <https://www.linkedin.com/in/luca-torresi-391b71121>

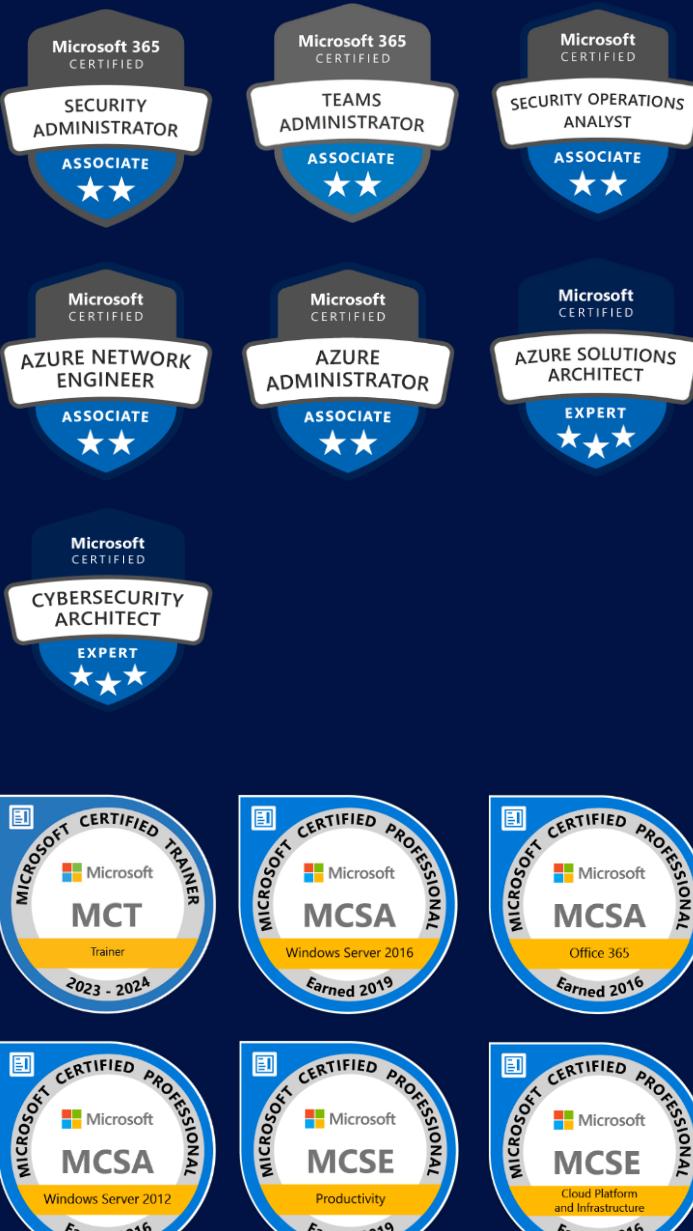


YouTube: <https://www.youtube.com/@LucaTorresi>



# Zeno Testoni

MS35 Security  
Competence Lead @ Porini



[www.linkedin.com/in/zenotestoni](https://www.linkedin.com/in/zenotestoni)  
zeno.testoni@porini.it



# Agenda

- I prerequisiti della migrazione verso Azure
- Azure Migrate, il servizio e le sue feature
- Sicurezza dei Workload in Azure
- Demo



# I prerequisiti della migrazione verso Azure

# Prima di migrare, fermati e pensa

- A** Conosco e/o ho documentato i processi del mio datacenter?
- A** Conosco e ho documentato le mie isole applicative?
- A** Il mio personale IT è stato adeguatamente formato?
- A** Il Business, quindi tutta l'azienda è d'accordo?
- A** Siamo disposti ad accettare dei nuovi paradigmi?
- A** Abbiamo stabilito un Budget per un POC?
- A** Una volta completata la migrazione, chi governerà Azure?
- A** Il mio Business può essere spostato completamente in Cloud o devo passare ad un modello Hybrid-Cloud?

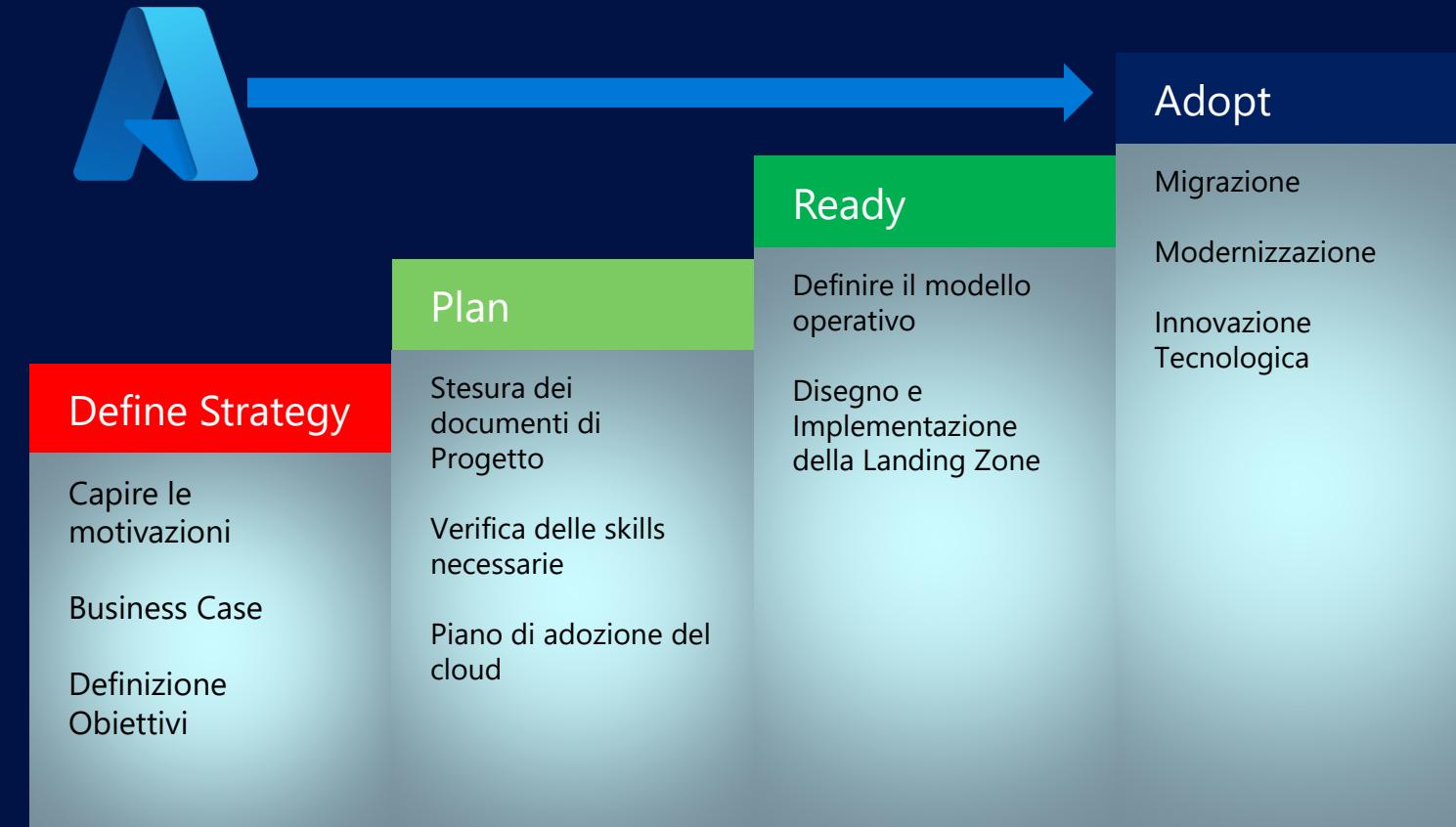


# Tutti i piani funzionano...

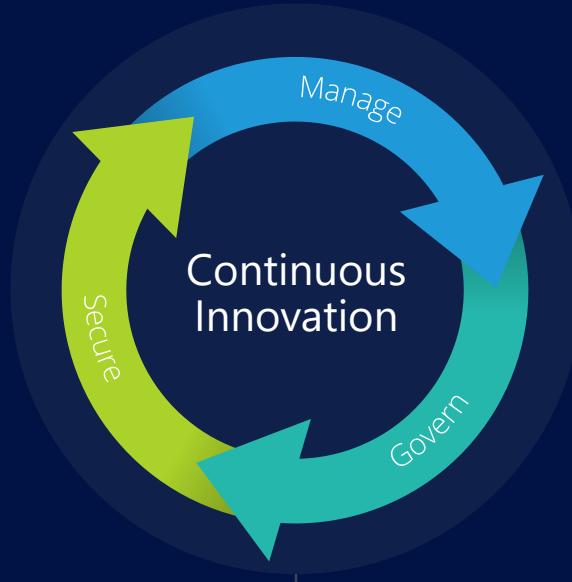


## Fino al primo assalto

# Cloud Adoption Framework



# Cloud Adoption Framework



## Manage

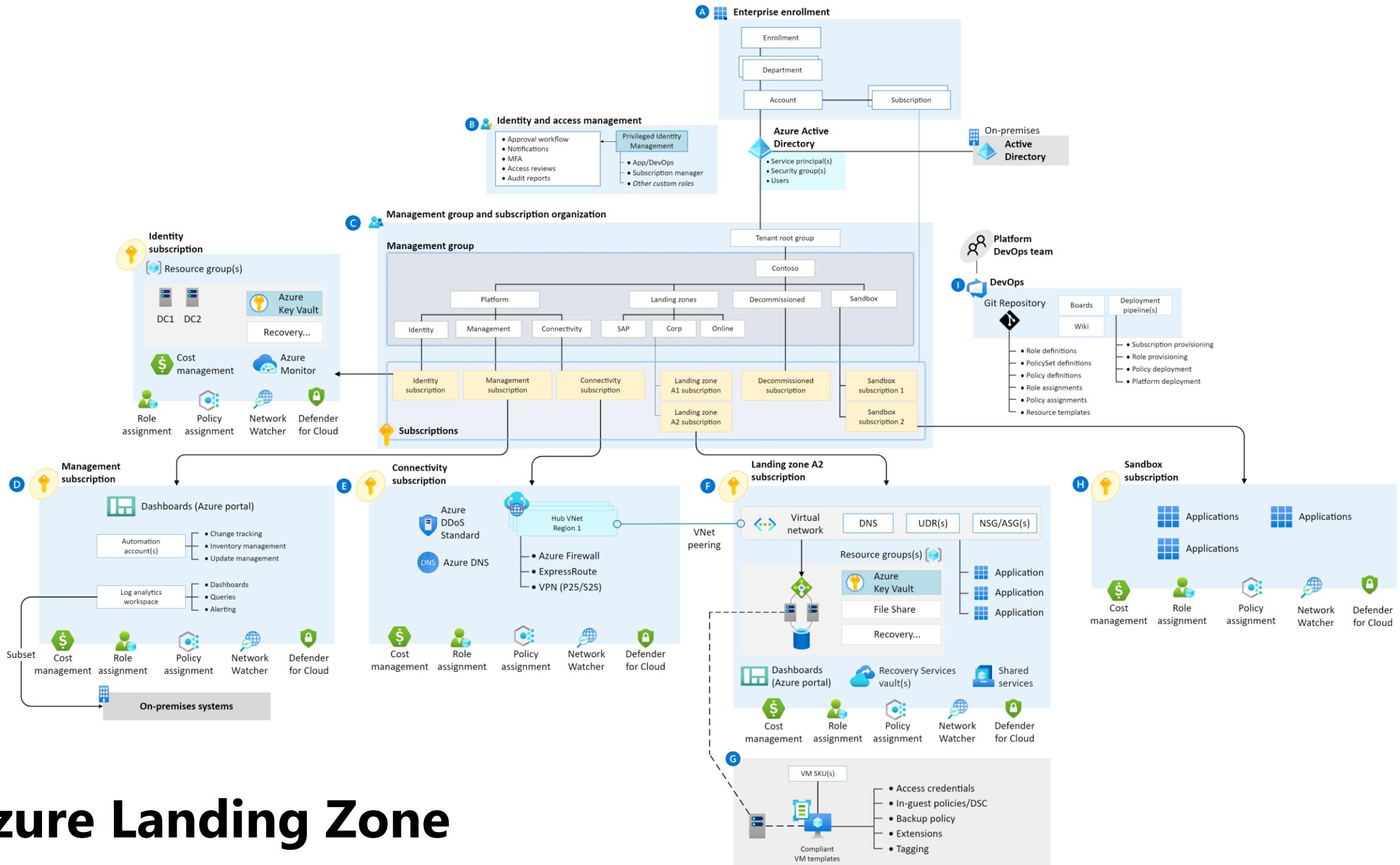
Gestione Operativa  
Definizione delle Baseline

## Govern

Gestione dei rischi  
Policy e Compliance

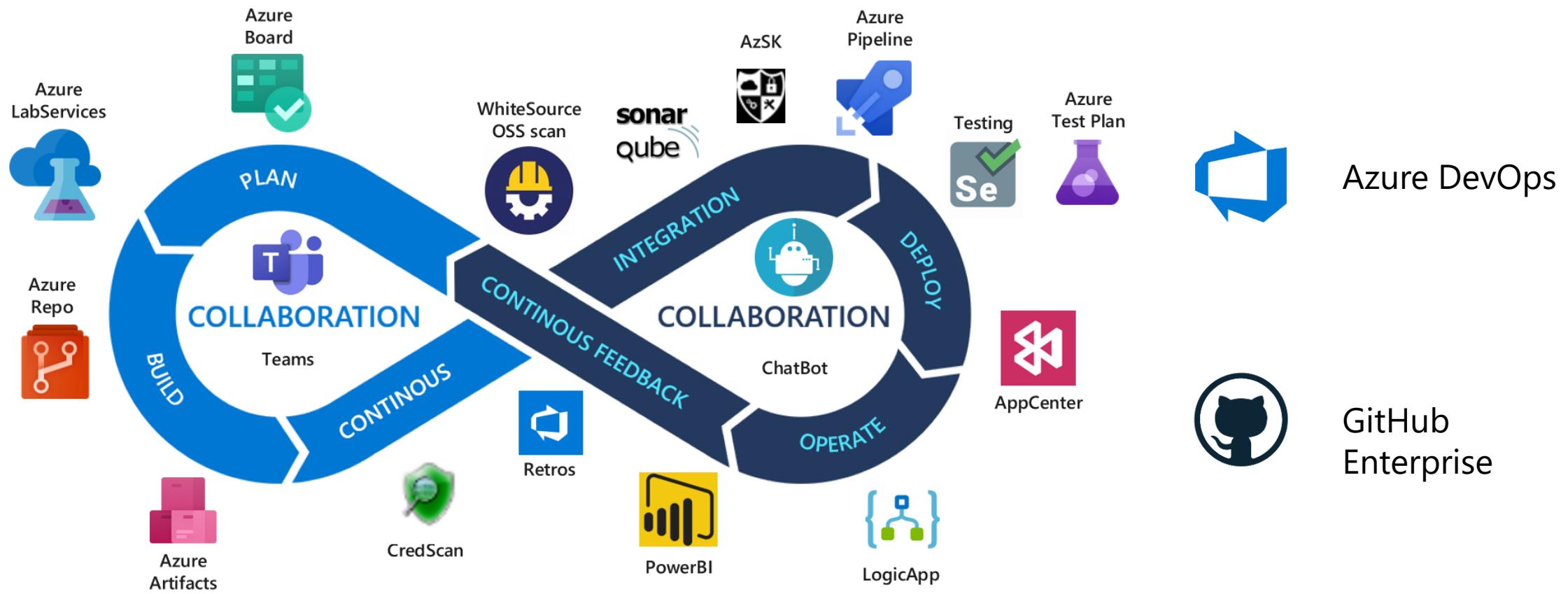
## Secure

Messa in sicurezza continua  
Protezione di tutte le risorse

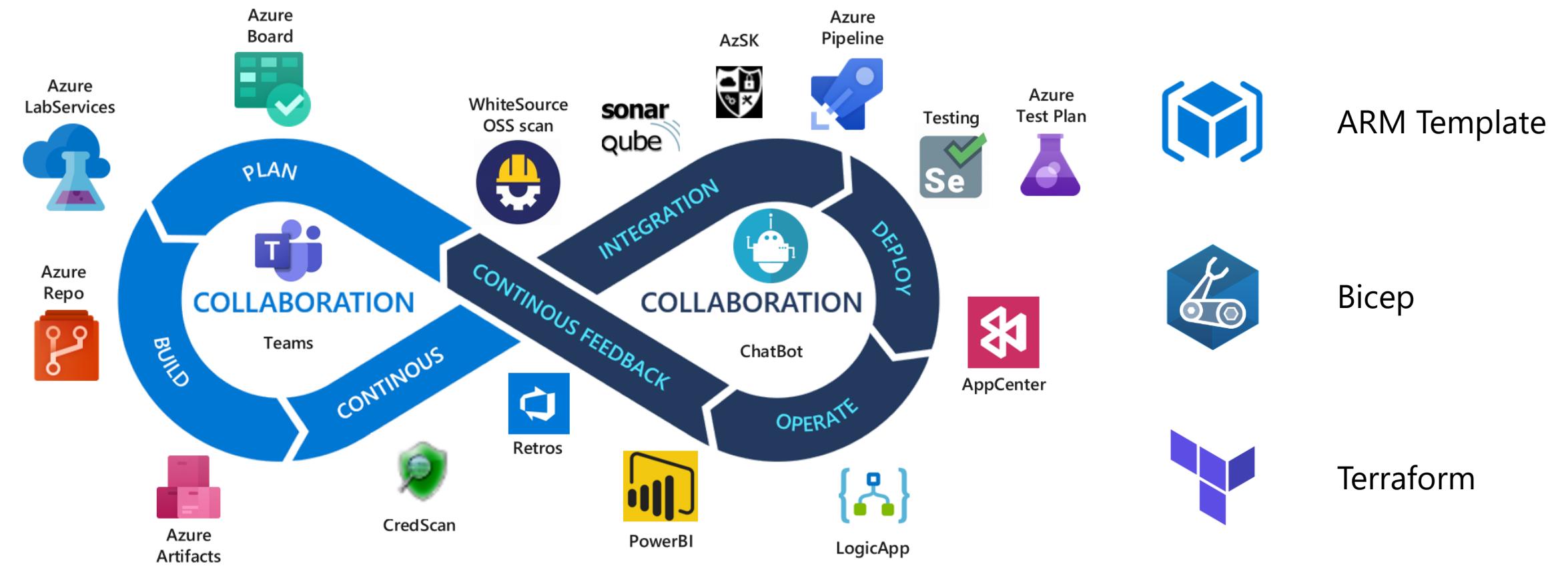


# Azure Landing Zone

# Dev(Sec)Ops



# Dev(Sec)Ops



# Azure Migrate, il servizio e le sue feature

# AZURE MIGRATE



## Azure Migrate – Hub for Datacenter Migration

Key migration scenarios



Integrated discovery,  
assessment, and  
migration capabilities



Azure Migrate

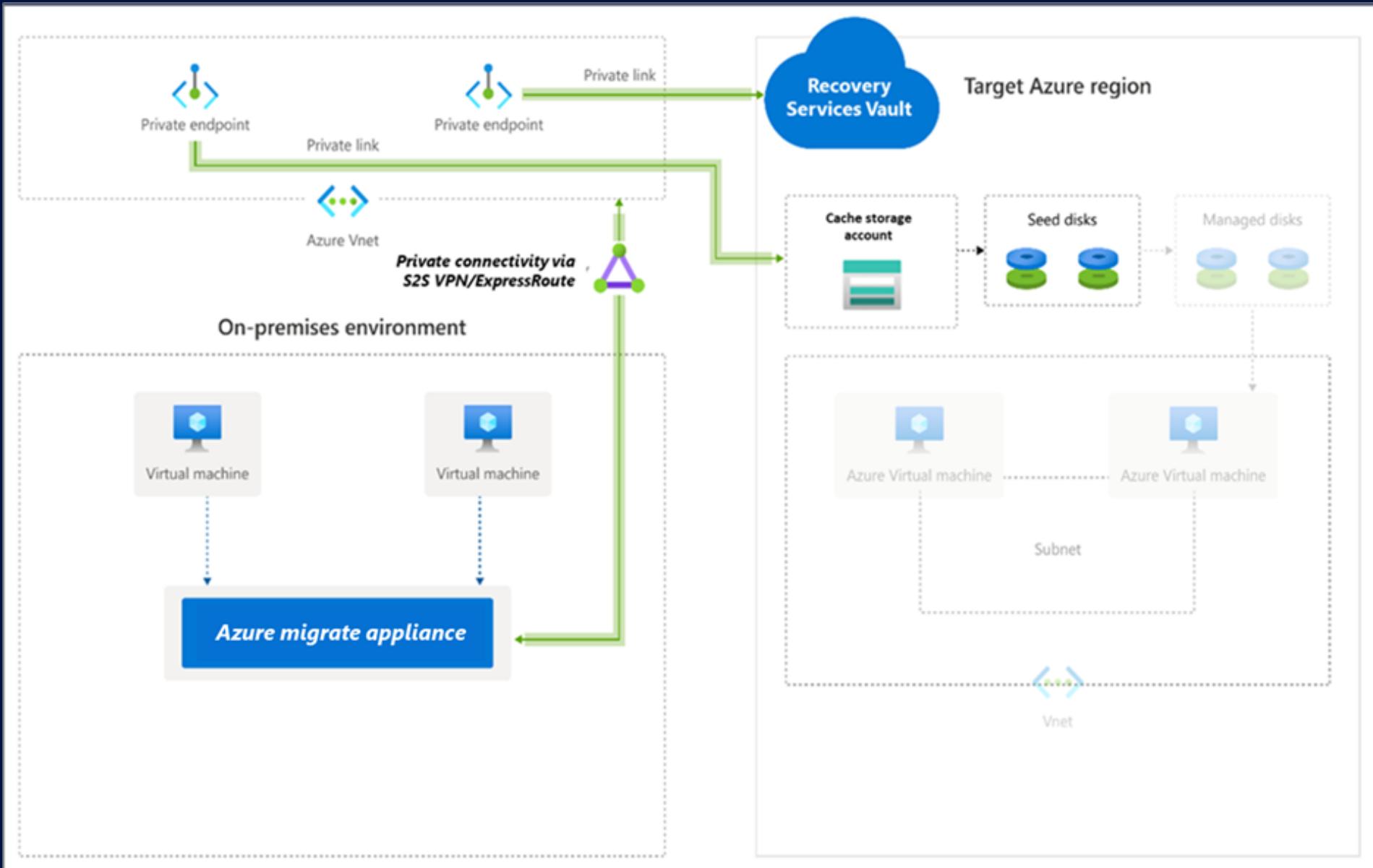
Centralized  
migration repository  
with end-to-end  
tracking



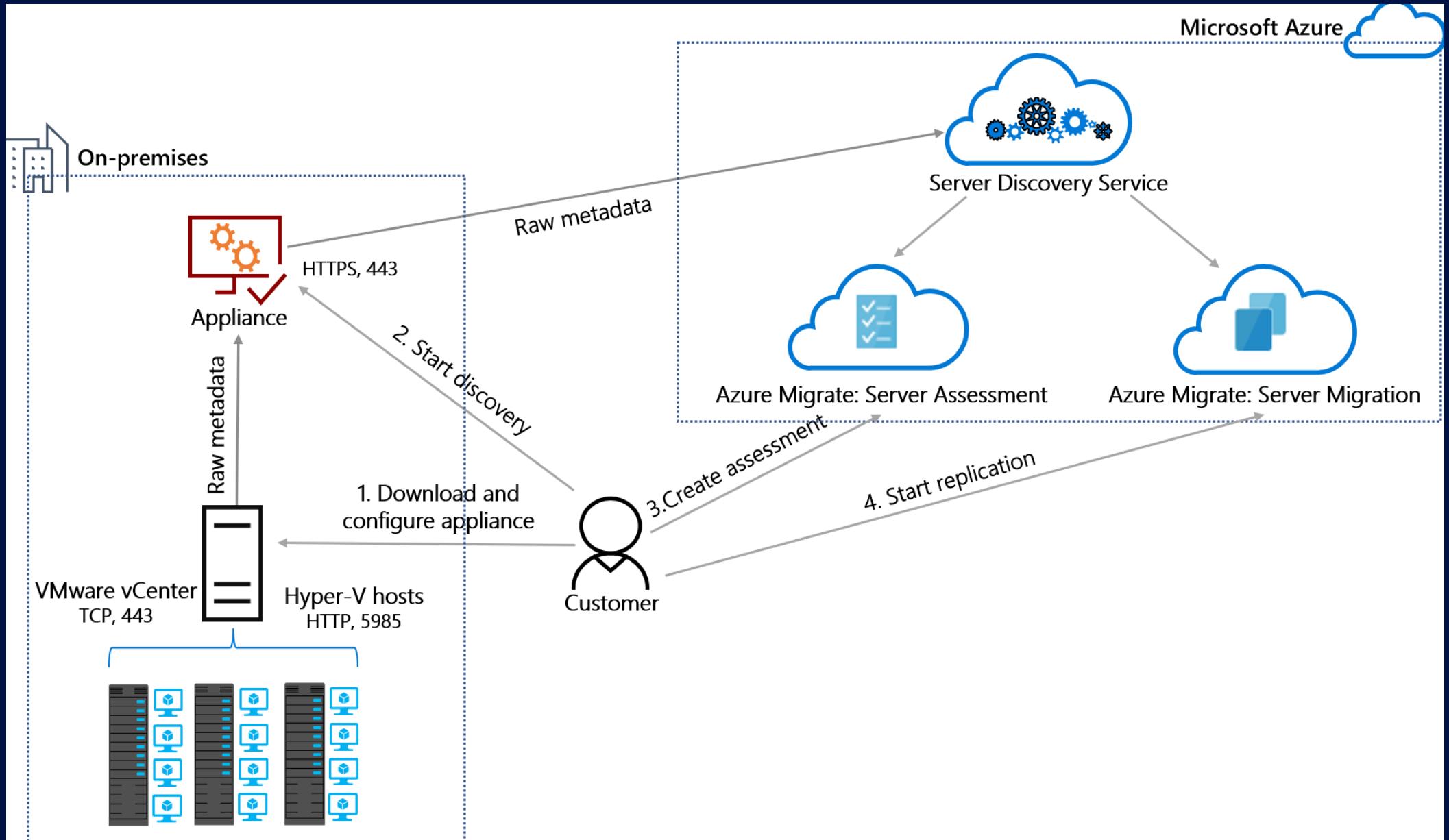
Powered by Microsoft and  
extensible with ISV partner  
tools



# Public or Private Link



# Discovery



# Assessment

ASSESS-01 ...  
Assessment

Search Settings Export assessment Recalculate assessment Refresh Delete assessment Feedback

Overview

The confidence rating of the assessment is low, ensure that you wait for at least a day after starting discovery, before creating performance-based assessments. Learn more.

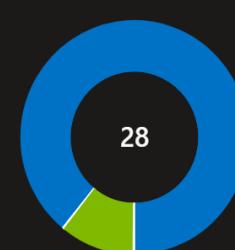
Assessment details

Azure readiness

Cost details

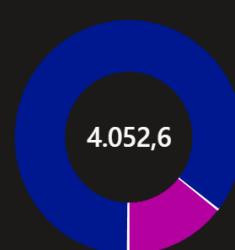
Essentials

**Azure readiness**



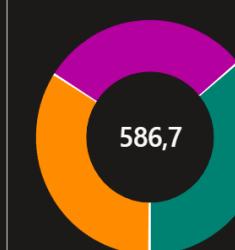
Status	Count
Ready for Azure	3
Ready with conditions	0
Not ready	0
Readiness unknown	25

**Monthly cost estimate (EUR)**



Category	Cost (EUR)
Compute	3465.94
Storage	586.7
Security	0

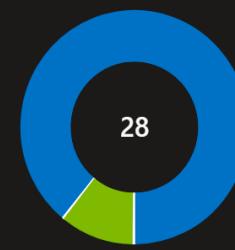
**Storage - Monthly cost estimate (EUR)**



Disk Type	Cost (EUR)
Standard HDD managed disks	0
Standard SSD managed disks	199.12
Premium managed disks	175.6
Ultra disks	211.98

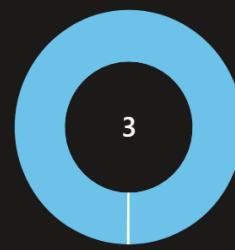
**Supportability**

**Distribution by OS License support status**



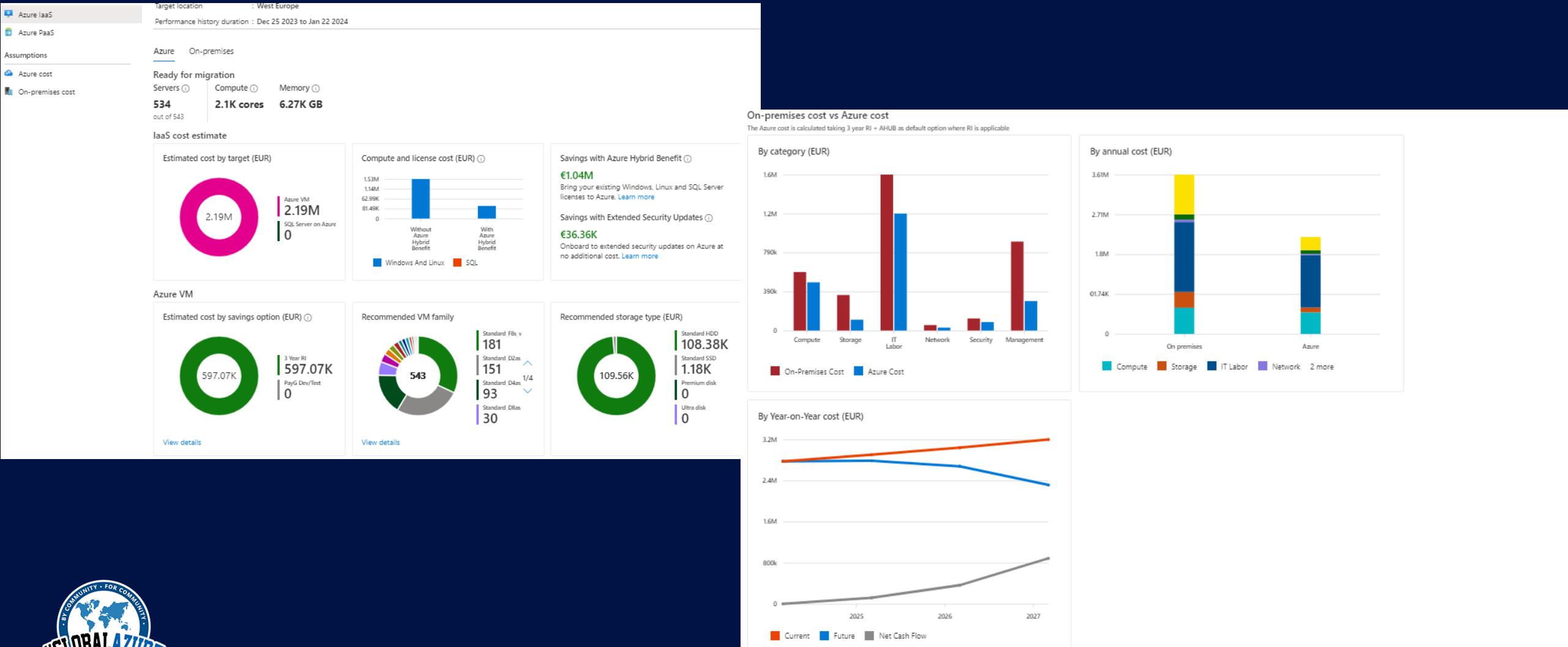
Status	Count
Mainstream	3
Extended	0
Out of support	0
Unknown	25

**Distribution by windows server version**



Version	Count
Windows Server 2022	3
Windows Server 2019	0
Windows Server 2016	0
Windows Server 2012	0
Windows Server 2008	0
Windows Server 2003	0
Windows Server NT	0
Other	0

# Creazione Business Case



# Server Discovery

La server Discovery consente di recuperare tutte le macchine virtuali, le loro applicazioni e i Workload che girano al proprio interno.

Home > Azure Migrate | Servers >

## Discovered servers

ContosoMigration

Create group Create assessment Replicate Export application inventory Refresh Columns

Agentless dependency analysis is now available in preview. Click here to request access. →

Azure Migrate appliance Import based

Appliance name VMware1 (VMware)

payroll

Name	IP address	Applications Discove...	Dependencies (Agen...	Cores	Memory
PayrollWeb04	10.150.10.189,2404:f8...	2 Applications	Requires agent ins...	4	1631
PayrollDB02	2404:f801:4800:25:58...	115 Applications	Requires agent ins...	2	2041
PayrollApp01	2404:f801:4800:25:a0...	17 Applications	Requires agent ins...	2	2041
PayrollWeb01	2404:f801:4800:25:f16...	25 Applications	Requires agent ins...	2	2041
PayrollWeb02	-	17 Applications	Requires agent ins...	2	2041
PayrollDB01	2404:f801:4800:25:a8...	126 Applications	Requires agent ins...	2	2041
PayrollWeb03	10.150.10.231,2404:f8...	2 Applications	Requires agent ins...	2	2041
PayrollApp02	2404:f801:4800:25:c98...	17 Applications	Requires agent ins...	4	4091
PayrollApp03	2404:f801:4800:25:bc...	15 Applications	Requires agent ins...	1	4091

## Application Inventory

PayrollDB02

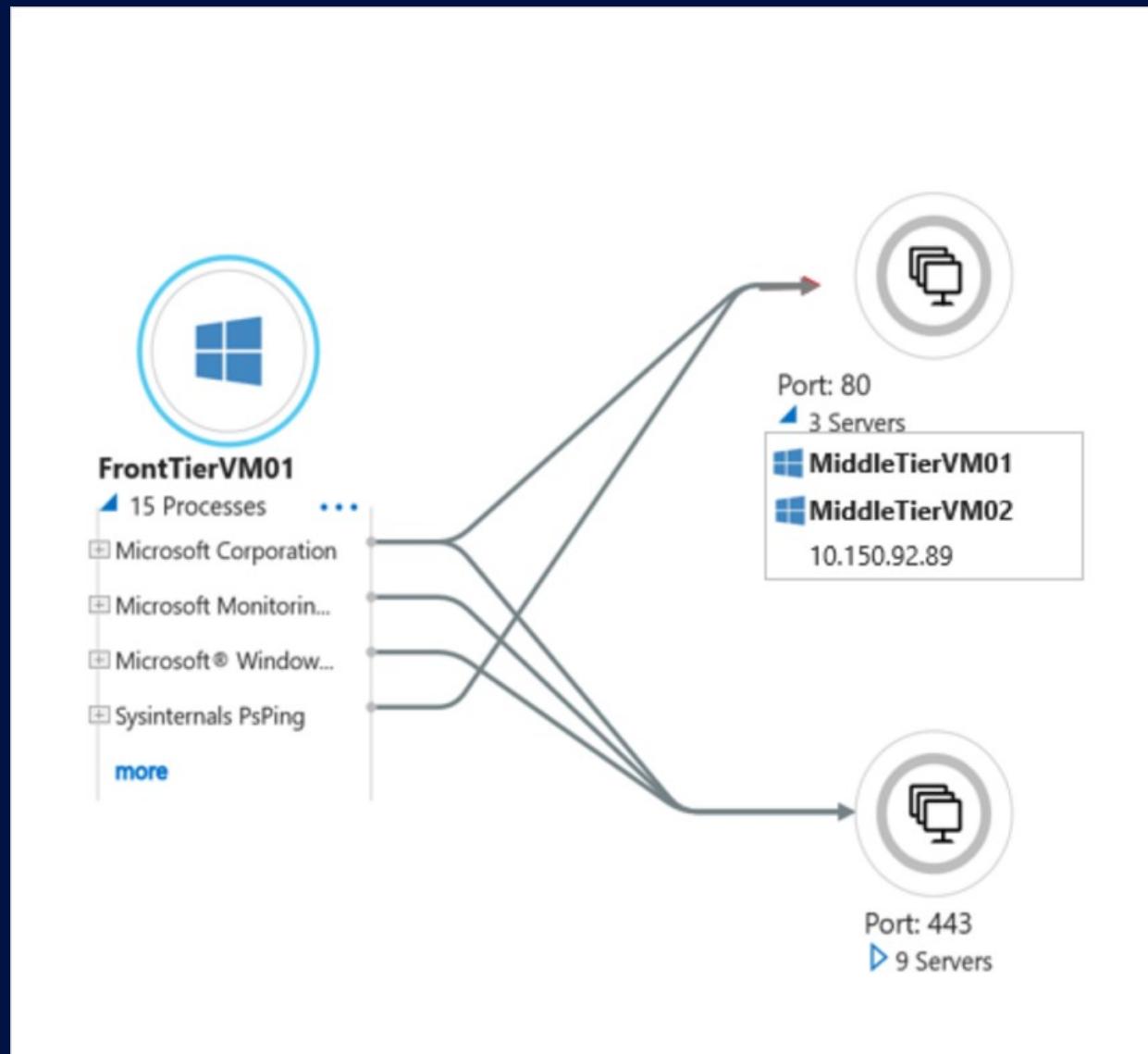
Applications Roles and Features

Name	Version
Tools for .Net 3.5	3.11.50727
Active Directory Authentication Library for SQL Server	14.0.1000.169
Browser for SQL Server 2017	14.0.1000.169
ConfigMgr Client Setup Bootstrap	5.00.7958.1000
Configuration Manager Client	5.00.7958.1000
Dependency Agent	9.0.5
Microsoft .NET Framework 4 Multi-Targeting Pack	4.0.30319
Microsoft .NET Framework 4.5 Multi-Targeting Pack	4.5.50710
Microsoft .NET Framework 4.5.1 Multi-Targeting Pack	4.5.50932
Microsoft .NET Framework 4.5.1 Multi-Targeting Pack (ENU)	4.5.50932
Microsoft .NET Framework 4.5.1 SDK	4.5.51641
Microsoft .NET Framework 4.5.2 Multi-Targeting Pack	4.5.51209
Microsoft .NET Framework 4.5.2 Multi-Targeting Pack (ENU)	4.5.51209
Microsoft Analysis Services OLE DB Provider	14.0.1000.397
Microsoft Analysis Services OLE DB Provider	14.0.1000.397
Microsoft Azure Site Recovery Mobility Service/Master Target S...	9.18.4946.1
Microsoft Build Tools 14.0 (amd64)	14.0.23107
Microsoft Build Tools 14.0 (x86)	14.0.23107
Microsoft Build Tools Language Resources 14.0 (amd64)	14.0.23107
Microsoft Build Tools Language Resources 14.0 (x86)	14.0.23107
Microsoft Help Viewer 2.2	2.2.23107
Microsoft Help Viewer 2.2	2.2.23107
Microsoft Monitoring Agent	8.0.11049.0
Microsoft ODBC Driver 13 for SQL Server	14.0.1000.169
Microsoft Policy Platform	1.2.3602.0
Microsoft Silverlight	5.1.20513.0
Microsoft SQL Server 2012 Native Client	11.3.6540.0

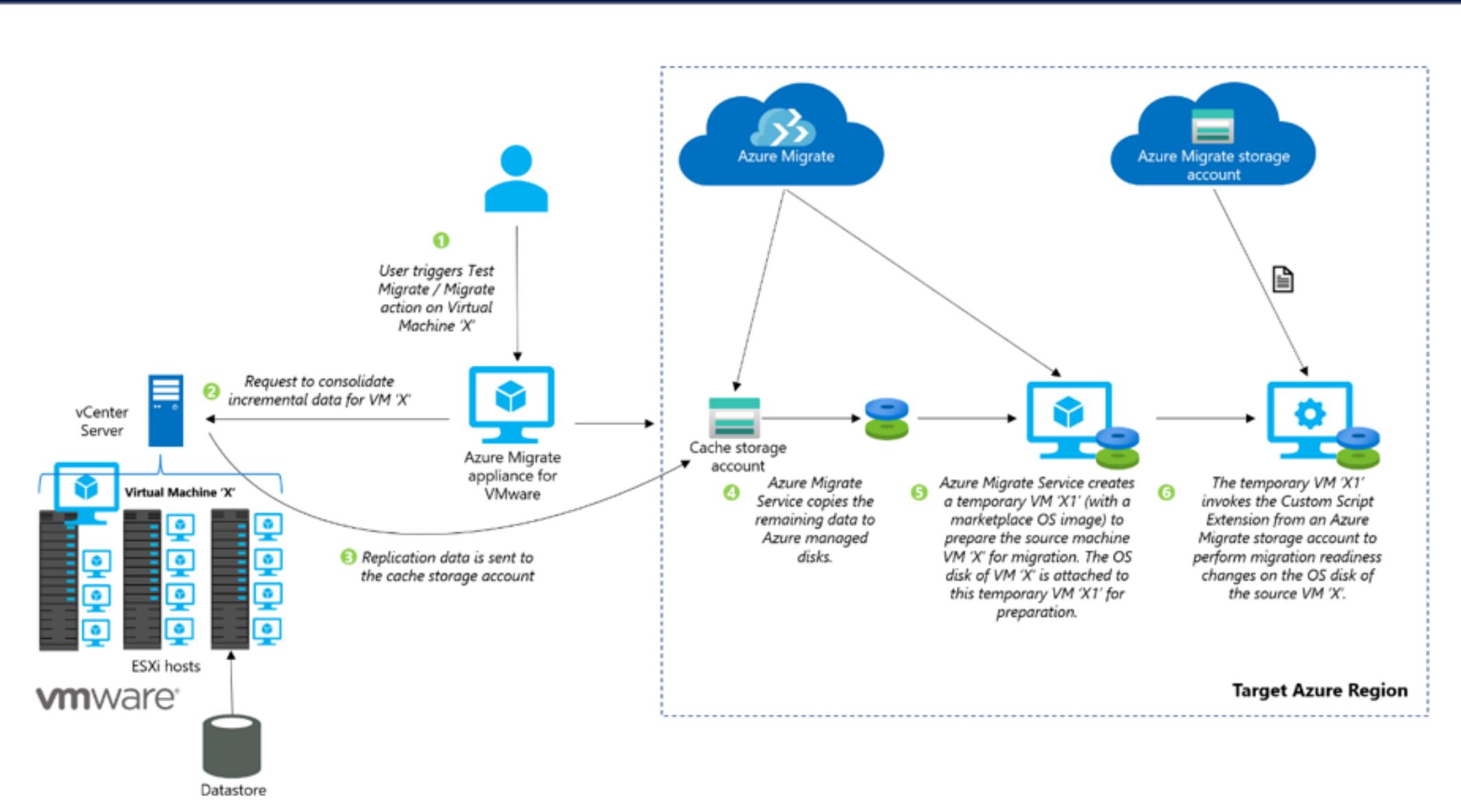


# Dependency Analysis

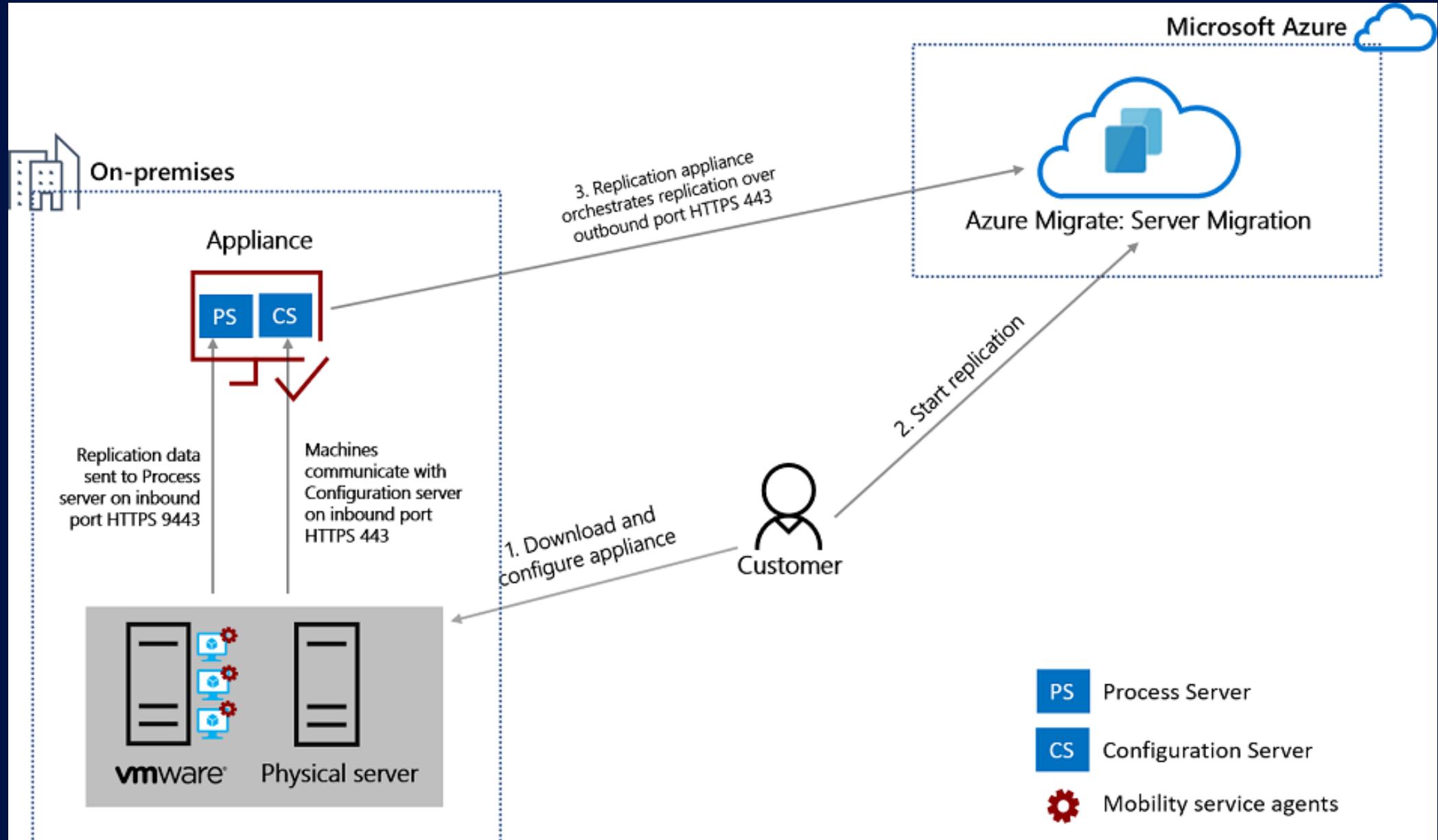
L'analisi delle dipendenze consente di avere a colpo d'occhio una visuale sulle isole applicative e più in generale sulla comunicazione che esse instaurano tra di loro.



# Agentless Migration



# Agent Based Migration



# Windows OS Upgrade During Migration

es and web apps > Azure Migrate: Migration and modernization

## Migration and modernization | Replications

Refresh Migrate Columns Feedback

To view the machines replicating via the Azure Migrate appliance, click on the 'Azure Migrate appliance' tab. For all other machines, click 'Other'.

Azure Migrate appliance Other

Last refreshed at: 17/7/2023, 3:28:21 pm

Filter items...

Name	Replication status	Replication health	Last sync	Test migration status	M
Ubuntu-20.04-desk7	Delta sync	Healthy	17/7/2023, 2:52:32 pm	12/7/2023, 1:11:10 pm	<a href="#">Pause replication</a>
Scale-Win2k22	Delta sync	Healthy	17/7/2023, 1:38:29 pm	17/7/2023, 2:28:12 pm	<a href="#">Resume replication</a>
Ubun22.04-desk1	-	-	17/7/2023, 1:50:44 pm	14/7/2023, 5:00:57 pm	<a href="#">Test migration</a>
Ubun22.04-desk3	Delta sync	Healthy	17/7/2023, 2:38:03 pm	12/7/2023, 1:11:21 pm	<a href="#">Clean up test migration</a>
Ubun20.04server2	Delta sync	Healthy	17/7/2023, 2:58:48 pm	12/7/2023, 1:11:29 pm	<a href="#">Migrate</a>
NewWS2016DC	Delta sync	Healthy	17/7/2023, 1:28:40 pm	Pending	<a href="#">Repair replication</a>
Ubuntu-20.04-server1	Delta sync	Healthy	17/7/2023, 2:58:47 pm	14/7/2023, 5:57:06 pm	<a href="#">Complete migration</a>
Ubuntu-22.04-server3	Delta sync	Warning	17/7/2023, 5:15:08 pm	17/7/2023, 2:47:27 pm	<a href="#">Stop replication</a>
Ubuntu-20.04-desk5	Delta sync	Healthy	17/7/2023, 2:56:27 pm	12/7/2023, 7:57:15 pm	<a href="#">Opting for OS upgrade will increase the overall time required for migration of the virtual machine. Learn more</a>
Scale-Win-10	Delta sync	Warning	14/7/2023, 2:28:35 pm	Completed with info	<a href="#">Ready to migrate</a>
Ubuntu-20.04-desk4	Delta sync	Healthy	17/7/2023, 2:55:39 pm	12/7/2023, 1:12:10 pm	<a href="#">Ready to migrate</a>
Ubun22.04-desk2	Delta sync	Healthy	17/7/2023, 2:55:40 pm	12/7/2023, 1:12:17 pm	<a href="#">Ready to migrate</a>
Ubuntu-22.04-server2	Delta sync	Healthy	17/7/2023, 6:38:00 pm	12/7/2023, 1:12:24 pm	<a href="#">Ready to migrate</a>

## OS Upgrade

NewWS2016DC

The OS upgrade will be automatically triggered after successful migration of the VM. In case of any issues, you can retry the Test Migrate or Migrate flow.

Current OS version:  
Microsoft Windows Server 2016 or later (64-bit)

Upgrade to:  
Microsoft Windows Server 2022 (64-bit)

**i** Opting for OS upgrade will increase the overall time required for migration of the virtual machine. [Learn more](#)



# DEMO



#GlobalAzureTorino

#GlobalAzure

# Sicurezza dei Workload in Azure



#GlobalAzure

## Security Operations / SOC

**Microsoft Security Experts**  
Defender Experts | Detection and Response Team (DART)

**Managed Security Operations**  
Using Microsoft Security

### Microsoft Defender XDR

Unified Threat Detection and Response across IT, OT, and IoT Assets  
Incident Response | Automation | Threat Hunting | Threat Intelligence

### Microsoft Security Copilot (Preview)

Microsoft Sentinel  
Cloud Native SIEM, SOAR, and UBA



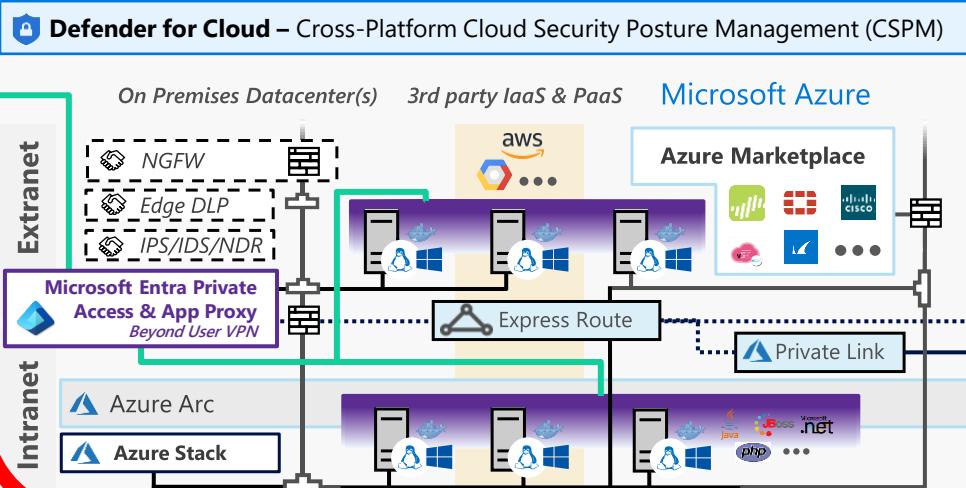
## Endpoints & Devices

Unified Endpoint Management (UEM)  
Intune Configuration Manager



Microsoft Defender for Endpoint  
Unified Endpoint Security  
Endpoint Detection & Response (EDR)  
Web Content Filtering  
Threat & Vuln Management  
Endpoint Data Loss Protection (DLP)  
...

## Hybrid Infrastructure – IaaS, PaaS, On-Premises



Securing Privileged Access – [aka.ms/SPA](https://aka.ms/SPA)

Entrada Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep

## Security Guidance

1. Present Slide
2. Hover for Description
3. Click for more information

1. [Security Adoption Framework](#)
2. [Security Documentation](#)
3. Cloud Security [Benchmarks](#)

This is interactive!

## Software as a Service (SaaS)

Microsoft Defender for Cloud Apps

- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Information Protection & Data Loss Prevention (DLP)



### Microsoft Entra Internet Access

## Identity & Access

**Conditional Access** – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

## Information Protection

Microsoft Purview

Information protection and governance across data lifecycle

Discover Monitor Classify Protect

File Scanner (on-premises and cloud)

Data Governance

Advanced eDiscovery

Compliance Manager

### Microsoft Entra

Passwordless & MFA  
Hello for Business  
Authenticator App  
FIDO2 Keys

Entra ID Protection  
Leaked cred protection  
Behavioral Analytics  
...

ID Governance  
Microsoft Entra PIM  
External Identities

Defender for Identity

Active Directory

Security Posture Management – Monitor and mitigate technical security risks using [Secure Score](#), [Compliance Score](#), [CSPM: Defender for Cloud](#), [Microsoft Defender External Attack Surface Management \(EASM\)](#) and [Vulnerability Management](#)

Windows 11 & 10 Security  
Network protection  
Credential protection  
Full Disk Encryption  
Attack surface reduction  
...

IoT and Operational Technology (OT)  
Microsoft Defender for IoT (and OT)  
• ICS, SCADA, OT  
• Internet of Things (IoT)  
• Industrial IoT (IIoT)  
• Asset & Vulnerability management  
• Threat Detection & Response  
Azure Sphere

Defender for Cloud – Cross-Platform, Multi-Cloud XDR  
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises  
Defender for APIs (preview)

## People Security

Attack Simulator

Insider Risk Management

Communication Compliance

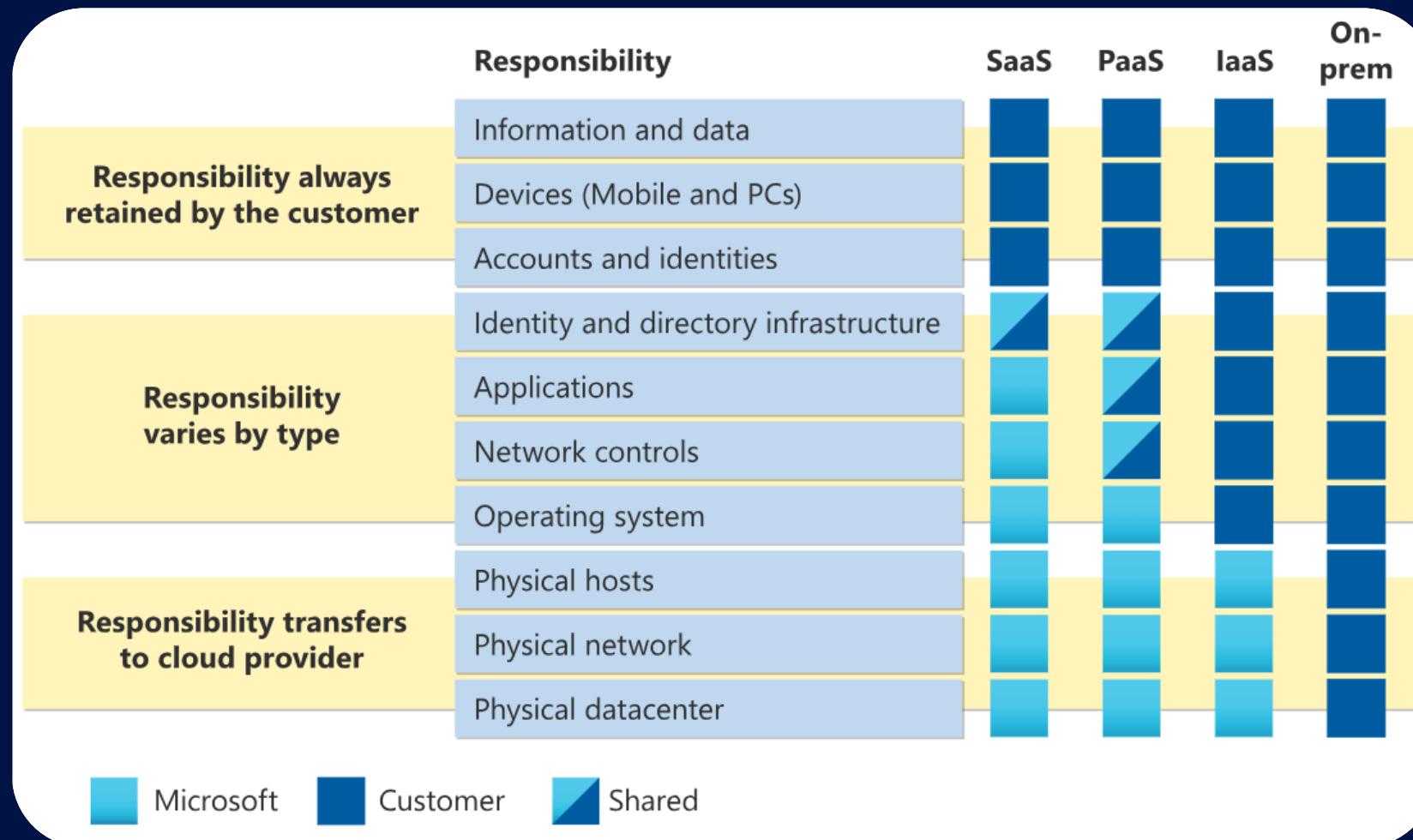
GitHub Advanced Security & Azure DevOps Security  
Secure development and software supply chain

Threat Intelligence – 65+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

# Everyone takes responsibility ... please!



# Zen.... Ehm ...Zero Trust !

Verify explicitly    Use least privilege access    Assume breach

Some tips!

- ✓ Workloads are monitored and alerted to abnormal behavior.
- ✓ Every workload is assigned an app identity—and configured and deployed consistently.
- ✓ Human access to resources requires Just-In-Time.
  
- ✓ Unauthorized deployments are blocked, and alert is triggered.
- ✓ Granular visibility and access control are available across workloads.
- ✓ User and resource access segmented for each workload.



# Let's get serious !

Define your business needs:

🛡️ Does your company need to assess and strengthen the security configuration of its cloud resources?

🛡️ Does your company want to manage the security posture of multicloud resources from a single point (single pane of glass)?

🛡️ What boundaries do you want to put in place to ensure that your entire organization is covered, and no areas are missed?

🛡️ Does your company need to comply with industry and regulatory standards? If so, which standards?

🛡️ What are your goals for protecting critical workloads, including containers and servers, against malicious attacks?

🛡️ Do you need a solution only in a specific cloud environment, or a cross-cloud solution?

🛡️ How will the company respond to alerts and recommendations, and remediate non-compliant resources?

🛡️ Will workload owners be expected to remediate issues?

# Let's get serious !

.... And define an adoption strategy



Centralized model - Security controls are defined, deployed, and monitored by a central team.

*The central security team decides which security policies will be implemented in the organization and who has permissions to control the set policy.*

*Workload owners on the other hand are responsible for managing their cloud workloads but need to follow the security policies that the central team has deployed.*

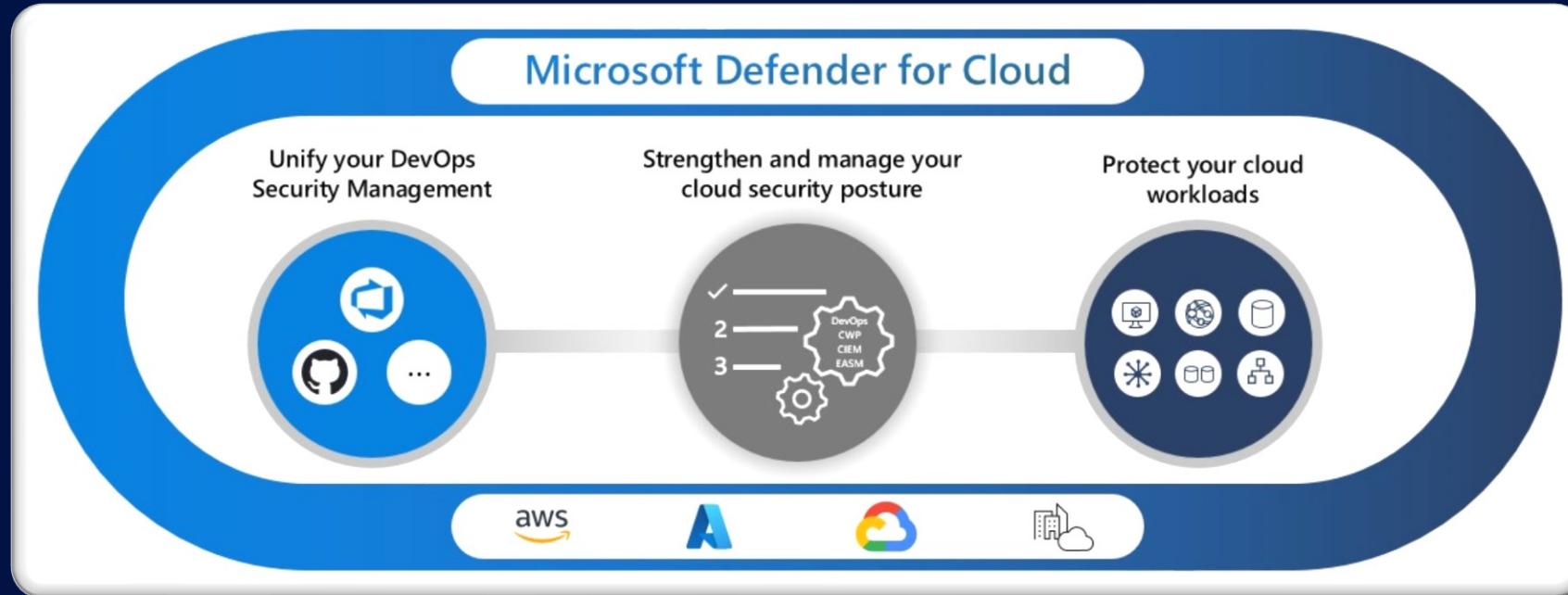


Decentralized model - Security controls are defined, deployed, and monitored by workload owners.

*Security control deployment is done by workload owners, as they own the policy set and can therefore decide which security policies are applicable to their resources.*

*The security team usually has insights into the overall security posture of the organization, and they might hold the workload owners accountable for improving their security posture.*

# Defender for Cloud



# Defender for Cloud

## Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/Billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
 Foundational CSPM	Free <a href="#">Details &gt;</a>		 Full	<span>Off</span> <span>On</span>
 Defender CSPM	\$5/Billable resource/Month <a href="#">Details &gt;</a>	0 resources <small>(1)</small>		<span>Off</span> <span>On</span>

## Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
 Servers	<a href="#">Plan 1 (\$5/Server/Month)</a> <small>(1)</small> <a href="#">Change plan &gt;</a>	0 servers	 Full <a href="#">Settings &gt;</a>	<span>Off</span> <span>On</span>
 App Service	\$15/Instance/Month <small>(1)</small>  <a href="#">Details &gt;</a>	0 instances		<span>Off</span> <span>On</span>
 Databases	Selected: 0/4 <small>(1)</small>  <a href="#">Select types &gt;</a>	Protected: 0/0 instances		<span>Off</span> <span>On</span>
 Storage	\$10/Storage account/month \$0.15/GB scanned for On-Upload Malware Scanning (config 0 storage accounts) <a href="#">Details &gt;</a>			<span>Off</span> <span>On</span>
 Containers	\$7/VM core/Month <small>(1)</small>  <a href="#">Details &gt;</a>	0 container registries; 0 kubernetes cores		<span>Off</span> <span>On</span>
 Key Vault	\$0.25/Vault/Month  <a href="#">Details &gt;</a>	0 key vaults		<span>Off</span> <span>On</span>
 Resource Manager	\$5/Subscription/Month <small>(1)</small>  <a href="#">Details &gt;</a>			<span>Off</span> <span>On</span>
 APIs	No plan selected <small>(1)</small>  <a href="#">Change plan &gt;</a>	0 Azure API Management services		<span>Off</span> <span>On</span>



# What we learned ?

*Se conosci il nemico e te stesso, la tua vittoria è sicura.*

*Se conosci te stesso ma non il nemico, le tue probabilità di vincere e perdere sono uguali.*

*Se non conosci il nemico e nemmeno te stesso, soccomberai in ogni battaglia.*

Sun Tzu – L'arte della guerra



# DOMANDE



# GRAZIE

