azuremeetup VENETO

meetup

Microsoft

25 ottobre 2024

La sicurezza del Cloud ibrido con Defender for Cloud

Luigi Pandolfino
Coordinatore Azure Meetup Veneto

Guido Imperatore
Microsoft Security MVP SIEM & XDR

Andrea Marchi
Moderatore

About Me

- Microsoft Security MVP Siem & XDR
- Senior Security Consultant
- Blogger di Tecnologia Microsoft Security

Microsoft® Most Valuable Professional

Microsoft Certified: Azure Administrator Associate

Microsoft 365 Certified: Endpoint Administrator Associate

Microsoft Certified: Azure Solutions Architect Expert

Microsoft 365 Certified: Security Administrator Associate

Microsoft Certified: Identity and Access Administrator Associate

Microsoft Certified: Azure Security Engineer Associate

Microsoft Certified: Security Operations Analyst Associate

Microsoft 365 Certified: Enterprise Administrator Expert

Microsoft Certified: Azure Virtual Desktop Specialty

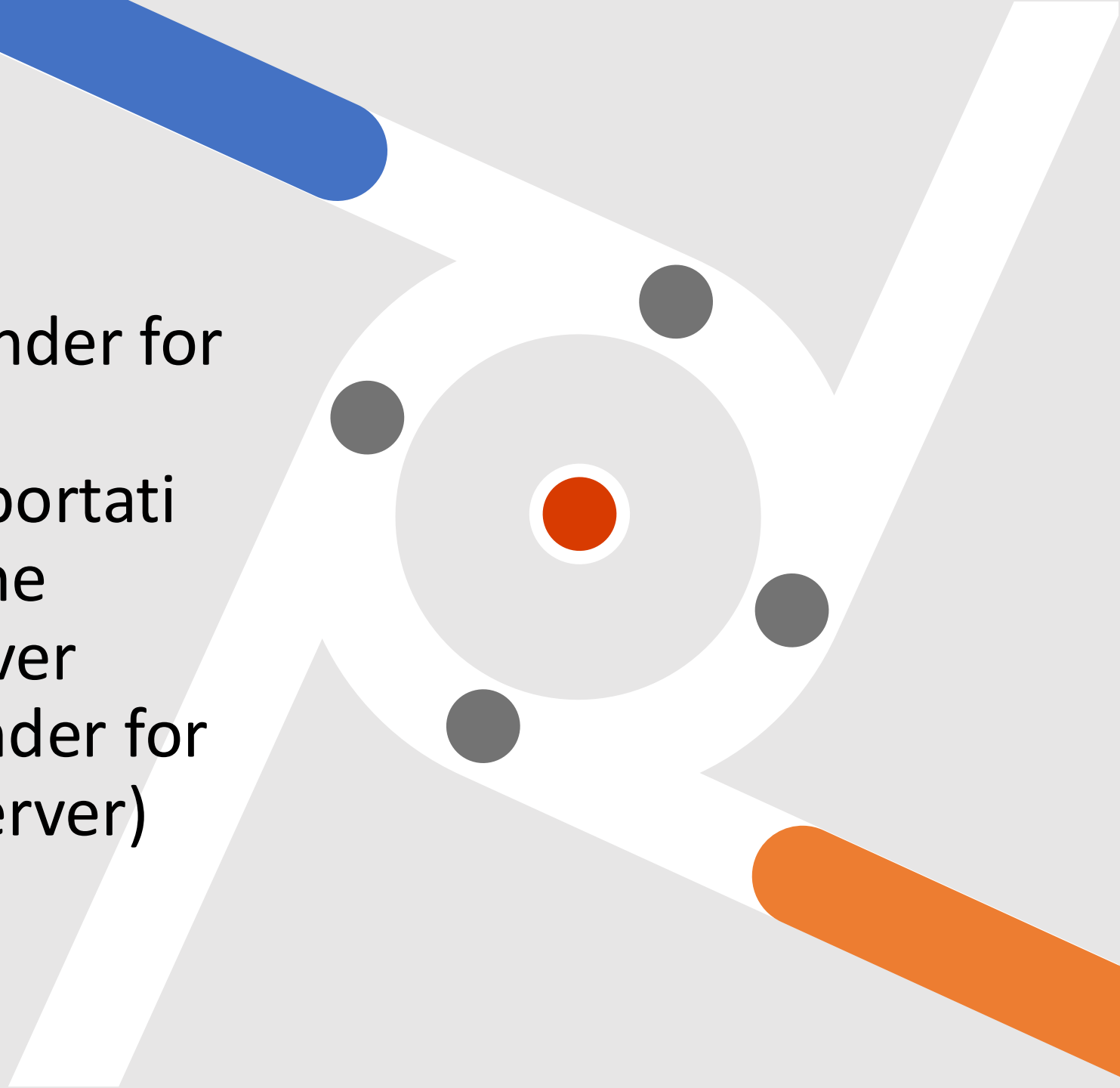
Microsoft Certified: Cybersecurity Architect Expert

Microsoft Certified: Information Protection Administrator Associate

Microsoft Security

Agenda

- Cosa è Microsoft Defender for Cloud
- Quali servizi sono supportati
- Vantaggi della soluzione
- Intro Defender for Server
- Demo Microsoft Defender for Cloud (Defender for Server)



Microsoft Security

Cosa è Microsoft Defender for Cloud

Soluzione devSecOps (Development Security Operations) che unifica la gestione della sicurezza a livello di codice in ambienti multicloud e con più pipeline

Una soluzione di gestione del comportamento di sicurezza cloud (CSPM) che illustra le azioni che è possibile eseguire per evitare violazioni

Una piattaforma CWPP (Cloud Workload Protection Platform) con protezioni specifiche per server, contenitori, archiviazione, database e altri carichi di lavoro

Defender CSPM (Foundational vs Advanced)

Defender CSPM (Foundational – Gratuita)

- Gestione Centralizzata dei criteri
- Punteggio di Sicurezza
- Copertura Multicloud
- Cloud Security Posture Management (CSPM)

VS

CSPM Defender (Avanzata – Costi aggiuntivi)

- Advanced Cloud Security Posture Management
- Gestore della postura di sicurezza dei dati
- Analisi del percorso di attacco
- Cloud Security Explorer
- Governance della sicurezza
- Gestione delle autorizzazioni di Microsoft Entra ID

[Pricing - Microsoft Defender for Cloud | Microsoft Azure]

Microsoft Security

Defender CWPP

Perché è importante avere la soluzione CWPP ?

- Attacchi sempre più frequenti e sofisticati
- Identificazione rapida della gravita degli indicident
- Risposta rapida ad Incident di Sicurezza
- Unica Soluzione per proteggere ambienti Ibridi

Workload di Protezione

- Protezione Server Cloud
- Identificazione delle minacce alle risorse di archiviazione
- Proteggere i database Cloud
- Proteggere i Containers
- Informazioni dettagliate sui servizi dell’infrastruttura
- Avvisi di Sicurezza
- Eventi imprevisti relativi alla sicurezza

Che cos'è Microsoft Defender for Cloud? - Microsoft Defender for Cloud | Microsoft Learn

Microsoft Security

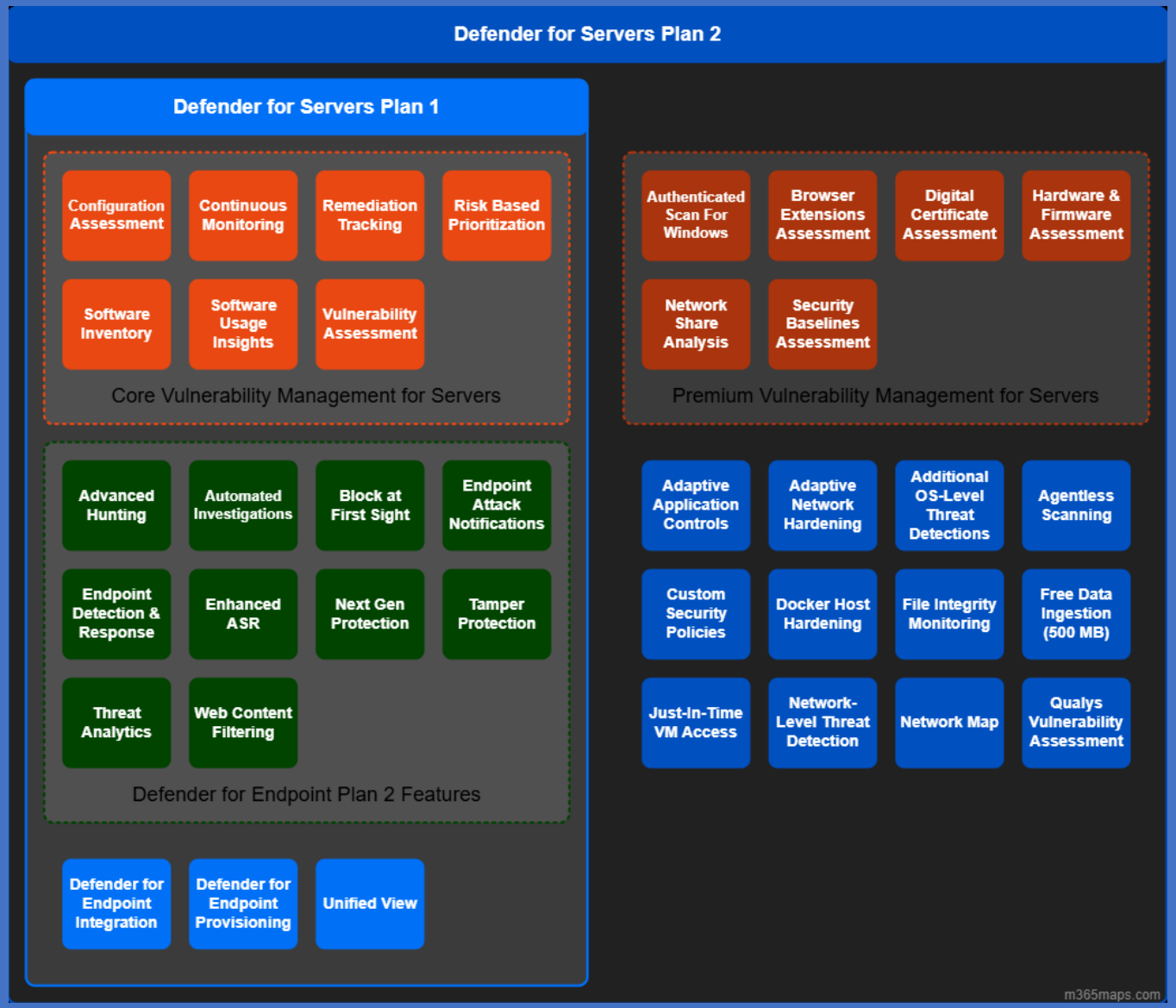
Vantaggi Defender for Cloud

- Rilevazione Minacce Informatica in infrastrutture Iaas (Infrasttuttura as a Service)
- Protezione Server in Hosting presso provider di terze parti
- Protezione Server in Hosting presso Microsoft Azure
- Protezione di piattaforme PaaS (Piattaforme as a Service)
- Possibilità di inviare i log verso SIEM (Microsoft Sentinel o Terze Parti)
- Generazione di avvisi personalizzati in base alle esigenze

Microsoft Security

Estendere la protezione di Defender for Server con Microsoft Defender for Cloud

Piani Defender for Server

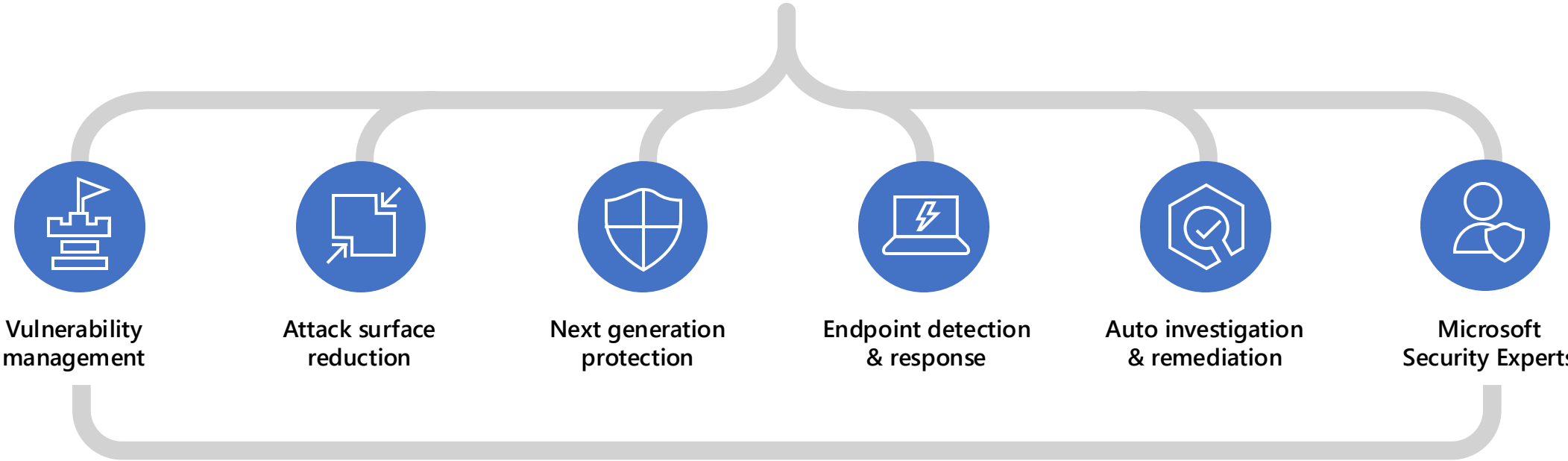


- Defender for Server Piano 1
- Defender for Server Piano 2
- Acquistabili come Addon
- Acquistabili con Defender for Cloud

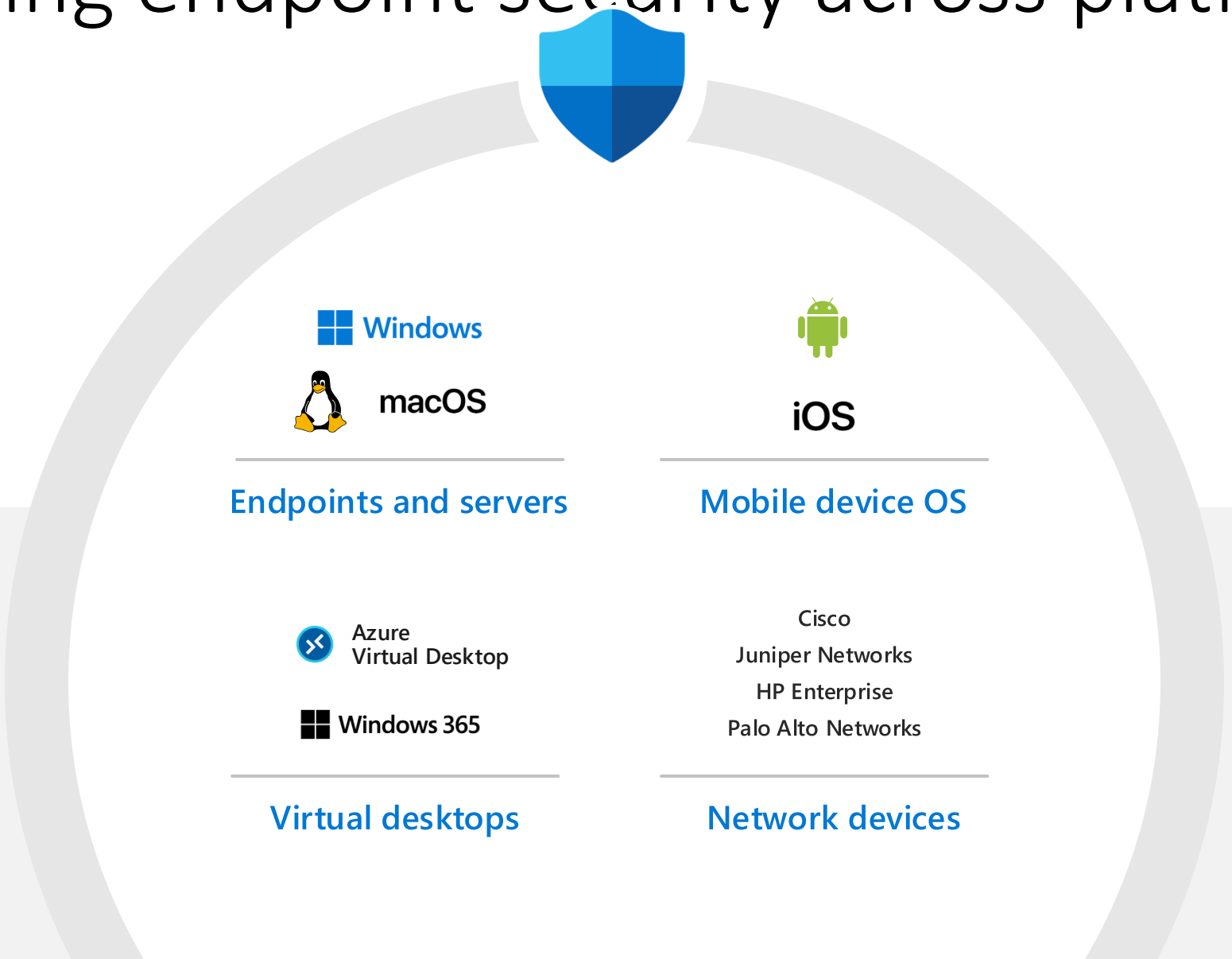
Microsoft Defender for Servers | M365 Maps

Microsoft Defender for Endpoint

Threats are no match.



Delivering endpoint security across platforms



Metodi di Onboarding

- Se Virtual Machine in Microsoft Azure, abilitando la funzionalità in Defender for Cloud
- Se Virtual Machine onpremise:
  - Onboarding della virtual machine in Azure ARC
  - Abilitando la funzionalità in Defender for Cloud

Azure ARC

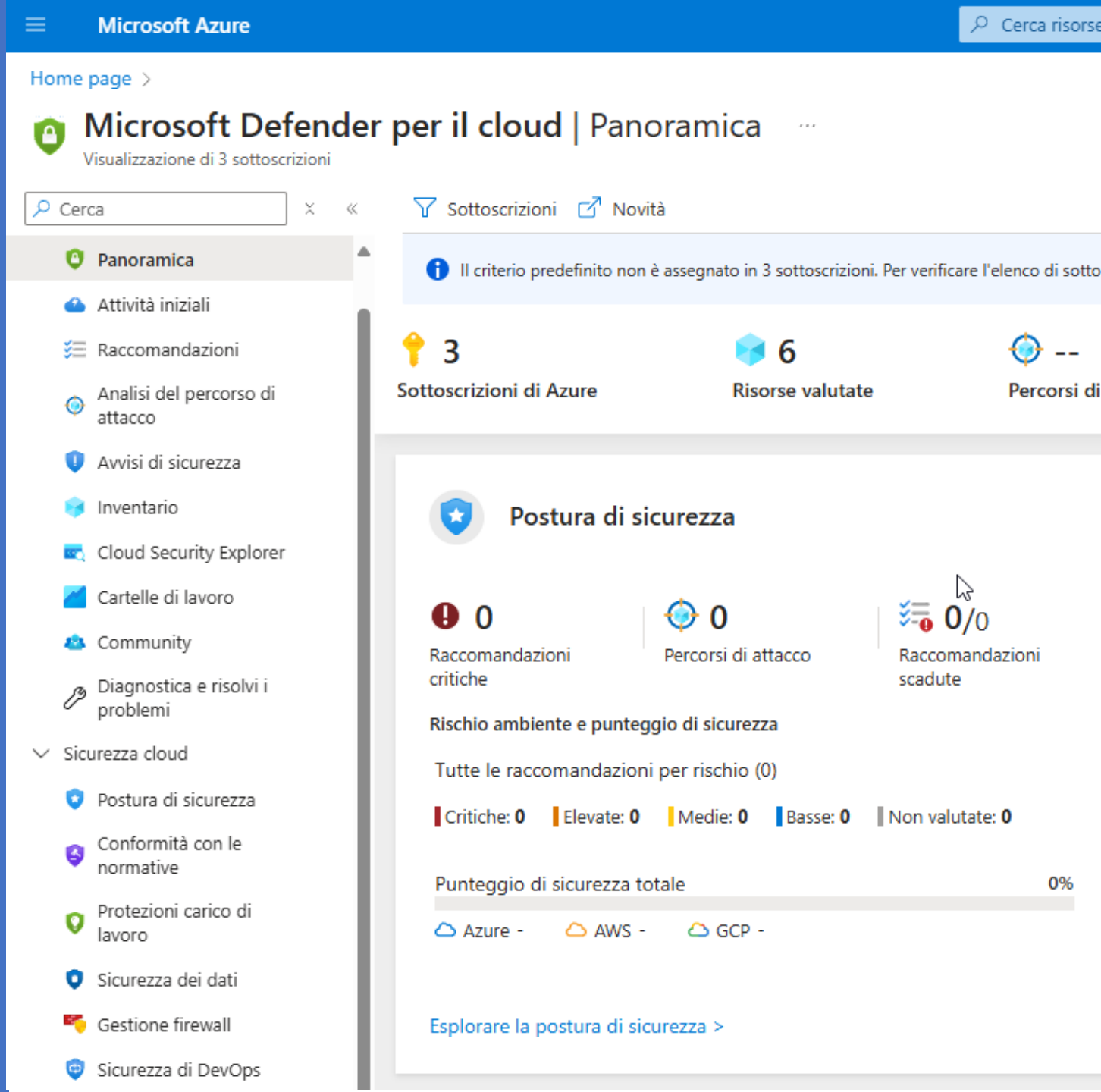
Microsoft Azure

Microsoft Defender for Server

Microsoft Security

Demo

Abilitare Defender For Cloud



Microsoft Security

Grazie mille!

Blog Tech-cloud.it

Guido Imperatore
Microsoft Security MVP SIEM & XDR
Guido.imperatore@tech-cloud.it

azureontrack
VENETO

TD SYNNEX

25 OTTOBRE 2024

skybackbone
engenio

azuremeetup VENETO

meetup

Microsoft

veneto@azuremeetup.it

BY COMMUNITY • FOR COMMUNITY •

#GLOBALAZURE

2025

YouTube

coffeebreak VENETO