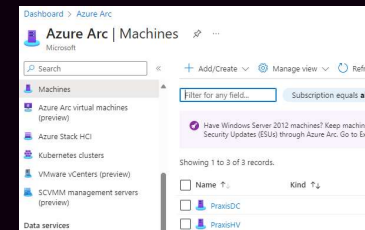
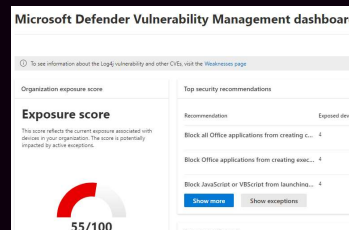
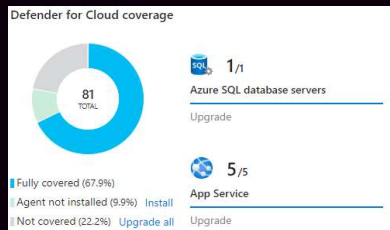
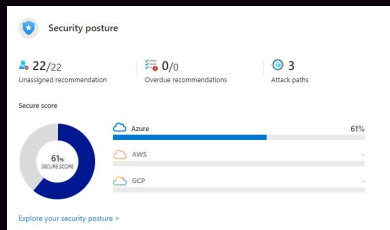


NIC
EMPOWER

November 13-15, Oslo Spektrum

Gregor Reimling

Harden your Multi Cloud environment with Defender for CSPM



About Me "Gregor Reimling"



Focus

Azure Governance, Security
and IaaS

From

Cologne, Germany



My Blog

<https://www.reimling.eu>

NIC
EMPOWER



www.cloudinspires.me

Certifications

Cloud Security Architect,
MVP for MS Azure and
Security

Hobbies

Family, Community,
Worldtraveler

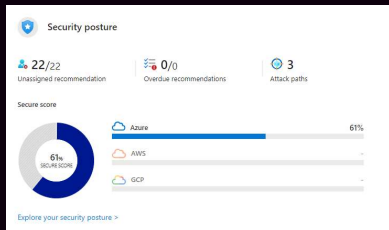
Contact



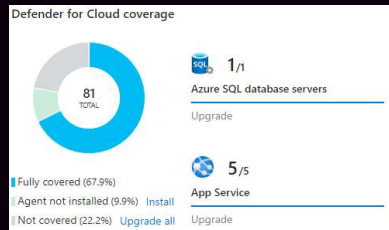
@GregorReimling

@CloudInspires

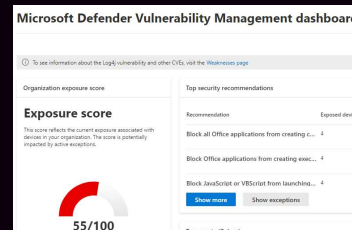
Agenda



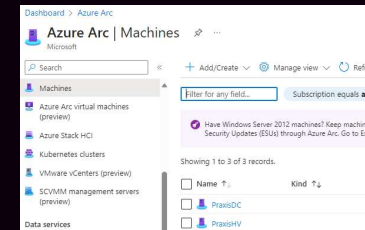
Defender
for Cloud Overview



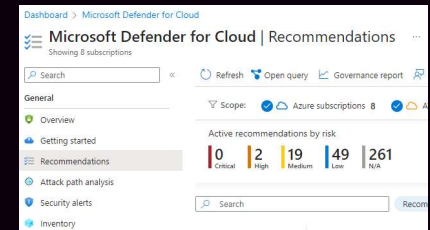
Defender
For CSPM



Agentless Scanning
and MDE

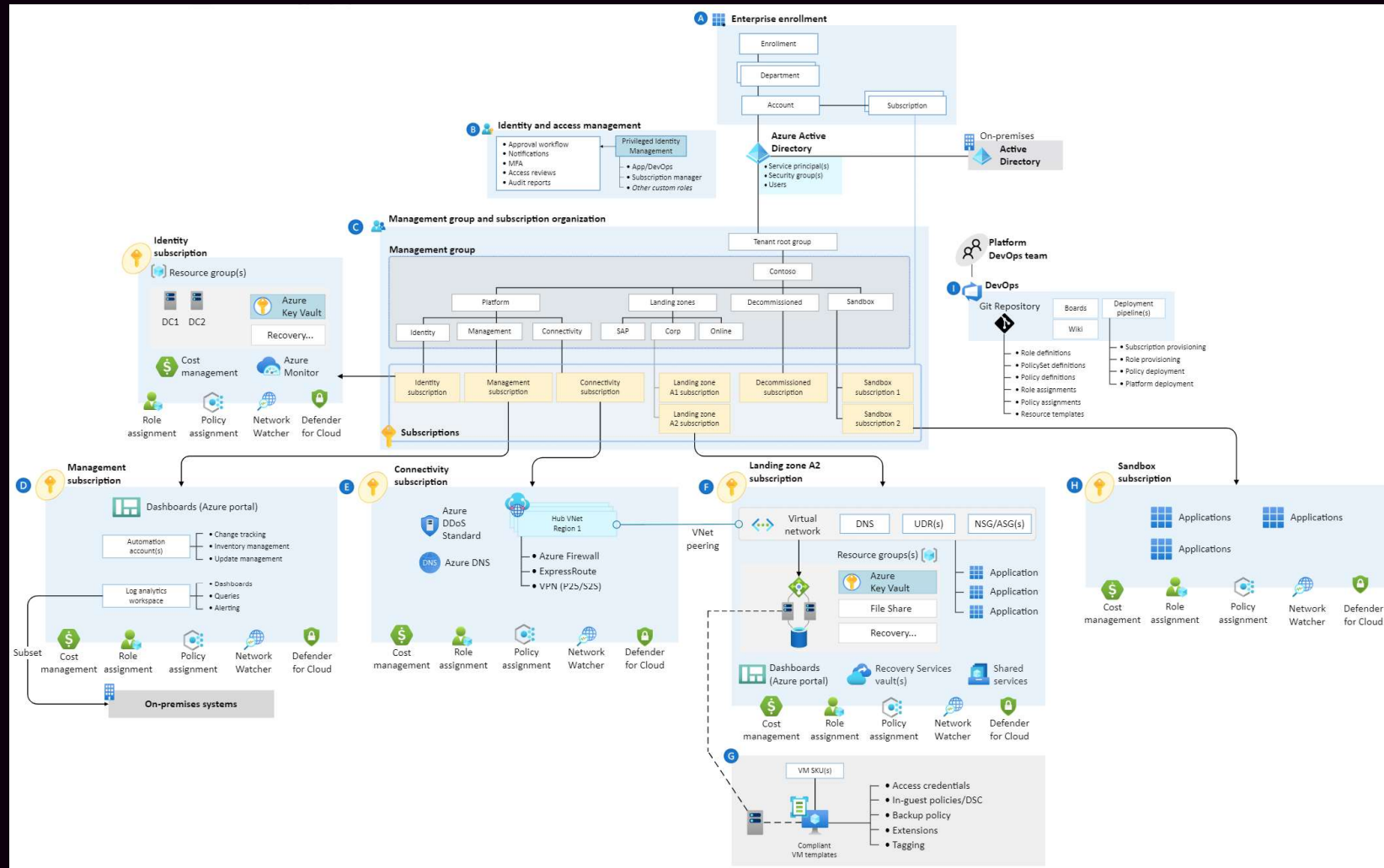


Multicloud
Capabilities

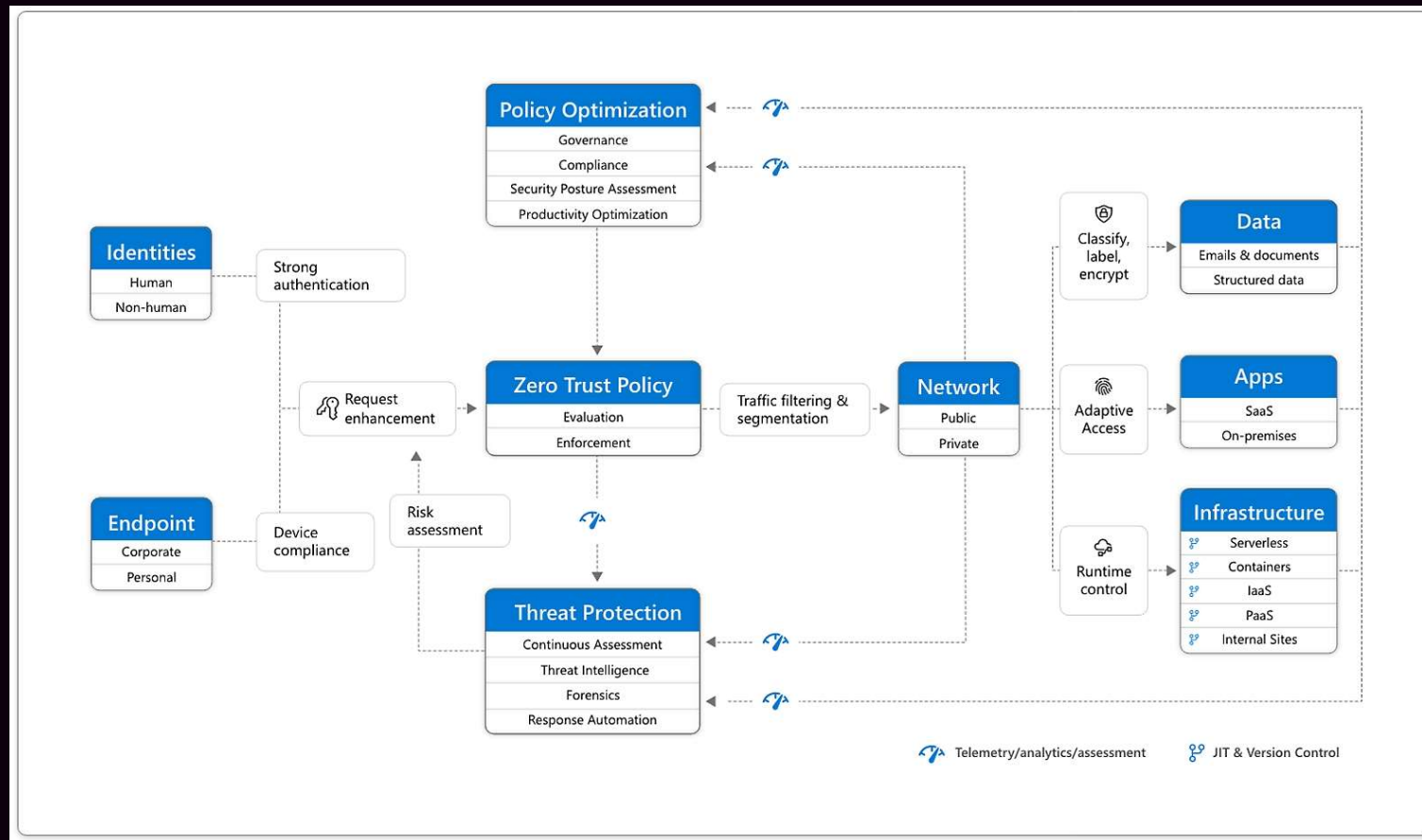


New Defender
features

Enterprise Scale



Microsoft Zero Trust Approach



Microsoft Cybersecurity Reference Architectures (MCRA)

Capabilities

What cybersecurity capabilities does Microsoft have?



Build Slide



Azure Native Controls

What native security is available?



Attack Chain Coverage

How does this map to insider and external attacks?

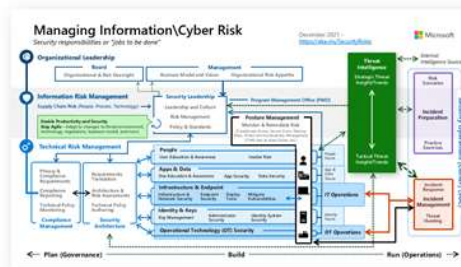


Build Slide



People

How are roles & responsibilities evolving with cloud and zero trust?



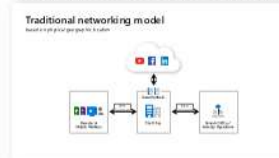
Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?



Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?



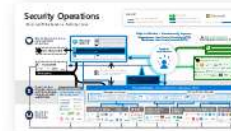
Zero Trust User Access

How to validate trust of user/devices for all resources?



Security Operations

How to enable rapid incident response?



Operational Technology

How to enable Zero Trust Security for OT?



aka.ms/MCRA | December 2021 | Microsoft

Microsoft Defender for Cloud

Microsoft Defender for Cloud

DevOps Security Management

Cloud Security Posture Management

Cloud Workload Protection

aws

A

Google Cloud

Microsoft Azure

[Defender for Azure Cosmos DB](#)

[Defender for Containers](#)

[Defender for App Service](#)

[Defender for DNS](#)

[Defender for CSPM](#)

[Defender for Servers](#)

[Defender for Key Vault](#)

[Defender for Resource Manager](#)

[Defender for Storage](#)

[Defender for SQL](#)



Agentless and agent-based vulnerability scanning

Visibility on software and CVEs | Disc snapshots | EDR



Integrated data and insights

Defender for DevOps | Defender EASM | Entra Permissions Management | Hybrid and multi-cloud environments



Contextual cloud security and risk prioritization

Attack path analysis to prioritize risk | Intelligent cloud security graph | Custom path queries on cloud security explorer



Integrated workflows and automated remediation

Regulatory compliance | Master group management | Multicloud Microsoft cloud security benchmark

NIC
EMPOWER


Microsoft Defender for Cloud


Strengthen and manage your security posture




Security compliance management


At-scale governance & automated remediation


Attack path-based prioritization



Full visibility with agentless and agent-based scanning


Unify your DevOps security management




DevOps posture visibility across pipelines


Infrastructure as Code security


Code to cloud contextualization



Integrated workflows & pull request annotations

Detect threats and protect your workloads




Full-stack threat protection


Vulnerability assessment & management


Automate with the tools of your choice and native integration in Microsoft Sentinel



Amazon Web Services



Microsoft Azure



Google Cloud Platform

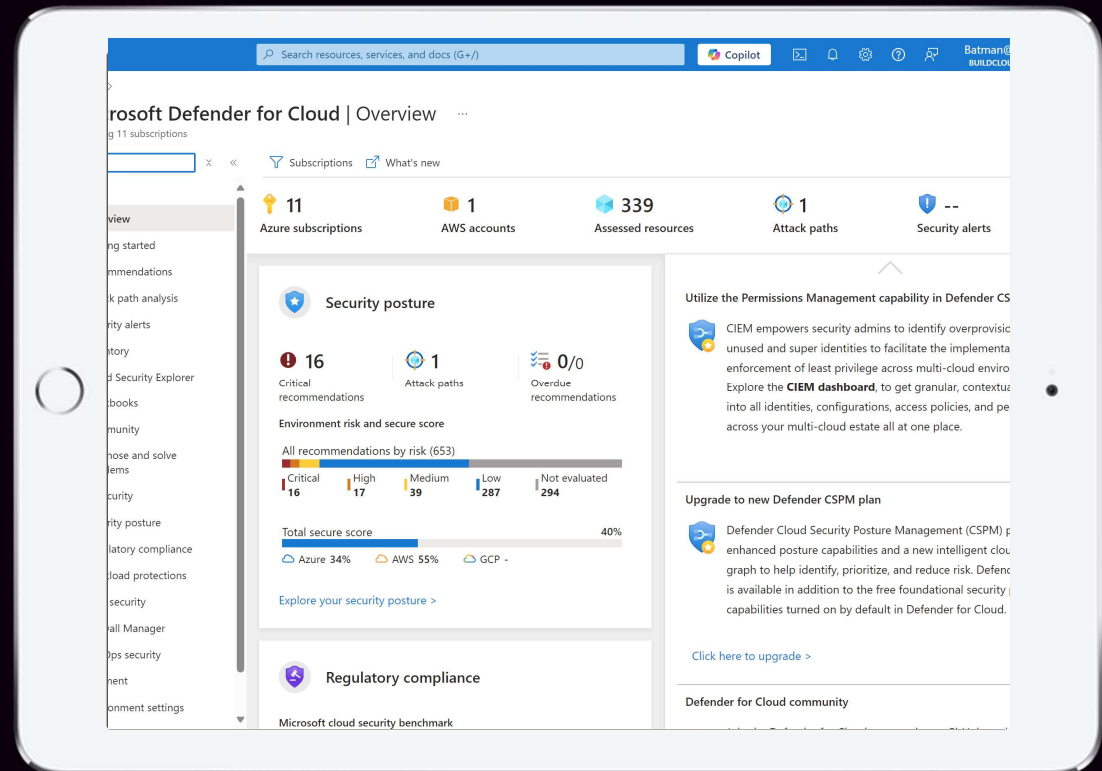


On-premises

Defender for Cloud overview

- **Comprehensive Visibility**
- **Risk Prioritization**
- **Proactive Threat Defense**
- **Compliance and Governance**
- **Secure Score**
- **Multicloud Support**
- **Advanced Features**

Demo Defender for Cloud/CSPM



Foundational vs Defender for CSPM

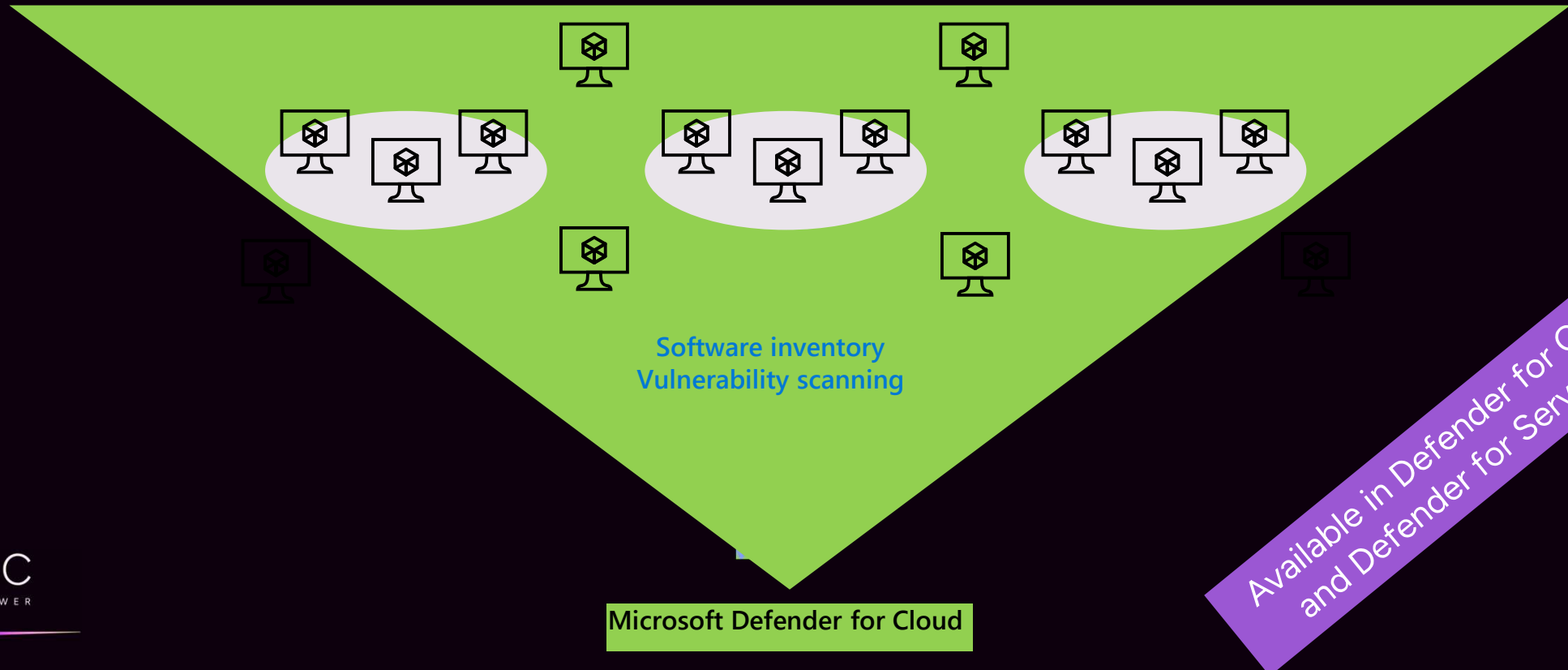
Features	Foundational CSPM	Defender for CSPM
Security recommendations to fix misconfigurations	✓	✓
Asset inventory	✓	✓
Secure score	✓	✓
Data exporting	✓	✓
Workflow automation	✓	✓
Tools for remediation	✓	✓
Microsoft Cloud Security Benchmark	✓	✓
Governance		✓
Regulatory compliance		✓
Cloud security explorer		✓
Attack path analysis		✓
Agentless scanning for machines		✓
Agentless discovery for Kubernetes		✓
Agentless VM secret scanning		✓
Data aware security posture		✓



Agentless Scanning

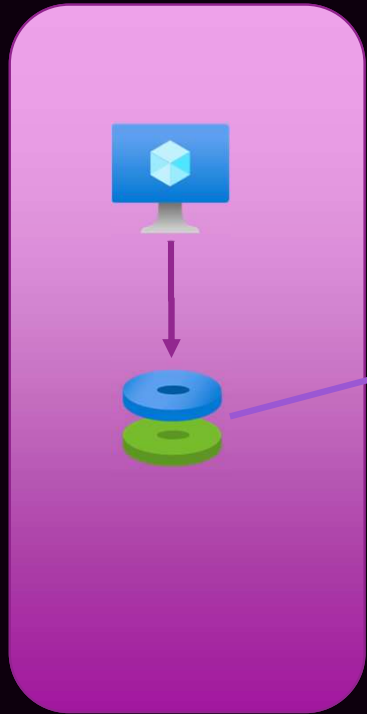
Agentless scanning for Machines

- ✓ Wide coverage within hours
- ✓ No performance impact, no connectivity required
- ✓ Transparent to workload owners

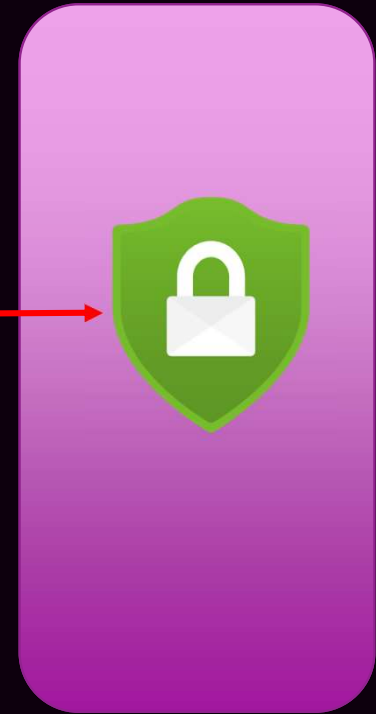
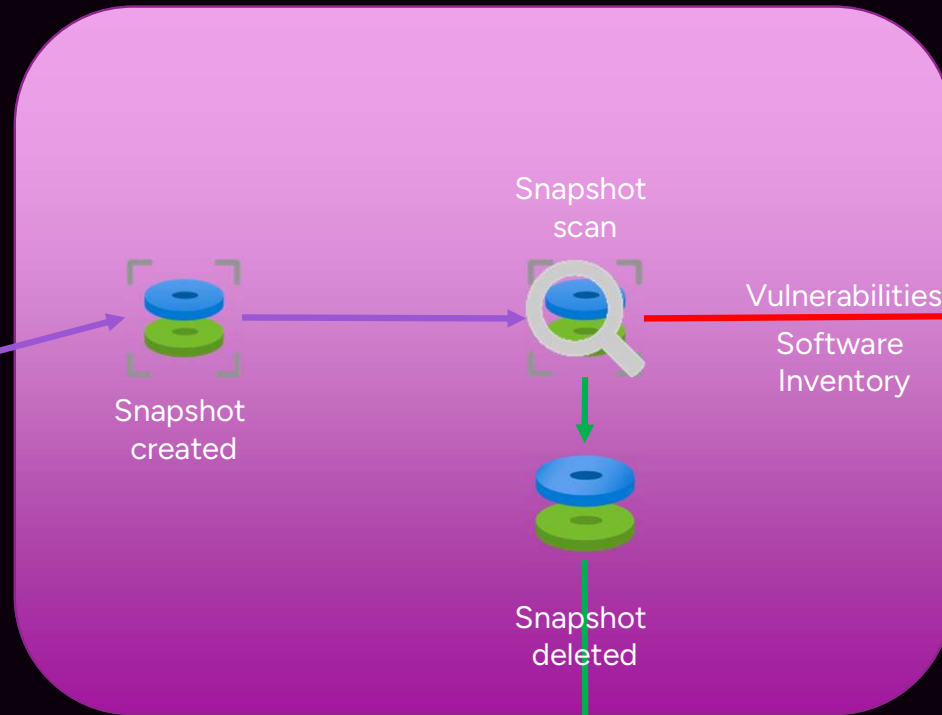


How Agentless scanning works

Customer Environment

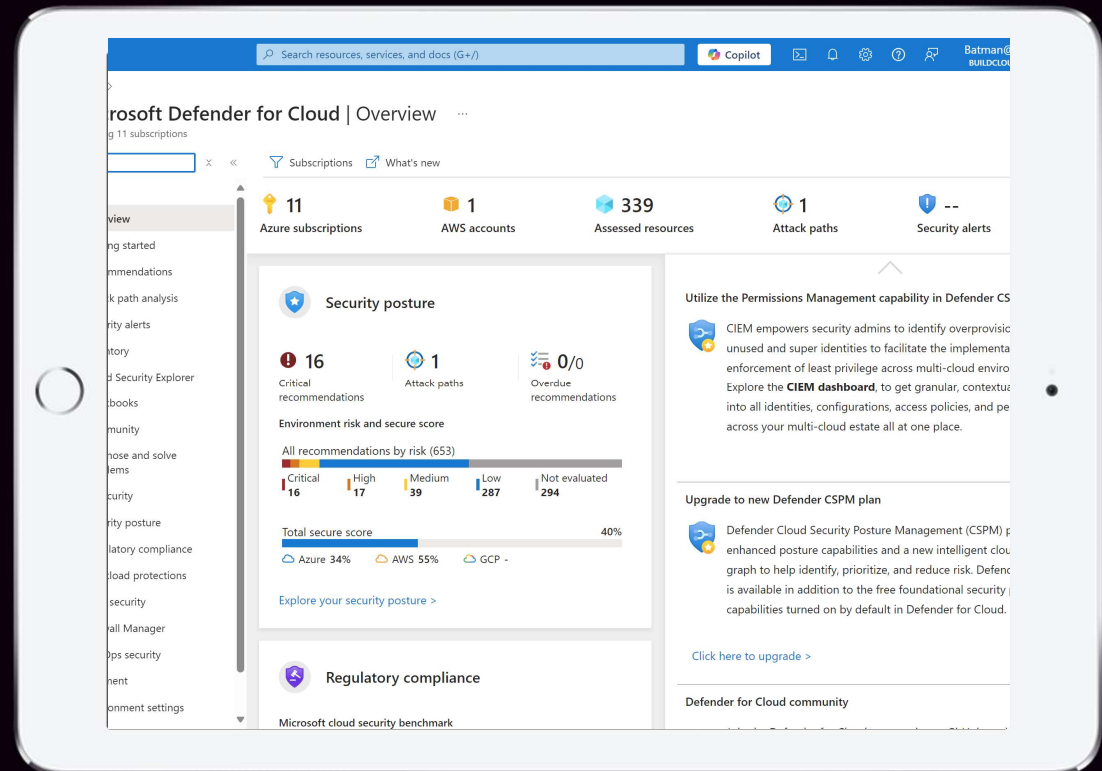


Isolated scanning Environment



Defender for Cloud

Demo Defender for CSPM



Hybrid security approach

Microsoft Defender for Endpoint

Deep OS visibility (processes, communications, etc.)

Realtime monitoring and detection of attacks

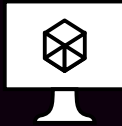
Active – ability to enforce policies, prevent, respond & remediate attacks

Agentless vulnerability scanning

At-scale, instantaneous visibility on OS posture issues

No performance impact on workloads

Security team does not depend on workload owners



VM secret scanning

VM secrets scanning

- Secrets scanning for VMs is agentless and uses cloud APIs
- After the Microsoft secrets scanning engine collects secrets metadata from disk, it sends them to Defender for Cloud
- The secrets scanning engine verifies whether SSH private keys can be used to move laterally in your network
- Supported with Defender for Server Plan 2 or CSPM



Cloud Security Explorer

Cloud Security Explorer



- proactively identify security risks in your cloud environment
- running graph-based queries on the cloud security graph
- Helps to query all of security issues like
 - assets inventory
 - exposure to internet
 - Permissions
 - lateral movement

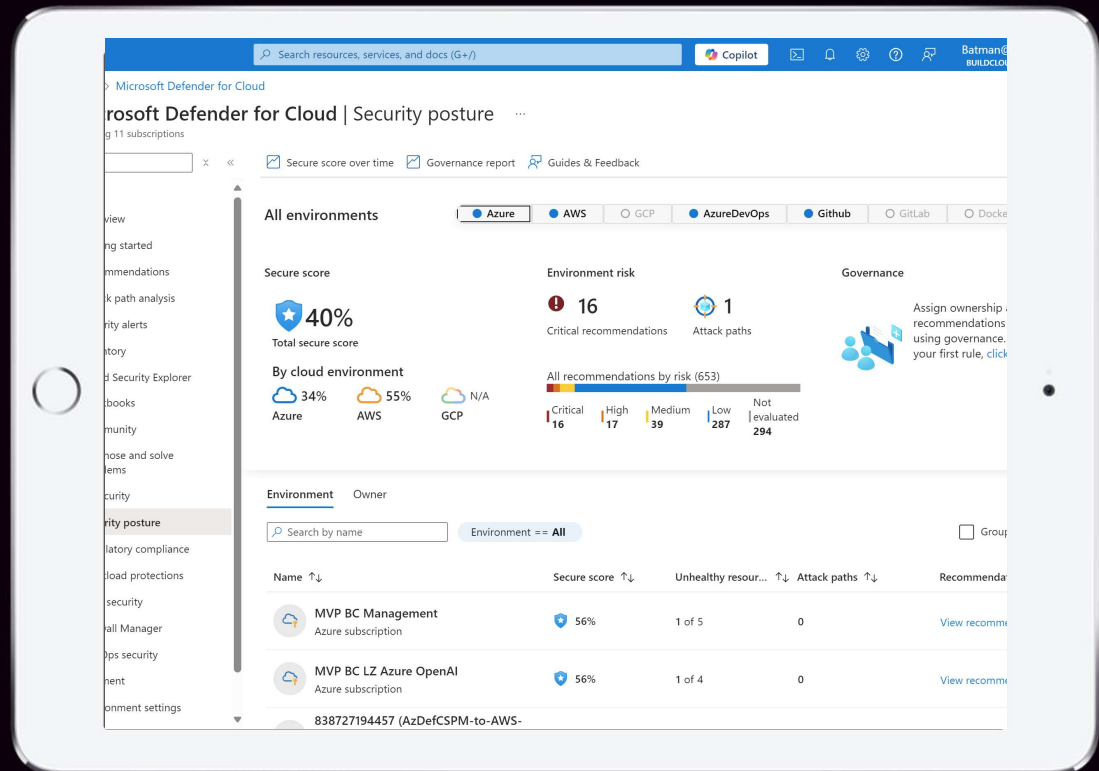


Attack Path analysis

Attack Path analysis

- Needs enabled agentless scanning
- detect potential attack paths based on security graph
- address security issues that pose immediate threats

Demo Cloud Security Explorer and more



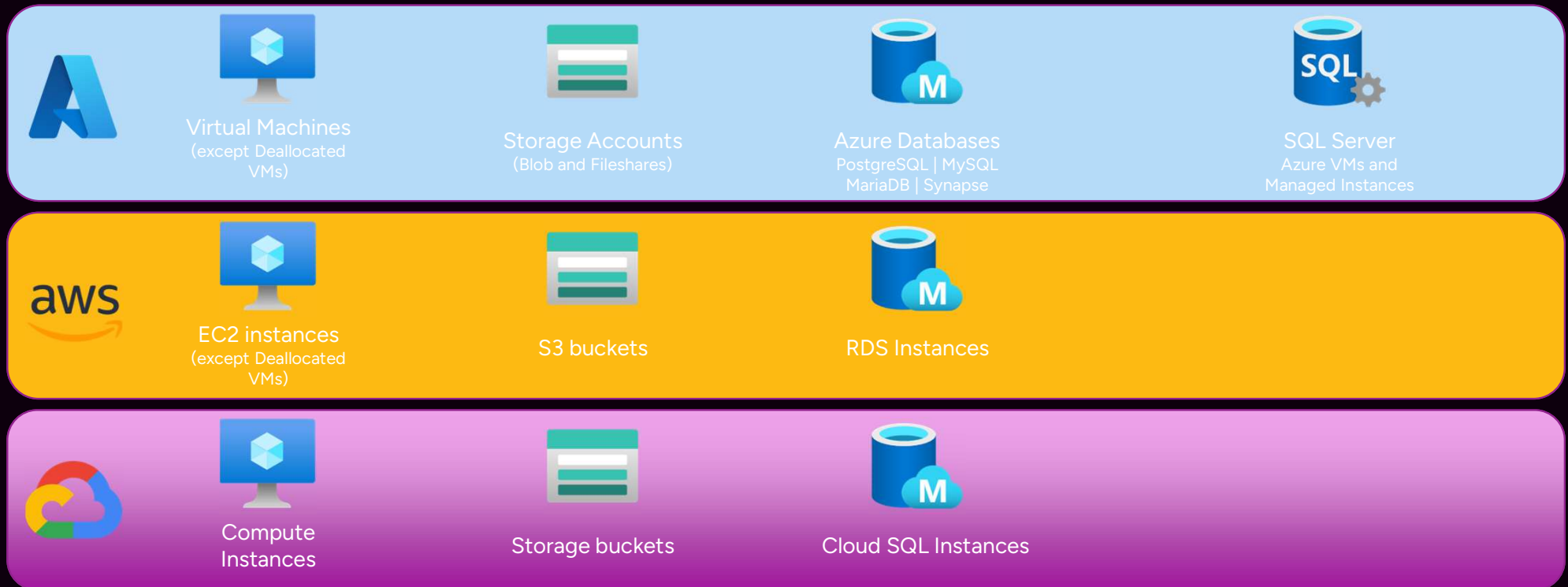
CIEM

Cloud Infrastructure Entitlement Management

- There are two types of CIEM available today
 - One as part of Defender for CSPM and the other one part of Entra permissions management
- Permissions discovery for risky identities (including unused identities, overprovisioned active identities, super identities) in Azure, AWS, GCP

Defender for CSPM Pricing

Billable workloads will be



Price **\$4.733** per **billable** resource/month

[Cloud Security Posture Management \(CSPM\) - Microsoft Defender for Cloud | Microsoft Learn](#)

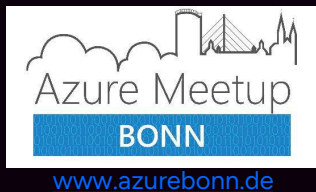
Recap

Recommendations

- Defender for CSPM is an great security addition
- Especially in Multi Cloud environments
- The actual pricing makes it an excellent addition under the following conditions
 - Between Azure one another Hyperscaler is in use
 - Infrastructure as Code is established or
 - DevOps and/or GitHub is used
- However, activation should take place step by step, just like the integration of other services (GitHub, DevOps...)

Links

- [Cloud Security Posture Management \(CSPM\) - Microsoft Learn](#)
- [Zero trust and Microsoft Defender for Cloud - Microsoft Learn](#)
- [Microsoft Defender for CSPM is GA – Information about activation, billing and new pricing information | Gregor Reimling](#)
- [GitHub - Azure/Microsoft-Defender-for-Cloud: Welcome to the](#)
- [Microsoft Defender for Cloud community repository](#)
- [Microsoft Defender PoC Series – Defender CSPM - Microsoft Community Hub](#)
- [Agentless scanning of cloud machines using Microsoft Defender for Cloud | Microsoft Learn](#)
- [Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn](#)
- [Join Our Security Community - Microsoft Community Hub](#)
- [Microsoft-Defender-for-Cloud/Policy/Enable Defender for Servers plans at main · Azure/Microsoft-Defender-for-Cloud \(github.com\)](#)
- [What's new in Microsoft Defender for Cloud features - Microsoft Defender for Cloud](#)



Blog

<https://www.Reimling.eu>

NIC
EMPOWER



Contact



- @GregorReimling



- Gregor Reimling