SQL KONFERENZ 2025



Top 10 Azure Security Best Practices

By Gregor Reimling



Gregor Reimling (he(him)

Chief Azure Technologist @ adesso SE, Germany

Gregor is awarded with the Microsoft MVP for Microsoft Azure and Security. He works as Chief Azure Technologist for adesso SE and is technical lead for Azure . His main areas are Microsoft Azure, Enterprise scale architectures, Cloud Security, Governance, Hybrid and Migration.

gregor@reimling.eu

reimling.eu

@GregorReimling

/in/GregorReimling

youtube.com/@GregorReimling

github.com/GregorReimling

Azure Meetup BONN

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

Microsoft MVP Most Valuable Professional

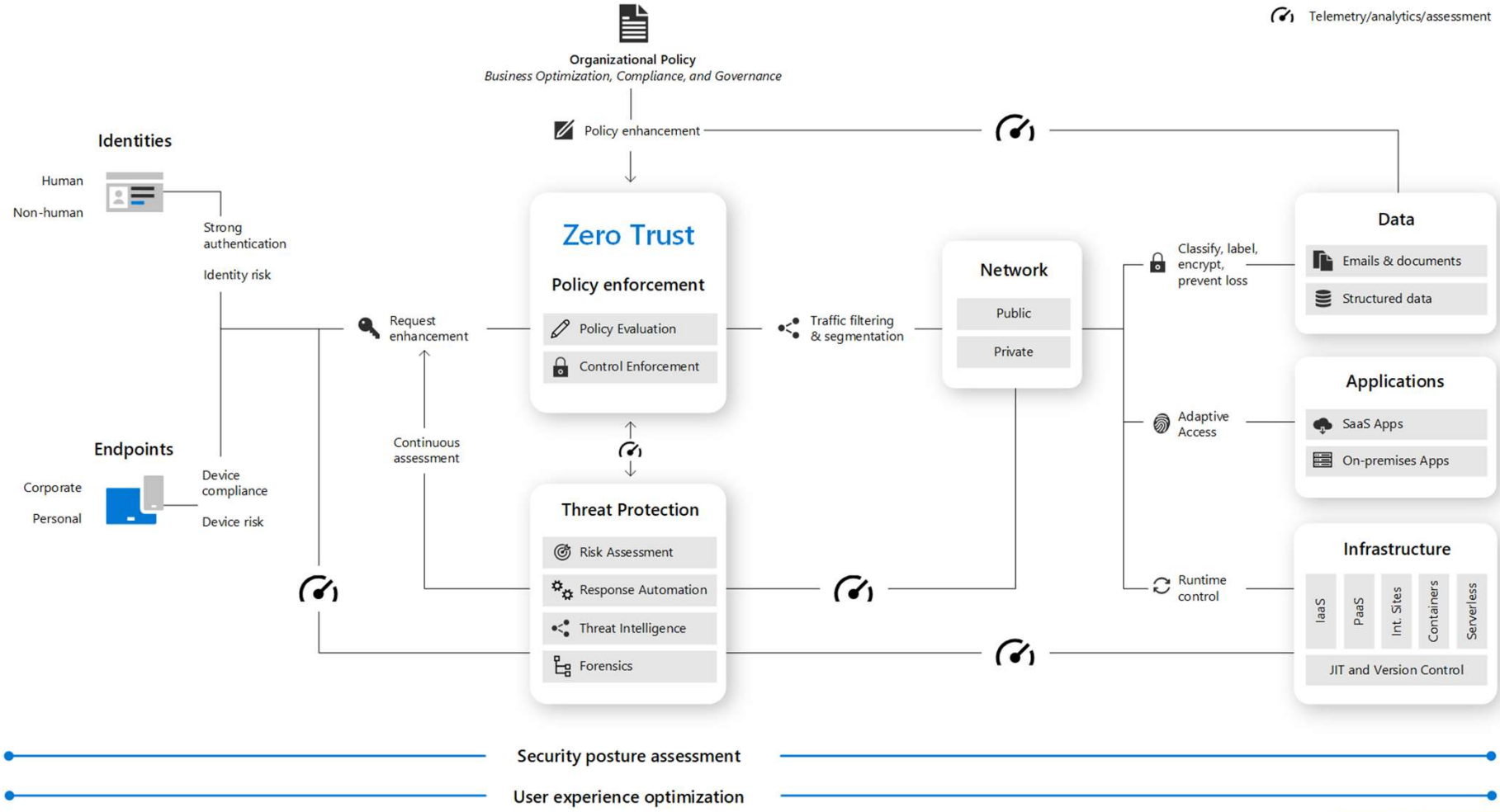


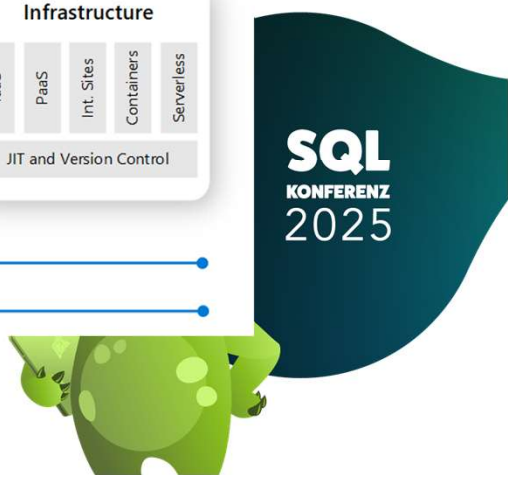
Agenda

- Entra ID Recommendations
- CAF and Enterprise Scale
- Defender for Cloud
- Azure Policy
- Azure Network Layer
- Azure Arc



Zero Trust architecture





SQL KONFERENZ 2025



Harden Identities

Entra ID recommendations

getting more intense

600 million

identity attacks per day…

Microsoft Entra data, Microsoft Digital Defense Report 2024

99%

are password attacks.

Microsoft Entra data, Microsoft Digital Defense Report 2024

111%

increase in token replay attacks.

Microsoft Entra data, How to break the token theft cyber attack chain, 2024.

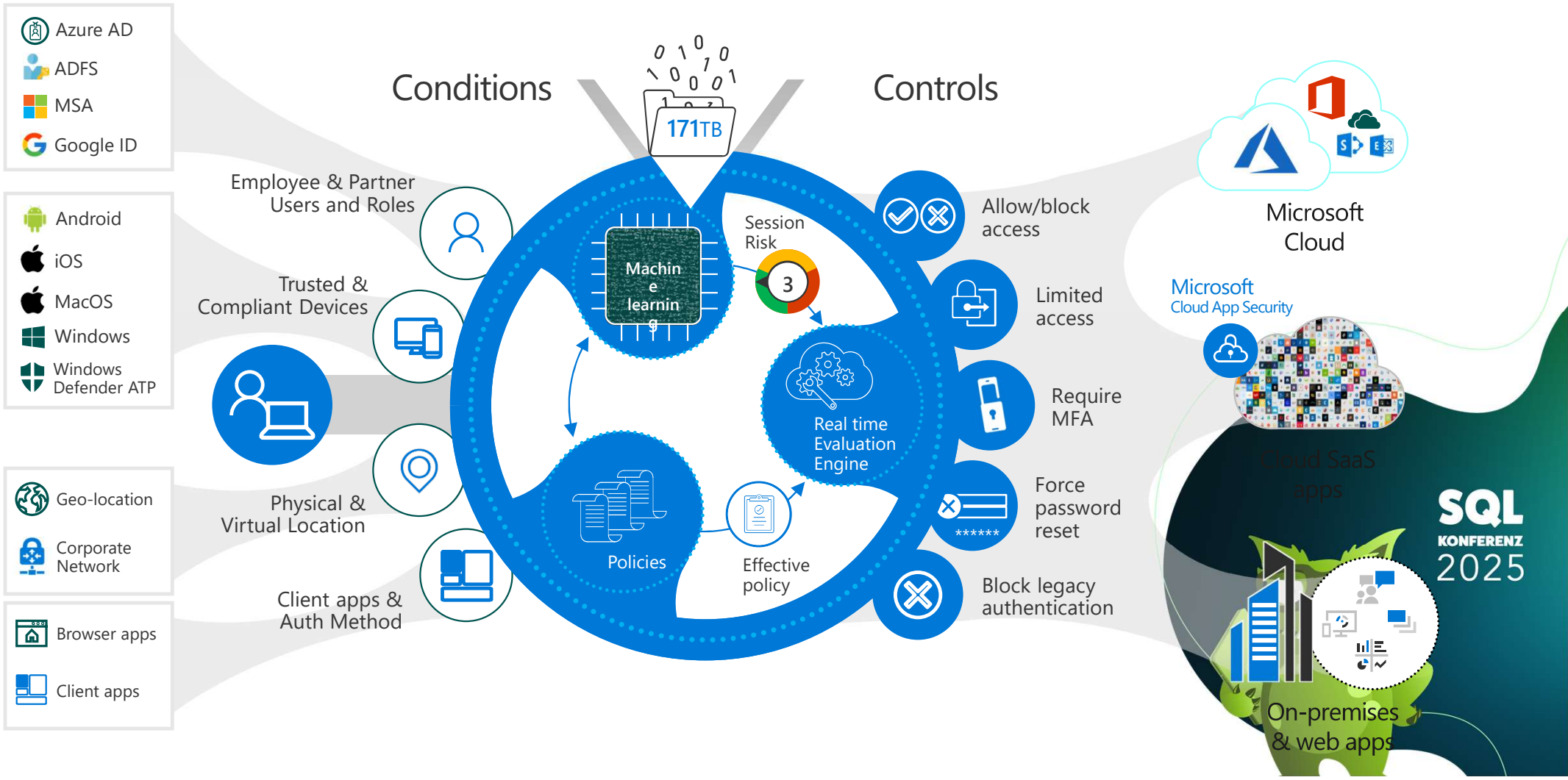
146%

rise in AiTM phishing attacks.

Microsoft Entra data, Microsoft Digital Defense Report 2024



1. Identity Protection with Conditional Access



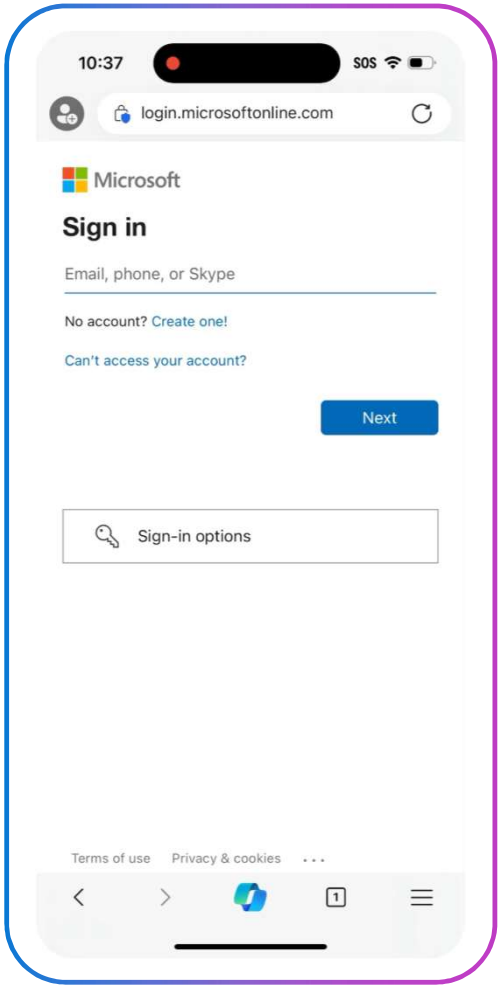
Poor	Fair	Better	Best
Password only	Password and...	Password and...	Phishing-resistant
123456	SMS	Microsoft Authenticator push notifications	Windows Hello for Business
admin	Voice	Software Tokens OTP	FIDO2 security key
quertyuiop		Hardware Tokens OTP	Certificate-based authentication (multifactor)
P@ssword2024!		Better	Platform credential for macOS
5%gHy*73xWcd#jQz89cn pGo!17		Passwordless	Passkey in Microsoft Authenticator (device-bound
		Microsoft Authenticator phone sign in	

Stronger authentication methods

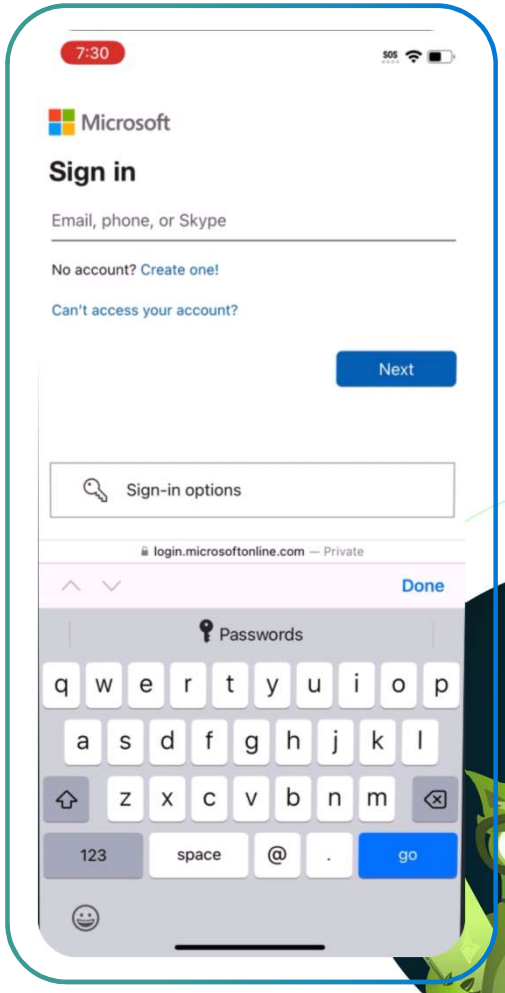


2. Passkeys





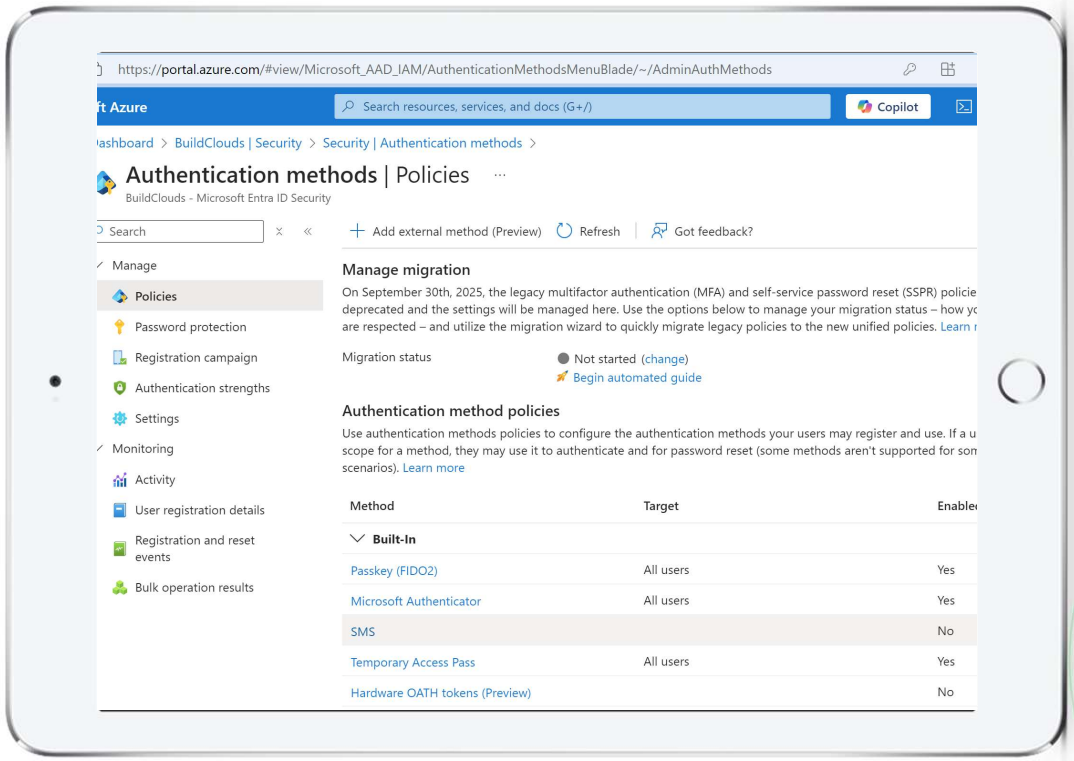
Passkey



Password



Demo
Identity Protection





3. Continuous Access Evaluation (CAE)

- Normally the grant token will store for 90 days on a device without need for relogin
  - Setup a CA for Sign-in frequency to enforce login more frequently as 90 days
- Conditional Access only works on Login
- No security after access is granted
  - CAE evaluate continuously the access and act on changes like
    - User termination
    - Network changes (VPN, new location, etc.)
    - Token export



PIM integration in Azure RBAC

New since 12/12/2024

So far Privilged access was only assignable on Entra ID roles

Now RBAC can be assigned on Azure RBAC roles directly



PIM for groups

Microsoft Entra Privileged Identity Management (PIM) enables just-in-time (JIT) access to the ownership or membership of the group.

Get free trial

Learn more about PIM

Enforce just-in-time access for owners and members of this group by requiring them to activate for a limited period of time. Create just-in-time access policies for these users like approval workflow, MFA challenge and much more.

Activate more in less time

Assign multiple roles to a single group so that users only need to activate once to get all the permissions they need.

[Microsoft Entra releases and announcements - Microsoft Entra | Microsoft Learn]

SQL KONFERENZ 2025



Harden Azure Environments

CAF & Enterprise Scale

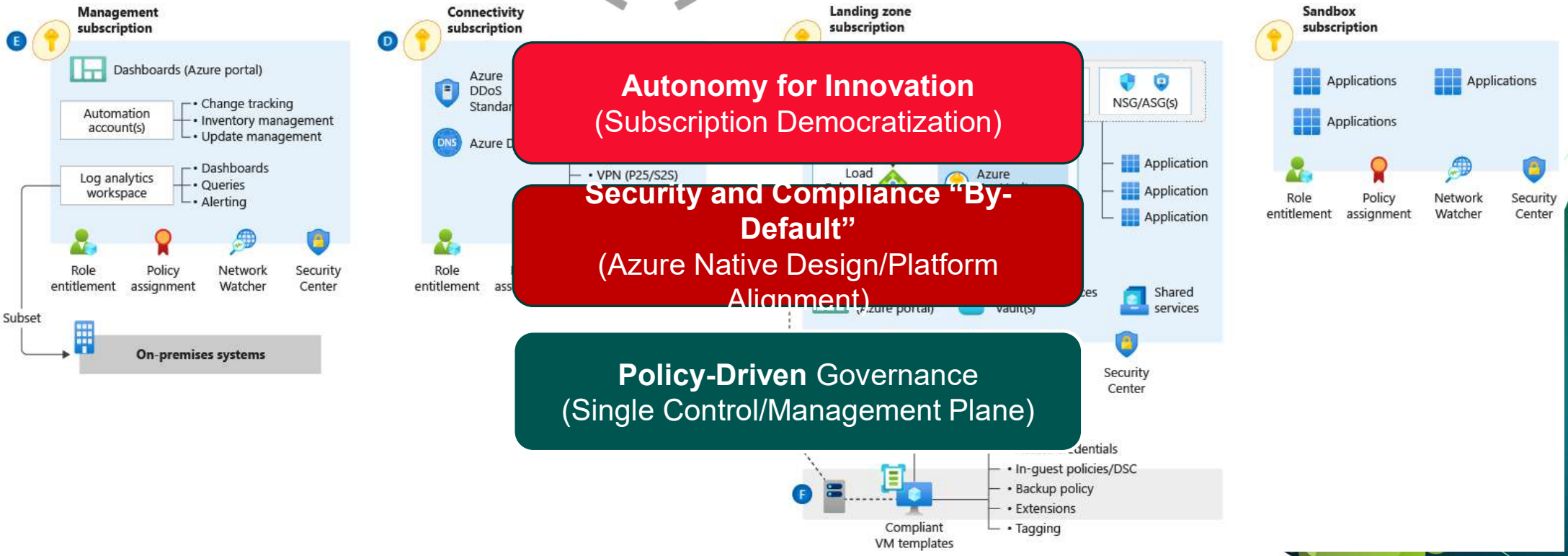
Azure Verified Modules

4. Enterprise-Scale - Design Principles

Tenant Root Group

Build Clouds





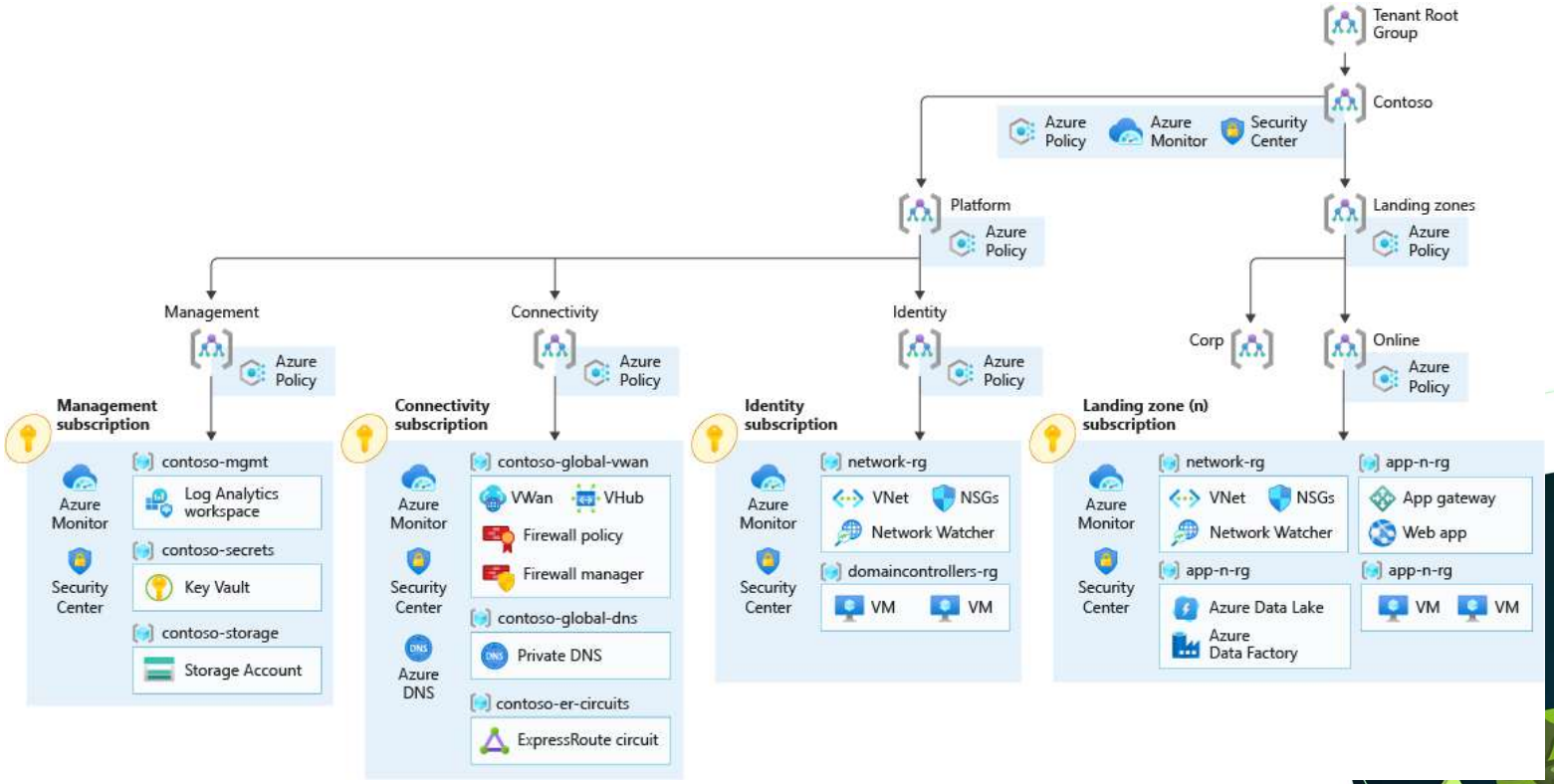
Autonomy for Innovation
(Subscription Democratization)

Security and Compliance "By-Default"
(Azure Native Design/Platform Alignment)

Policy-Driven Governance
(Single Control/Management Plane)

GitHub Enterprise Scale Templates

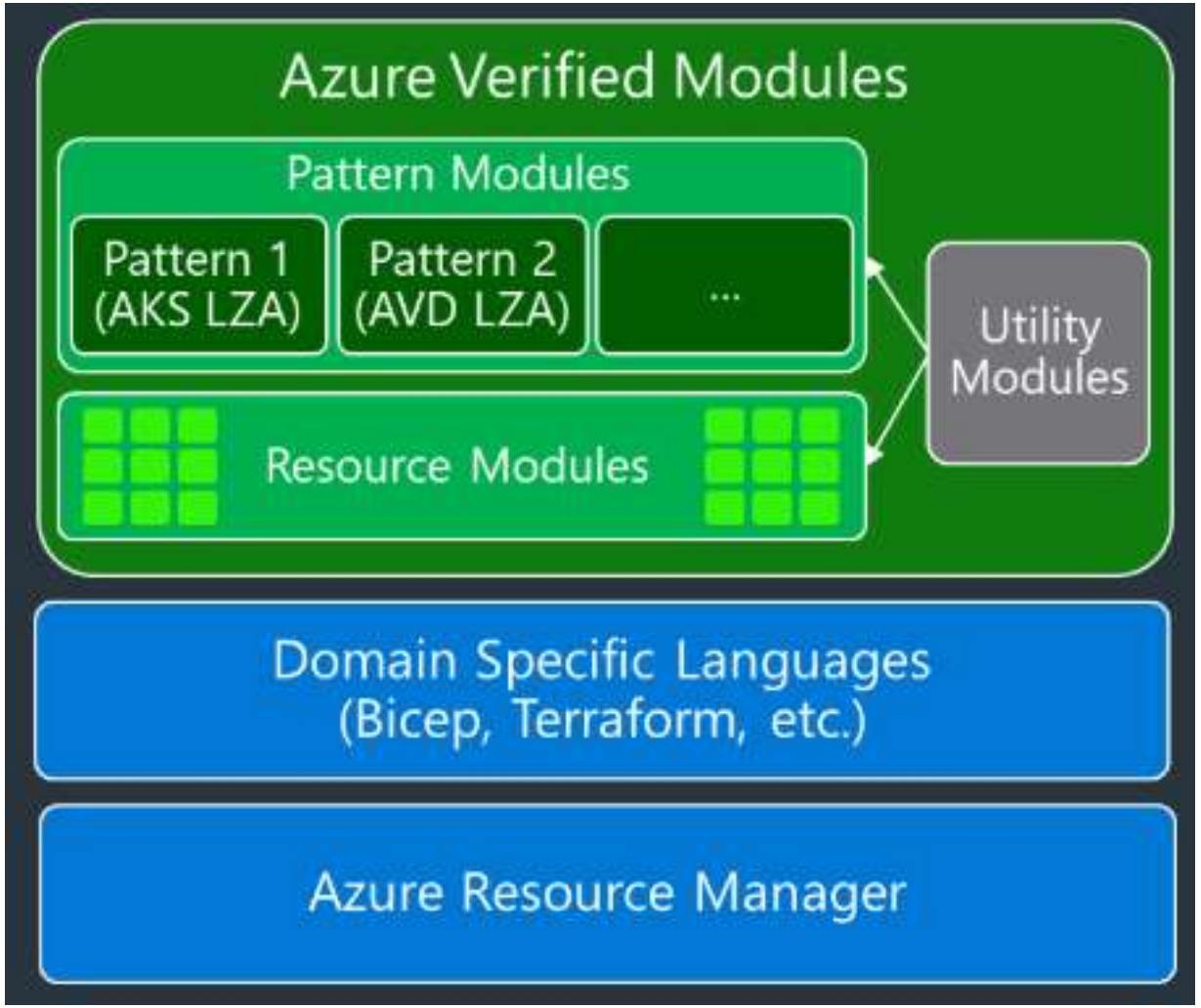
Deploy Enterprise-Scale with Azure VWAN



[GitHub - Azure/Enterprise-Scale: The Azure Landing Zones (Enterprise-Scale) architecture provides prescriptive guidance coupled with Azure best practices, and it follows design principles across the critical design areas for organizations to define their Azure architecture]



Use Azure Verified Modules (AVM)





5. Manage Subscription Policies

Subscriptions | Manage policies ···

Feedback

Configure policy settings for Azure subscription operations.

Subscription leaving AAD directory:

This policy controls if users can change the AAD directory of Azure subscriptions from this directory to a different one. Learn more

- (•) Allow everyone (default)
- ( ) Permit no one

Subscription entering AAD directory:

This policy controls if users can bring Azure subscriptions from a different AAD directory into this directory. Learn more

- (•) Allow everyone (default)
- ( ) Permit no one

Exempted Users

These are special users who can bypass the policy definitions and will always be able to take subscriptions out of this AAD directory or bring subscriptions into this one.

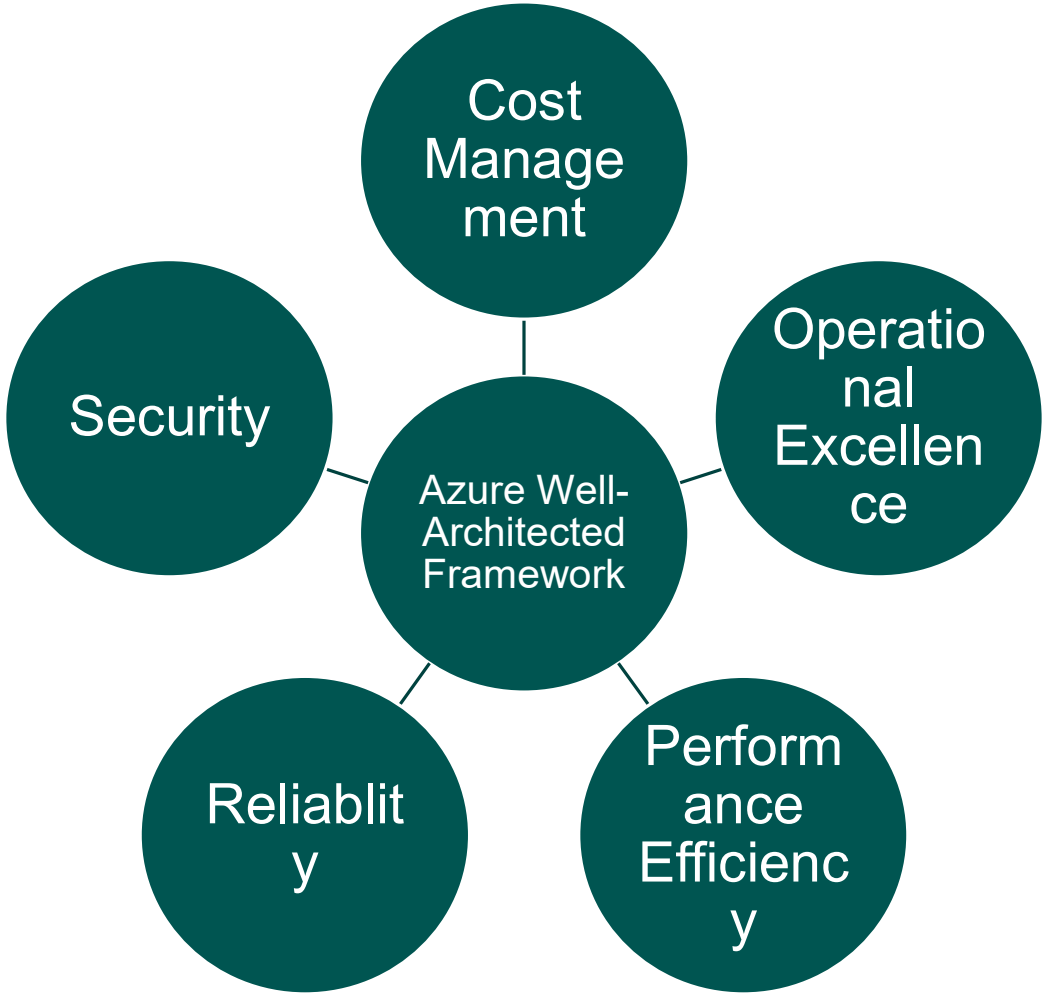
Search user name or email: Search by name or email address

Can be configured in the Overall subscription blade



Well-architected Framework

"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."

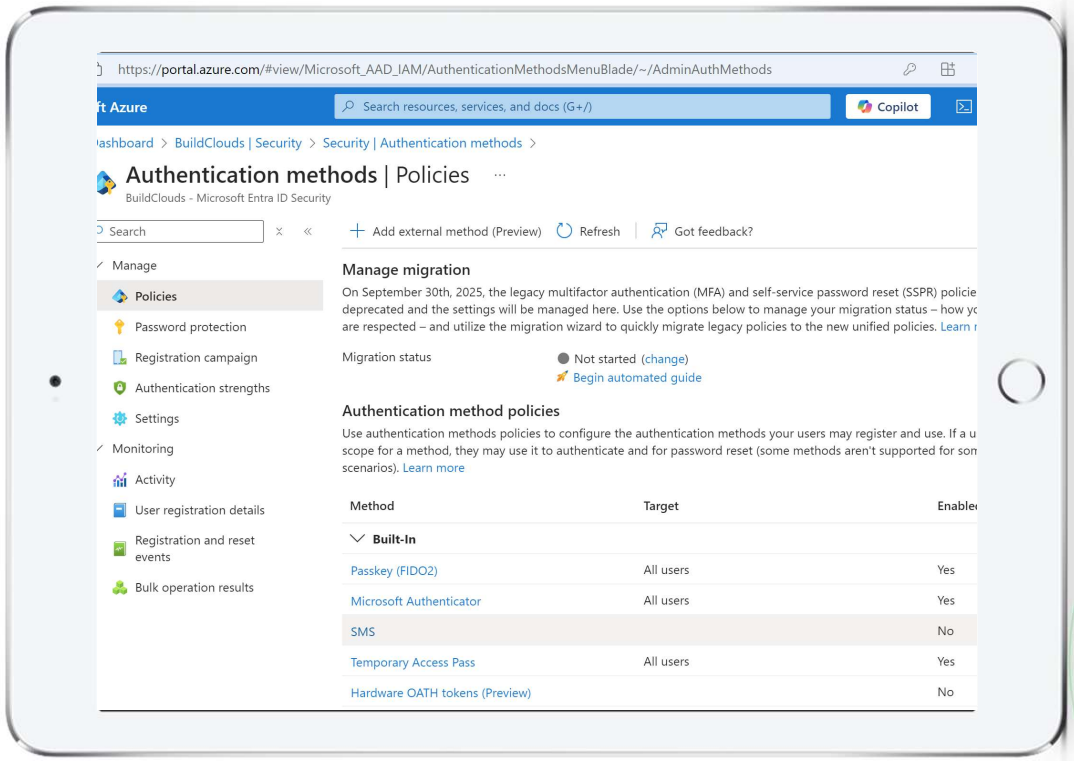


Azure Advisor



https://docs.microsoft.com/en-us/azure/architecture/framework/

Demo Enterprise Scale





SQL
KONFERENZ
2025



Azure Policy

Define guardrails with Azure Policy

6. Leverage built-in initiative & policies



Security

Azure Security Center

Guest Config

baselines

Key Vault certificate

NSG rules

AKS & AKS Engine

RBAC role

assignment



Regulatory Compliance

NIST SP 800-53 R4

ISO 27001:2013

CIS

PCI v3.2.1:2018

FedRAMP Moderate

Canada Federal PBMM

SWIFT CSP-CSCF v2020

UK Official and UK NHS

IRS 1075



Tags

Require specified tag

Add or replace a tag

Inherit a tag from the

RG

Append a tag



Resource standardization

Allowed/ not allowed

RP

Allowed locations

Naming convention

Back up VMs

Allowed images for

AKS



Cost

Allowed VM SKUs

Allowed Storage

SKUs

Demo

Azure Policy

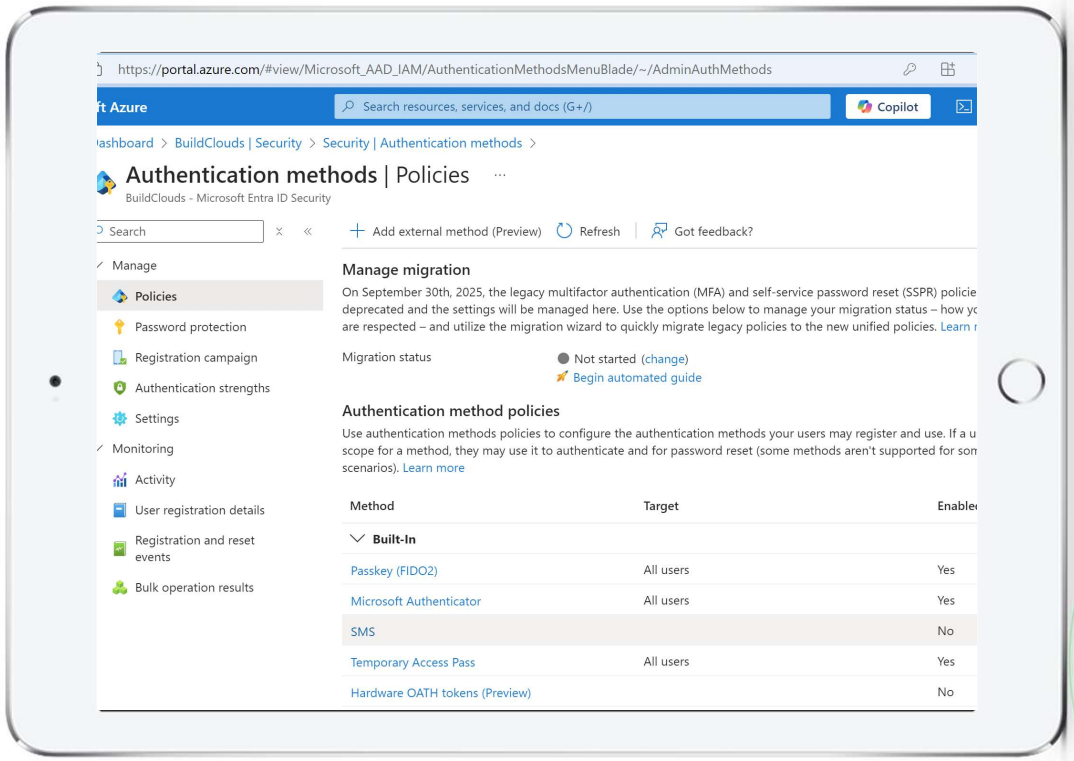
E4 v5 = 333,56€

E48_v5 = 4002,70€

Deny Public Ips

Deny VNET usage without NSGs

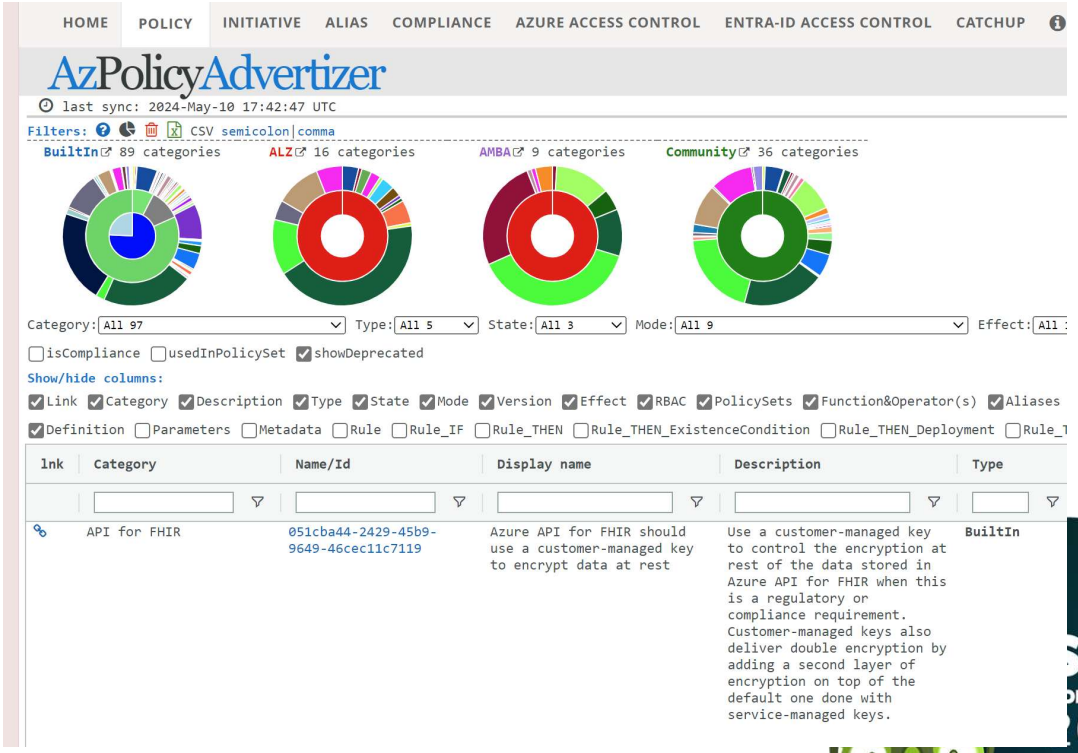
Deny Public Storage Accounts





Who knows AzAdvertizer?

- Is a free tool which helps to get an overview about new Azure Gov capabilities
- Informed about new releases, updates and deprecation:
  - of Policy Definition and Initiatives
  - of Landing Zone updates
  - For Azure RBAC changes
  - And more





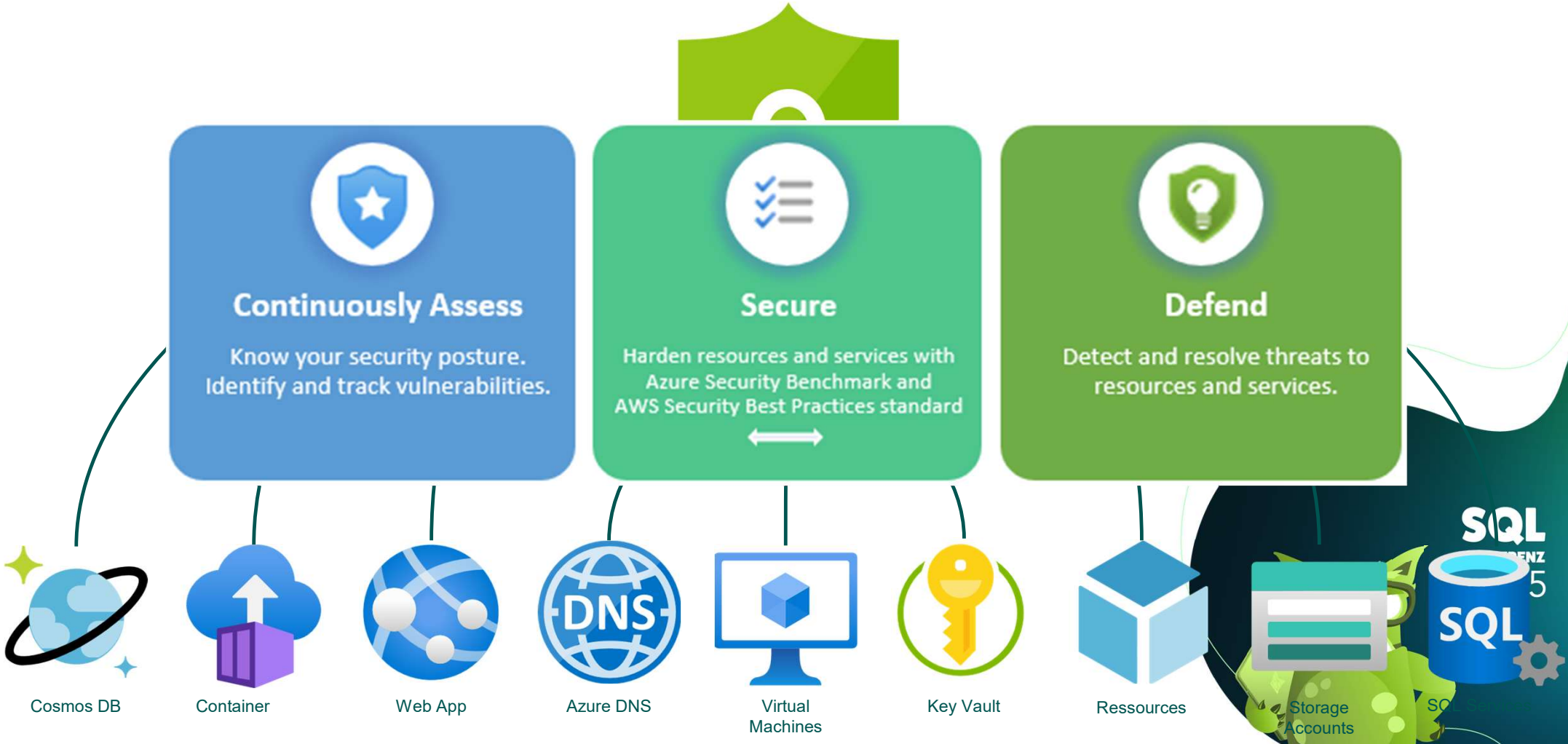
SQL KONFERENZ 2025



Enable Defender for Cloud

Evaluate Defender for Cloud Plans

7. Microsoft Defender for Cloud



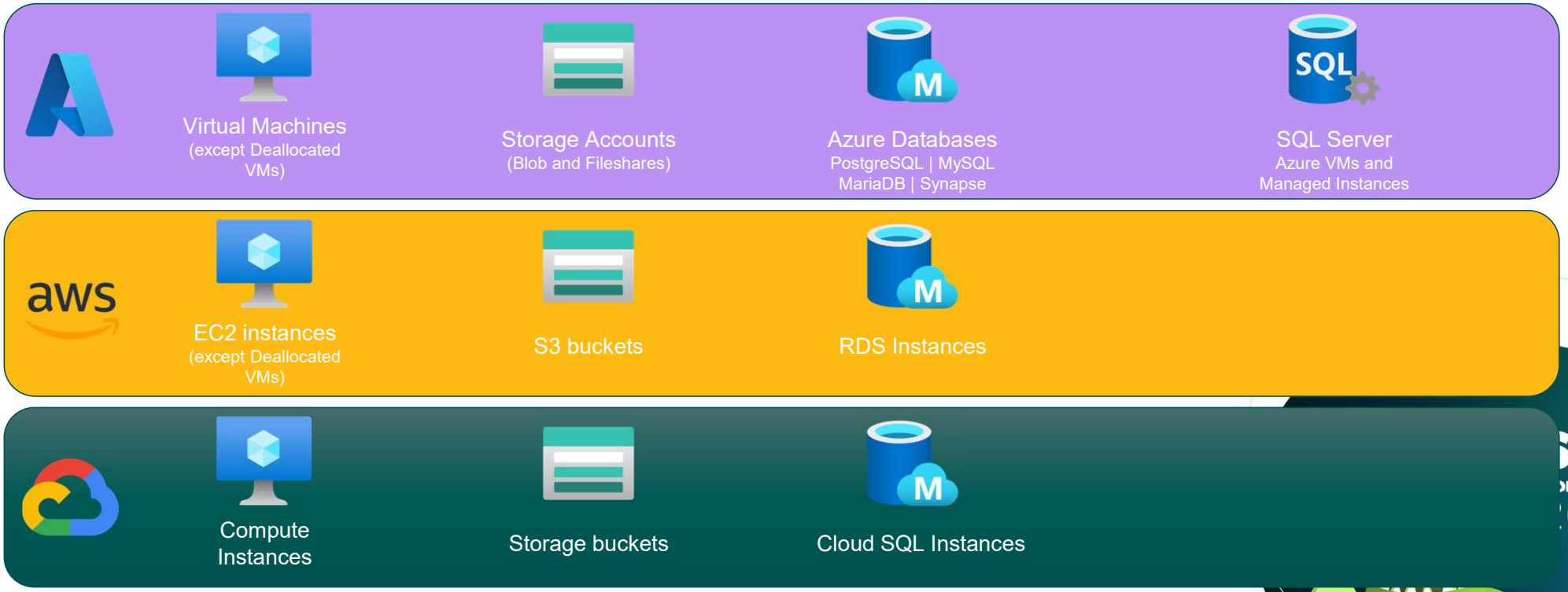
MS Defender for Cloud



Security posture & compliance	Secure score	Asset management	Policy
Server protection (Microsoft Defender for Cloud for VMs)	Threat detection	VA (power by Qualys)	Application control
Automation & management at scale	Automation	SIEM integration	Export

Defender for CSPM

Billable workloads will be

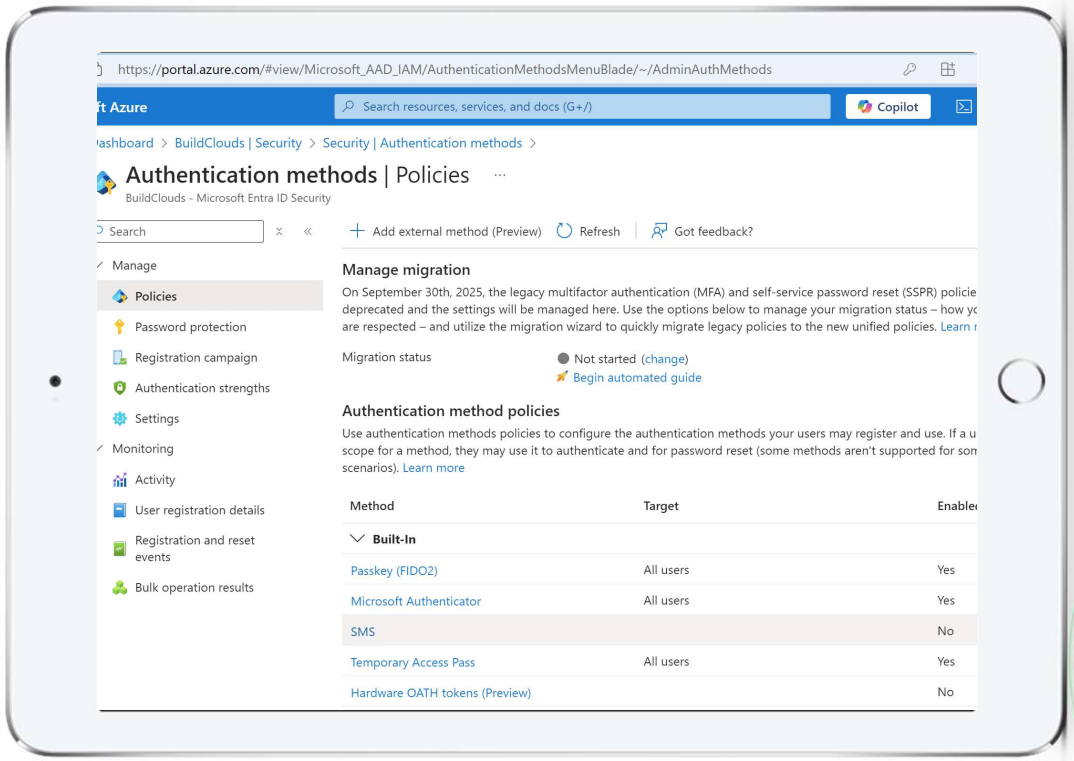


Price $4.733 per **billable** resource/month

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

Demo

Defender for CSPM





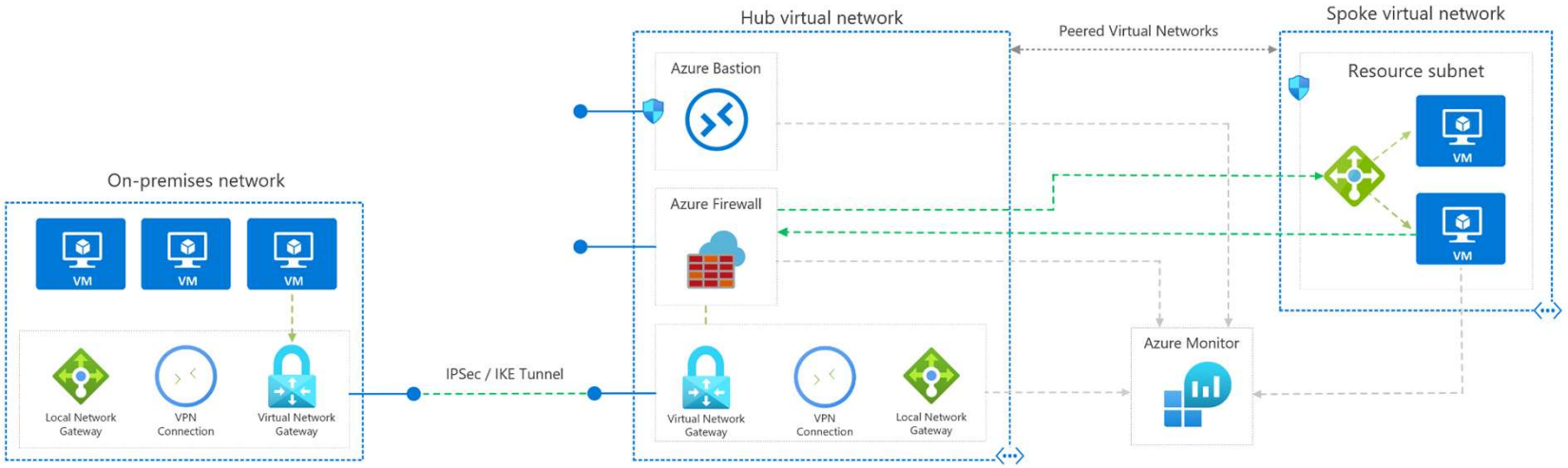
SQL KONFERENZ 2025



Harden Azure Network

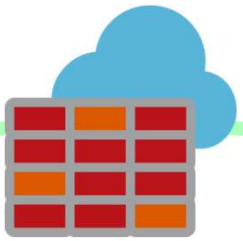
Think on the Network

8. Network - Hub and Spoke





8. Network - Azure Firewall



Azure Firewall Basic
2 VMs fixed under the hood
Availability Zones
App FQDN Filtering Rules?
Fixed Scale
Threat Intelligence (Alert Mode only)
FQDN in Network rules
250-500MBps
Around 300€

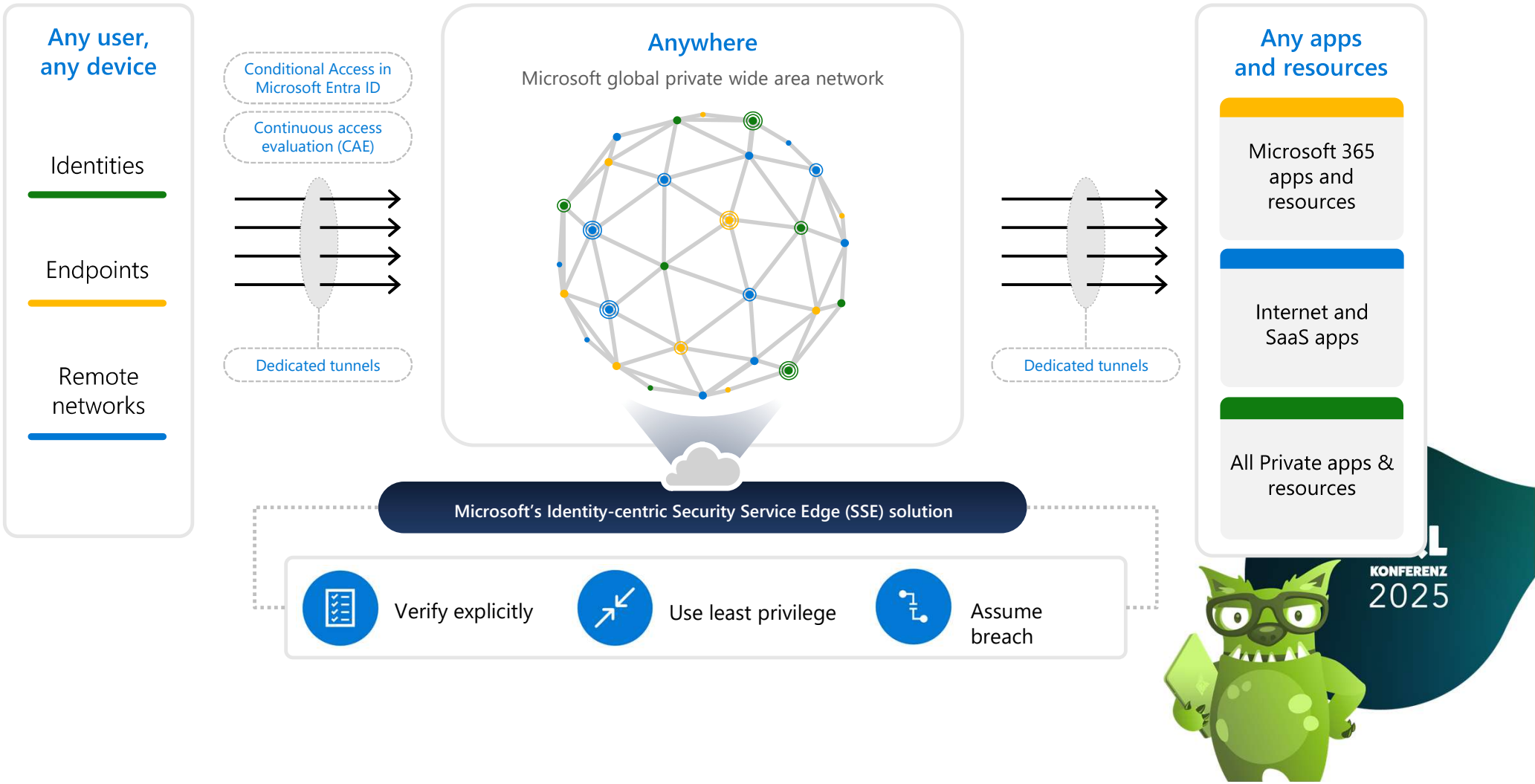
Azure Firewall Standard
Built-in high availability
Availability Zones
Application FQDN Filtering Rules
Unrestricted Cloud Scalability
Threat Intelligence
FQDN in Network rules
30GBps
901,24€ per month

Azure Firewall Premium
All from Standard +
TLS Inspection
IDPS
URL Filtering
Web categories
FQDN in Network rules
30GBps
1.262,29€ per month



SQL KONFERENZ 2025

Microsoft's Identity-centric SSE solution



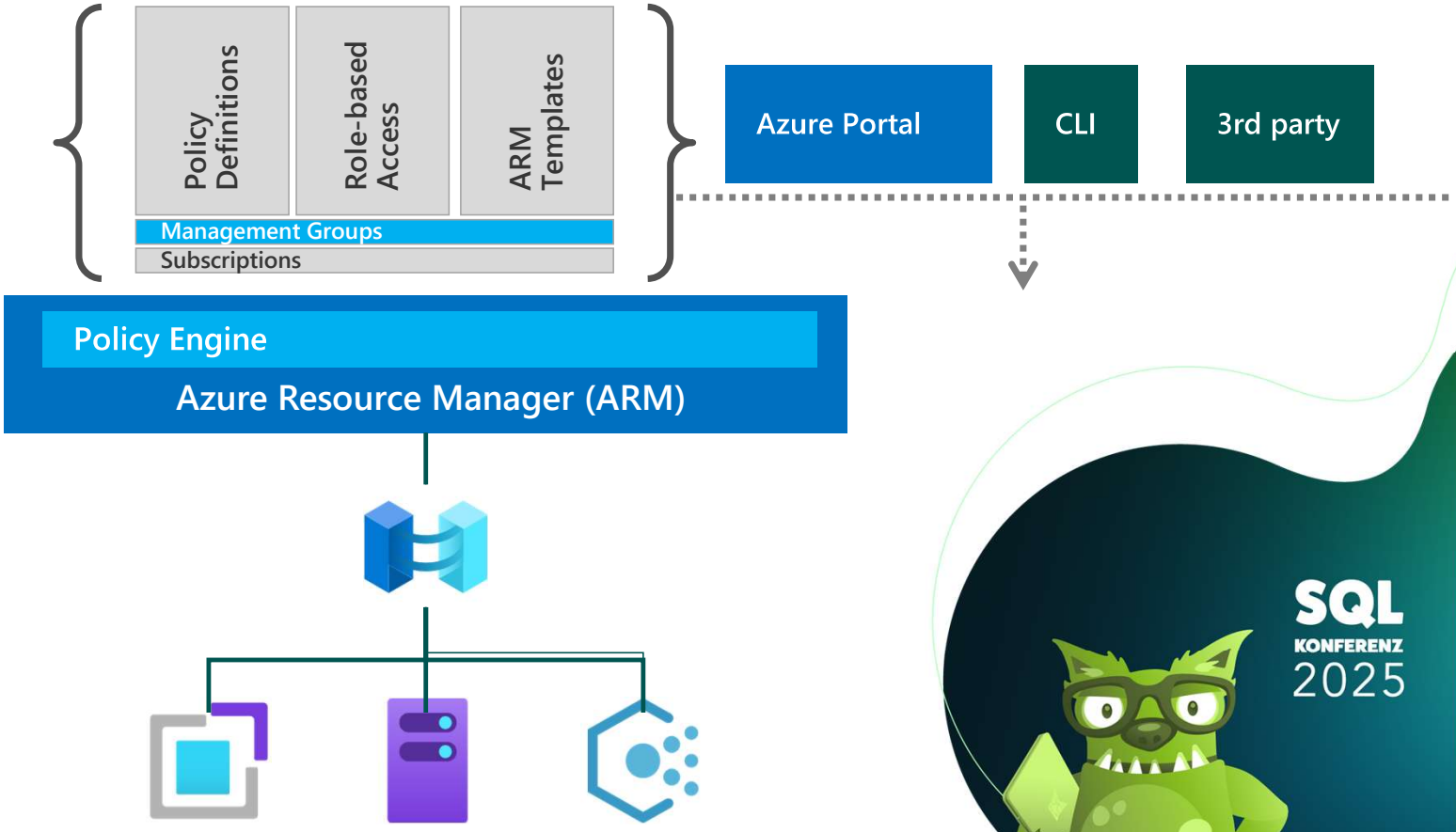
9. Azure Arc

providing control over the cloud environment, without sacrificing developer agility

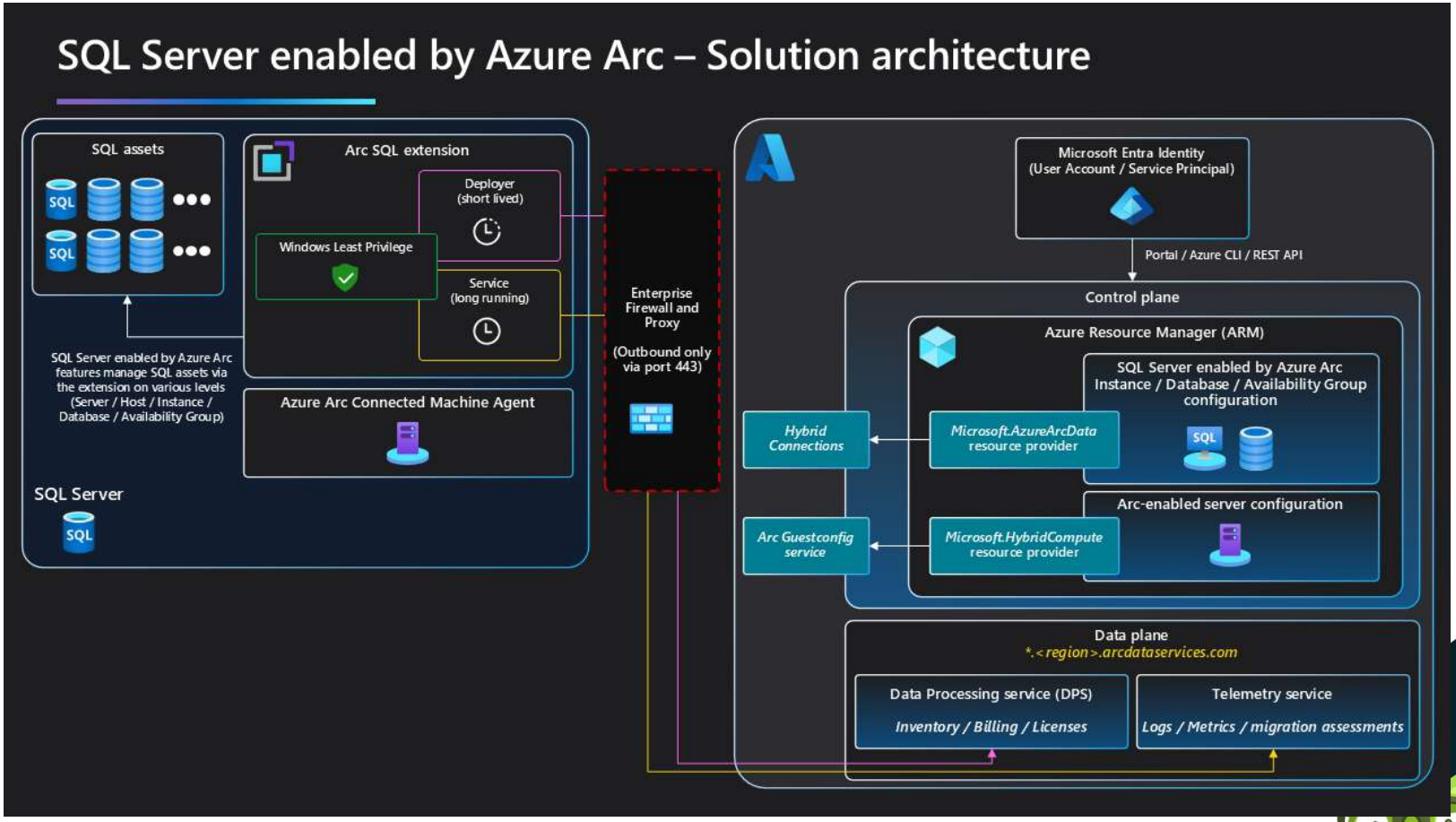
1. Environment Factory: Deploy and update cloud environments in a repeatable manner using composable artifacts

2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

3. Resource Visibility: Query, explore & analyze cloud resources at scale



SQL Server enabled by Azure Arc – Solution architecture





SQL KONFERENZ 2025

SQL Server with Azure Arc

- Central pane of glass for all SQL Servers
  - Name, Version, Cores and more
  - Query of all Servers with Azure Resource Graph
- Best Practices Assessment
- Pay-as-you-Go for SQL Server
- Extended Security Updates (ESU)
- Migration assessment



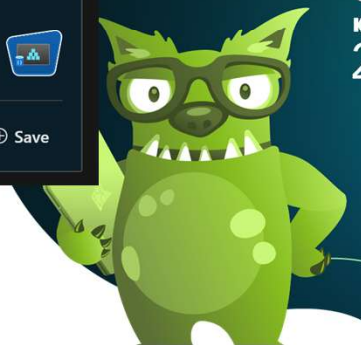
SQL
KONFERENZ
2025



Summary

10. Learning





SQL KONFERENZ 2025

Conditional Access → PIM for Azure RBAC → Token Security & CAE → Tenant Security

↓

CAF & Enterprise Scale → Azure Verified Modules → Define guardrails with Azure Policy → Enable Defender for Cloud

↓

Harden Azure Network Layer → Learning



Links

- Reimling.eu – Microsoft will disable Basic auth – What this means and what you have to do
- New Identity Secure Score recommendations in General Availability | Microsoft Community Hub
- Reference table for all data security recommendations in Microsoft Defender for Cloud
- Common Conditional Access policies - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Configure a TAP in Azure AD to register Passwordless authentication - Microsoft Entra | Microsoft Docs
- Azure AD Connect: Version release history - Microsoft Entra | Microsoft Docs
- Zero Trust security in Azure | Microsoft Docs
- Enterprise-Scale/README.md at main · Azure/Enterprise-Scale · GitHub
- Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs
- Azure Arc | Microsoft Learn
- Update management center (preview) overview | Microsoft Docs
- Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
- Join Our Security Community - Microsoft Tech Community
- Managed identities for Azure resources - Microsoft Entra | Microsoft Learn
- Microsoft Certified: Azure Security Engineer Associate - Certifications | Microsoft Learn



Please rate this session!

Your feedback will help with

- speaker evaluation
- content relevance
- decision making for future events
- quality improvement

Conference Feedback

Session Feedback





Thank you!

Gregor Reimling

gregor@reimling.eu

reimling.eu

@GregorReimling

/in/GregorReimling

youtube.com/@GregorReimling

github.com/GregorReimling

Azure Meetup BONN

Cloud Inspires Podcast
Stories and people behind Cloud Transformation

Microsoft MVP Most Valuable Professional

Azure & Security SQL KONFERENZ 2025

