

Azure Governance Best Practices

by Thomas Naunheim & Gregor Reimling

Gregor Reimling



Cloud Consultant @Sepago

 Cloud and Datacenter, Governance

 Azure Infrastructure (Governance, IaaS, Security)

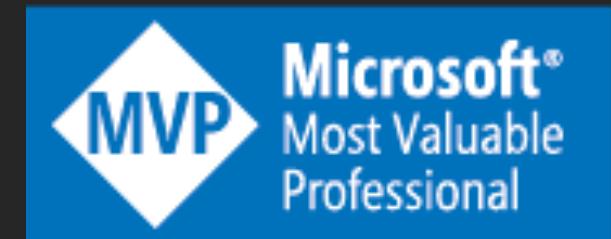
 info@reimling.eu

 @GregorReimling | @AzureBonn

 www.reimling.eu | www.neutralien.com

Identity Summit 2020
follow

 @IdentitySummit



www.AzureBonn.de

Thomas Naunheim



-  Cloud Engineer
(Identity + Azure Security)
-  Azure Cloud Platform, PaaS, Security
-  thomas@naunheim.net
-  @Thomas_Live | @AzureBonn
-  www.cloud-architekt.net

Identity Summit 2020
follow
 @IdentitySummit

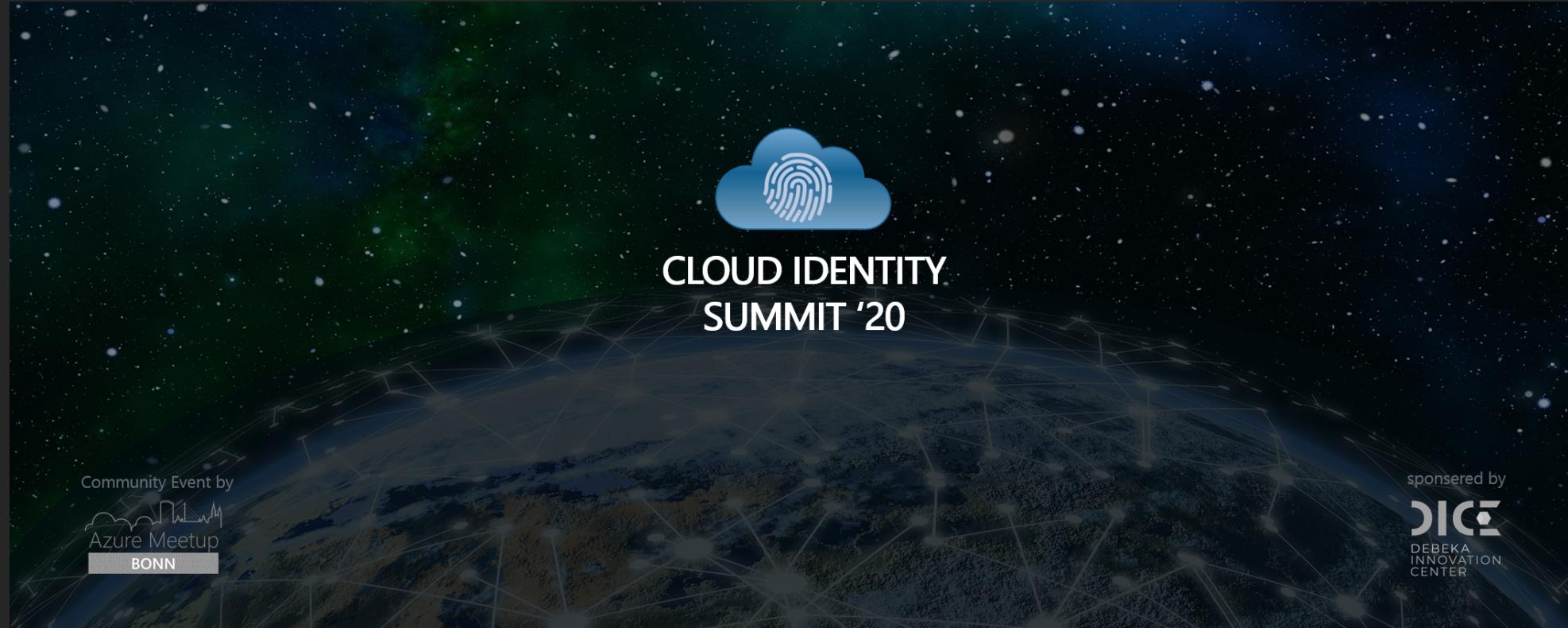


www.AzureBonn.de

Azure Bonn – Event Tipps

- 04.09. – SharePoint Saturday Cologne (Online)
 - <https://www.meetup.com/de-DE/Office-365-Meetup/events/269623756/>
- 10.09. – Manage Hybrid Environments with Azure Arc by Thomas Maurer
 - <https://www.meetup.com/de-DE/Azure-Bonn-Meetup/events/272462127/>
- 24.09. – Rdbuzz Late Night Show zur MS Ignite 2020 (Azure CGN)
 - <https://www.meetup.com/de-DE/Office-365-Meetup/events/272661417/>
- 06.10. – Azure Ignite Recape (Anmeldung möglich – aktuell in Planung)
 - <https://www.meetup.com/de-DE/Azure-Bonn-Meetup/events/257995108/>
- 08.10. – Datacenter migration with Sarah Lean (Azure CGN)
 - <https://www.meetup.com/de-DE/Azure-Cologne-Meetup/events/272236551/>
- 20.10. – Azure Architecture Best Practice by Thomas Maurer & Dominik Zemp
 - <https://www.thomasmaurer.ch/2020/09/azure-architecture-best-practices-virtual-event-october-20/>
- Many more @ Techwiese Events
 - <https://www.microsoft.com/de-de/techwiese/events/default.aspx>

Cloud Identity Summit 2020



<https://www.identitysummit.cloud/>

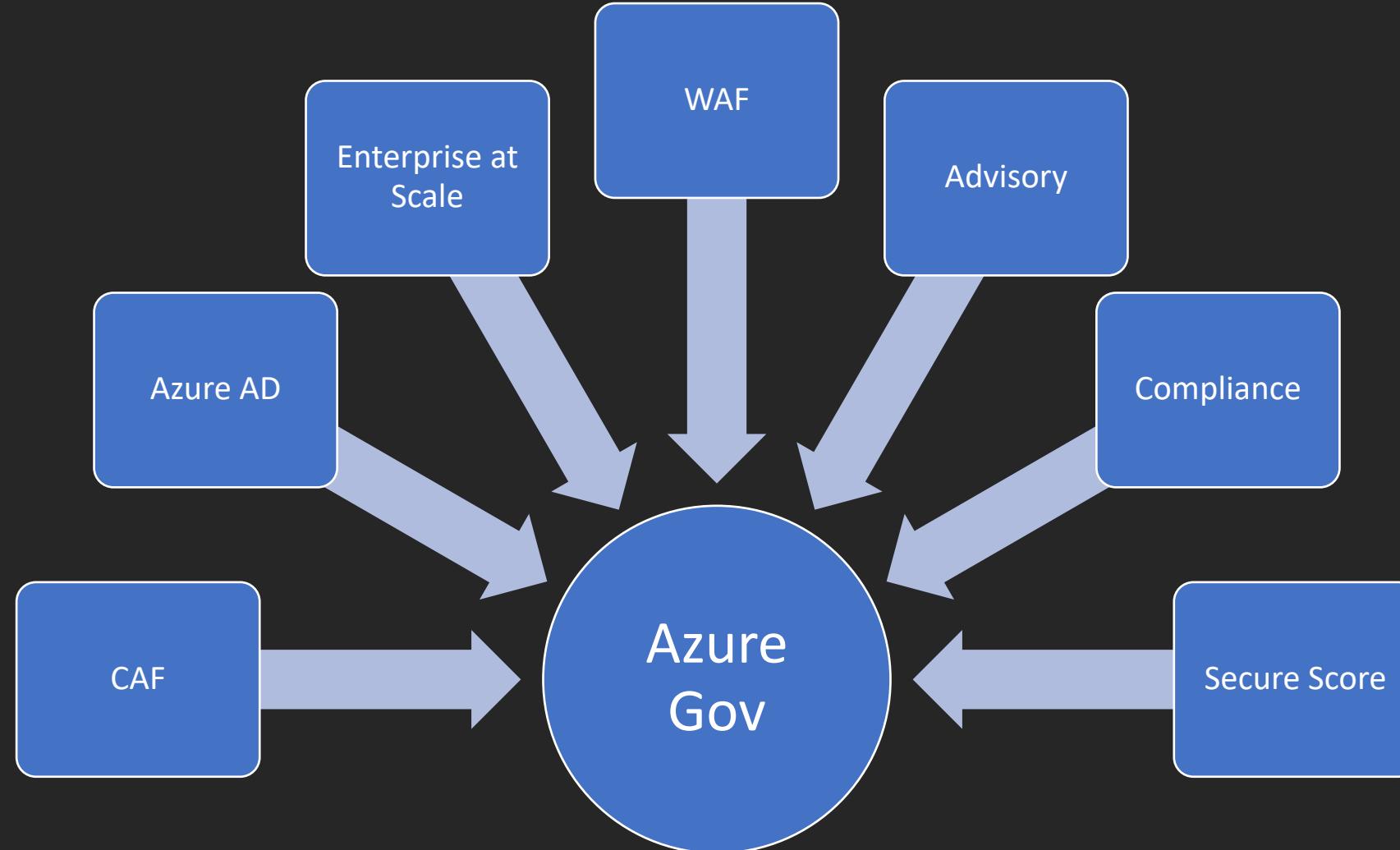
Agenda

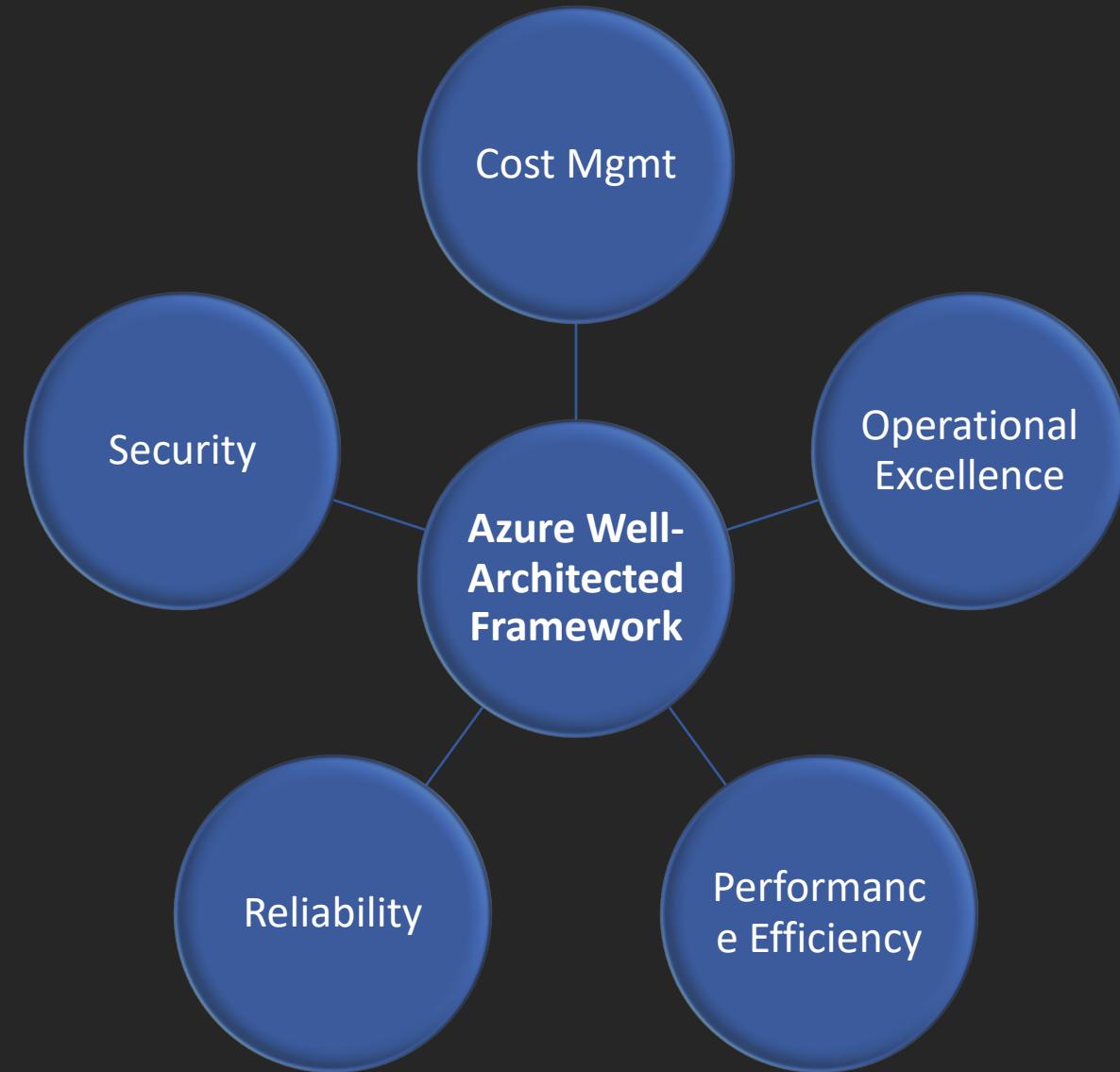
- Overview Architecture Recommendations and Best Practices
- Technical Implementations
- Management of Security and Compliance Status
- Azure Enterprise-Scale Landing Zones
- Secure Azure Environments with Azure AD (RBAC)



Overview of Architecture Recommendations

Topic Overview





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

Microsoft Assessments

Azure Well-Architected Review

Security

- What design considerations did you make in your workload in regards to security?
- What considerations for compliance and governance do you need to take?
- How are you managing encryption for this workload?
- How are you managing identity for this workload?
- How have you secured the network of your workload?
- What tradeoffs do you need to make to meet your security goals?
- How are you ensuring your critical accounts are protected?

Examine your workload through the lenses of reliability, cost management, operational excellence, security and performance efficiency [20 minutes].

Assessment name *

Microsoft Azure Well-Architected Review - Aug 24, 2020 - 7:43:58 PM

Choose your interests

Cost Optimization

An effective architecture achieves business goals and ROI requirements while keeping costs within the allocated budget.

Operational Excellence

To ensure that your application is running effectively over time, consider multiple perspectives, from both an application and infrastructure angles. Your strategy must include the processes that you implement so that your users are getting the right experience.

Performance Efficiency

Prioritize scalability as you design and implement phases. Scalability leads to lower maintenance costs, better user experience, and higher agility.

Reliability

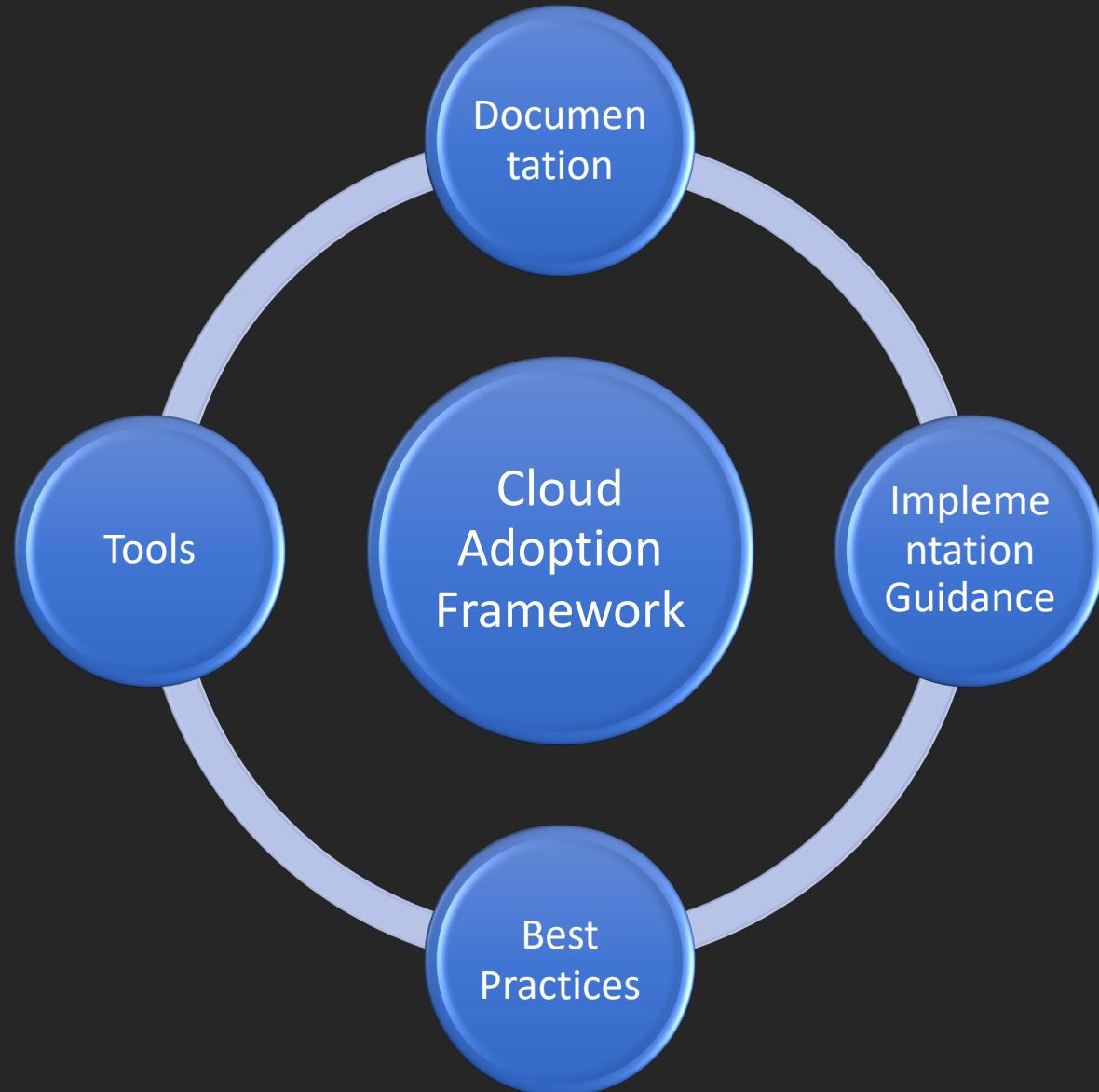
In a cloud environment you scale out rather than buying higher-end hardware to scale up. While it's always desirable to prevent all failure, focus your efforts in minimizing the effects of a single failing component.

Security

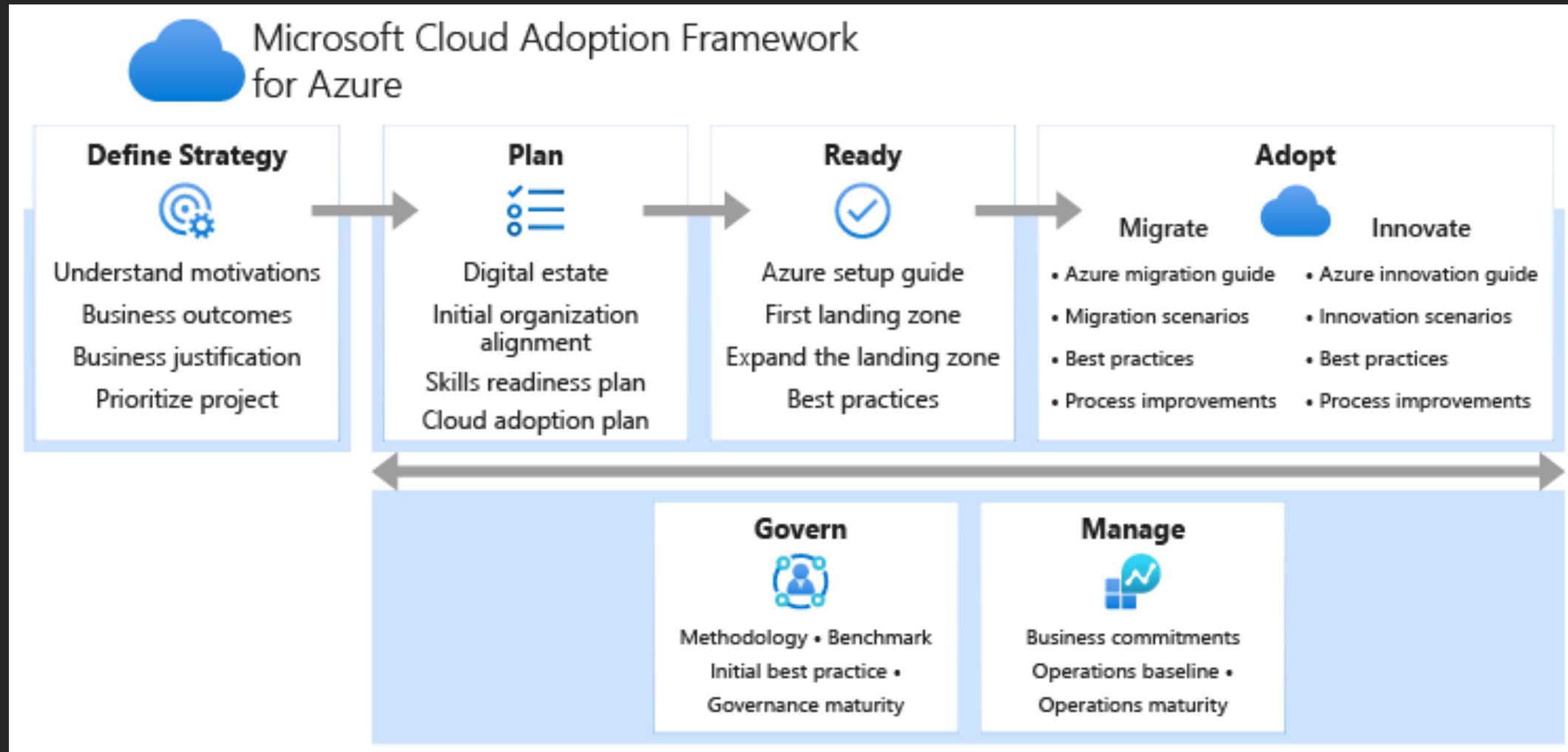
Security is one of the most important aspects of any architecture. It provides confidentiality, integrity, and availability assurances against deliberate attacks and abuse of your valuable data and systems. Losing these assurances can negatively impact your business operations and revenue, as well as your organization's reputation in the marketplace. In the following series of articles, we'll discuss key architectural considerations and principles for security and how they apply to Azure.

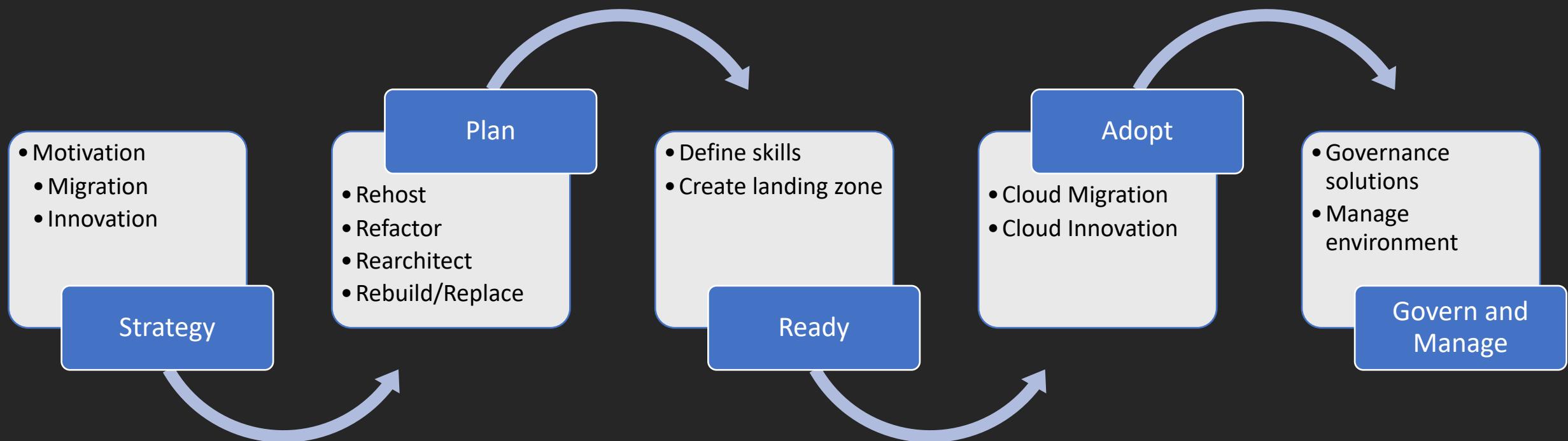
Next →

Cloud Adoption Framework



CAF Overview





Cloud Adoption Framework

Well Architecture Framework



DEMO

Azure Policy Concepts



- Create, assign and manage policies
- Enforce rules to ensure your resources are compliant
- Focus on resource properties for new and existing deployments
- A definition is a set of conditions in audit or deny mode
- An assignment is a policy definition placed on a specific scope
- An initiative is a collection of policies

Azure Policy



- ❯ Turn on built-in policies or build custom ones for all resource types
- ❯ Real-time policy evaluation and enforcement
- ❯ Periodic & on-demand compliance evaluation
- ❯ VM In-Guest Policy (NEW)

Enforcement & Compliance



- ❯ Apply policies to a Management Group with control across your entire organization
- ❯ Apply multiple policies and & aggregate policy states with policy initiative
- ❯ Exclusion Scope

Apply policies at scale



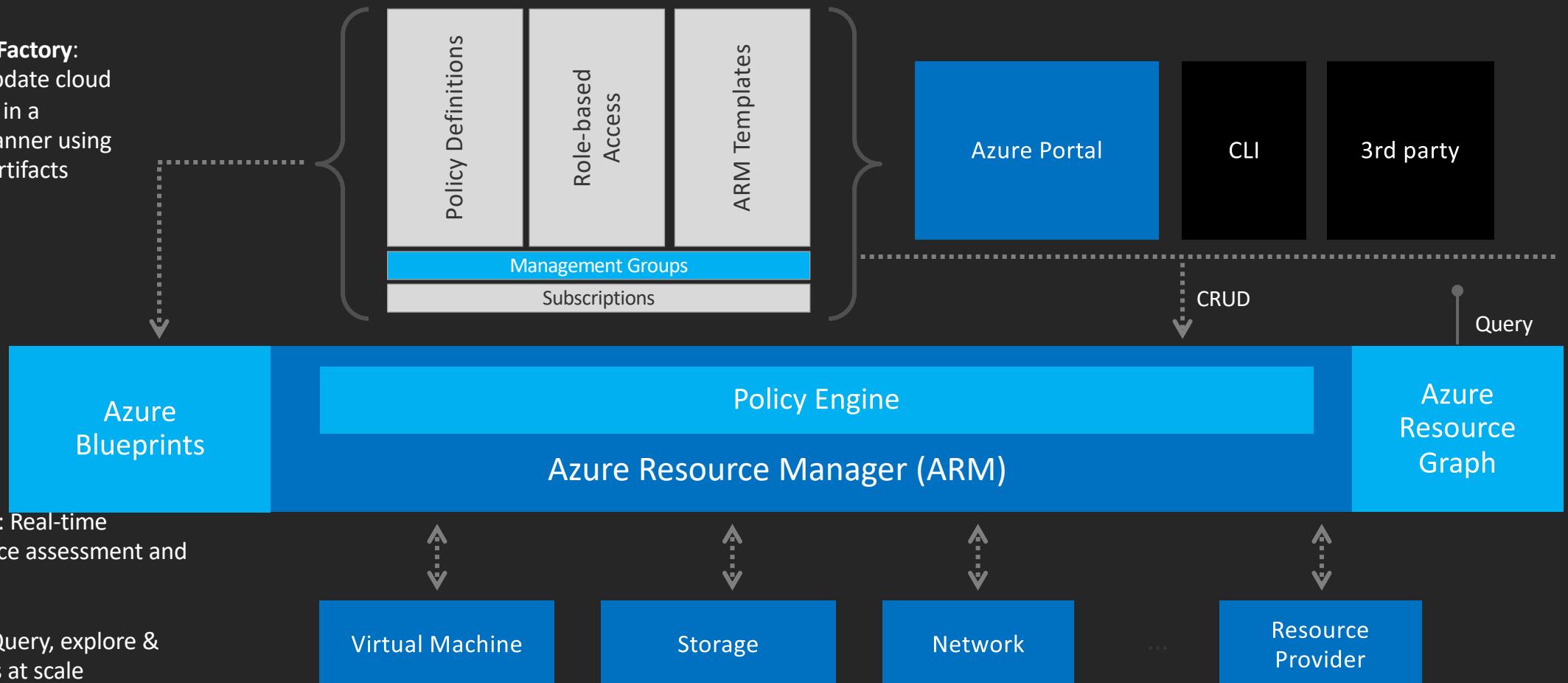
- ❯ Real time remediation
- ❯ Remediation on existing resources (NEW)

Remediation

Azure Governance Architecture

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

Leverage built-in initiative & policies



Security	Regulatory Compliance	Tags	Resource standardization	Cost
Azure Security Center	NIST SP 800-53 R4	Require specified tag	Allowed/ not allowed RP	Allowed VM SKUs
Guest Config baselines	ISO 27001:2013	Add or replace a tag	Allowed locations	Allowed Storage SKUs
Key Vault certificate	CIS	Inherit a tag from the RG	Naming convention	
NSG rules	PCI v3.2.1:2018	Append a tag	Back up VMs	
AKS & AKS Engine	FedRAMP Moderate		Allowed images for AKS	
RBAC role assignment	Canada Federal PBMM SWIFT CSP-CSCF v2020 UK Official and UK NHS IRS 1075			

Azure Policy



DEMO

Policy

- 250 policy definitions per scope
- 100 policy set definitions per scope
- 1000 policy set definitions per tenant
- 100 policyDefinition references per policySetDefinition
- 100 policy assignments per scope
- 250 notScopes per policyAssignment
- <https://github.com/Azure/azure-policy>

Azure Security Center



Azure Security Center



- A service to strengthen your security posture
- Available in two Tiers – Basic and Standard
- Basic -> Free – Activated by default for all subscriptions
- Based on an security score – scope based
- Available for all workloads (Server, Container, SQL, IoT and more)

Protect your workloads

- Detect & block advanced malware and threats for Linux and Windows Servers on any cloud
- Protect cloud-native services from threats
- Protect data services against malicious attacks
- Protect your Azure IoT solutions with near real time monitoring
- Service layer detections: Azure network layer and Azure management layer (ARM)



Azure Security Center



DEMO

How it works together

- All Azure Security Center recommendations based on Azure Policy
- Secure score is result of Azure Policy settings
- Recommendation is also a result of Azure Policy
- All Azure Policy are defined in Compliance mode

Azure Policy Recap

- Powerful solution to define Cloud Guards for own Tenant
- Start with an audit effect instead of a deny effect
- Define Management Groups to group subscriptions and set Policies at Higher level
- Use Deny effect for Production workloads with wisdom
- Creating initiatives even for single policy definition
- Integrate Azure Policy in your regulary Azure check

Azure Security Center



- Start with ASC to get a Security Overview
- Use ASC to strengthen your infrastructure
- Check the status in ASC regularly
- Create own security policies for secure score
- Use ASC to proof your infrastructure
- Integrate Azure Policy in your regulary Azure check

Dashboard >

Advisor

Search (Ctrl+ /) < Feedback Download as CSV Download as PDF

Your recommendations have been loaded

Subscriptions: All 3 selected – Don't see a subscription? Open Directory + Subscription settings

All subscriptions ▾ All types ▾

Cost 38 EUR savings/yr *

Security

Reliability

Operational excellence

Performance

All recommendations

Monitoring

Alerts (Preview)

Recommendation digests

Settings

Configuration

Cost 38 EUR savings/yr *

2 Recommendations

0 High impact 2 Medium impact 0 Low impact

2 Impacted resources

Security

42 Recommendations

22 High impact 7 Medium impact 13 Low impact

254 Impacted resources

Reliability

4 Recommendations

0 High impact 4 Medium impact 0 Low impact

15 Impacted resources

Operational excellence

1 Recommendation

0 High impact 0 Medium impact 1 Low impact

2 Impacted resources

Performance

1 Recommendation

1 High impact 0 Medium impact 0 Low impact

1 Impacted resource



Azure Enterprise-Scale Landing Zones

Landing Zone?



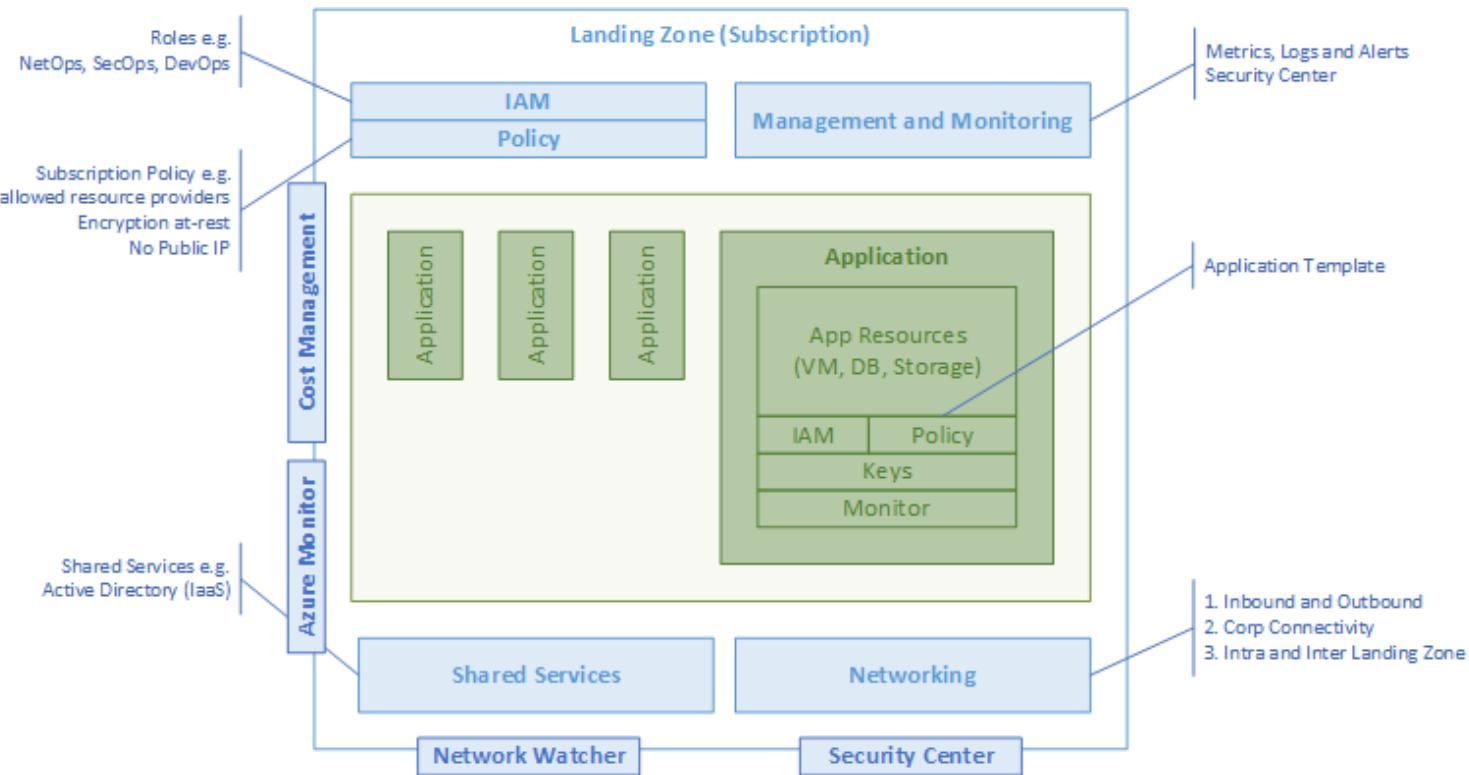
Landing Zone?



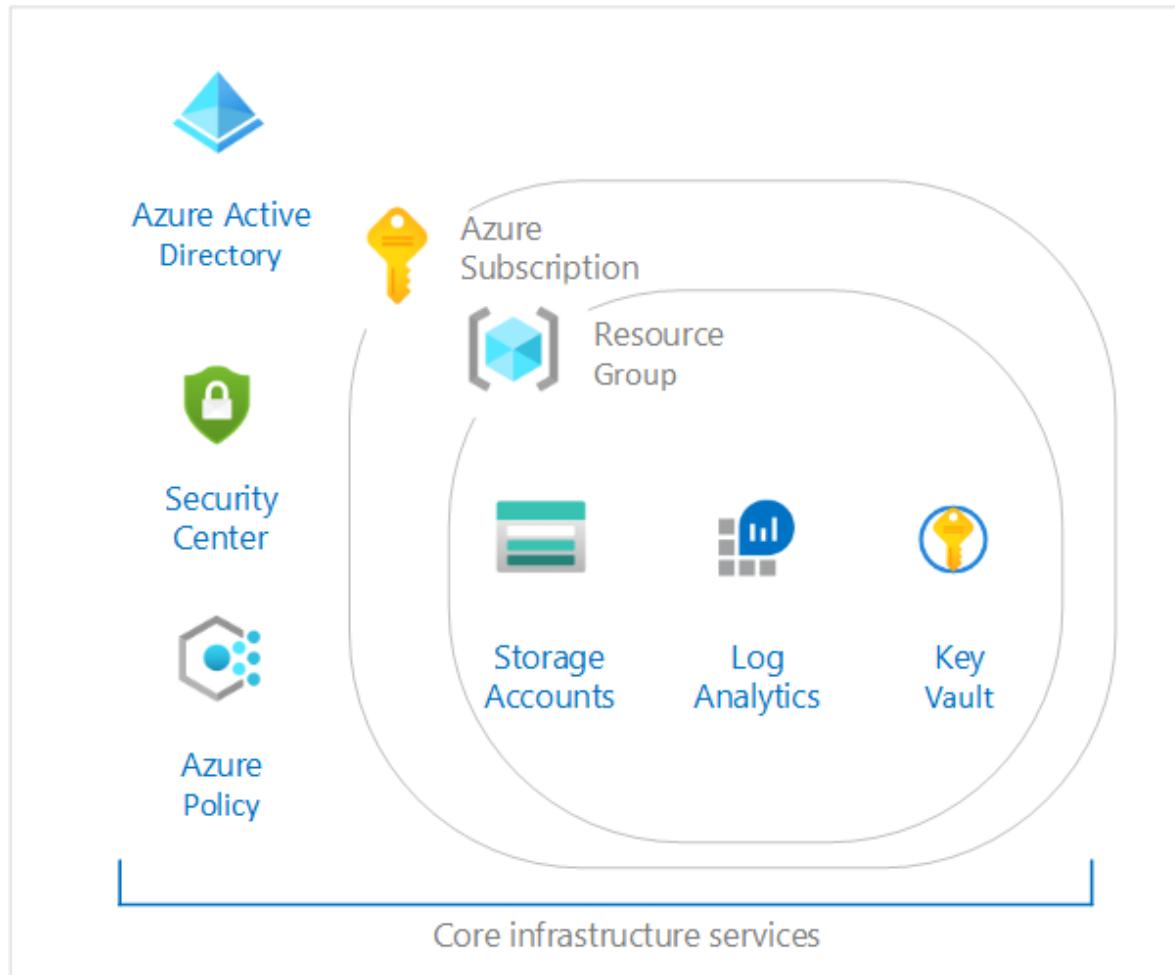
Landing Zone?



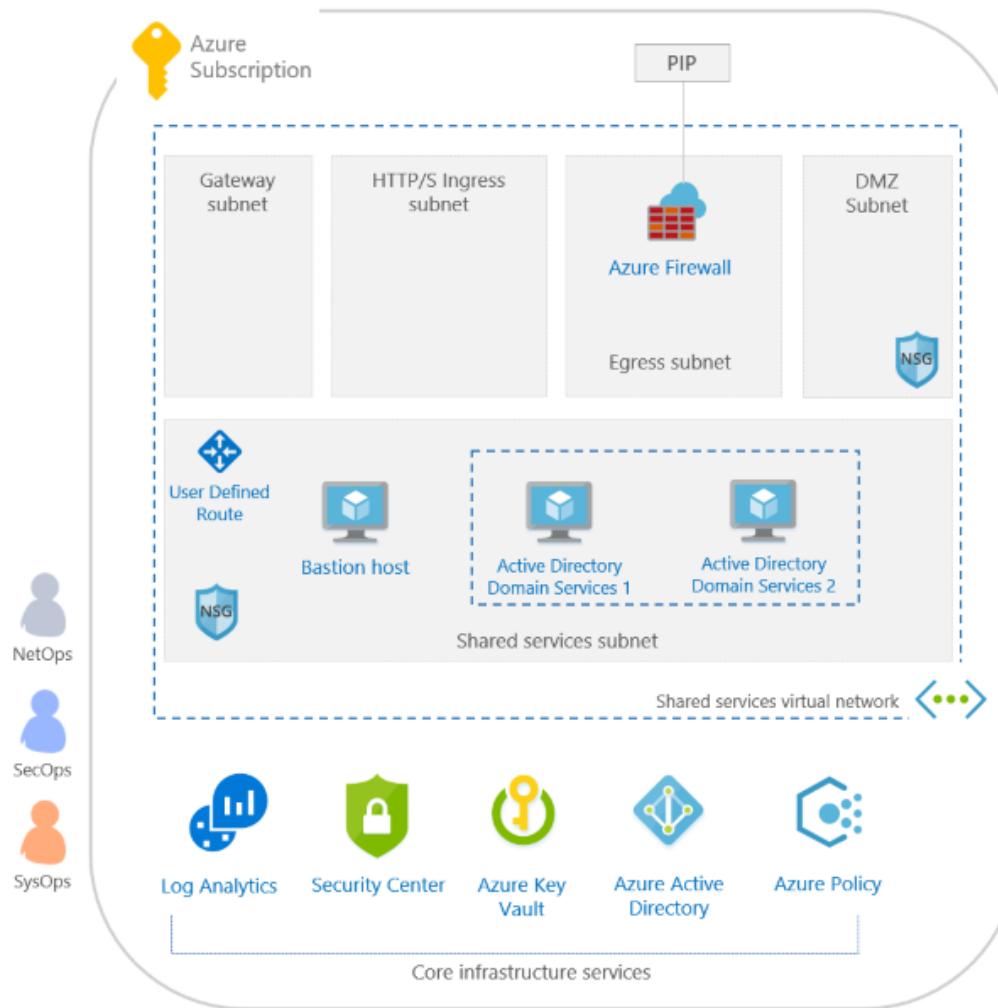
Design areas of Landing Zone(s)



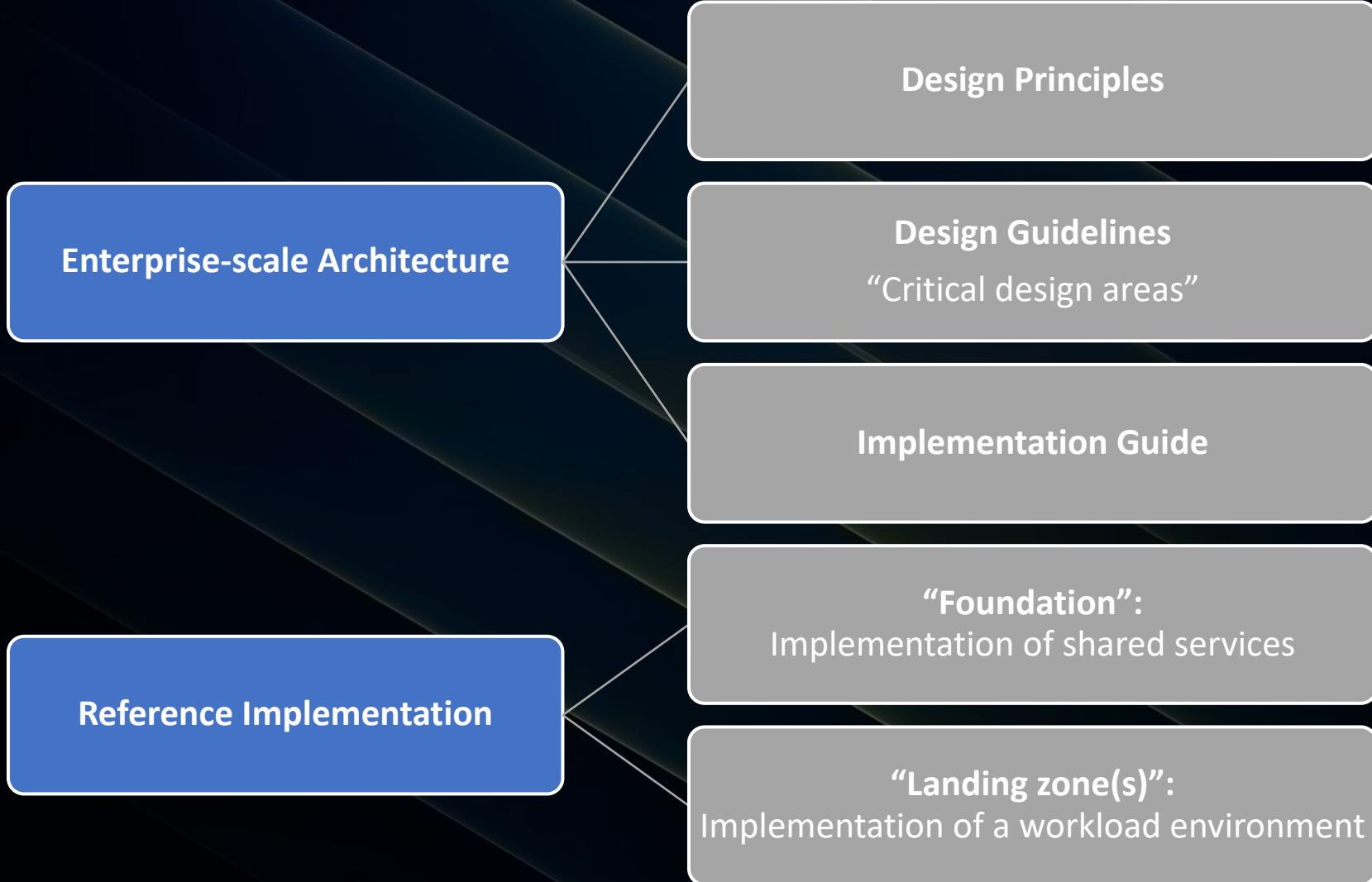
„CAF Foundation“ Blueprint



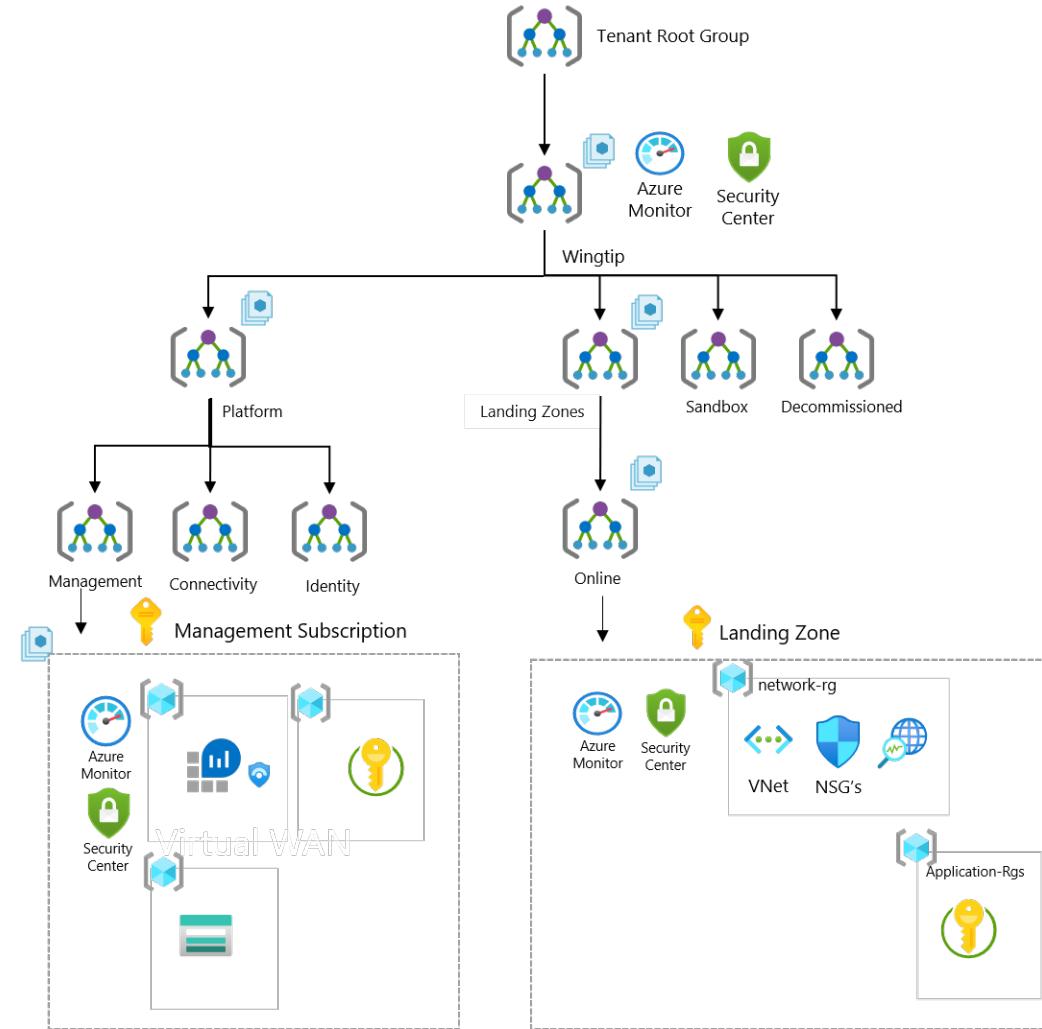
„ISO 27001 – Shared Services“ Blueprint



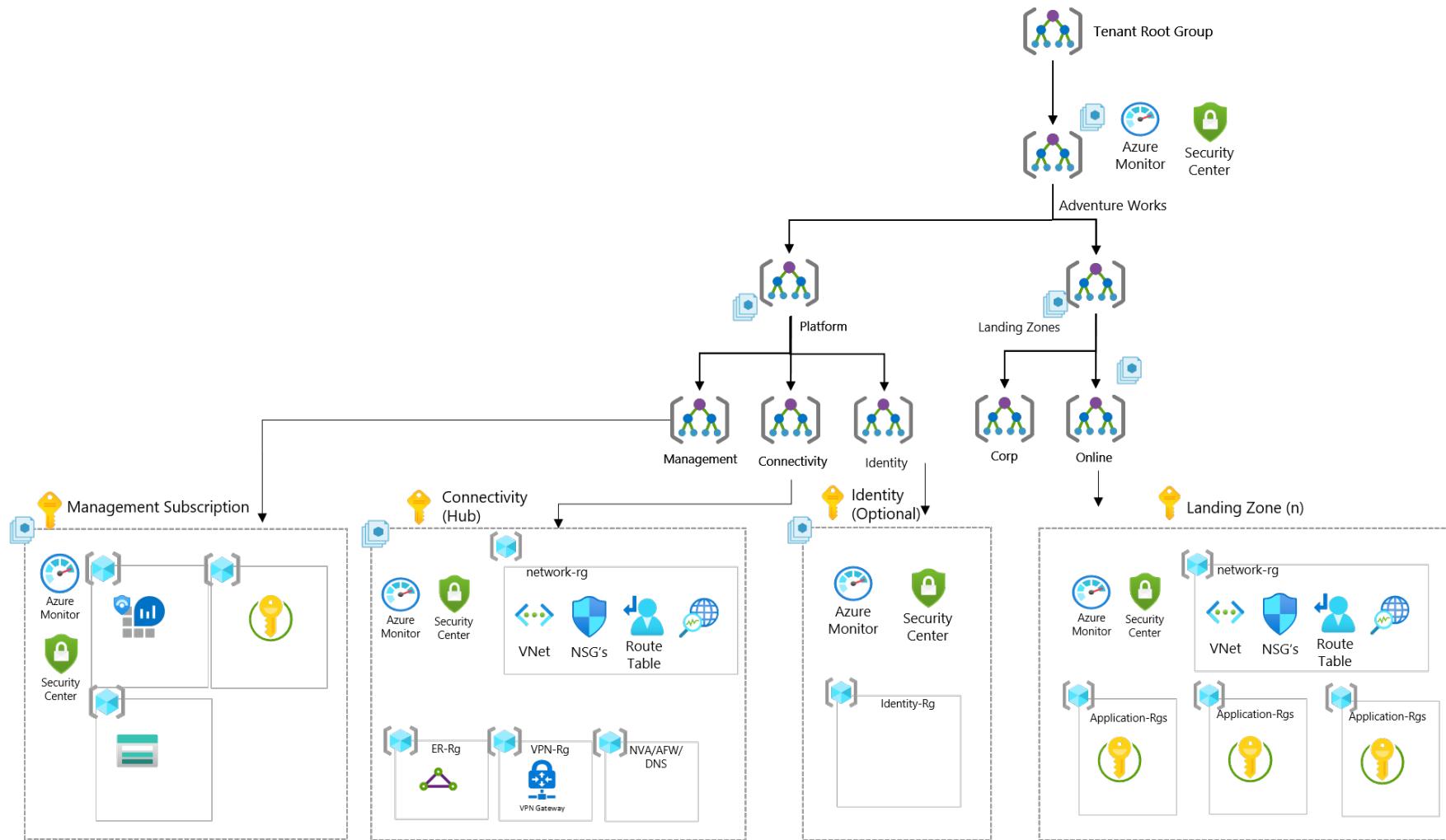
Enterprise-scale?



Enterprise-Scale without hybrid connectivity



Enterprise-Scale (hub & spoke architecture)

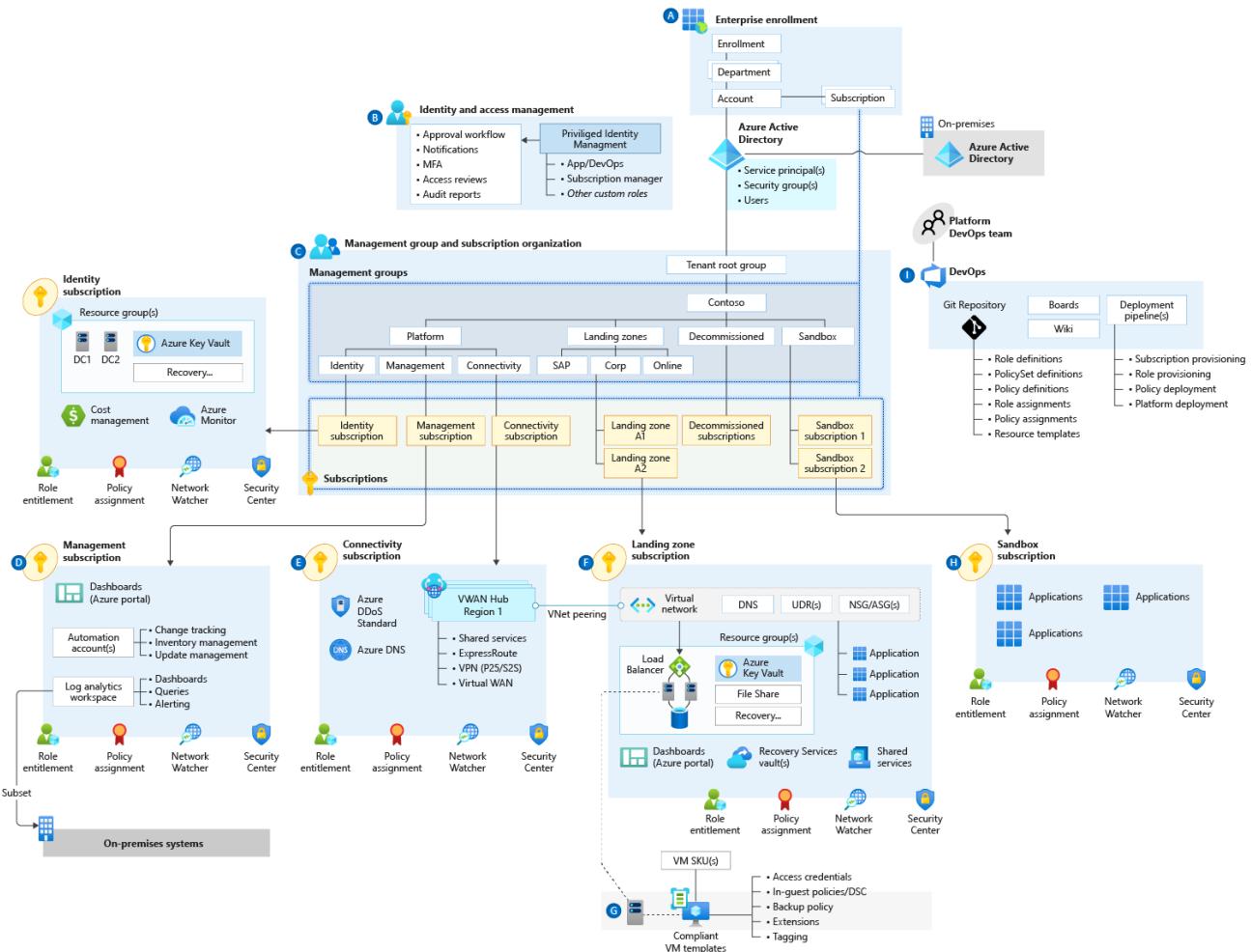


Enterprise-Scale Deployment and Policies

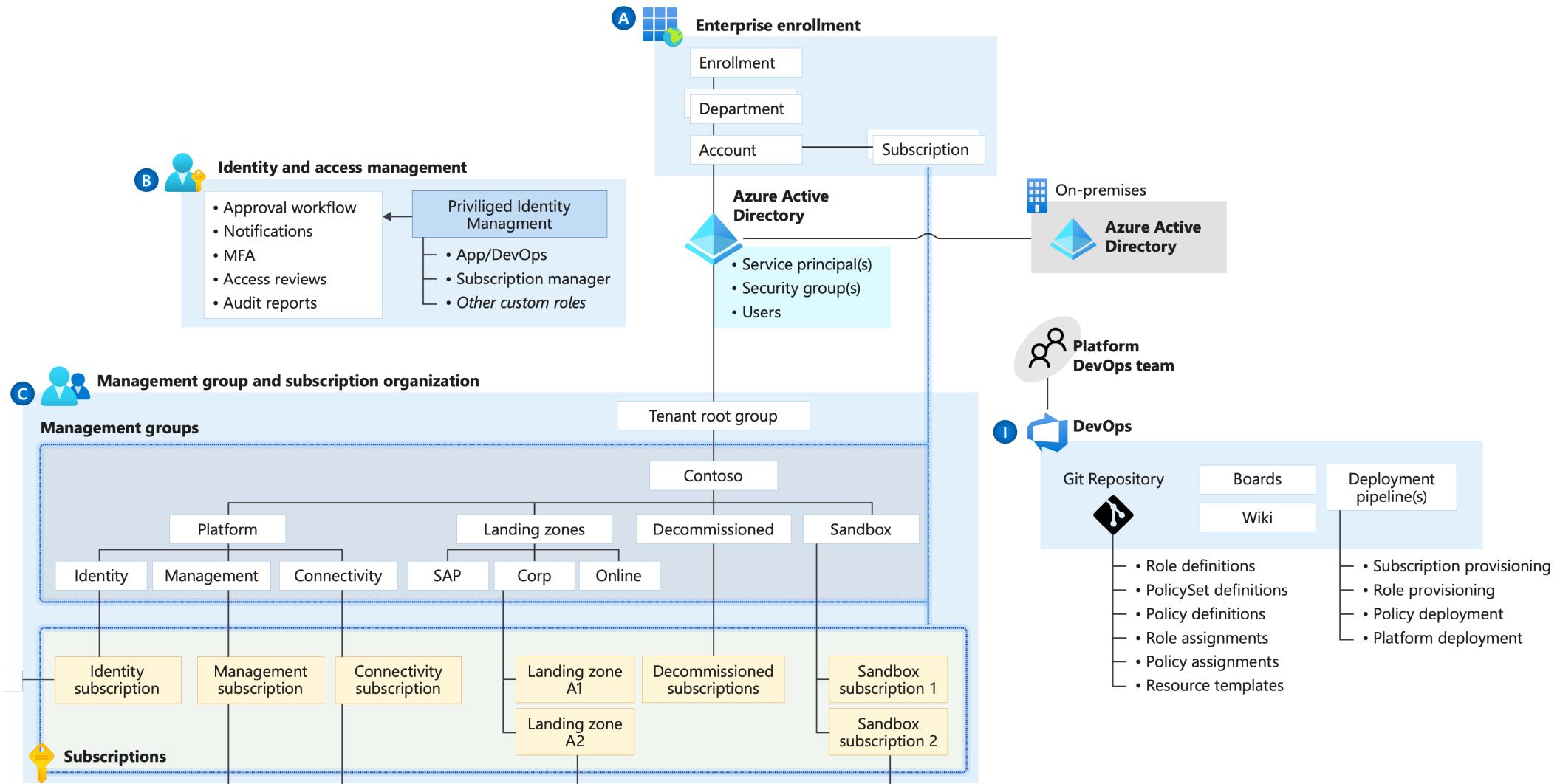


DEMO

Enterprise-Scale Architecture



Critical Design Areas





Securing Azure Environments with Azure AD (RBAC)

Securing Azure environments with Azure AD



A thumbnail image of a Microsoft Azure white paper titled "Securing Azure environments with Azure Active Directory". The image shows a city skyline at sunset with several skyscrapers. At the top left, there are navigation links: "Resource center" and "White papers". At the top right, there are social media sharing icons for Facebook, Twitter, and LinkedIn. The title "Securing Azure environments with Azure Active Directory" is centered in large white text.

Published: 7/21/2020

In Microsoft Azure, Azure Active Directory is the identity governance and administration layer that is used to manage access to resources such as instances of virtual machines, databases, applications, APIs, websites, etc. This identity layer is the control plane that helps protect your resources from intruders.

In this paper, we describe the architectures and best practices for implementing identity and access management across separate Azure environments. Not all organizations need to run separate environments. This document will help you understand if this configuration is appropriate for your organization.

We begin with an *Introduction to delegated administration and isolated environments*. In this introduction we describe various deployment scenarios and critical considerations for deciding if separate environments are appropriate for your organization. Ultimately, we help you choose the right architecture for your organization: *Delegated administration in a single tenant*, *Resource isolation in multiple tenants*, or *Resource and identity isolation in multiple tenants*. We then provide a comprehensive list of design considerations, or best practices.

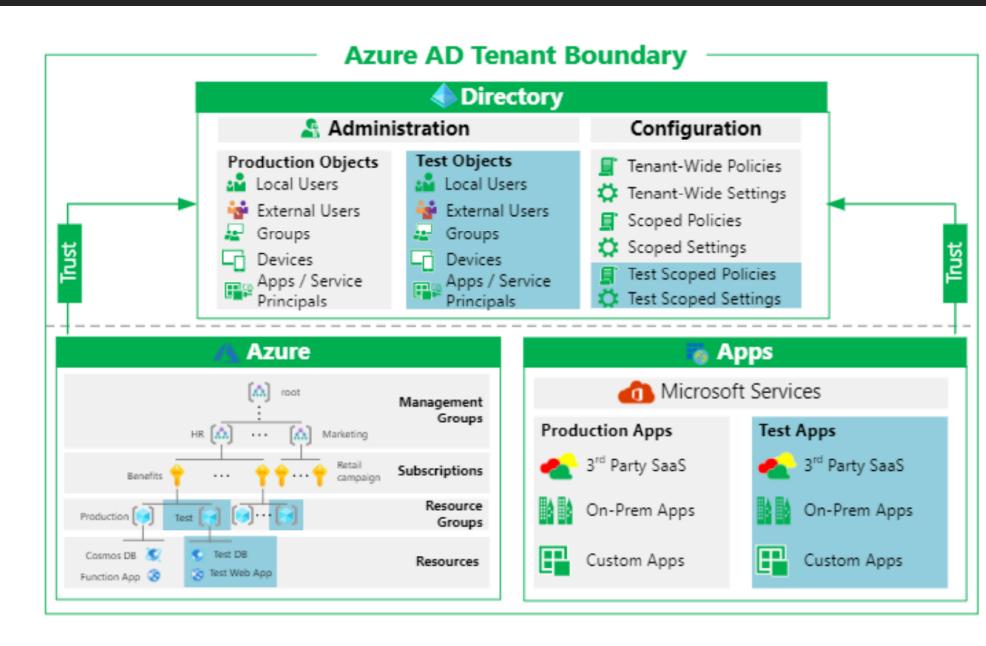
[Download >](#)

Identity guidance and best practices for designing and securing isolated environments in Azure.

→ <https://aka.ms/AzureADSecuredAzure>

Securing Azure environments with Azure AD

Azure AD Tenant Boundary



- **Resource Isolation**
DevOps Teams, Staging, "Secret resources" (shielded from discovery for regulatory or business critical reasons)
- **Tenant Isolation**
Tenant-wide configurations, External identities, Compliance (geo-political reasons)
- **Administrative Isolation**
Regulations to manage (scoped) environment based on conditions, current limitations of delegation, multi-industry-company

Securing Azure environments with Azure AD

Azure AD Tenant Boundary



*„To mitigate risk of identity compromise, or bad actors, implement tiered administration and ensure that you **follow principles of least privilege for Azure AD Administrator Roles.**“*

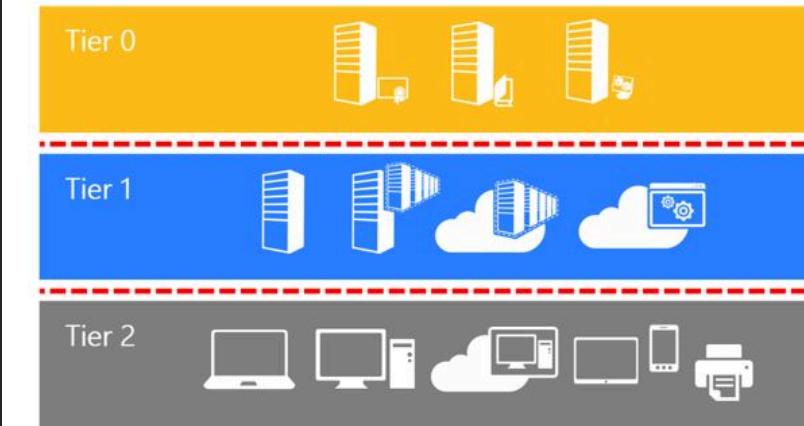
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8

Active Directory administrative tier model

02/14/2019 • 33 minutes to read • 6 comments +6

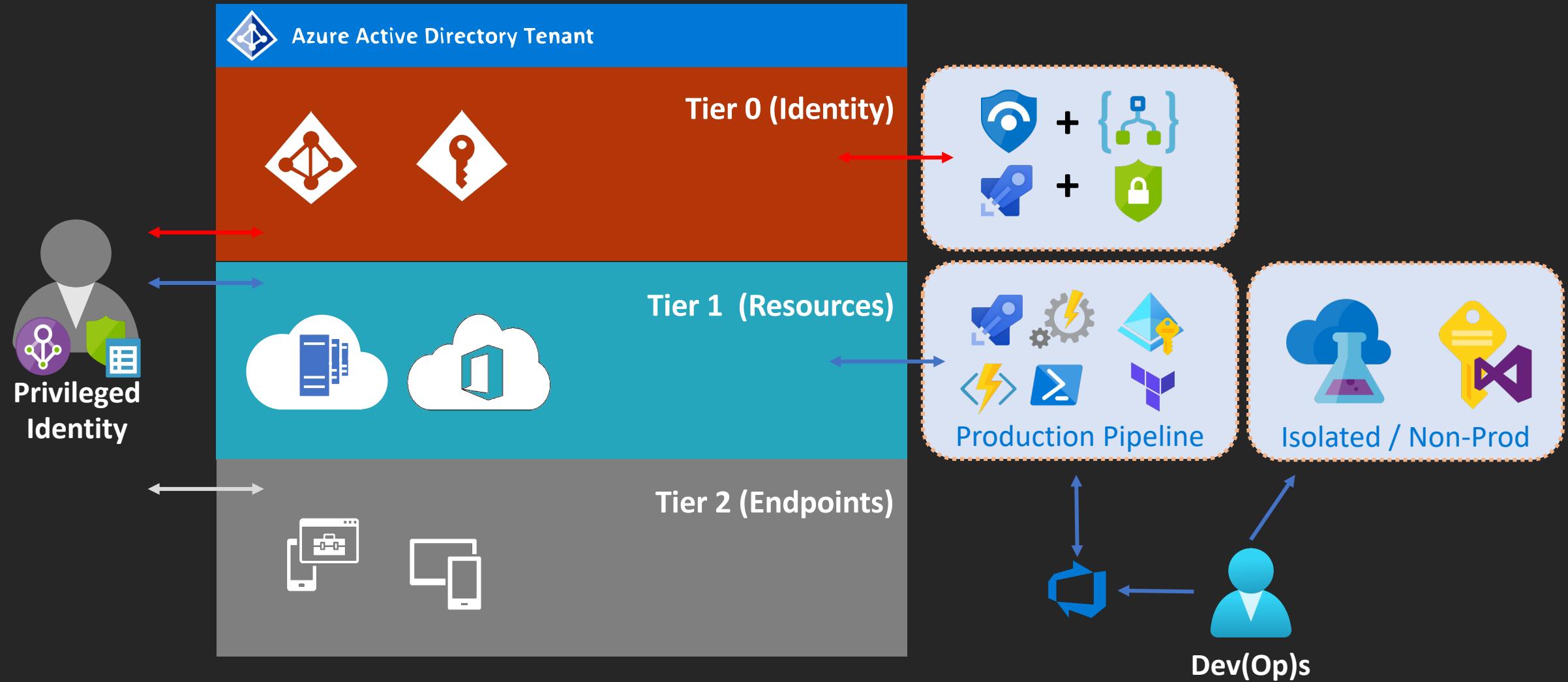
Applies To: Windows Server

The purpose of this tier model is to protect identity systems using a set of buffer zones between full control of the Environment (Tier 0) and the high risk workstation assets that attackers frequently compromise.



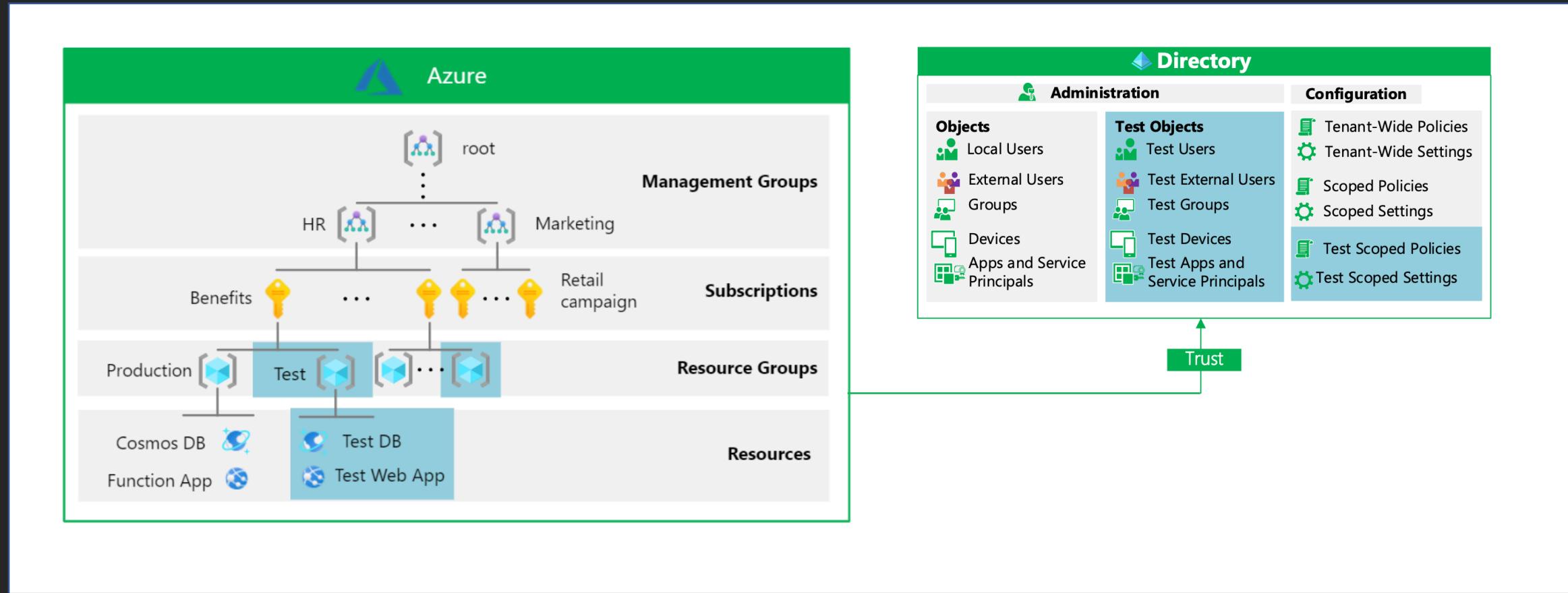
Securing Azure Environment with Azure AD

Example of Tiered Administration Model



Securing Azure Environment with Azure AD

Resource Isolation in a single tenant





Demo Scenario

Role Delegation to DevOps Team

“NCC-1701”

-
- Manage Credentials of “Test User”
 - Manage Service Principal of “DevOps Service Connection”
 - Temporary Read Permission of SQL Server Properties for all Project Team Members



Administrative Units, Azure AD Custom Roles and Custom Roles in Azure RBAC



DEMO

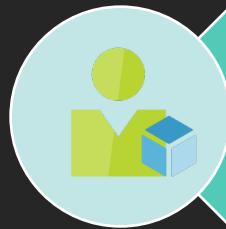


Simplified, Secured & Least Privileged Access



Evaluate built-in roles instead of creating custom roles

- Custom Roles are powerful but can be also complex
- RBAC-as-Code approach



Avoid permissions referencing to specific resources or user

- Using Management Groups (Enterprise) or Resource Groups Level Permissions



Assign eligible permissions based to Azure AD Groups

- Reduce standing access (Just in Time, Access Review)
- Implement Break-Glass /Emergency access for Tier1

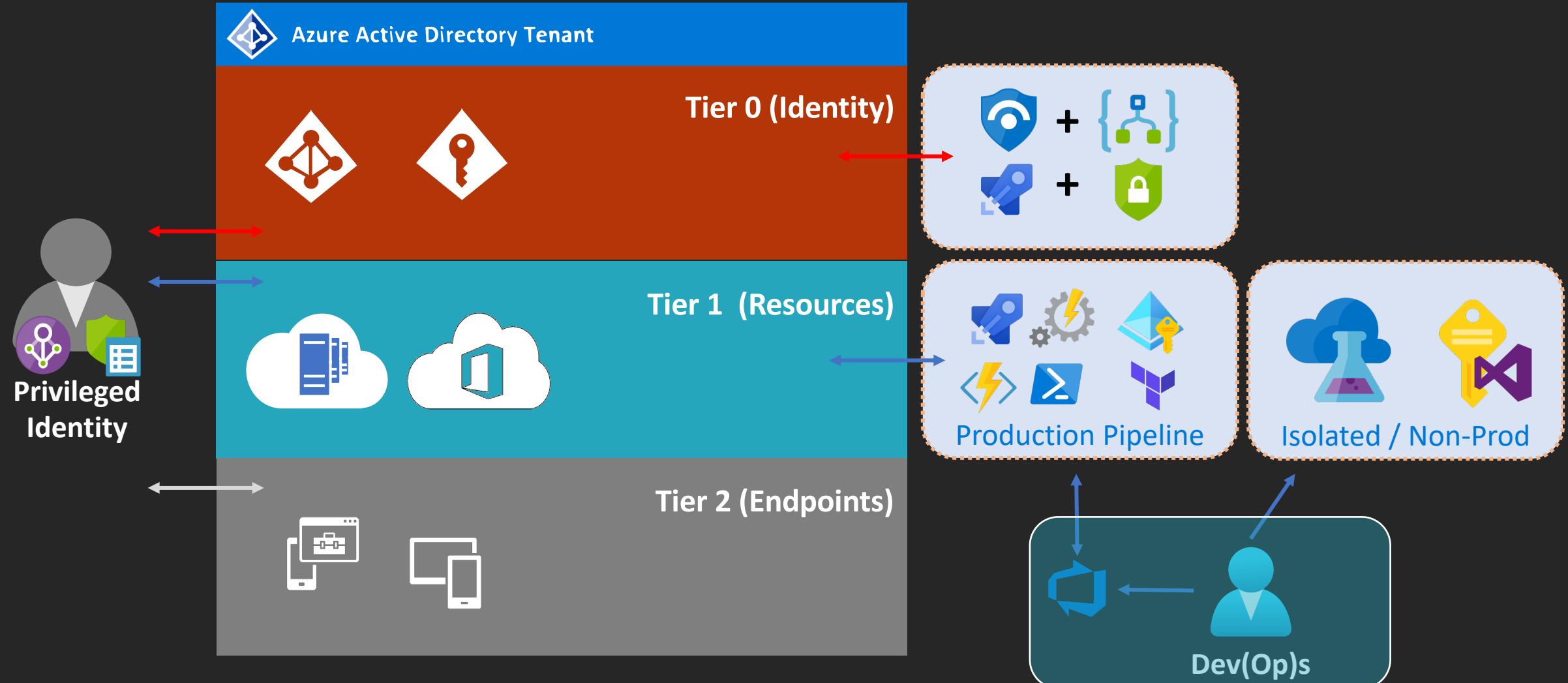


Access to Azure resources by „Managed identities“ / KeyVault

- where service principals are needed, use certificate credentials for service principals
- use Azure KeyVault to protect your secrets, keys or certificates

Securing Azure Environment with Azure AD

Example of Tiered Administration Model



Azure PIM Privileged Access Groups



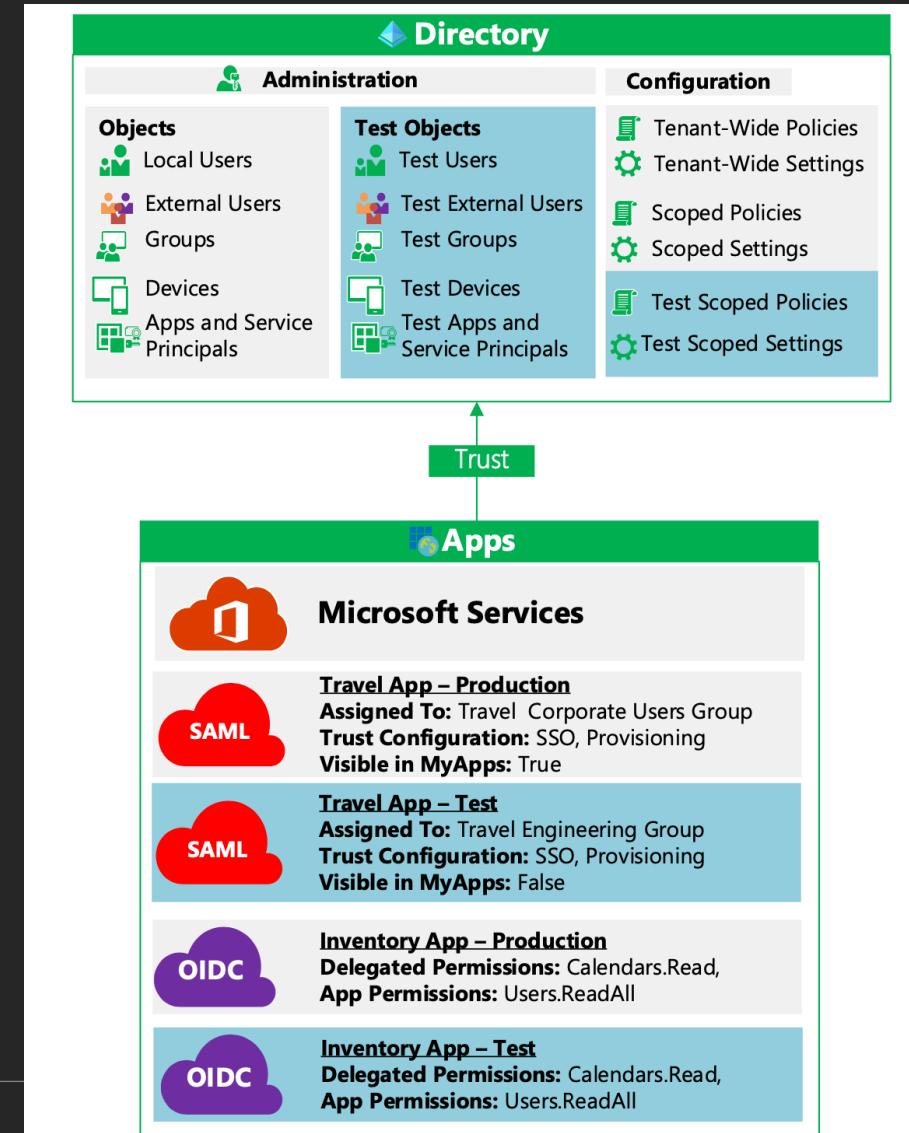
Securing Azure Environment with Azure AD

Azure AD Tenant Boundary



„The lifecycle of Microsoft SaaS services such as Office 365, Microsoft Dynamics, and Microsoft Exchange are bound to the Azure AD tenant. As a result, multiple instances of these services necessarily require multiple Azure AD tenants.“

Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 14



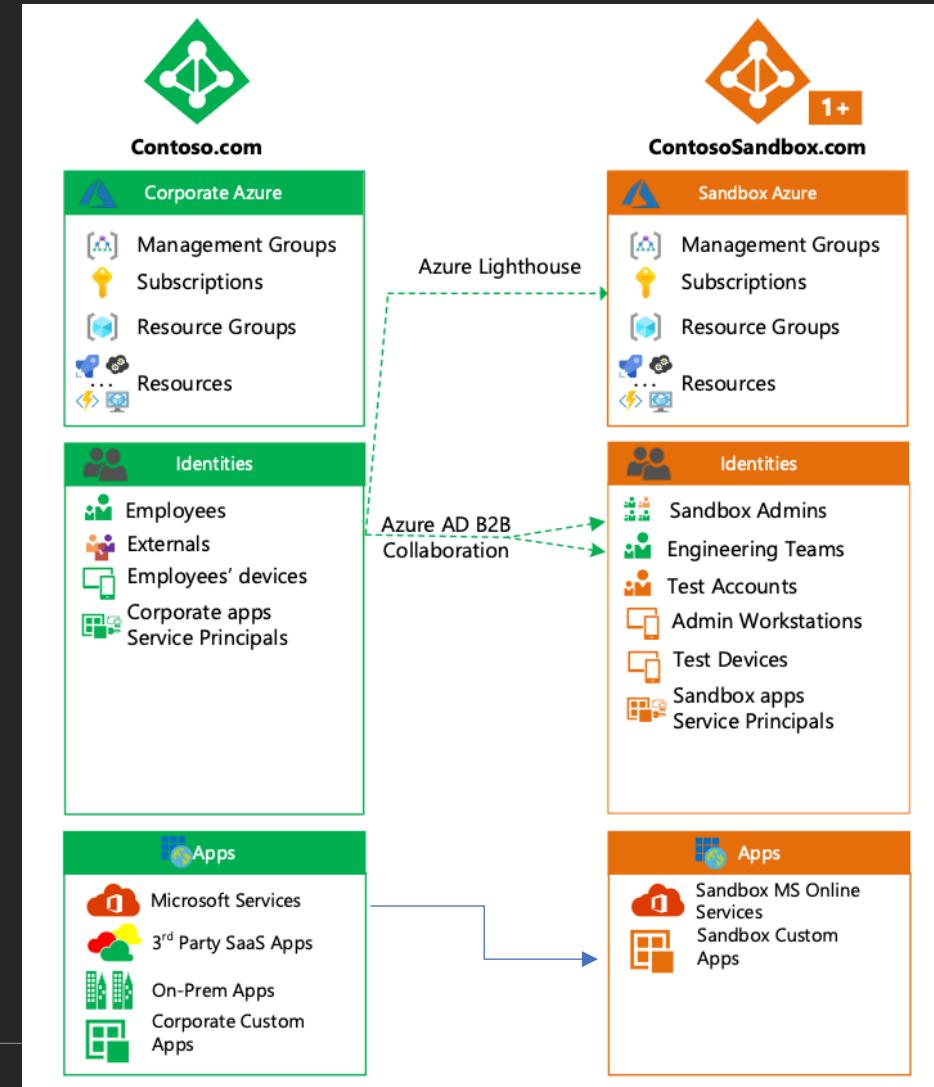
Securing Azure Environment with Azure AD

Resource Isolation in a multiple tenant

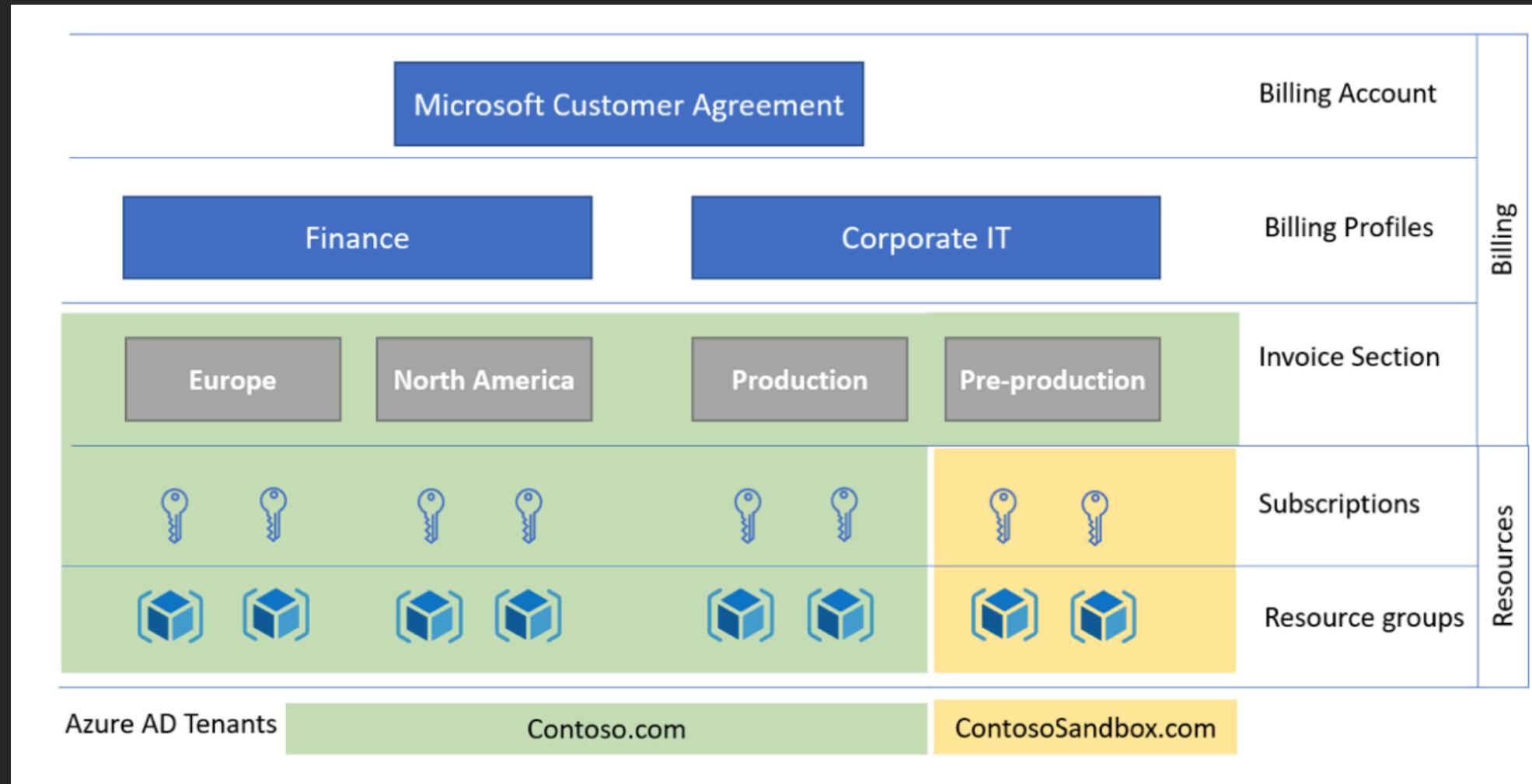


„Multi-tenant architectures with external identity access enabled provide only resource isolation, but do not enable identity isolation. Resource isolation using Azure AD B2B collaboration and Azure Lighthouse do not mitigate risks related to identities.“

Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 17



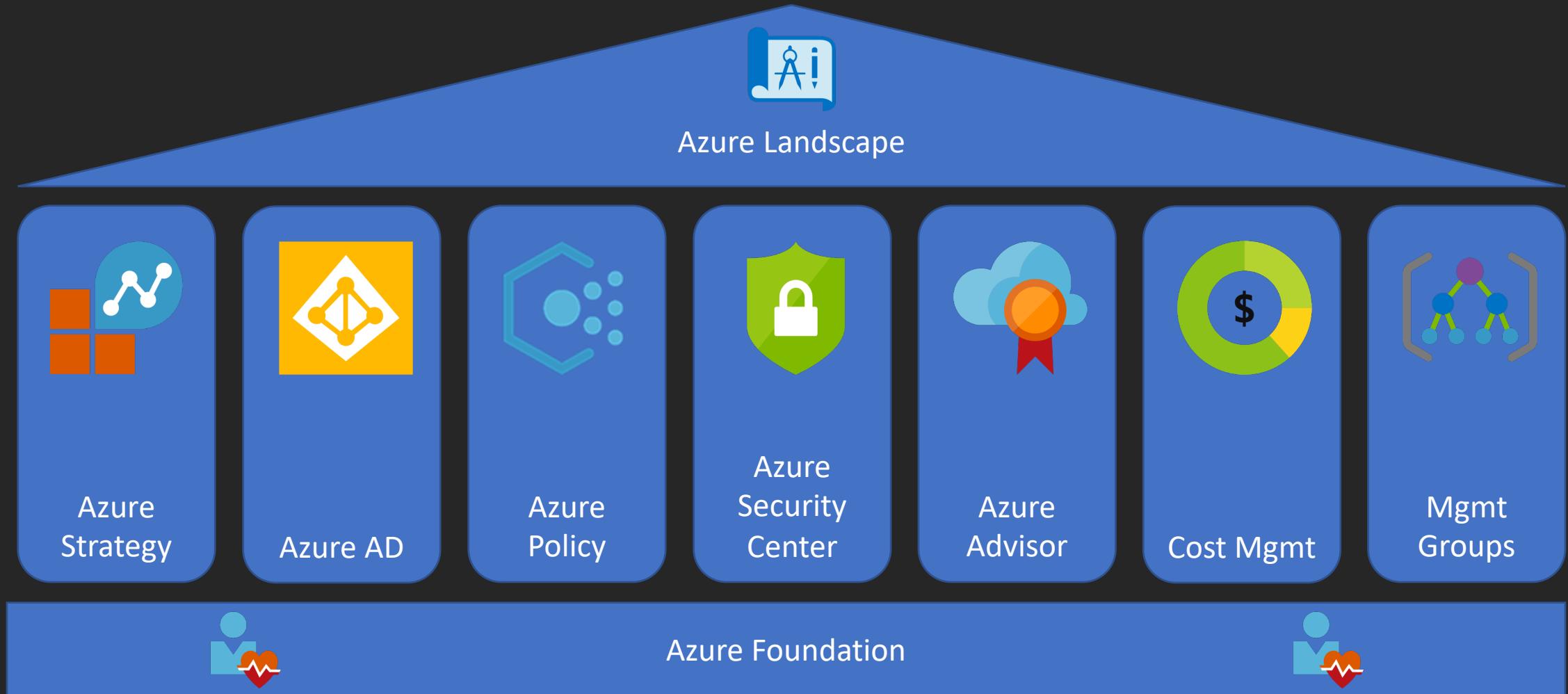
Securing Azure Environment with Azure AD Microsoft Customer Agreement Hierarchy



Links

- <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/>
- <https://docs.microsoft.com/en-us/azure/architecture/framework/>
- <https://docs.microsoft.com/en-us/azure/advisor/>
- <https://docs.microsoft.com/en-us/azure/governance/policy>
- <https://www.reimling.eu/2019/03/azure-management-groups-und-blueprints-ueberblick-und-einrichtung-teil-1/>
- <https://aka.ms/SecurityCommunity>
- <https://blog.azureandbeyond.com/2020/04/24/mastering-azure-security-my-latest-adventure/>
- Virtual Live Event (October 20th): Azure Architecture Best Practices
<https://mktoevents.com/Microsoft+Event/198675/157-GQE-382>

How brings it to Azure?



Our Recommendations

- Define a Cloud Strategy
 - Use the available Tools and Guidelines
 - Define the added value of the cloud
- Create a Team for Cloud Services of different people
- Evaluate guidelines and best practices
- Organize a regular meeting/call for Cloud news
- Get in touch with Partners and Community for help and support



Questions? ->
Reach us via Twitter ☺

Identity Summit 2020
follow
@IdentitySummit

 [@Thomas_Live](https://twitter.com/Thomas_Live)
 www.cloud-architekt.net

| [@GregorReimling](https://twitter.com/GregorReimling)
| www.reimling.eu

| [@AzureBonn](https://twitter.com/AzureBonn)
| www.azurebonn.de