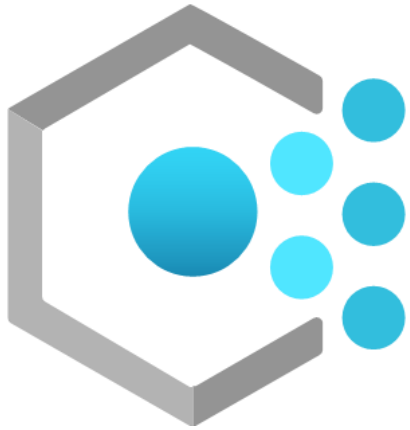
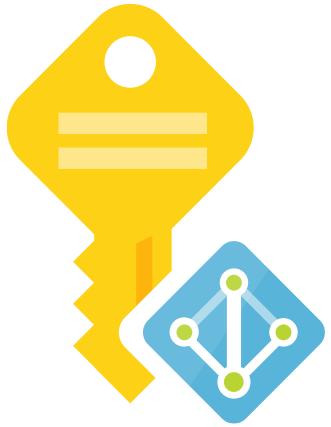
DATA SATURDAYS #34 RHEINLAND 2023

Azure Governance Best Practices and Enterprise-Scale

Gregor Reimling,
Thomas Naunheim





Gregor Reimling

Cloud Consultant
@adesso SE

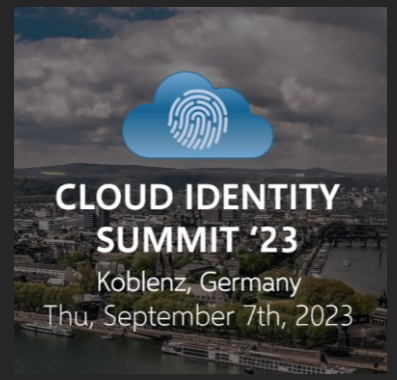
Cloud & Datacenter, Governance

@GregorReimling

www.reimling.eu

DATA SATURDAYS

Azure Meetup BONN



Thomas Naunheim

Cyber Security Architect
@glueckkanja-gab AG

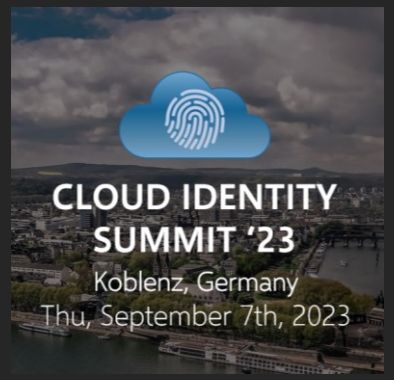
Azure Identity + Security

@Thomas_Live | @AzureBonn

www.cloud-architekt.net

DATA SATURDAYS

Azure Meetup BONN



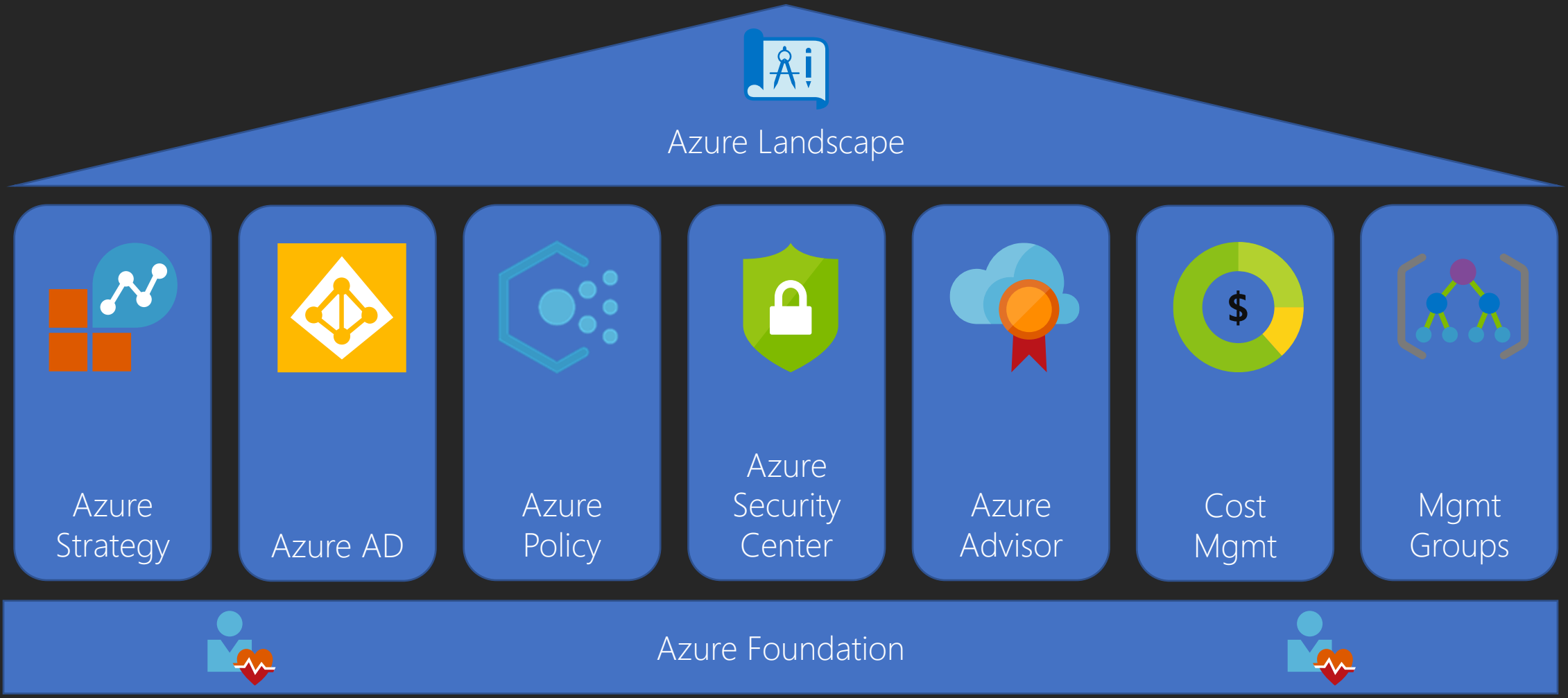
Agenda

- Overview of Cloud Adoption Framework and Well-architecture Framework
- Azure Policy and Microsoft Defender for Cloud
- Azure Enterprise-Scale Landing Zone
- Best Practices in Azure Identity & Access

General

- Fragen sind ausdrücklich erwünscht!
- Wir haben auch Fragen an Euch… Eure Erfahrung mit…
  - Enterprise-Scale?
  - Azure Hub- and Spoke-Design?
  - Defender for Cloud?
  - Azure RBAC to Identity Team?
  - GitHub vs. Azure DevOps?

Azure Governance House



Overview of CAF and WAF

Azure Cloud Adoption Framework (CAF)

„The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey."

Azure Well-Architected Framework (WAF)

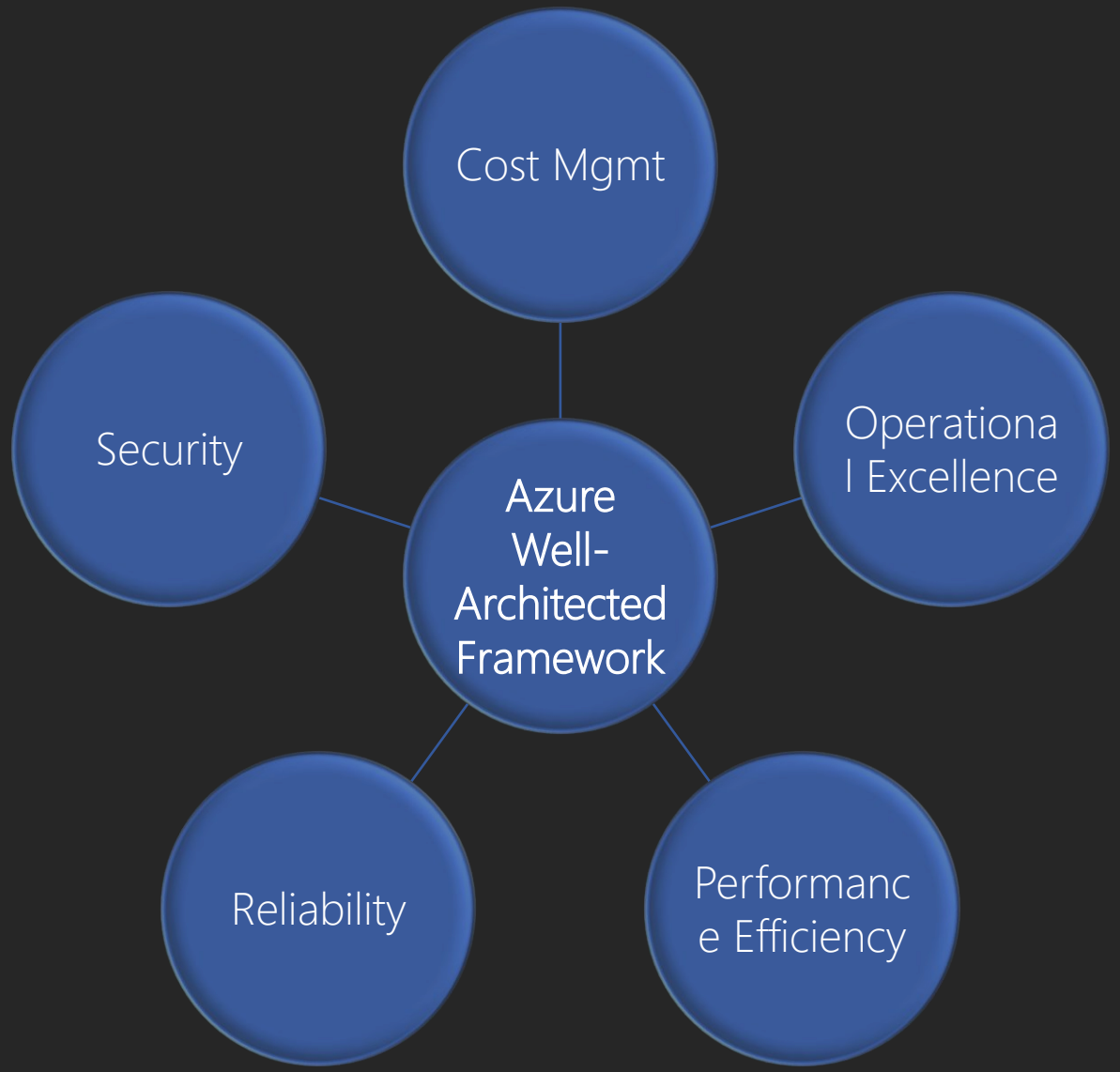
"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."

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

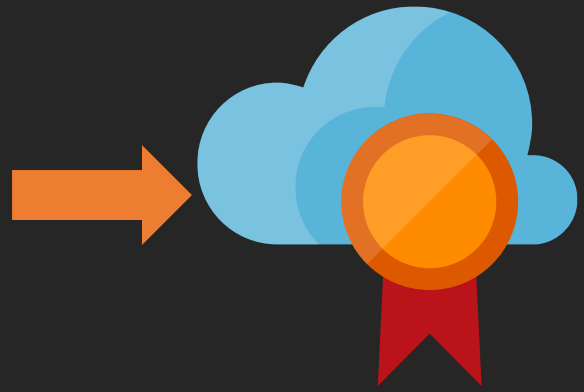
Cloud Adoption Framework

https://docs.microsoft.com/en-us/azure/cloud-adoption-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/

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?

Microsoft Assessments Azure Well-Architected Review

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.

- [x] **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
Well Architecture Framework

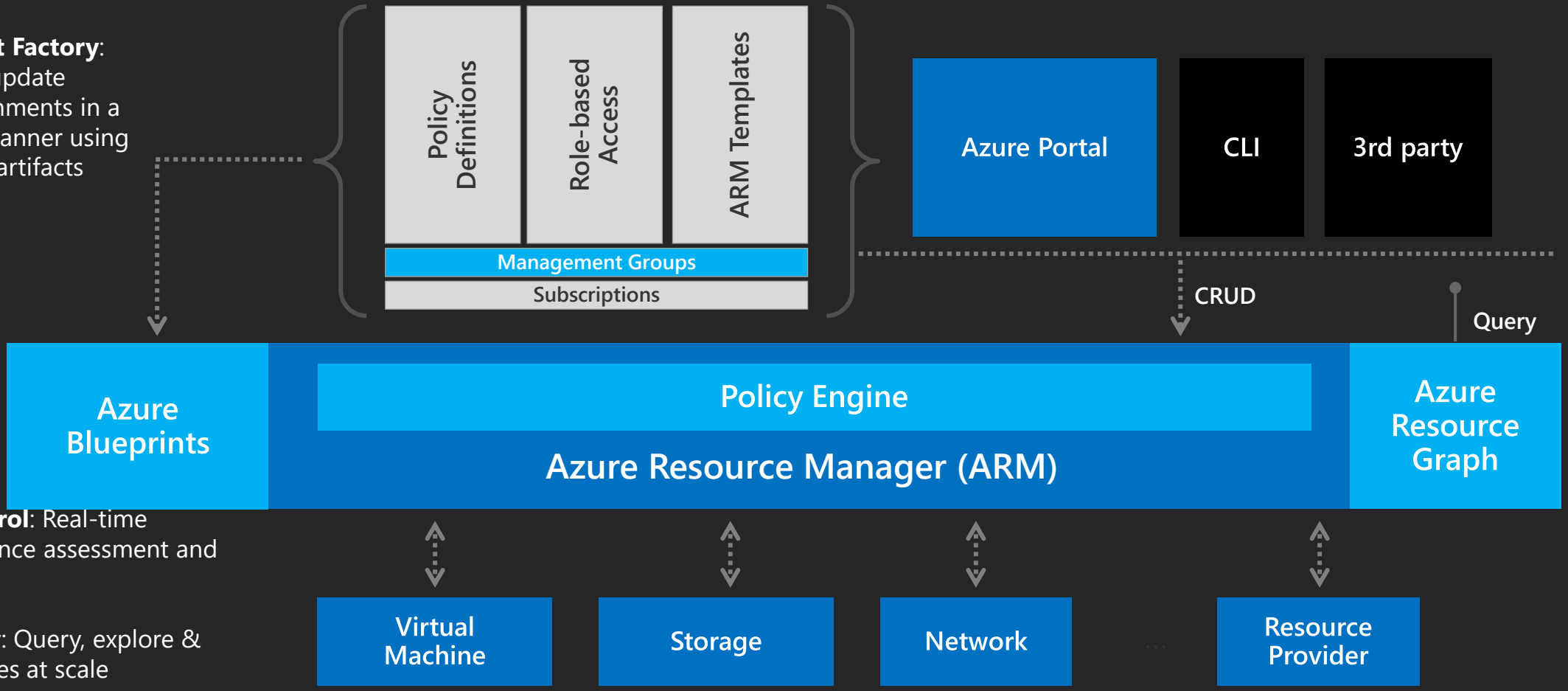
DEMO

Azure Policy and Microsoft Defender for Cloud

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

Azure Policy Concepts 

- Part of CAF to support WAF
- Create, assign and manage policies
- Enforce rules to ensure your ressoures are compliant
- Focus on ressource 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

https://docs.microsoft.com/en-us/azure/governance/policy/overview

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

Leverage built-in initiative & policies

DATA SATURDAYS

 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 Security Benchmark v3

- Released with the renaming of Azure Security Center to MS Defender for Cloud
- Mapping to industry frameworks:
  - PCI-DSS and CIS Controls
  - NIST SP800
- Control guidance more granular

Azure

DEMO

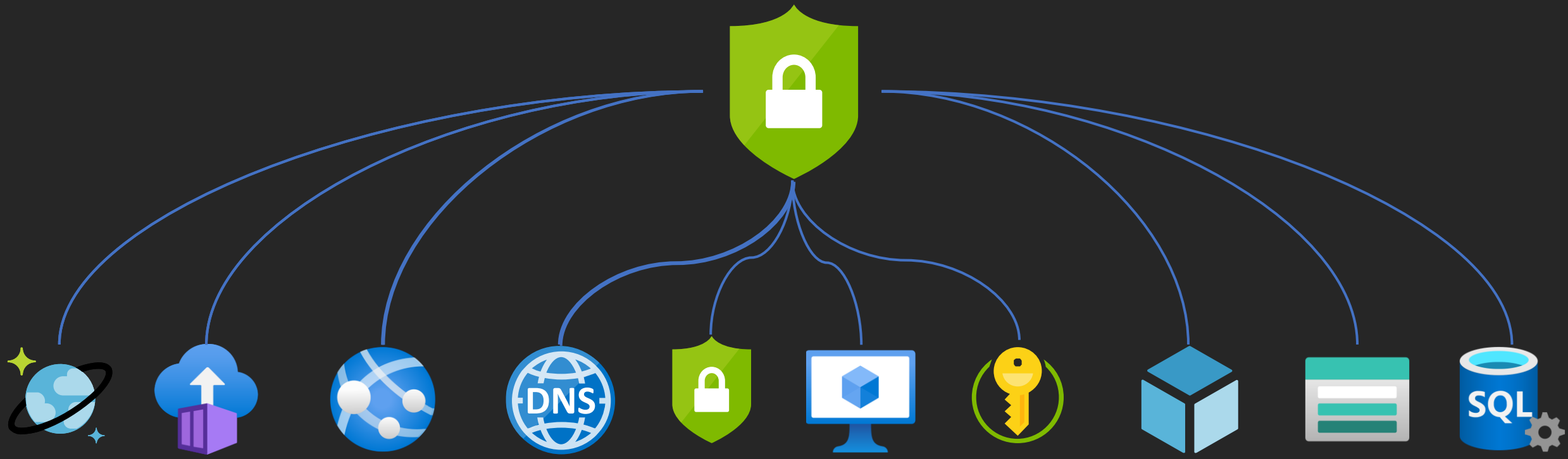
Microsoft Defender for Cloud

~~Azure Security Center~~

Microsoft Defender for Cloud

- A service to strengthen your security posture
- Available in two Tiers
  1. Free
  2. Azure Defender for (Server, App Service, …,)
- Free – Activated by default for all subscriptions
- Based on an security score – scope based

Microsoft Defender for Cloud



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

Microsoft Defender for Cloud

Microsoft Defender for Cloud - an introduction | Microsoft Docs

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

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
- Recommendations are a result of Azure Policy
- All Azure Policies are defined in Compliance mode
- Azure Policy settings for ASC will firstly applied when Subscription is created

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

DATA SATURDAYS

Azure Enterprise-Scale Architecture

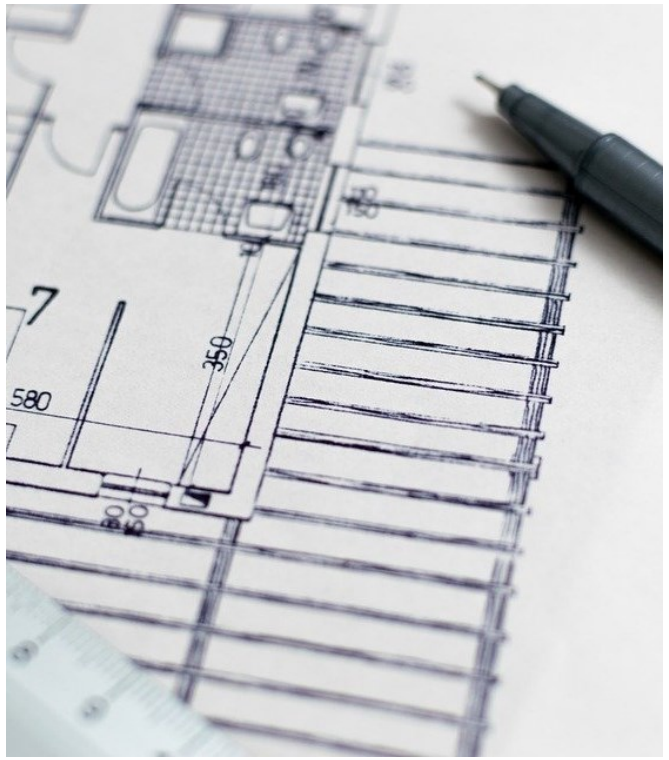
Introduction and Implementation

Challenges of starting **Cloud Journey**

Challenges of starting **Cloud Journey**

Challenges of starting **Cloud Journey**

What is Enterprise-Scale?



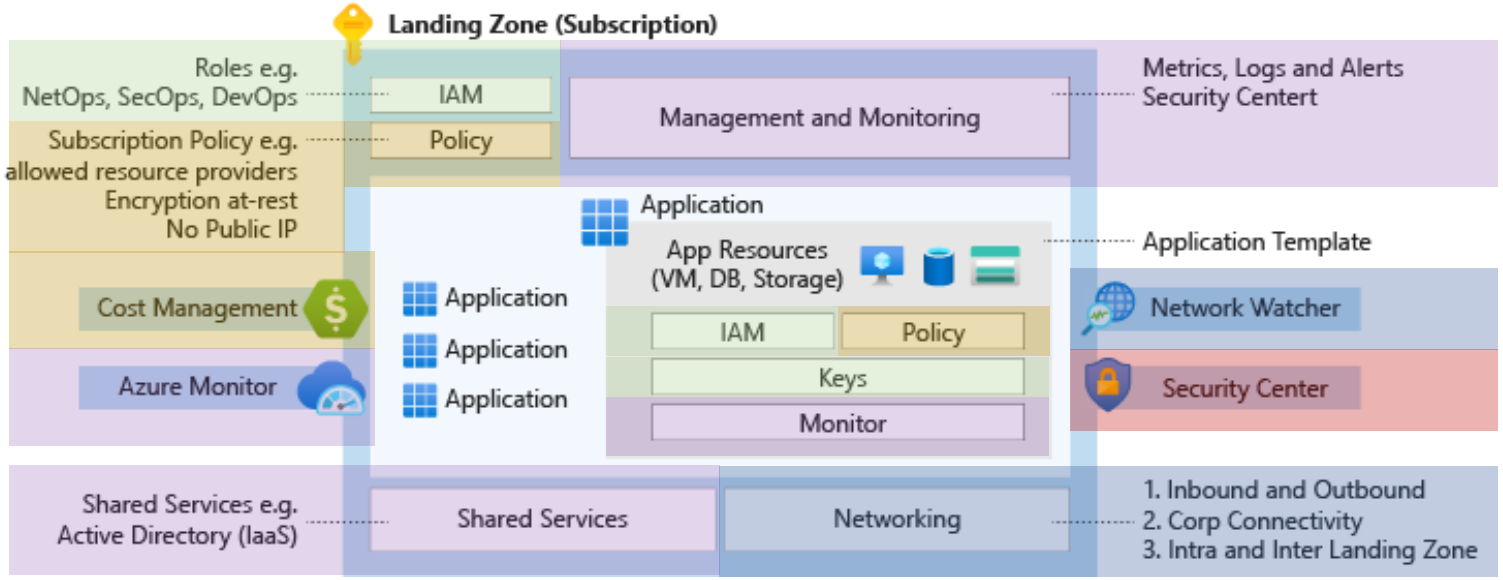
What is Enterprise-Scale?

„Azure landing zones help customers **set up their Azure environment** for scale, security, governance, networking, and identity."

„Draw on Microsoft's proven technical guidance, resources, and templates, to guide your customers through iteration and learning as they gain confidence and successfully adopt Azure."

Source: Cloud Adoption Framework enterprise-scale landing zone architecture

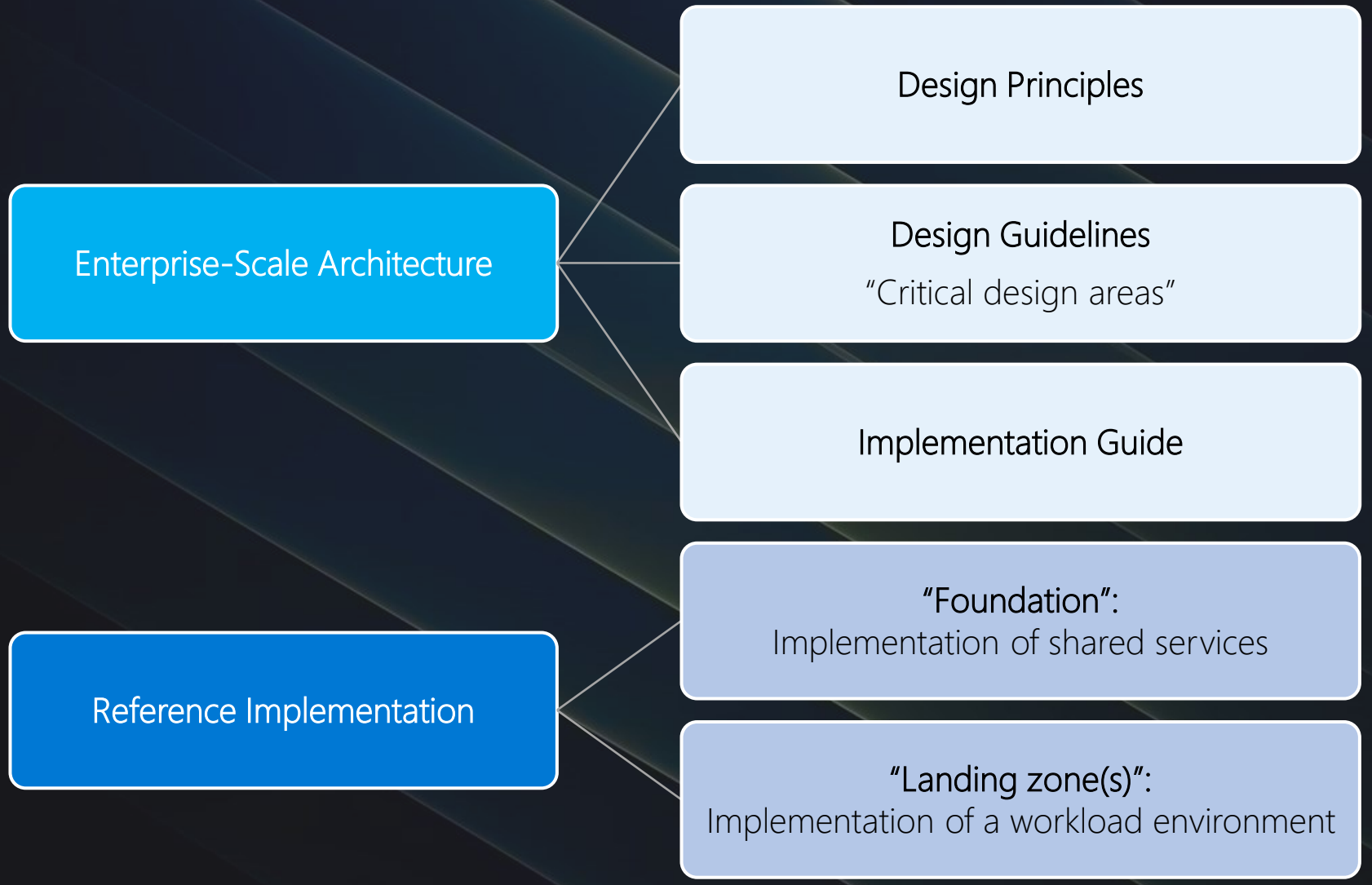
Design areas of Landing Zone(s)



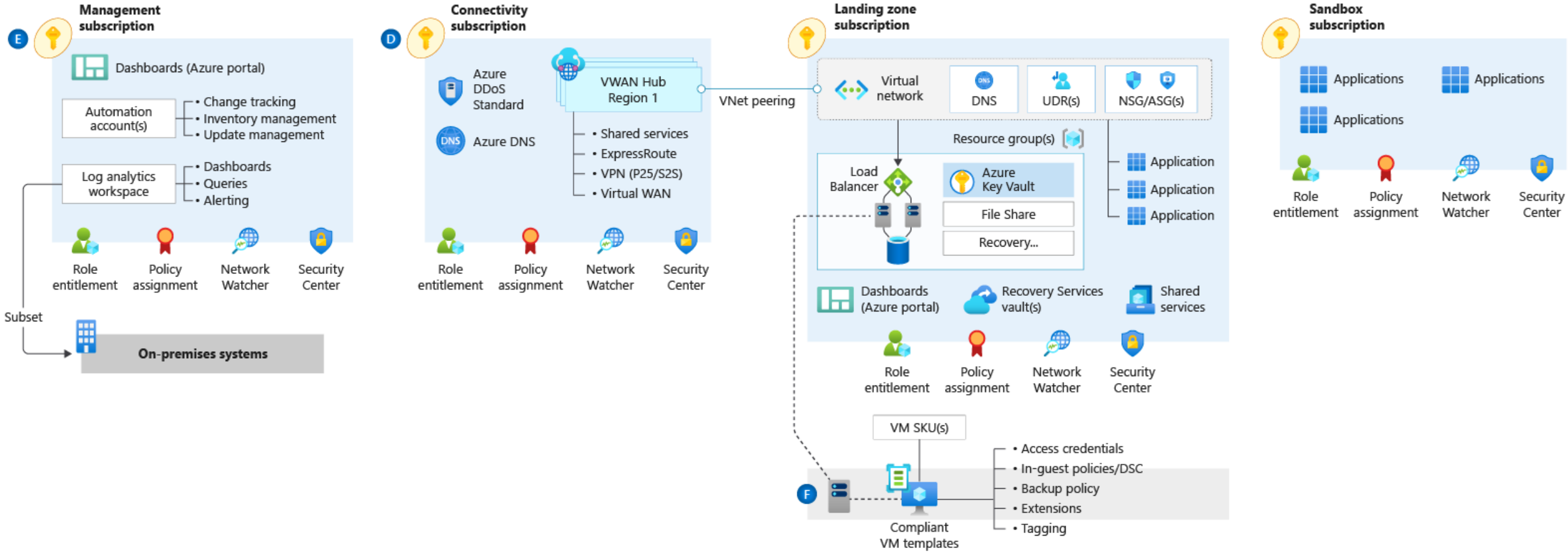
Connectivity, Identity, Governance, Operations and Security

Source: Cloud Adoption Framework enterprise-scale landing zone architecture

Enterprise-Scale Architecture & Reference

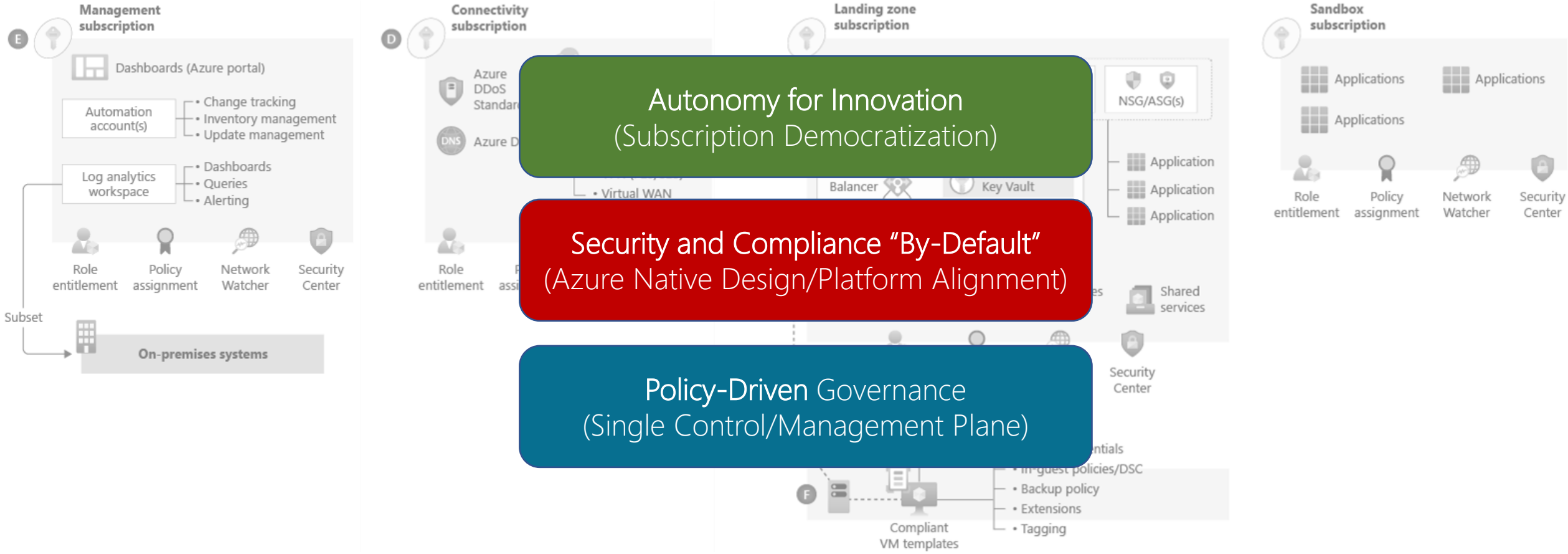


Enterprise-Scale Design Principles



Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

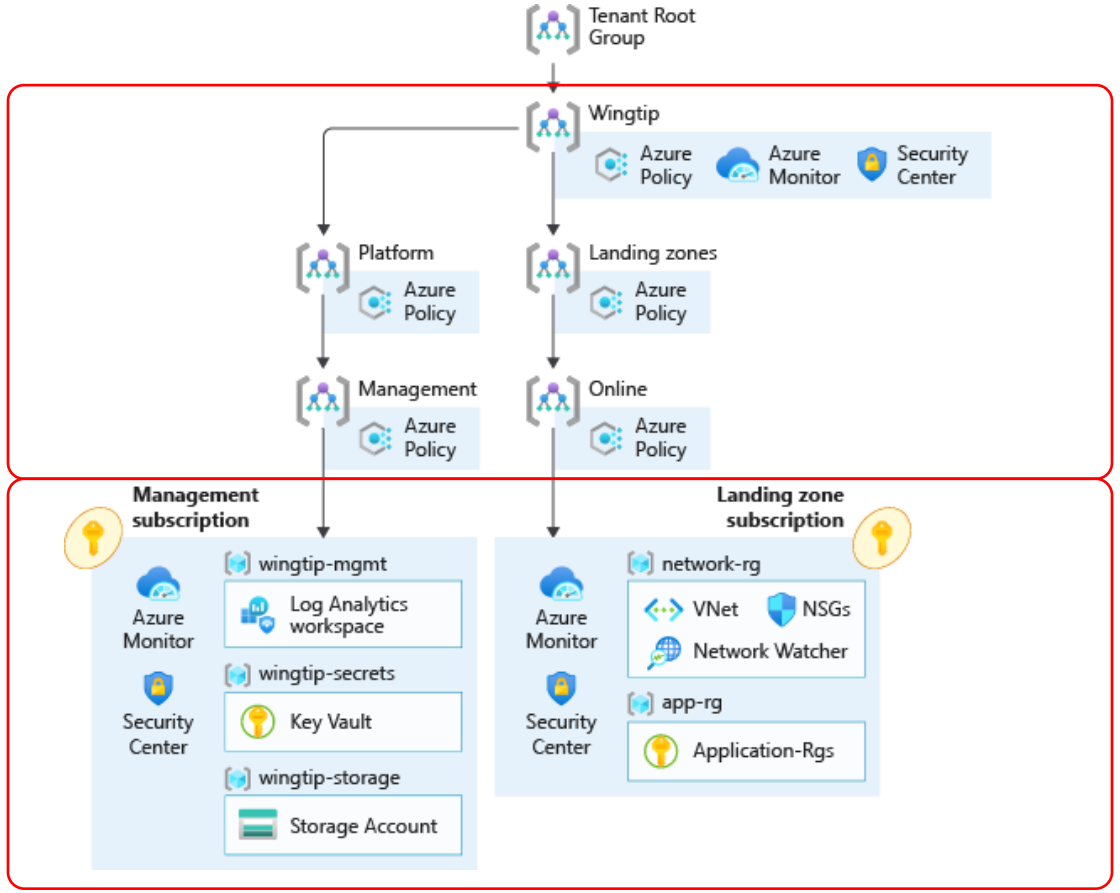
Enterprise-Scale Design Principles



Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

Enterprise-Scale Reference Implementation

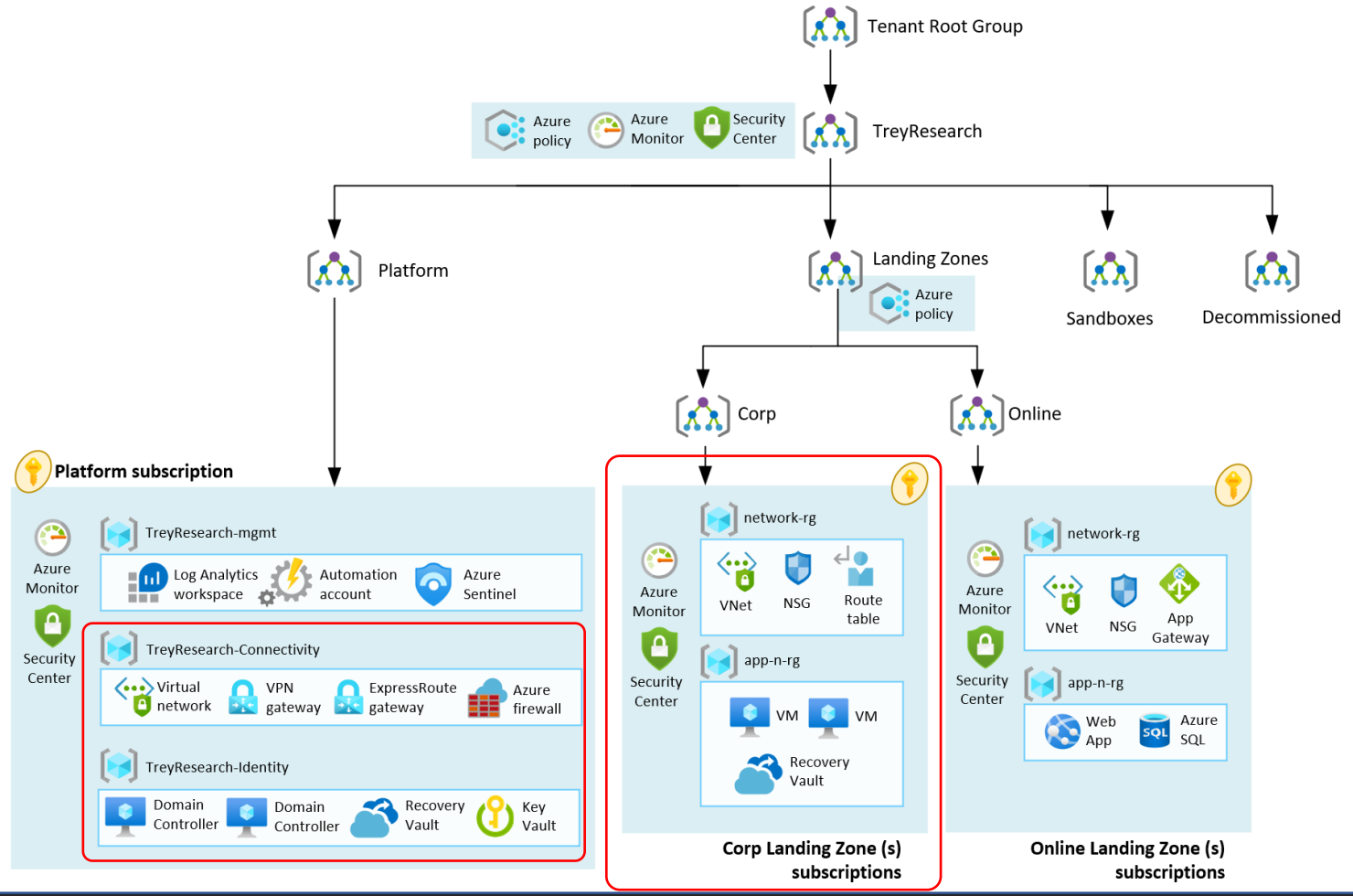
Foundation without hybrid connectivity (cloud-only)



Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

Enterprise-Scale Reference Implementation

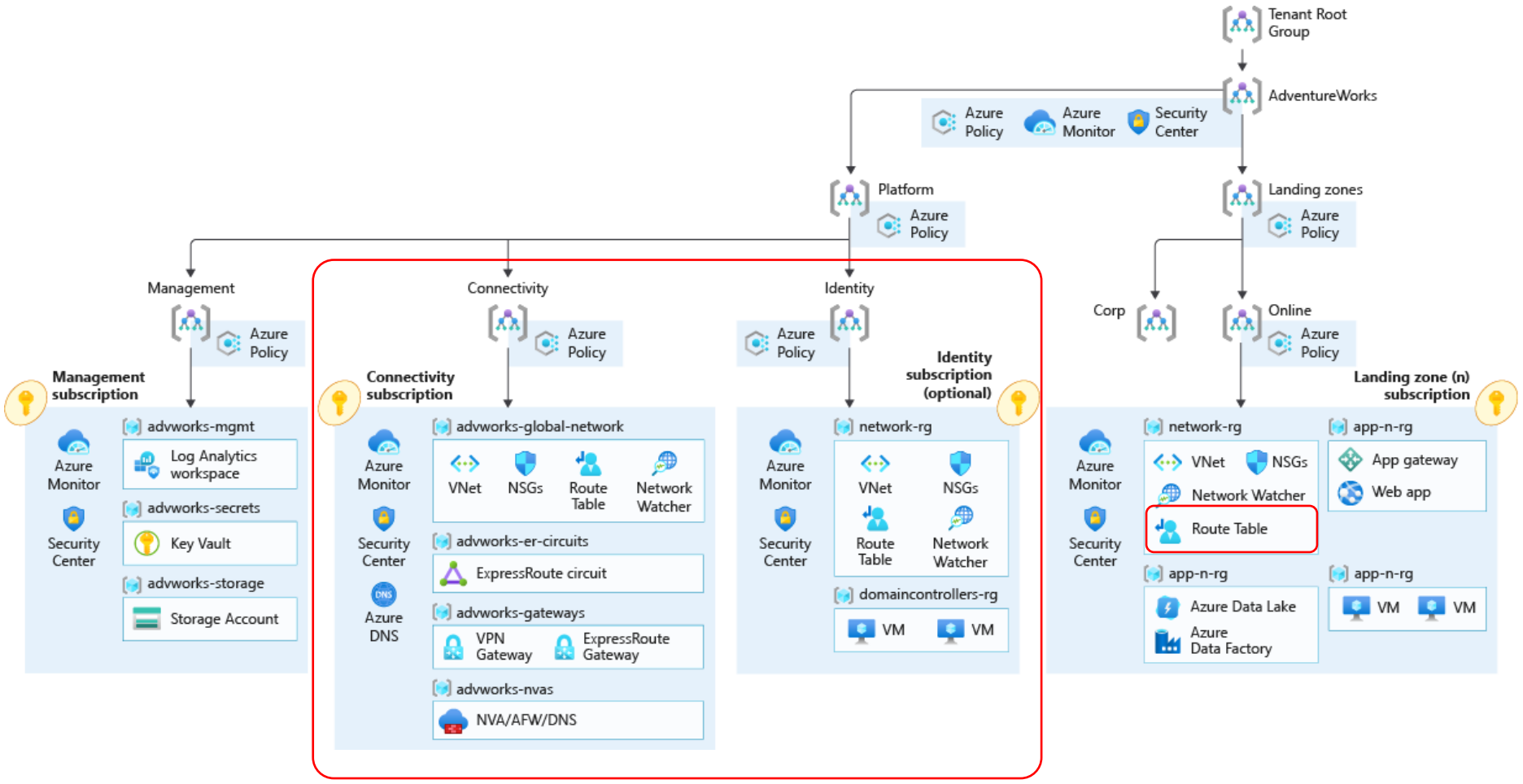
Foundation with hybrid connectivity (Small enterprise)



Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

Enterprise-Scale Reference Implementation

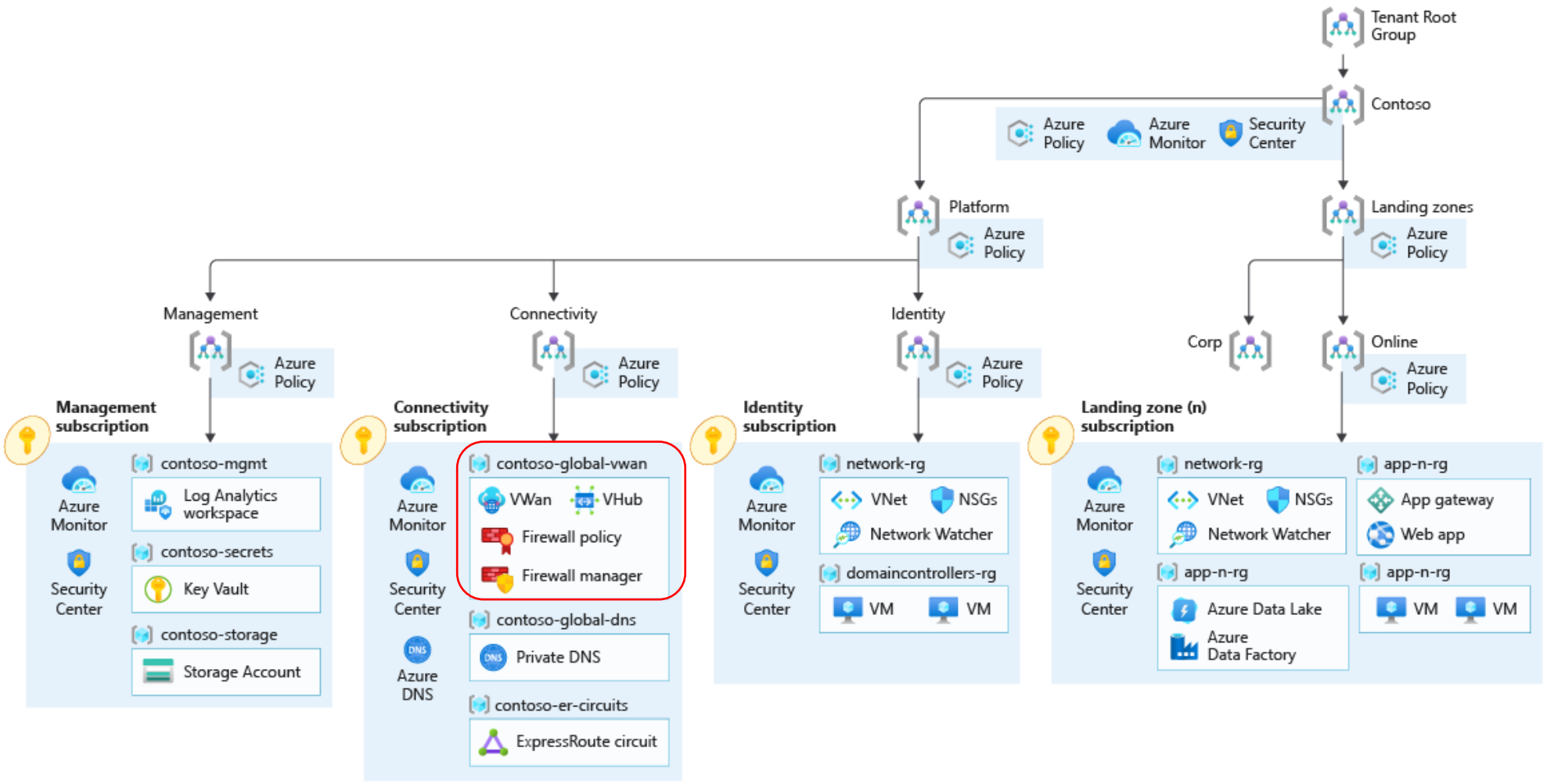
Foundation with Advanced Connectivity (Enterprise)



Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale with hub and spoke architecture

Enterprise-Scale Reference Implementation

Foundation with Azure VWAN Connectivity



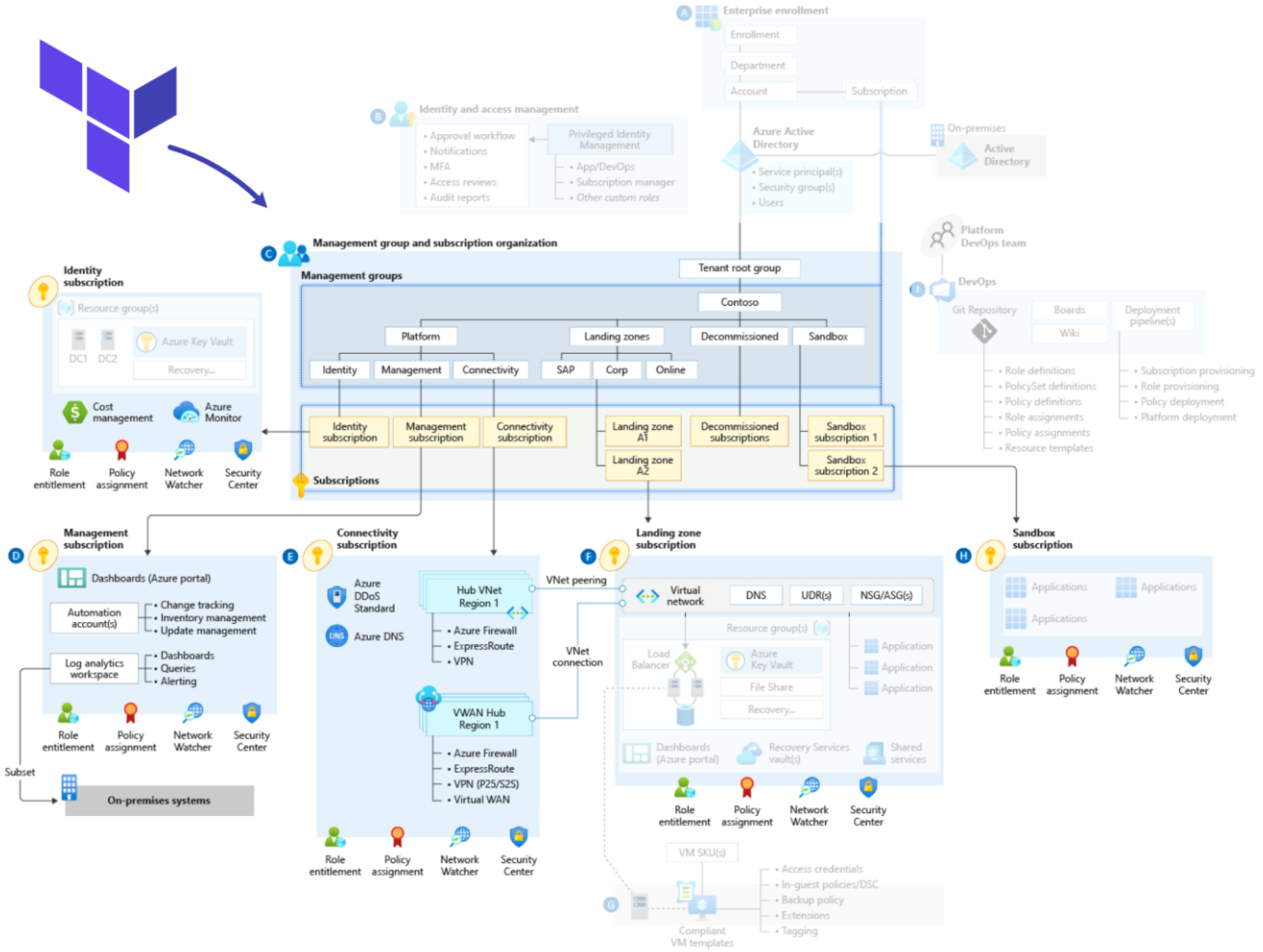
Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale with hub and spoke architecture

Enterprise-Scale
Deployment and Policies

DEMO

Enterprise-Scale Reference Implementation

Azure landing zones (Terraform Module)



[Azure Export for Terraform (fka Azure Terrafy)]
Existing Azure resources into HCL/tfstate

[AzAPI Terraform provider]
Layer on top of ARM API to complements the AzureRM Terraform provider

[AzureAD Terraform Provider]
Supports Core IAM, Access Packages, Conditional Access operations

Source: Azure landing zones Terraform module

Enterprise-Scale and AzOps

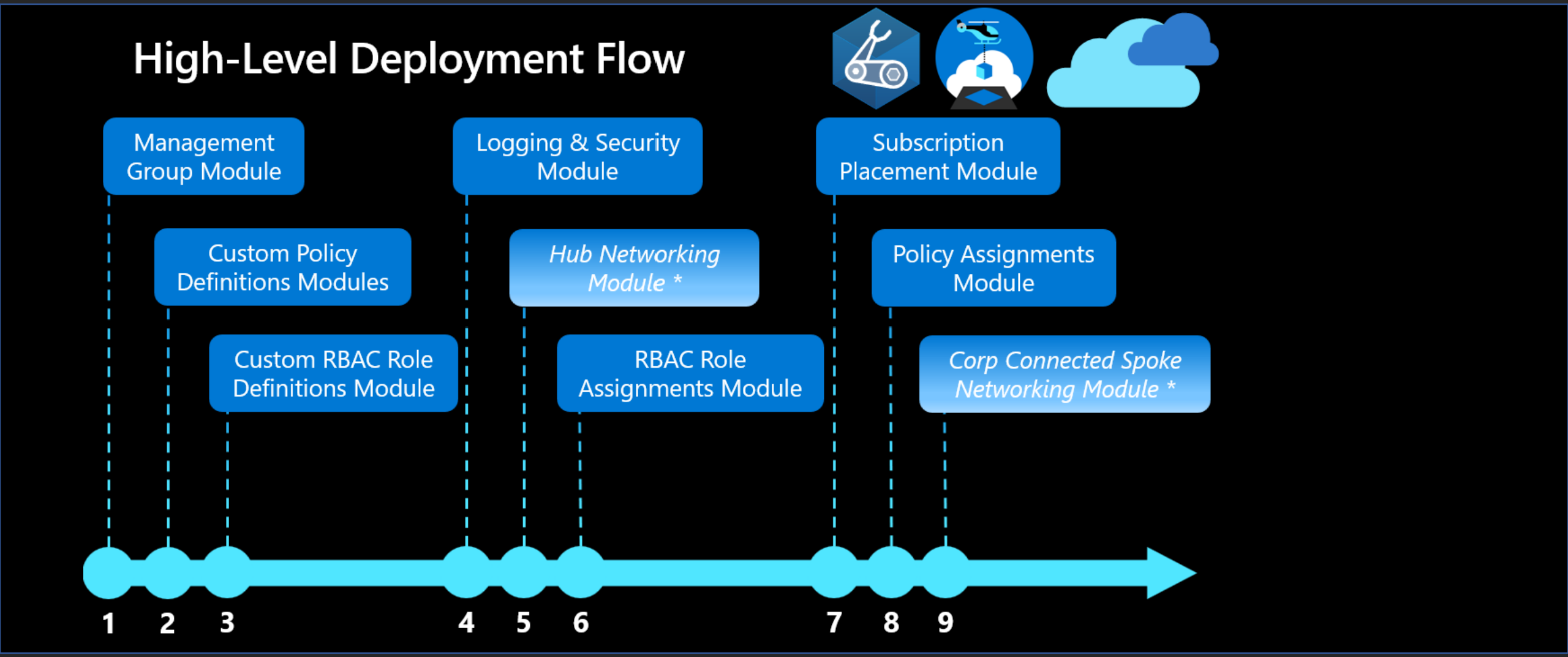
Git->Clone->Azure/Northstar	ARM as orchestrator to declare Goal-state at all 4 scopes: Tenant -> MGs -> Subs -> RGs	Operationalize: Configuration Drift and Reconciliation
Git -> Commit is new "az deploy"	**E2E orchestration for "North Star" to create Landing Zones**	**Azure-Native immutable configuration in Git**
Git repository scoped at customer AAD tenant for all Azure infrastructure	Integrated CI/CD pipeline with File->New Regions and Landing Zones i.e. subscriptions	Native platform capabilities for what-if, rollback, rollforward and complete mode
Discover existing Azure environment as-is	Autonomous Landing Zones - enforced by Azure Policy in platform	Inclusive of DevOps (Git) and ITPros (Portal)
Turn-on the lights for existing resources and configuration	Azure Engineering and platform roadmap aligned	Consistent export of all resources at all scopes across the tenant with implicit dependencies

Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

AzOps
Repository and CI/CD Pipelines

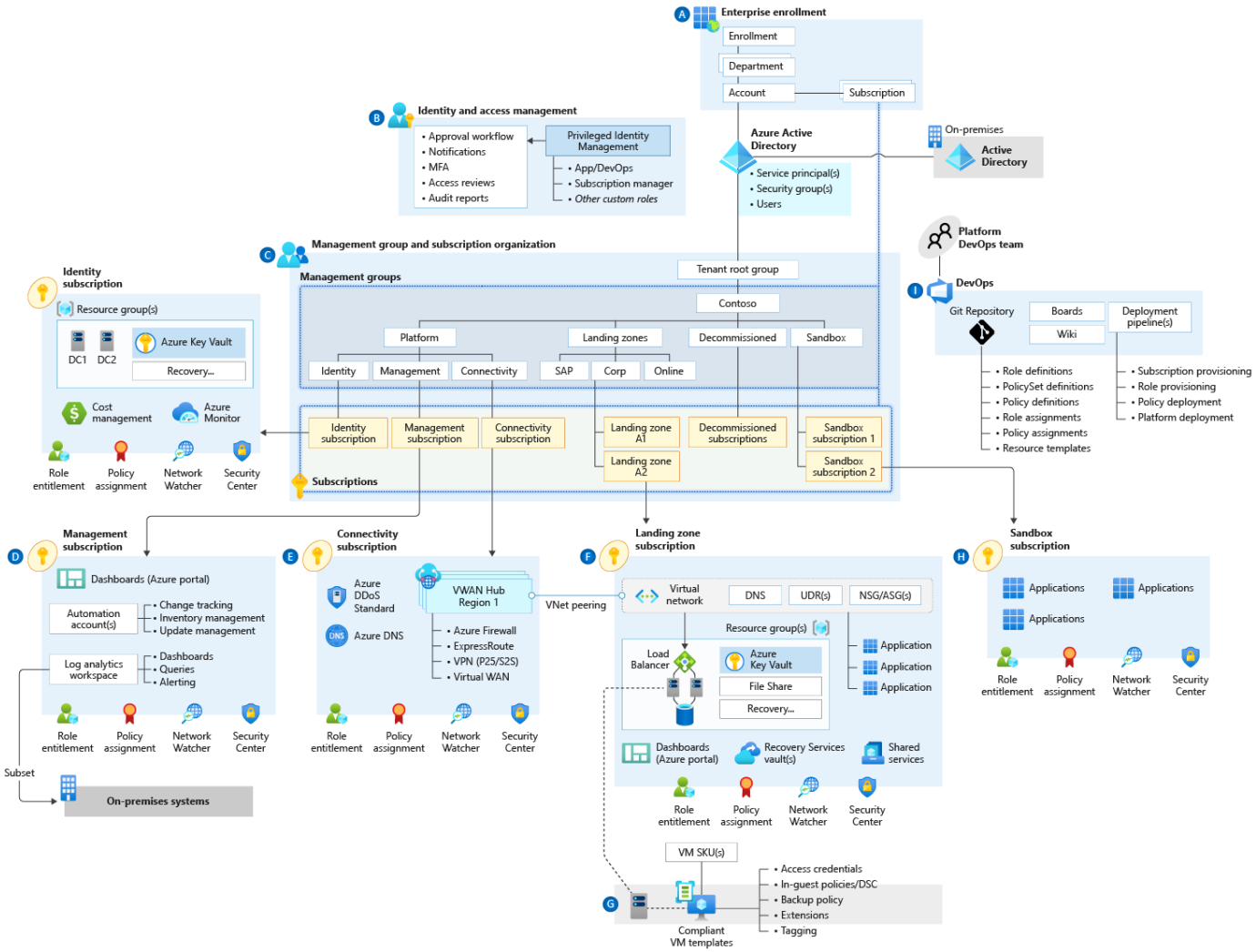
DEMO

Enterprise-Scale Architecture



Source: Azure landing zones - Bicep modules design considerations - Azure Architecture Center | Microsoft Learn

Enterprise-Scale Architecture



Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

Enterprise-Scale **Critical Design Areas**

Enterprise Enrollment & Azure AD Tenants

Identity & Access Management

Management Group & Subscription Organization

Network Topology & Connectivity

Management & Monitoring

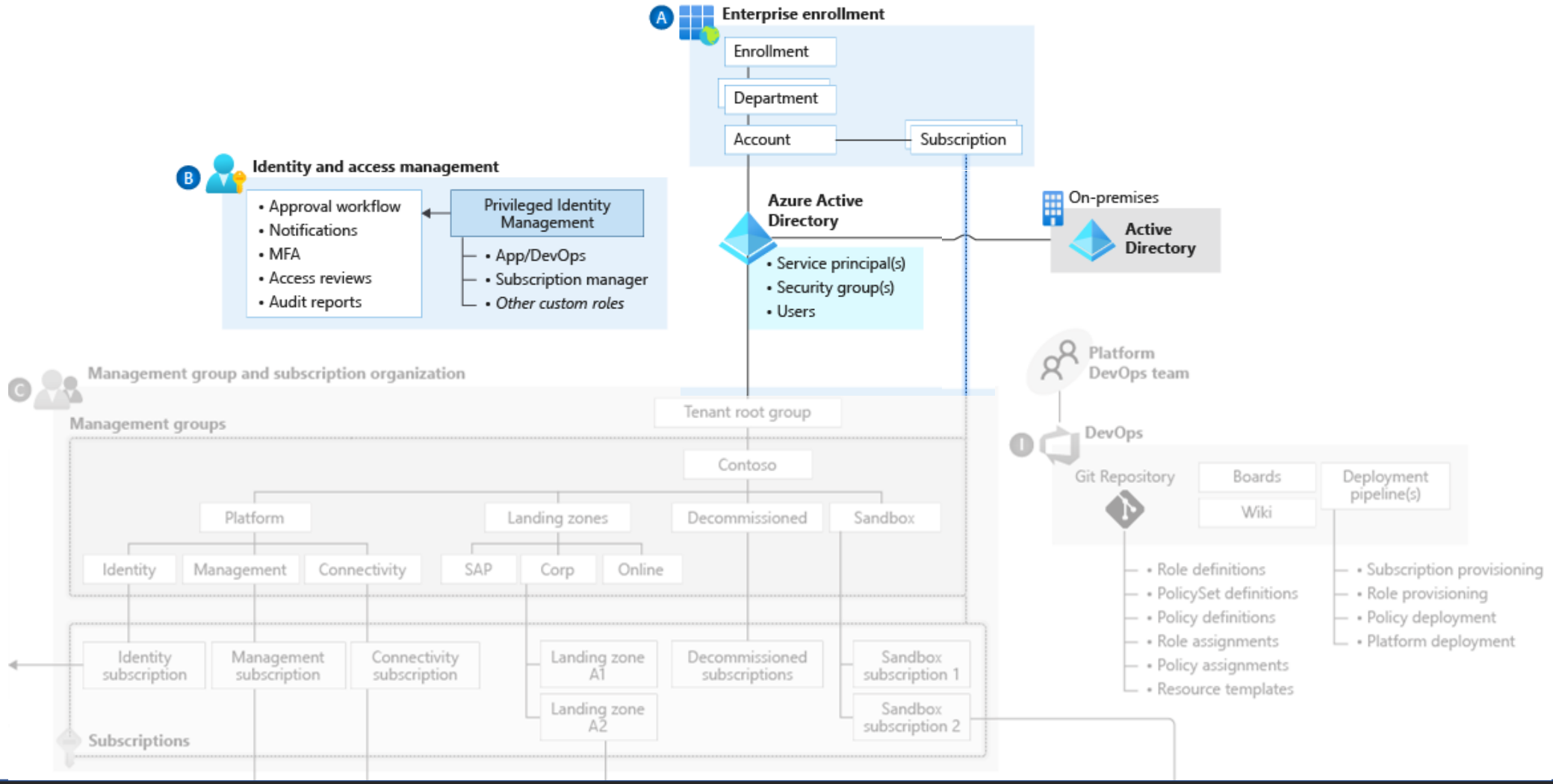
Business Continuity & Disaster Recovery

Security, Governance & Compliance

Platform Automation & DevOps

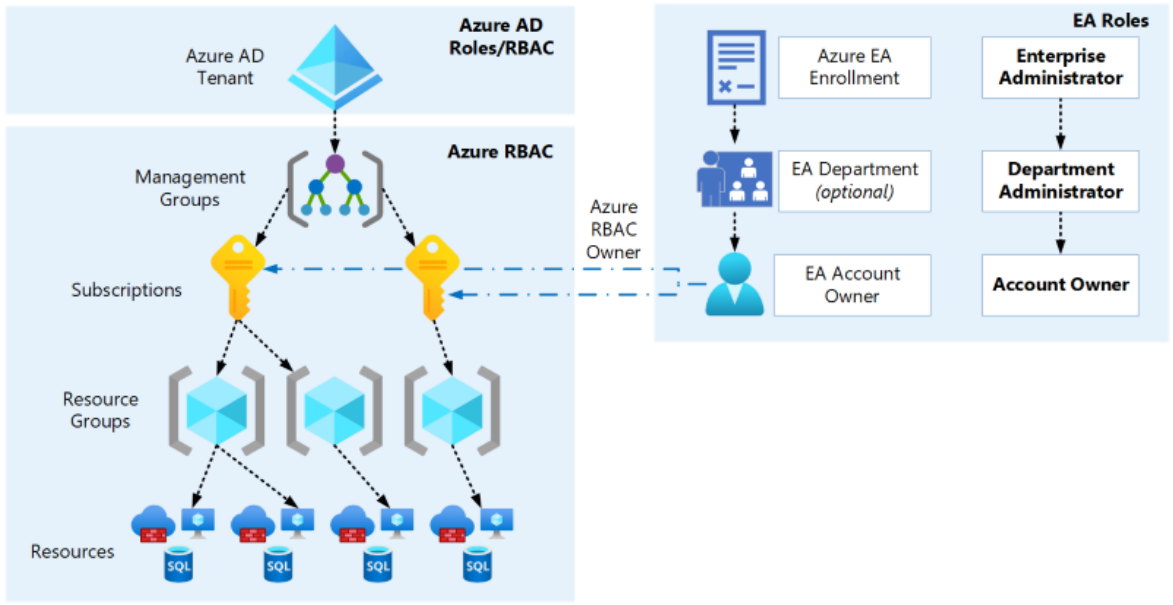
Source: GitHub-Repo "Azure/Enterprise-Scale" - Deploy Enterprise-Scale foundation

Critical Design Areas: Enrollment and Tenants



Source: Start with Cloud Adoption Framework enterprise-scale landing zones

Critical Design Areas: Enrollment & Tenants
Enterprise Agreement Hierarchy

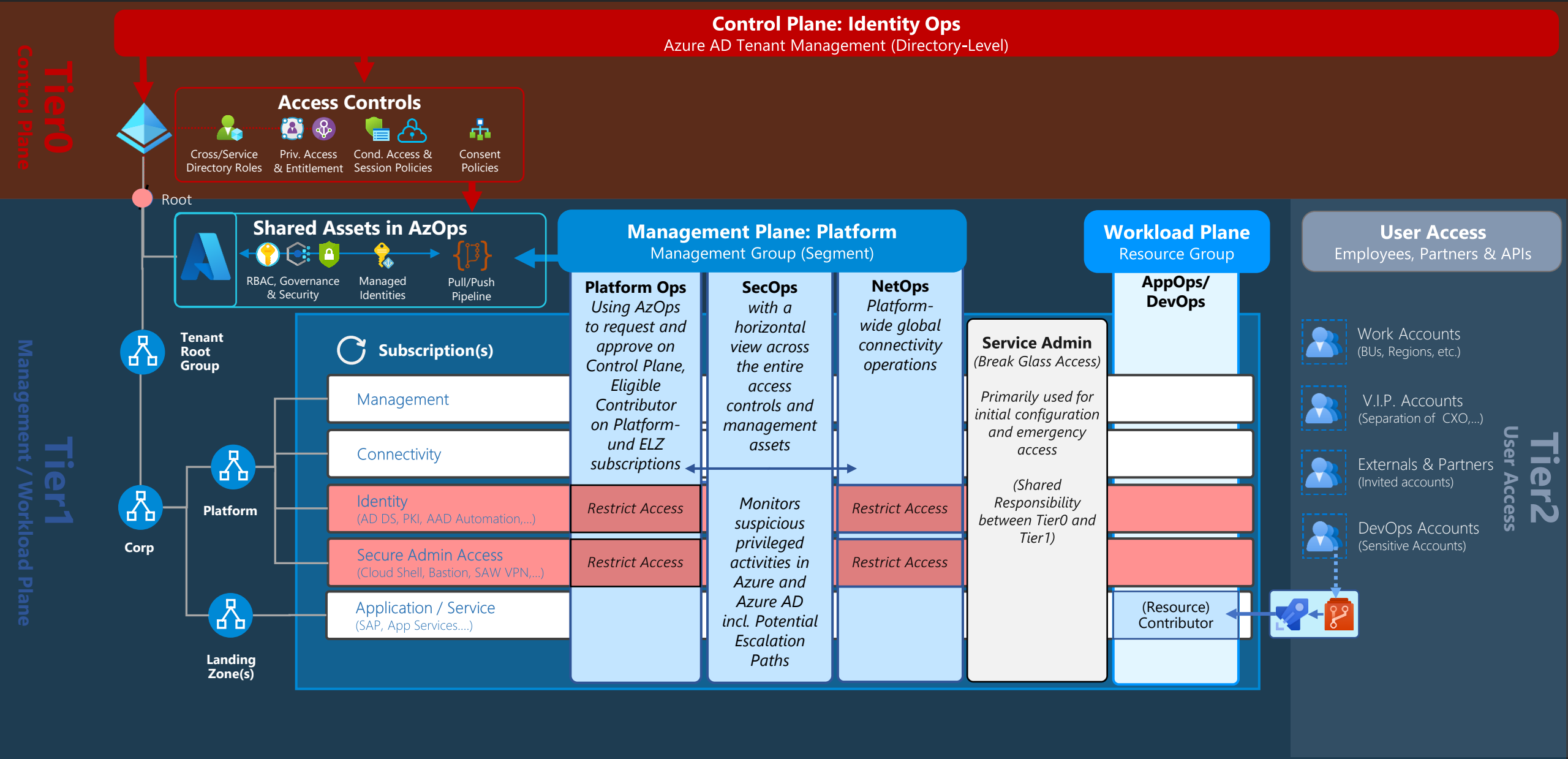


- Account Owner = Privileged User
  Restrict and minimize the number of account owners within the enrollment
- No Auditing and PIM integration
  Periodically audit the EA portal to review and avoid "manual management"

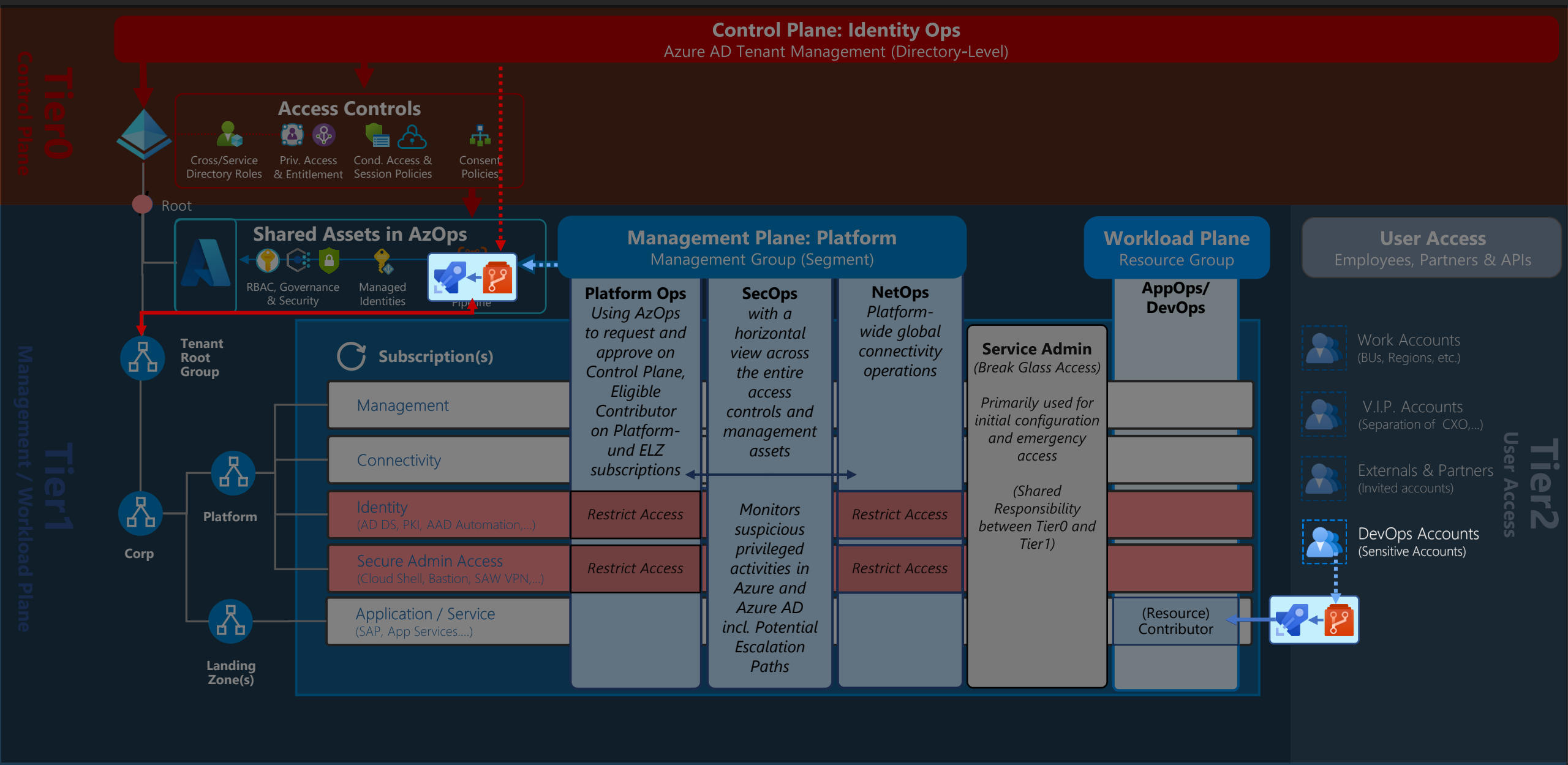
→ Automation (as part of AzOps) and Account Owner as "Break Glass"

Source: Complete Enterprise Agreement tasks in your billing account for a Microsoft Customer Agreement

Example of Tiered Administration Model



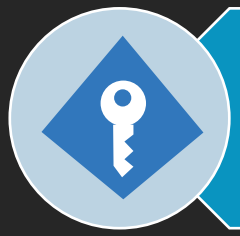
Example of Tiered Administration Model



Managing and monitoring of privileged DevOps access

DEMO

Take Aways: Best Practices in Azure IAM



Evaluate built-in roles, considerations in creating custom roles

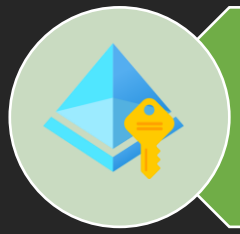
- Custom Roles are powerful but can be also complex
- RBAC-as-Code approach and/or managed with Entra Permissions Management

Avoid permissions referencing to specific resources or user

- Create role-based design for wide-scope permissions (PlatformOps, NetOps, etc.)

Assign eligible permissions based to Azure AD Groups

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



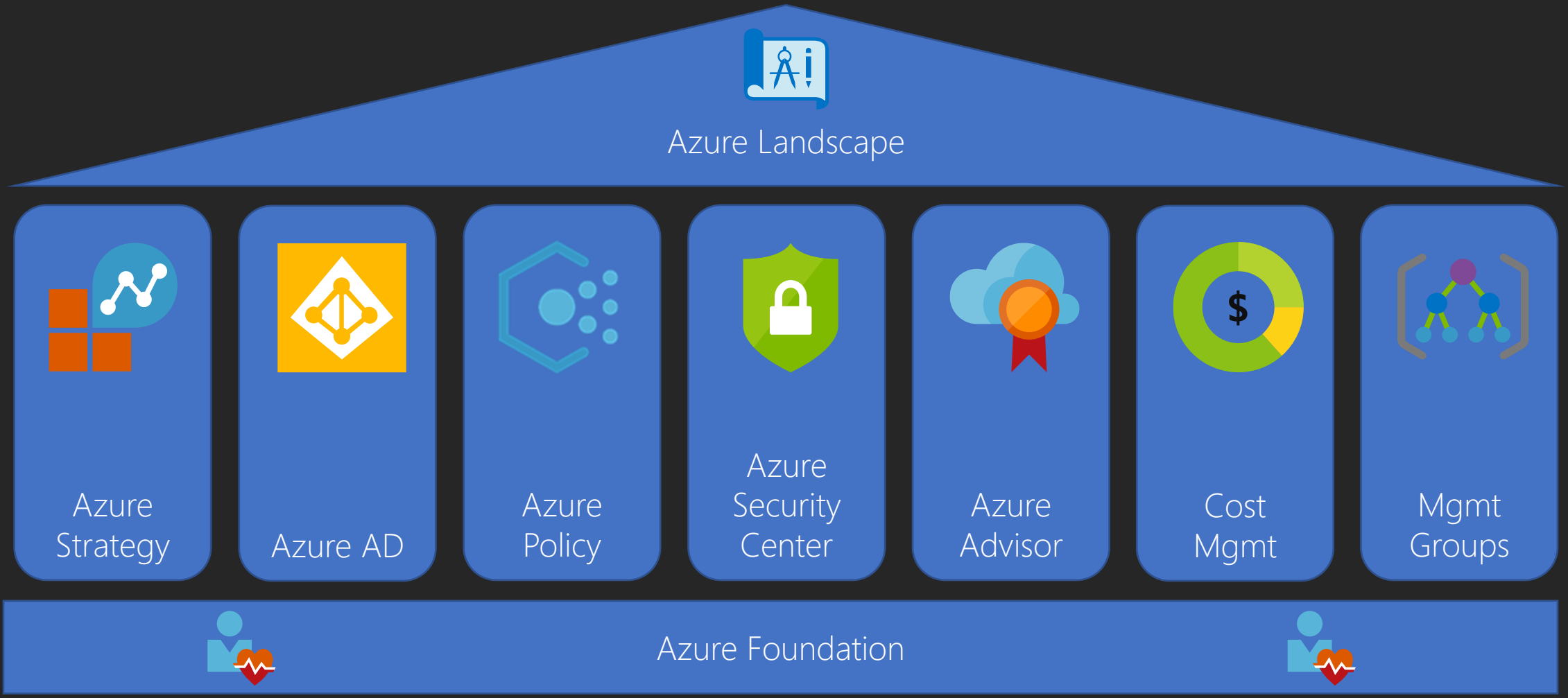
Access to Azure resources by „Managed identities“ / KeyVault

- Use Managed Identity/Federated Credentials, certificate for other service principals
- use Azure KeyVault to protect your secrets, keys or certificates

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/azure-portal/azure-portal-quickstart-center
- 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/

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 regulary meeting/call for Cloud news
- Get in touch with Partners and Community for help and support

DATA SATURDAYS

Session Slides

Questions?
Reach us via Twitter ☺


@Thomas_Live

www.cloud-architekt.net

| @GregorReimling
| www.reimling.eu

| @AzureBonn
| www.azurebonn.de