Empower Security and Compliance with Azure Policy

Gregor Reimling

aMS Aachen
16.11.2023

Thanks to our SPONSORs

Vielen Dank an unsere Partner!

Organizing sponsor

Sponsors

audiocodes

AvePoint

BARCO

Lenovo

Magic Leap

nureva

Associates EST. 1992

Yealink

EPSON

Organisatorischer Partner

About “Gregor Reimling”

Azure Meetup BONN

www.azurebonn.de

Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

https://www.Reimling.eu

Certifications

Cloud Security Architect, MVP for MS Azure & Security

Hobbies

Family, Community, Worldtraveler

Contact

Cloud Inspires Podcast

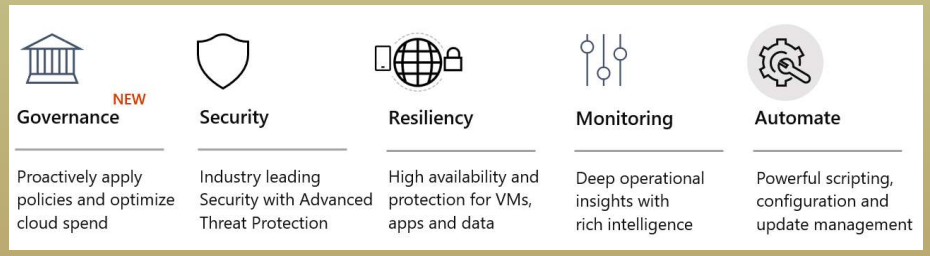
Stories and people behind Cloud Transformation

www.cloudinspires.me

@GregorReimling

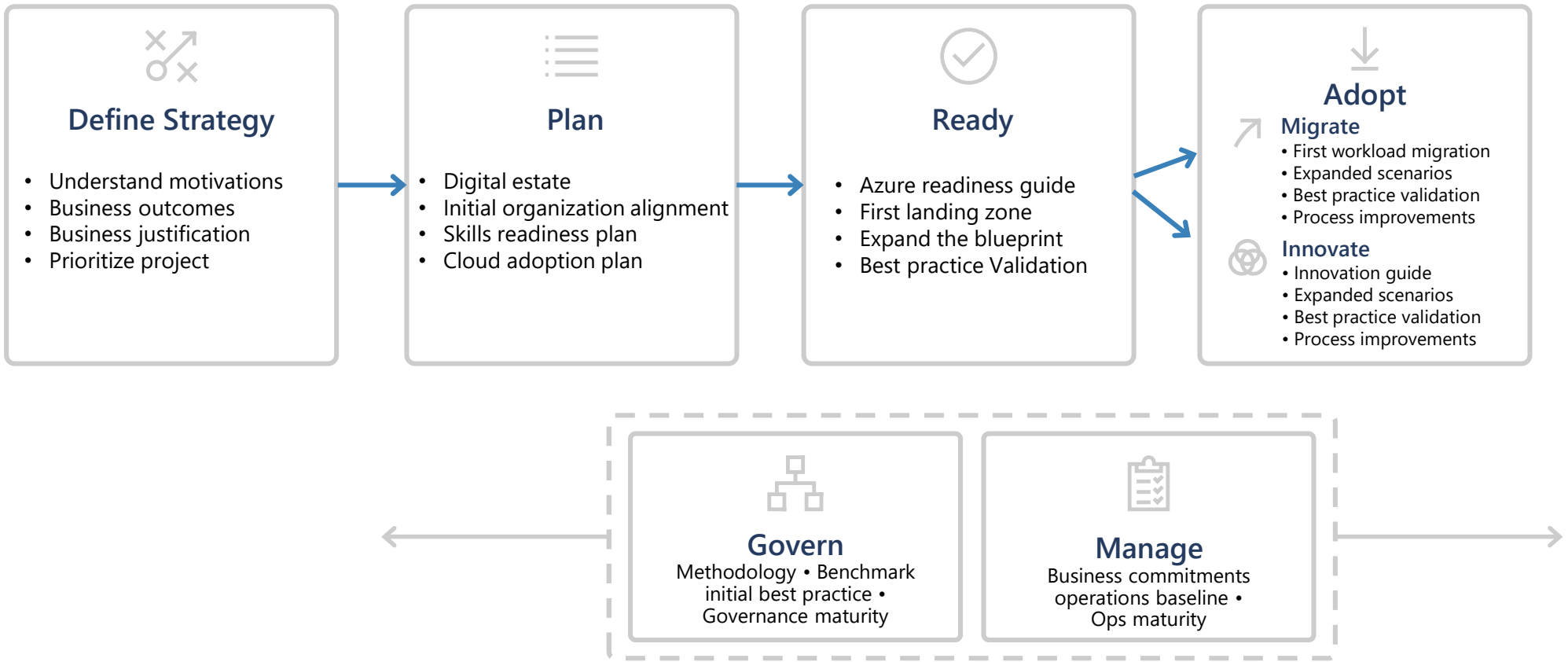
Gregor Reimling

Agenda



- How it works
- Policies at scale
- Recommended Policies
- Automation and Remediation
- MS Defender for Cloud

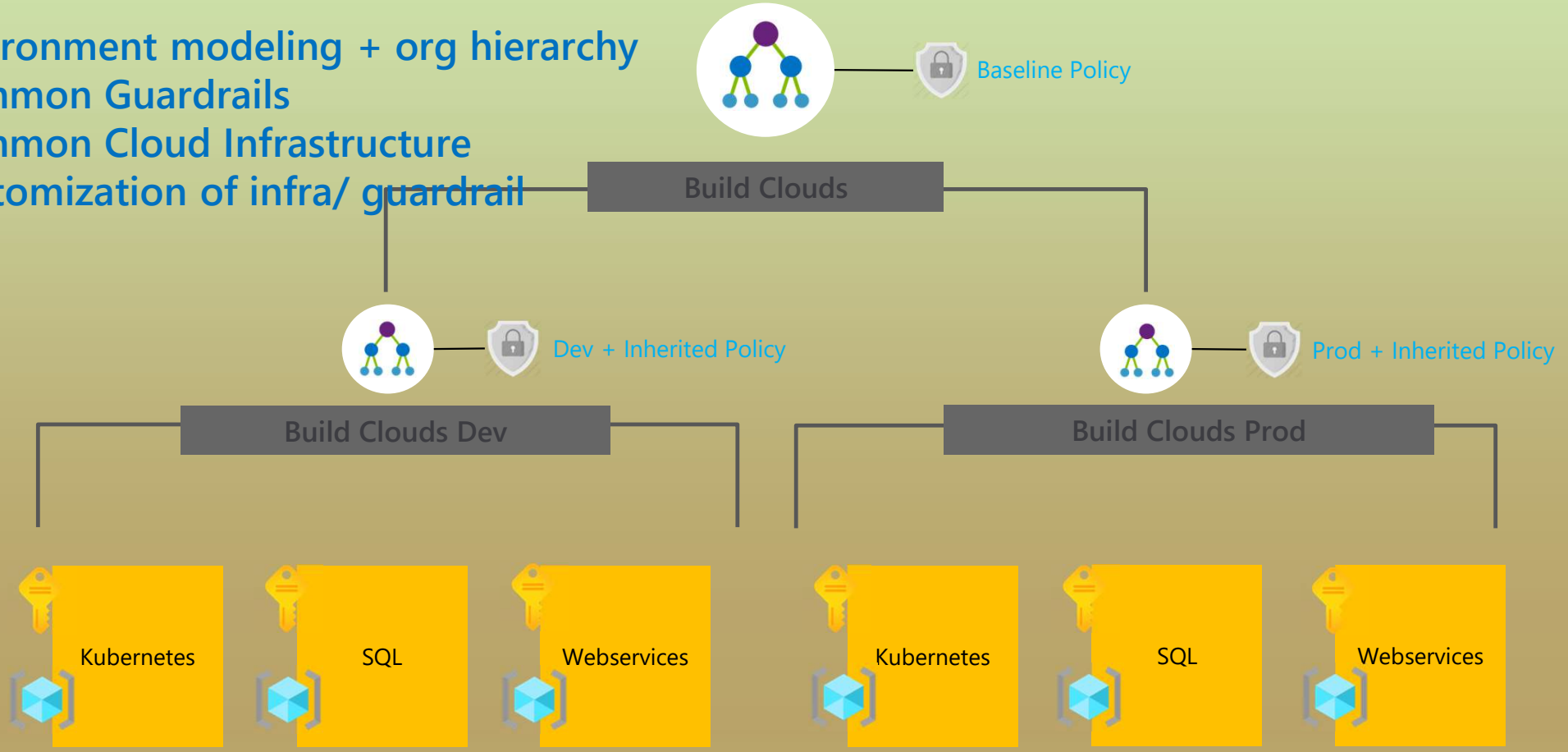
Microsoft Cloud Adoption Framework for Azure



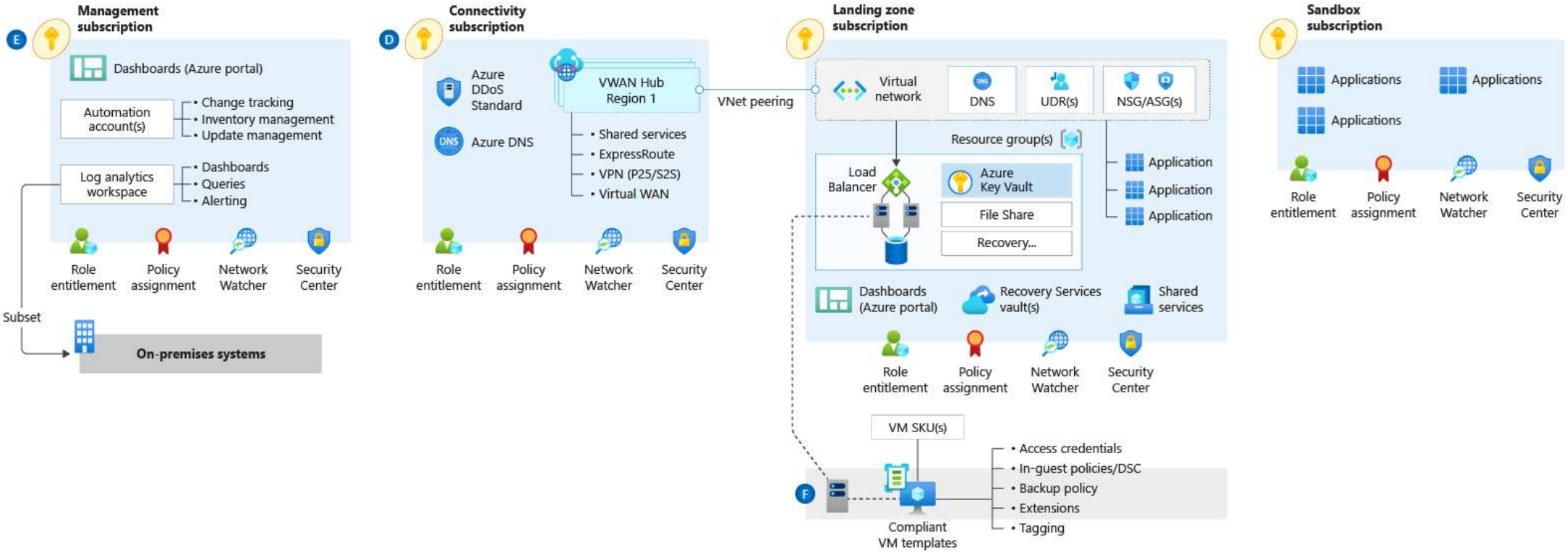
https://azure.microsoft.com/en-us/cloud-adoption-framework/

Management Groups

Environment modeling + org hierarchy
Common Guardrails
Common Cloud Infrastructure
Customization of infra/ guardrail

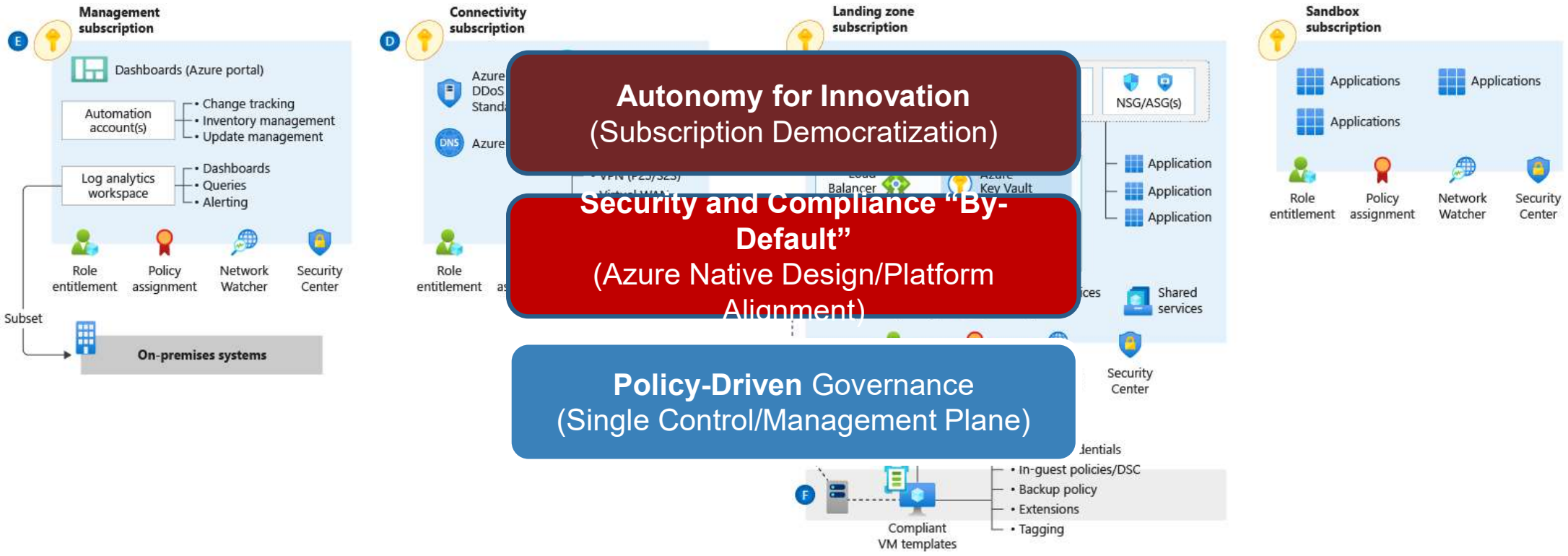


Enterprise-Scale - Design Principles



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

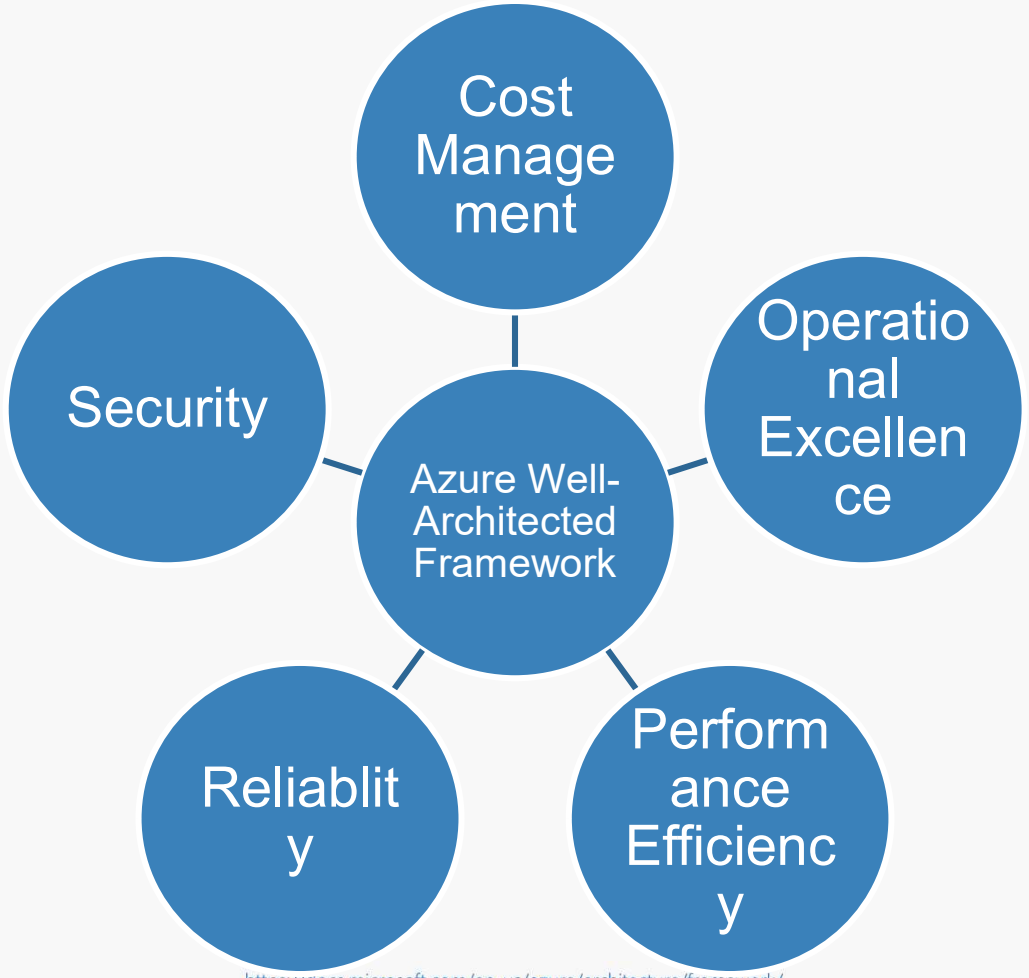
Enterprise-Scale - Design Principles



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

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."



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

Azure Advisor

What are Azure Policy

- 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

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

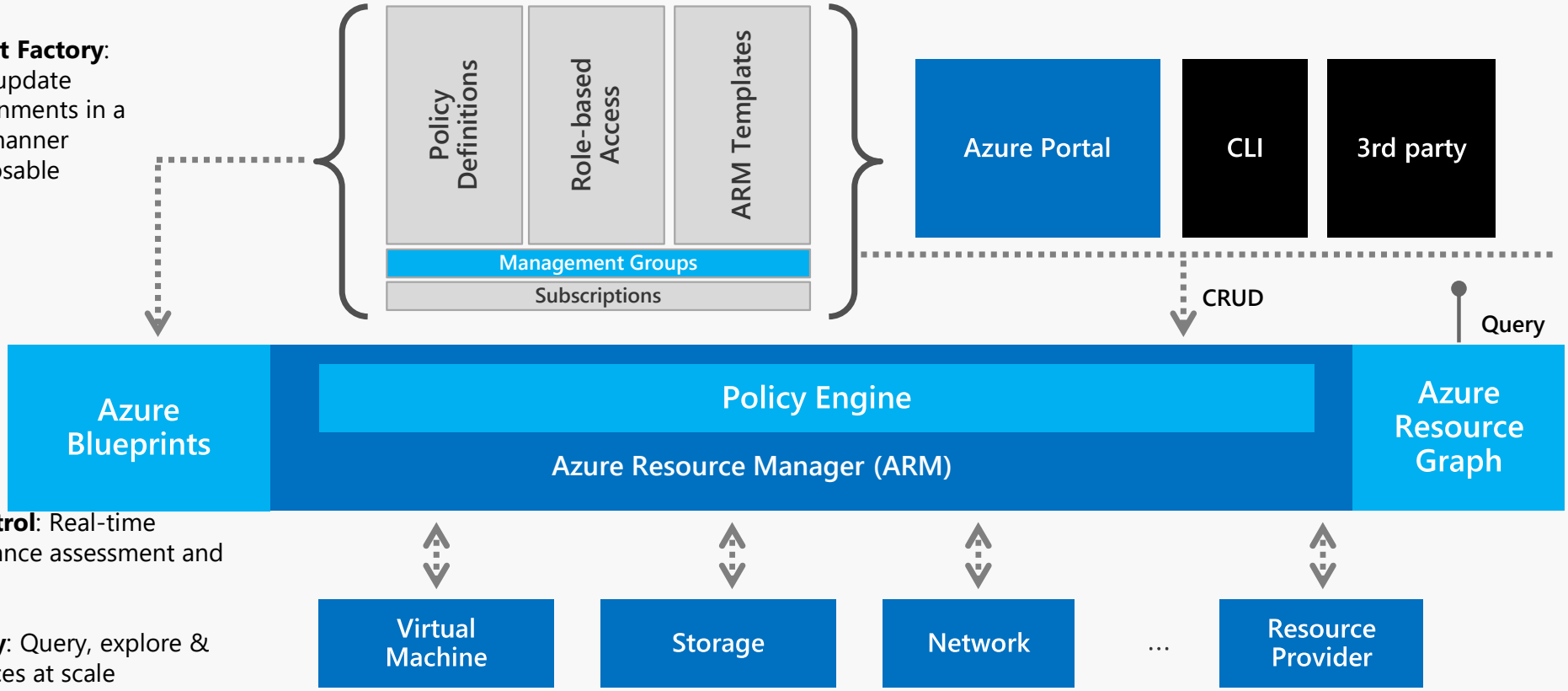
- Real time remediation
- Remediation on existing resources (**NEW**)

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

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

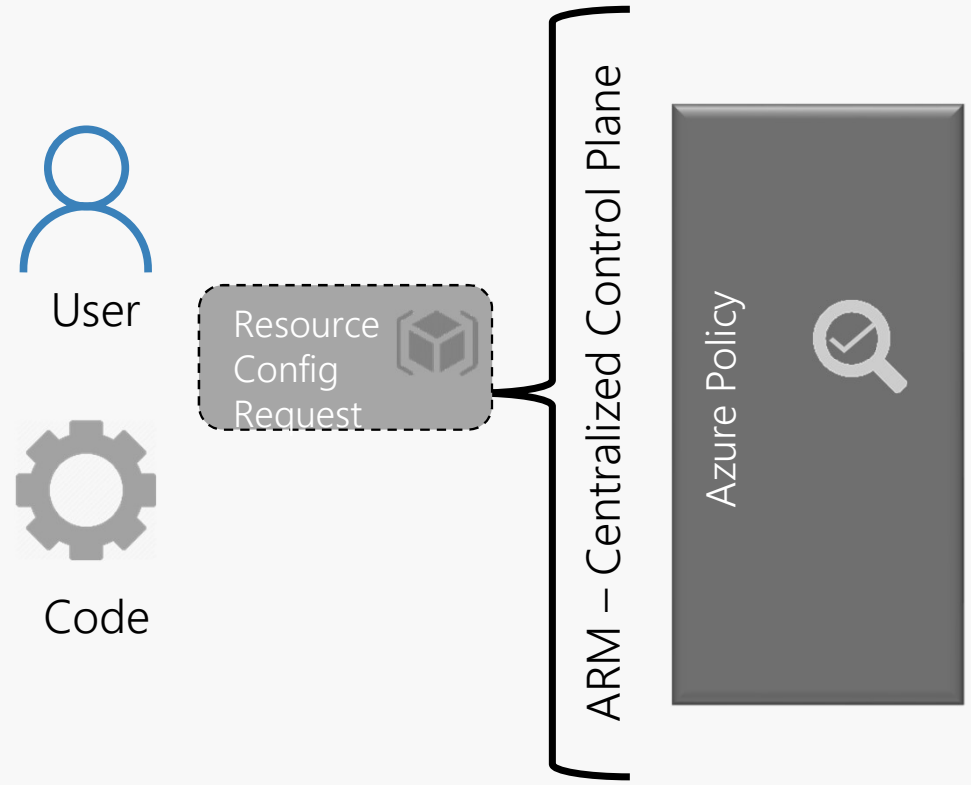
Cost

Allowed VM SKUs

Allowed Storage

SKUs

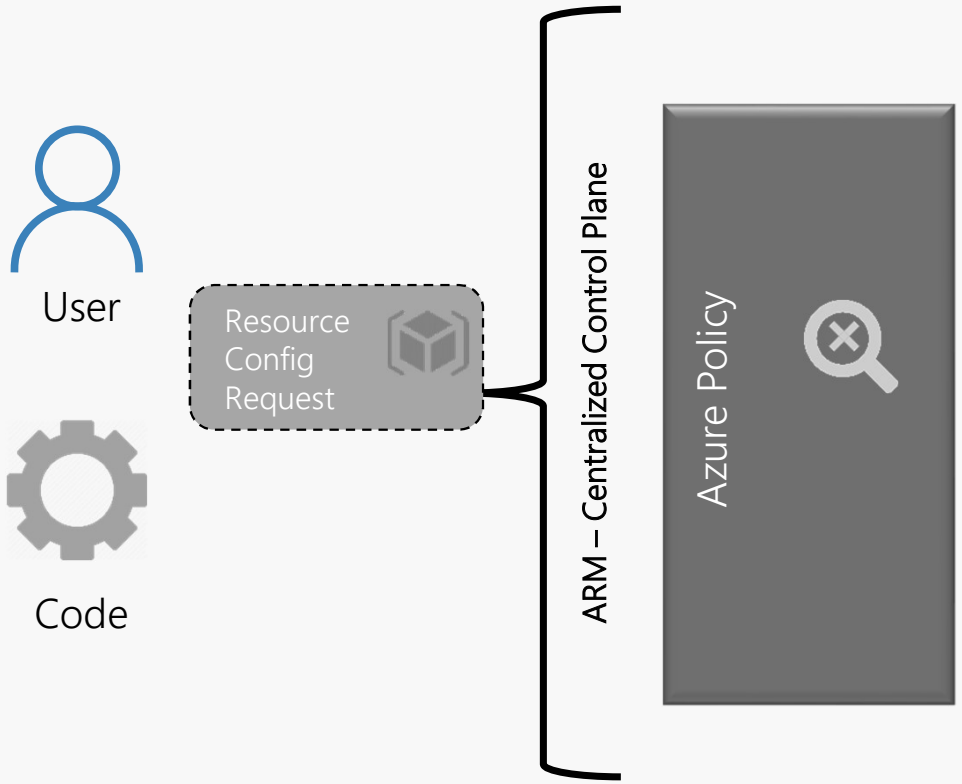
How does it work?



Order of evaluation

1. Append
2. Audit
3. AuditIfNotExists (on the fly)
4. Deny
5. DeployIfNotExists (check after 15 min)

How does it work?



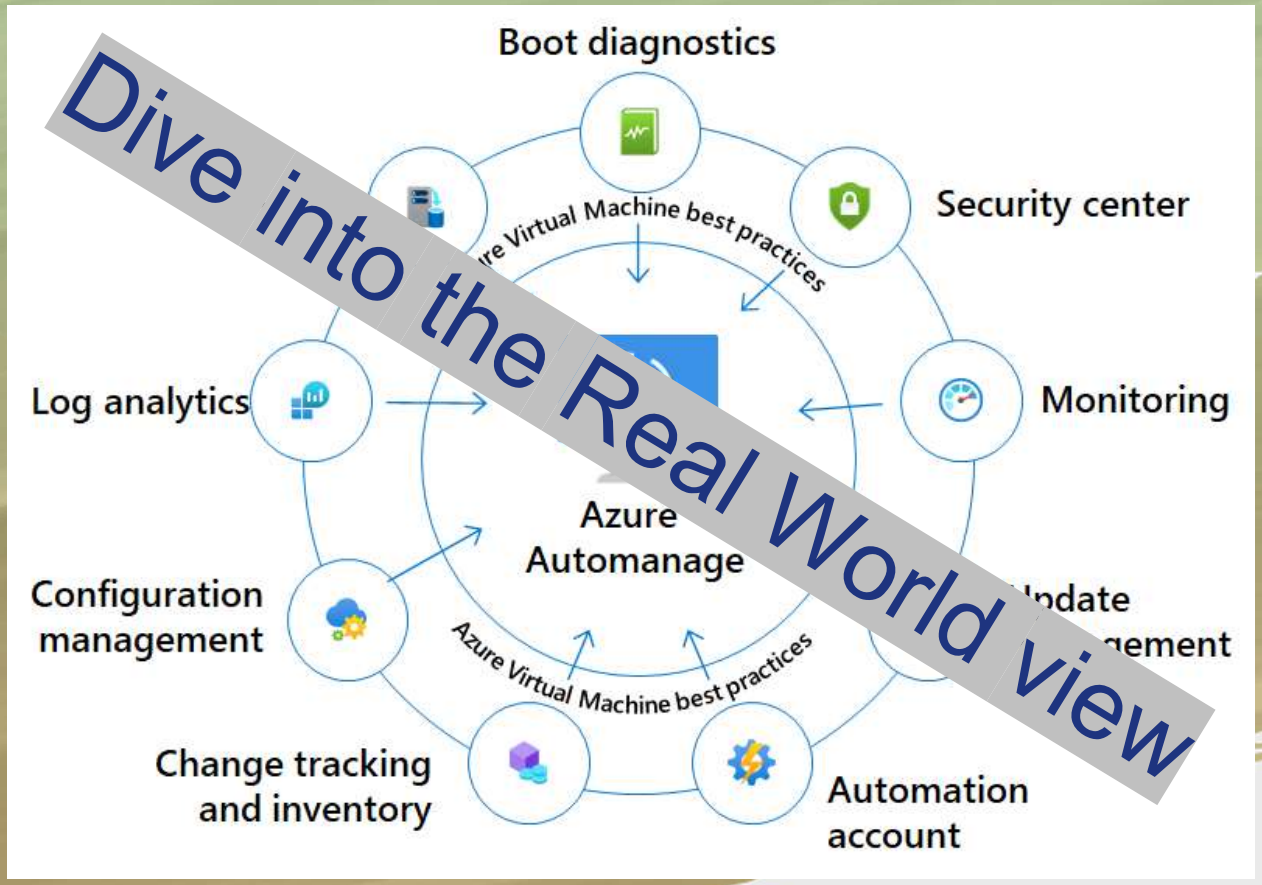
Append

Audit

AuditIfNotExists (on the fly)

Deny

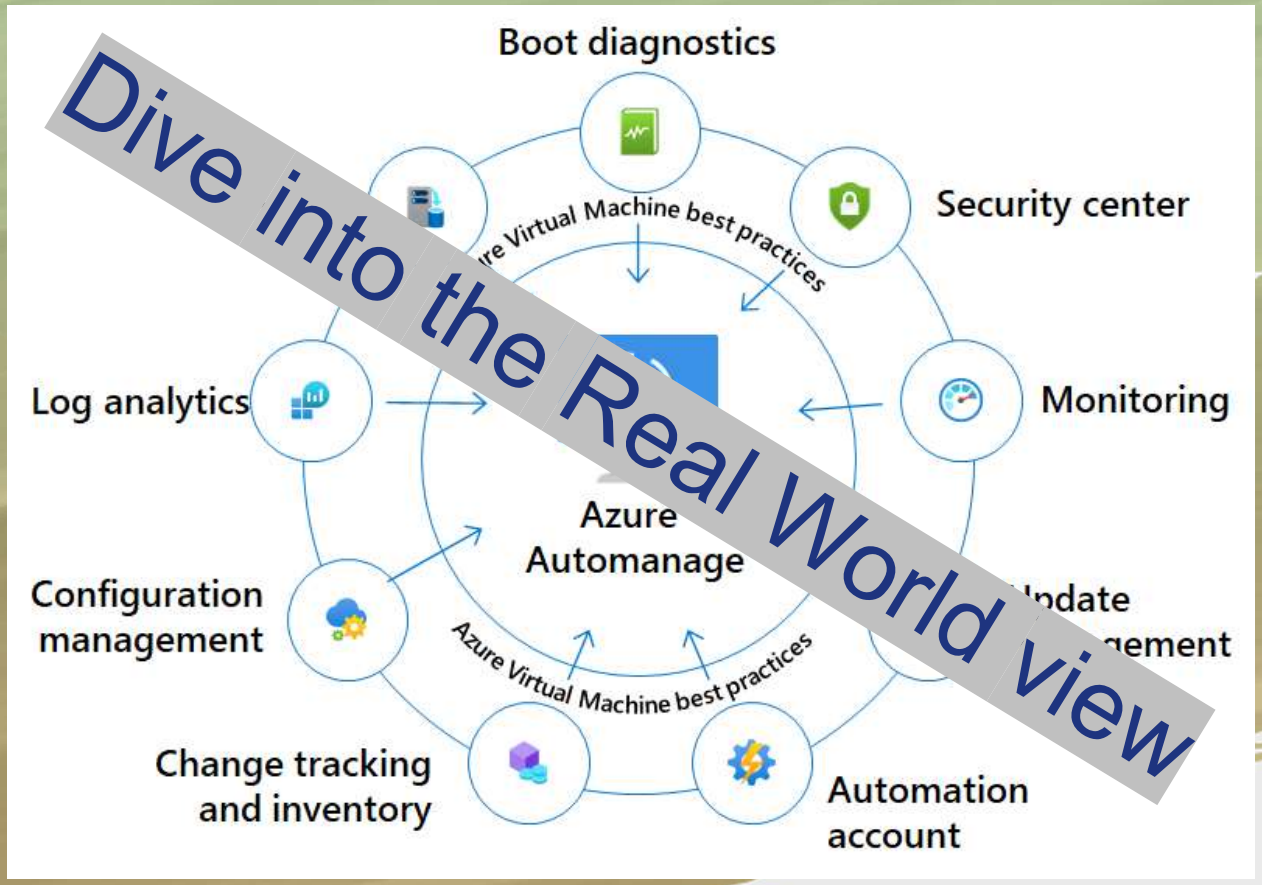
DeployIfNotExists (check after 15 min)



Dive into the Real World view

Azure Policy Definition structure

```
{   "properties": {
      "mode": "all",
      "parameters": {
        "allowedLocations": {
          "type": "array",
          "metadata": { "description": "The list of locations that can be specified when deploying resources",
            "strongType": "location",
            "displayName": "Allowed locations"  },  "defaultValue": [ "westus2" ]
        } },
      "displayName": "Allowed locations",
      "description": "This policy enables you to restrict the locations your organization can specify when deploying resources.",
      "policyRule": {
        "if": {
          "not": {
            "field": "location",  "in": "[parameters('allowedLocations')]"
          } },
        "then": {  "effect": "deny"
```



Dive into the Real World view

Microsoft Defender for Cloud

A SERVICE TO STRENGTHEN YOUR SECURITY POSTURE

AVAILABLE IN TWO TIERS – ASC BASIC AND AZURE DEFENDER

BASIC -> FREE – ACTIVATED BY DEFAULT FOR ALL SUBSCRIPTIONS

BASED ON AN SECURITY SCORE – SCOPE BASED

AVAILABLE FOR ALL WORKLOADS (SERVER, CONTAINER, SQL, IOT AND

Microsoft Defender for Cloud

Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Protect against threats

For servers

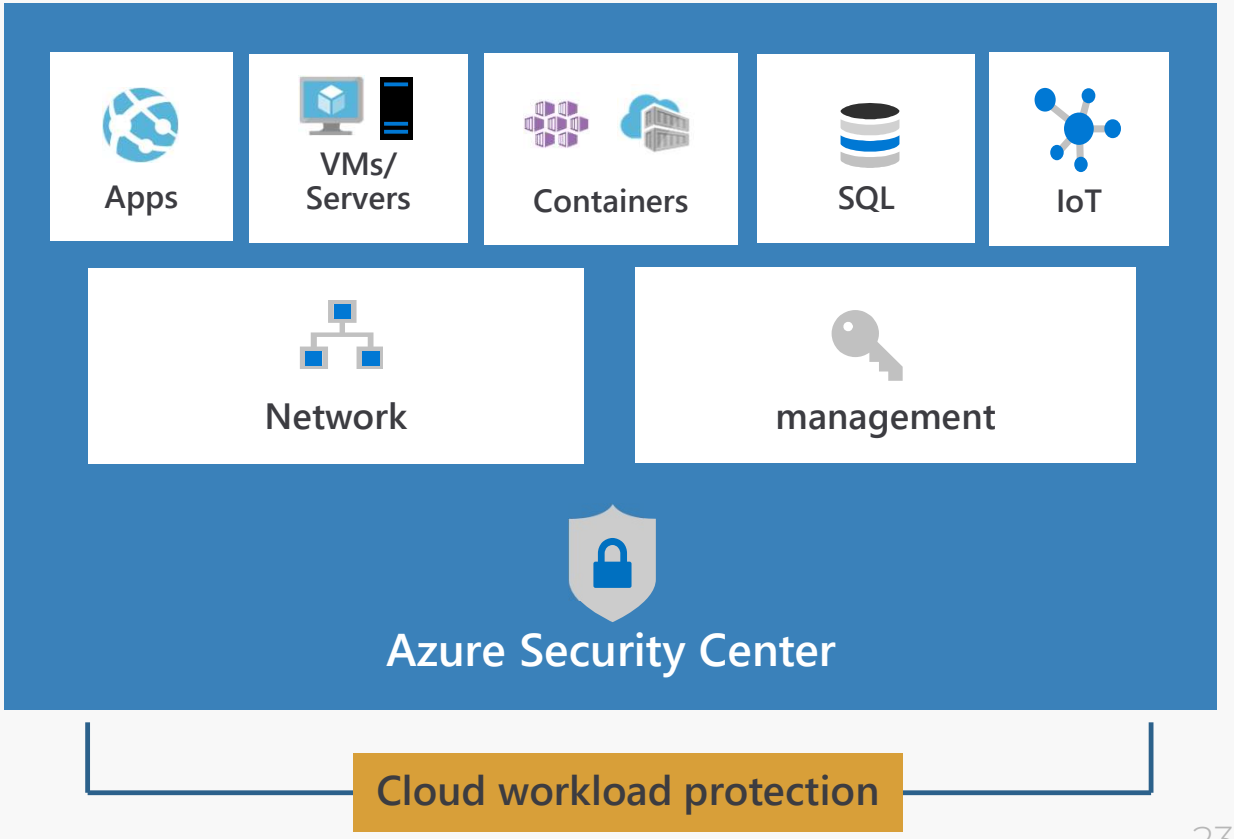
For cloud native workloads

For databases and storage

Get secure faster

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)



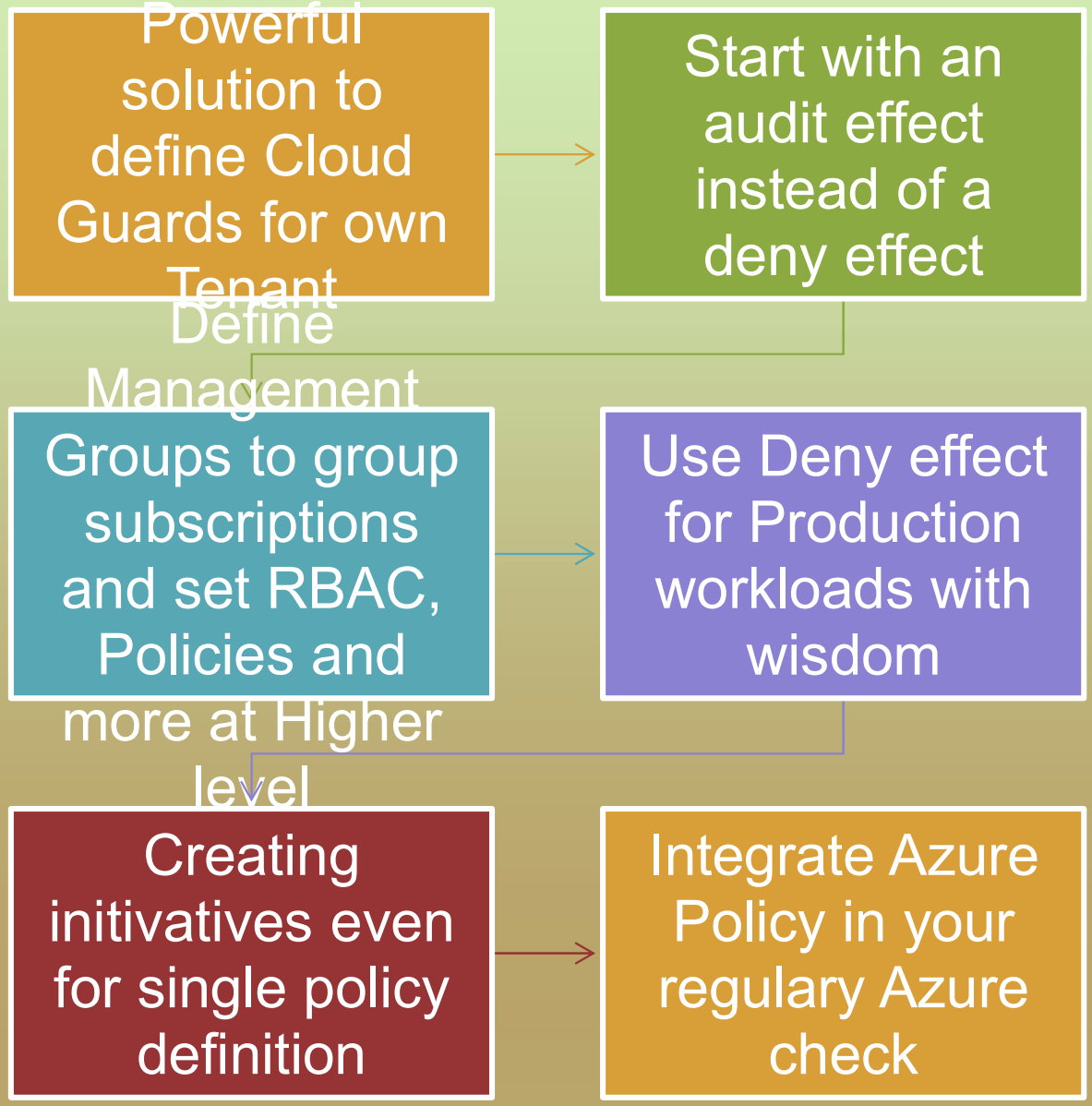
Microsoft Defender for Cloud

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 settings for ASC will firstly applied when Subscription is created

Azure Policy Recap



Microsoft Defender for Cloud

- 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 and ASC in your regulary Azure check

Links

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

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

https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

https://www.reimling.eu/2019/03/azure-management-groups-und-blueprints-ueberblick-und-einrichtung-teil-1/

https://github.com/Azure/azure-policy/

https://aka.ms/SecurityCommunity

https://docs.microsoft.com/en-us/azure/security-center/

https://docs.microsoft.com/en-us/azure/security-center/security-center-policy-definitions

https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies

https://blog.azureandbeyond.com/2020/04/24/mastering-azure-security-my-latest-adventure/

https://github.com/Azure/Azure-Security-Center

https://techcommunity.microsoft.com/t5/azure-security-center/weekly-secure-score-progress-report/ba-p/2159354

https://github.com/Azure/Azure-Security-Center/tree/master/Secure%20Score/SecureScoreOverTimeReport

Training: https://aka.ms/ascninja

Videos: https://aka.ms/ascinthefiled

ASC Lab: https://aka.ms/aslabs

Thank You

Azure Meetup BONN

www.azurebonn.de

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

www.cloudinspires.me

Blog

https://www.Reimling.eu

Contact

- @GregorReimling
- Gregor Reimling