Gregor Reimling

Thomas Naunheim

Azure Governance Best Practices and Enterprise-Scale

Start 15:25

Gregor Reimling

Cloud Consultant
@adesso SE

DELL Technologies · SquaredUp · infinity · INTERSTELLAR · kpn Partner Network · INSPARK · cegeka

Thomas Naunheim

Cyber Security Architect
@glueckkanja AG

DELL Technologies · SquaredUp · infinity · INTERSTELLAR · kpn Partner Network · INSPARK · cegeka

What are we going to discuss?

1. Challenges & Best Practices in Azure Architecture
2. Overview of Enterprise Scale & Landing Zones
3. Govern & Secure workloads with Policy and MDC
4. Critical design areas in Identity & Access

1. Challenges & Best Practices in Azure Architecture

„Quick start“ in Cloud Adoption

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Biggest challenge in your project(s)?

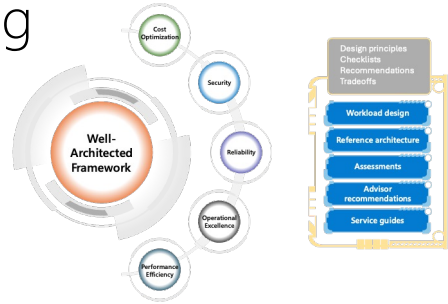
- lack of knowledge and insufficient time
- low degree of automation
- Regulatory/Compliance vs. Agile
- Cost transparency
- Considerations in security and data privacy
- …

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)

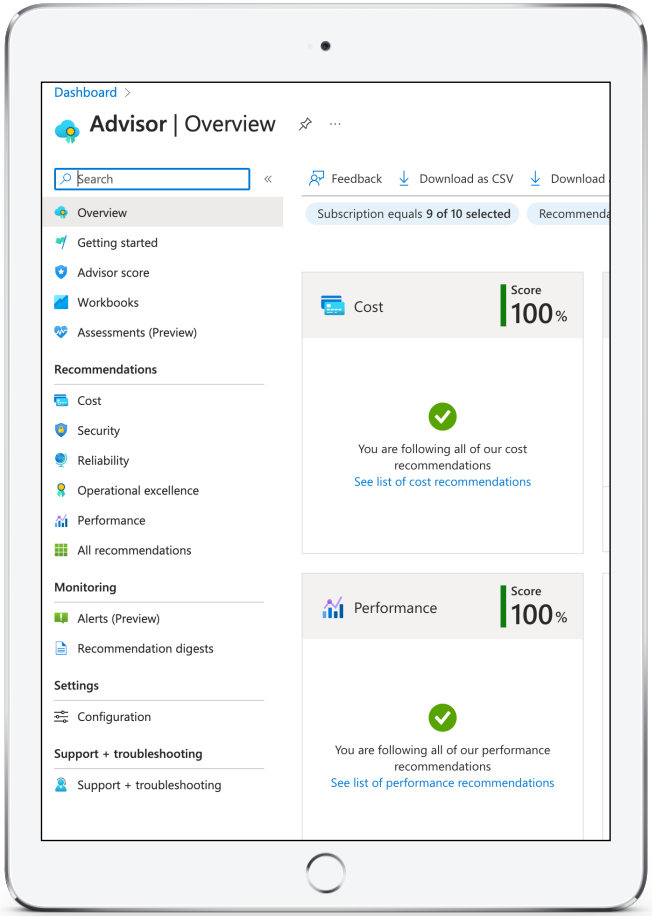
“The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload.”



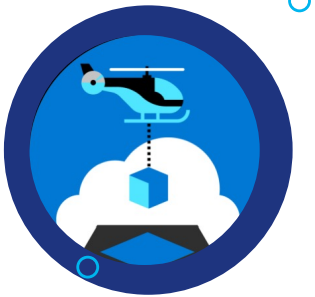
DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Demo

Azure Advisor & FinOps



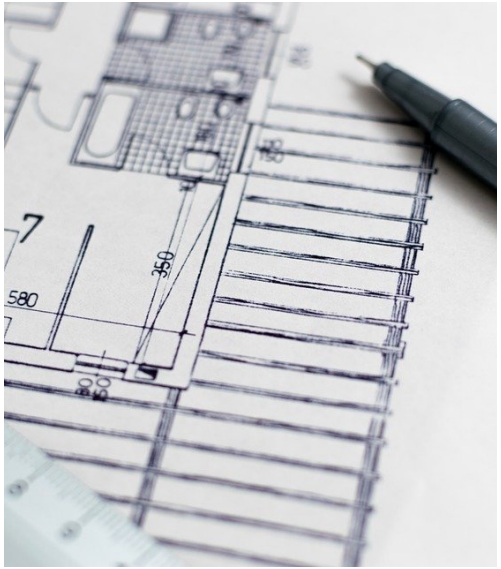
DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



2. Overview of Enterprise Scale & Landing Zones

Environment for your cloud workloads





DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

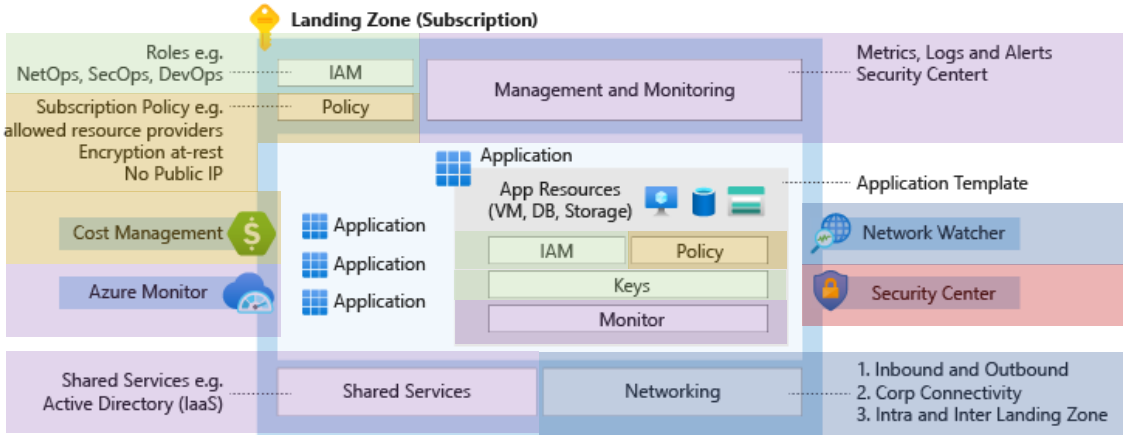
What is Enterprise-Scale?

„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

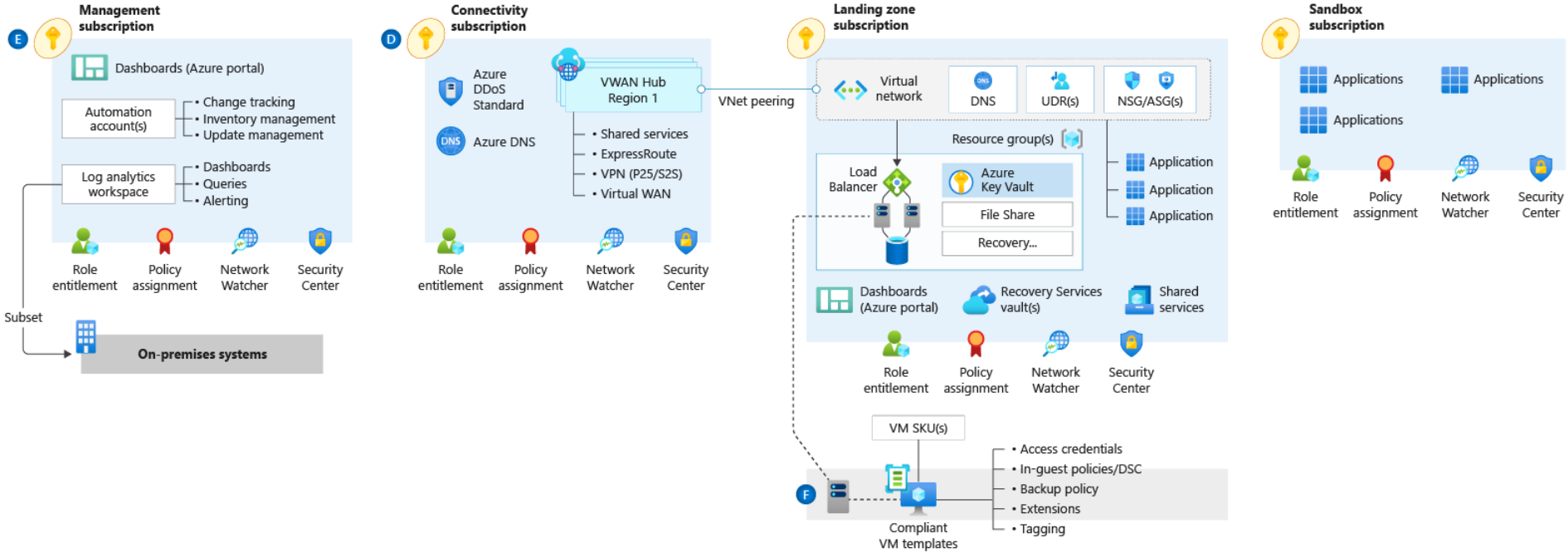
Design areas of Landing Zone(s)



Connectivity, Identity, Governance, Operations and Security

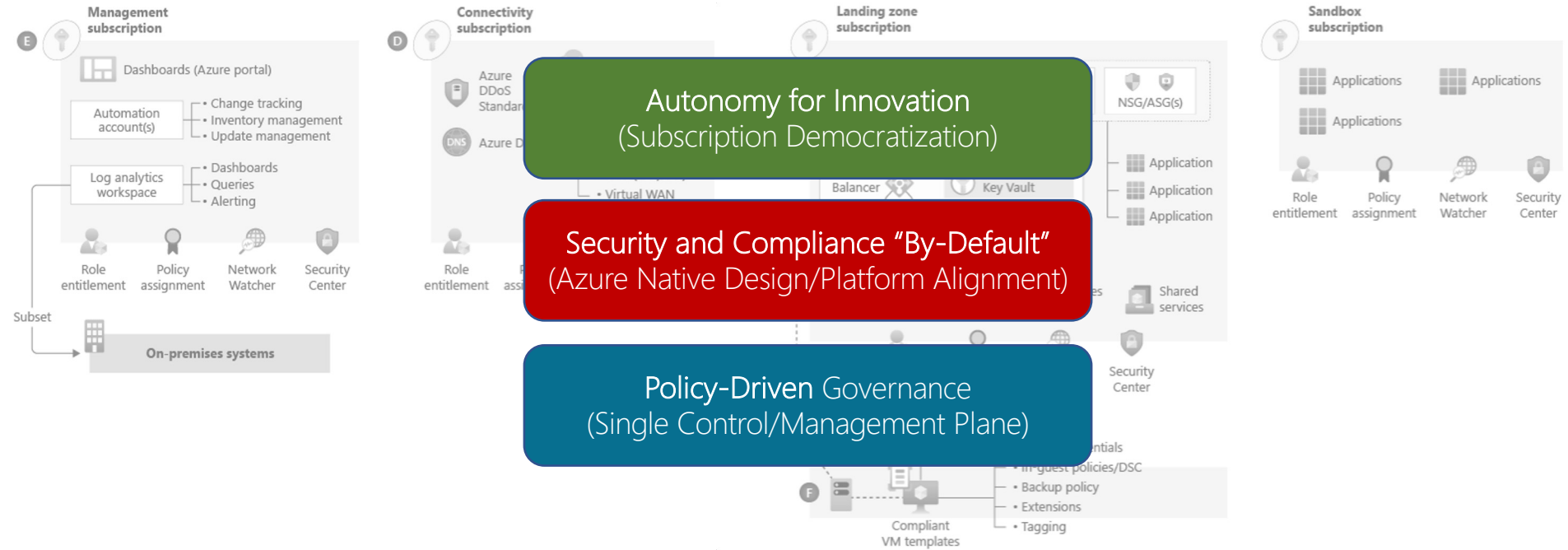
Source: Cloud Adoption Framework enterprise-scale landing zone architecture

Enterprise-Scale Design Principles



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

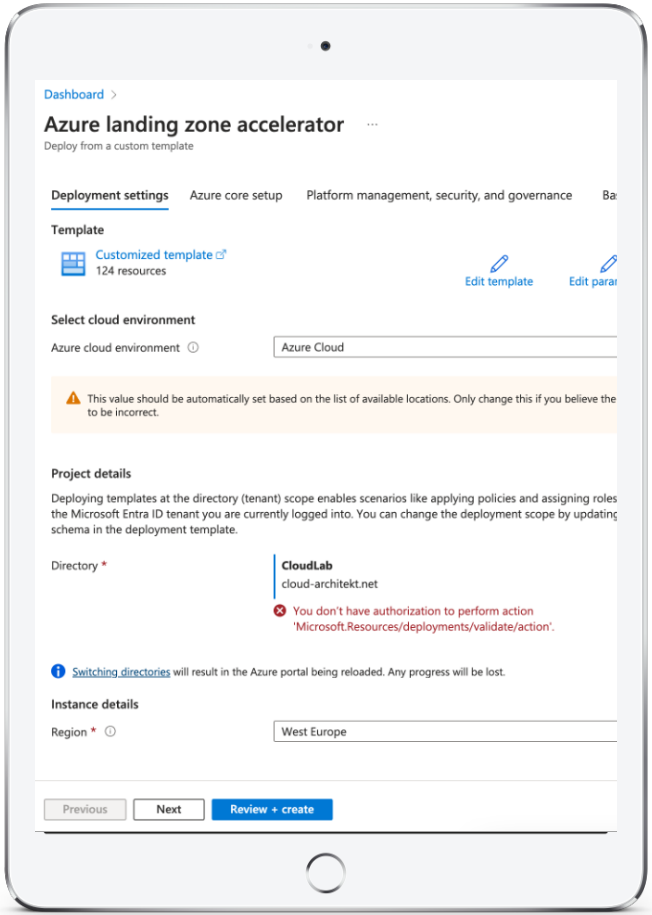
Enterprise-Scale Design Principles



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

Demo

Deploy and manage EAS/ELSZ

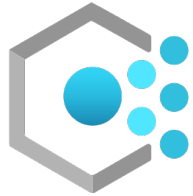


DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

3. Govern and Secure your workloads with Azure Policy and Defender for Cloud

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Azure Policy Concepts

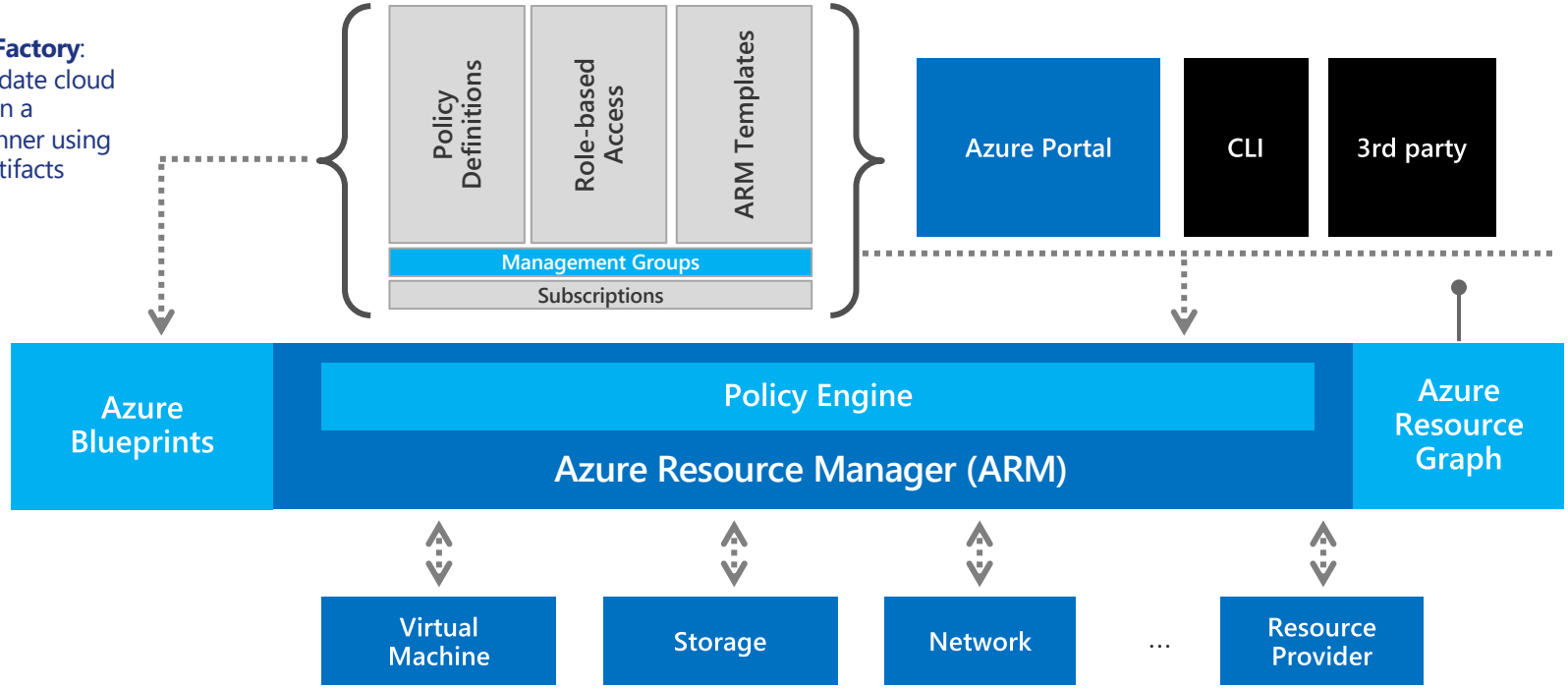


- Part of CAF to support WAF
- Create, assign and manage policies
- Enforce rules to ensure your ressoures are compliant
- Focus on ressource properties for new and existing deployments
- A definition is a set of conditions in audit or deny mode
- An assignment is a policy definition placed on a specific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

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Azure Governance Architecture

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



DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Leverage built-in initiative & policies

Security

Defender for Cloud

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

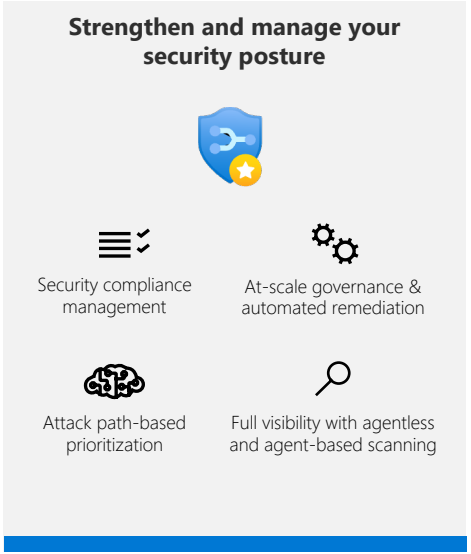
Allowed images for AKS

Cost

Allowed VM SKUs

Allowed Storage SKUs

Microsoft Defender for Cloud



Amazon Web Services

Microsoft Azure

Google Cloud Platform

On-premises

DELL Technologies

SquaredUp

infinity

INTERSTELLAR

kpn Partner Network

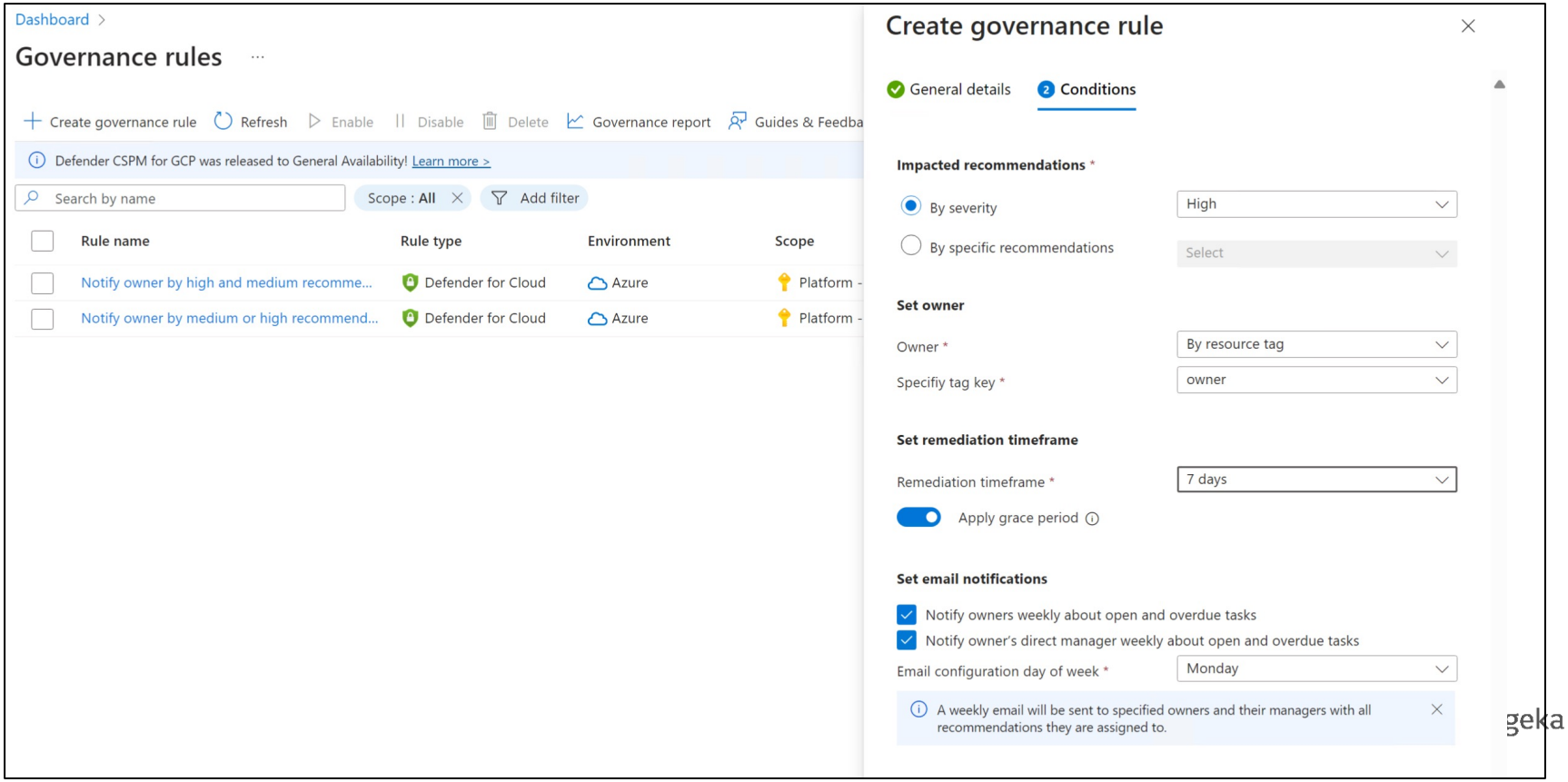
INSPARK

cegeka

How it works together with Azure Policy

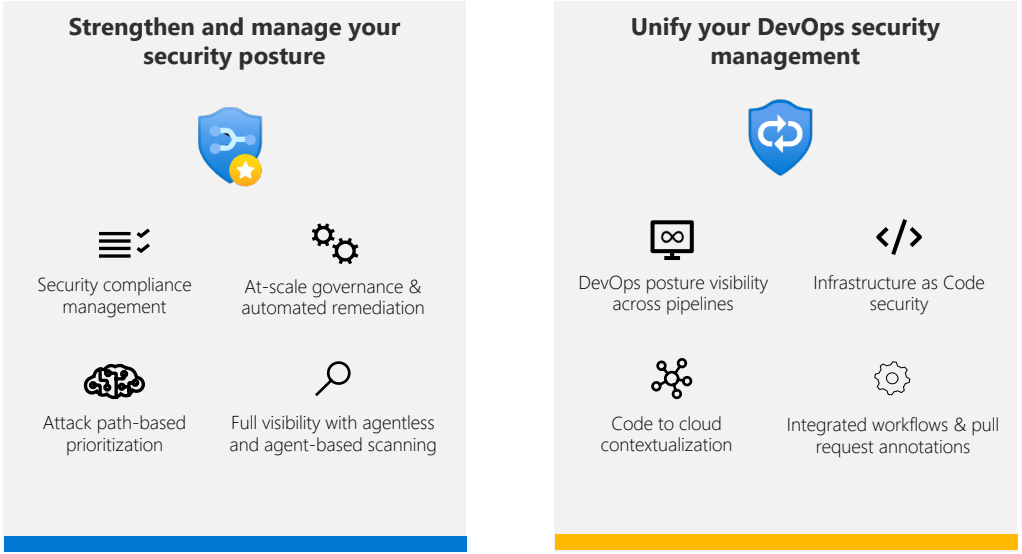
- All MDC recommendations based on Azure Policy
- Secure score is result of Azure Policy settings
- Recommendations are a result of Azure Policy
- All Azure Policies are defined in Compliance mode

Assign recommendations to LZ Owner



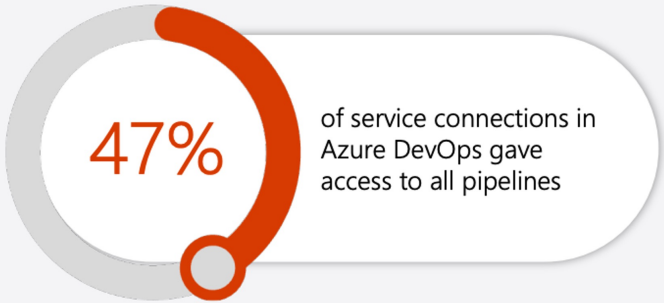
geka

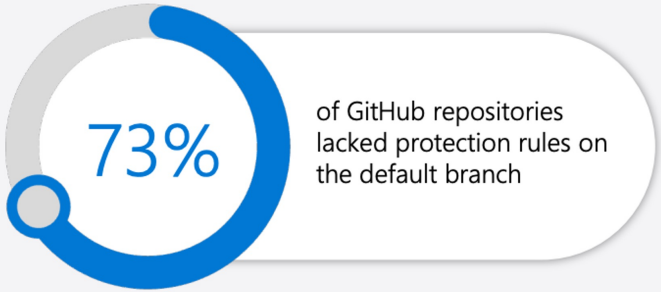
Microsoft Defender for Cloud

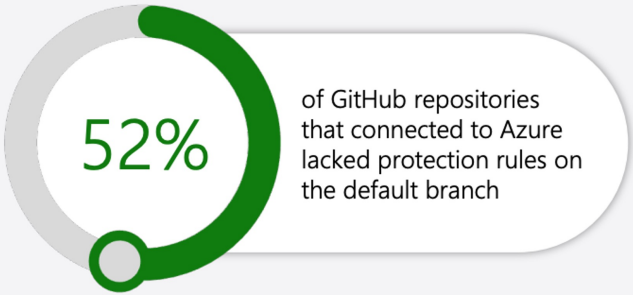


DELL Technologies · SquaredUp · infinity · INTERSTELLAR · kpn Partner Network · INSPARK · cegeka

Why DevOps Security is important?





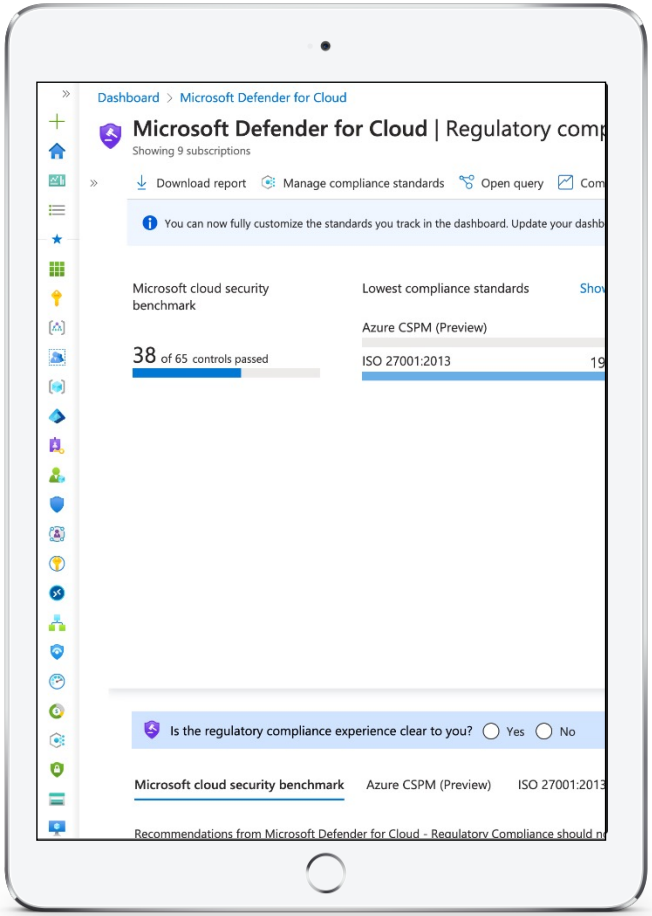


DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Source: 2024 State of Multicloud Security Report (Microsoft)

Demo

Policy and Defender for Cloud CSPM



DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

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

DELL Technologies

SquaredUp

infinity

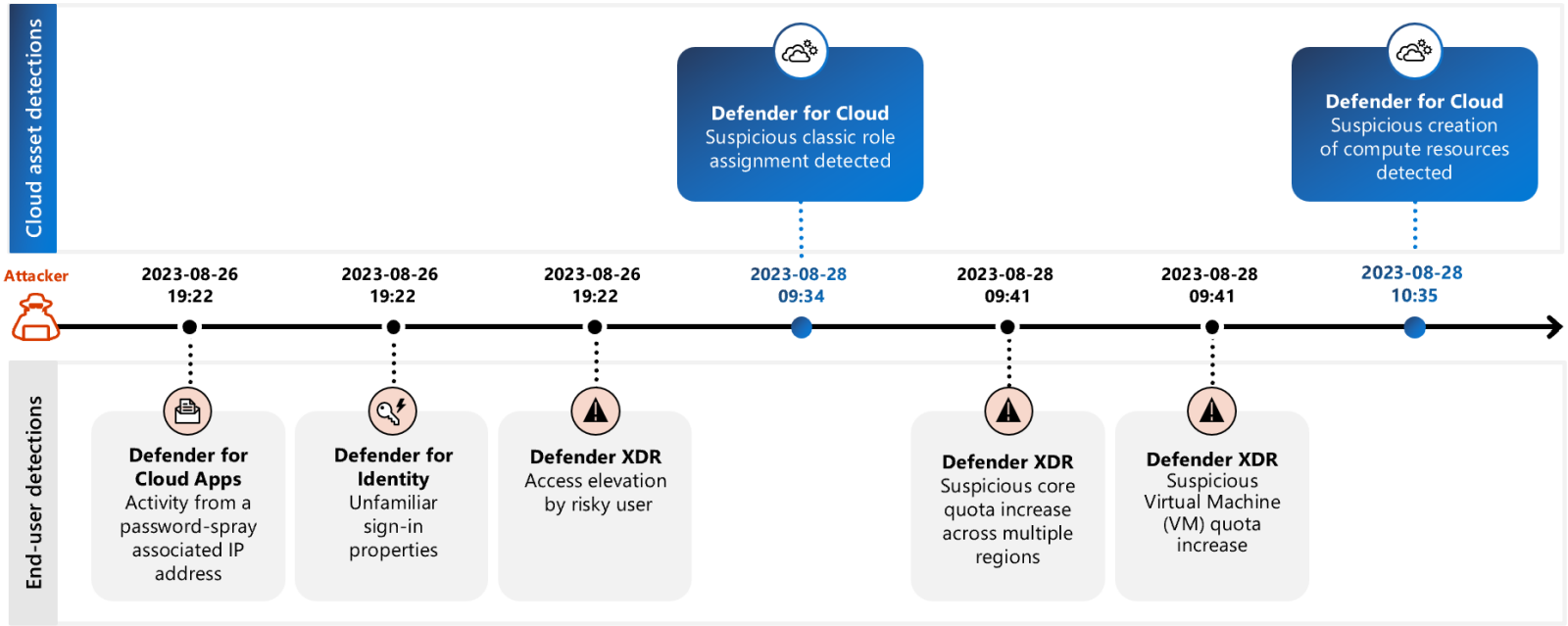
INTERSTELLAR

kpn Partner Network

INSPARK

cegeka

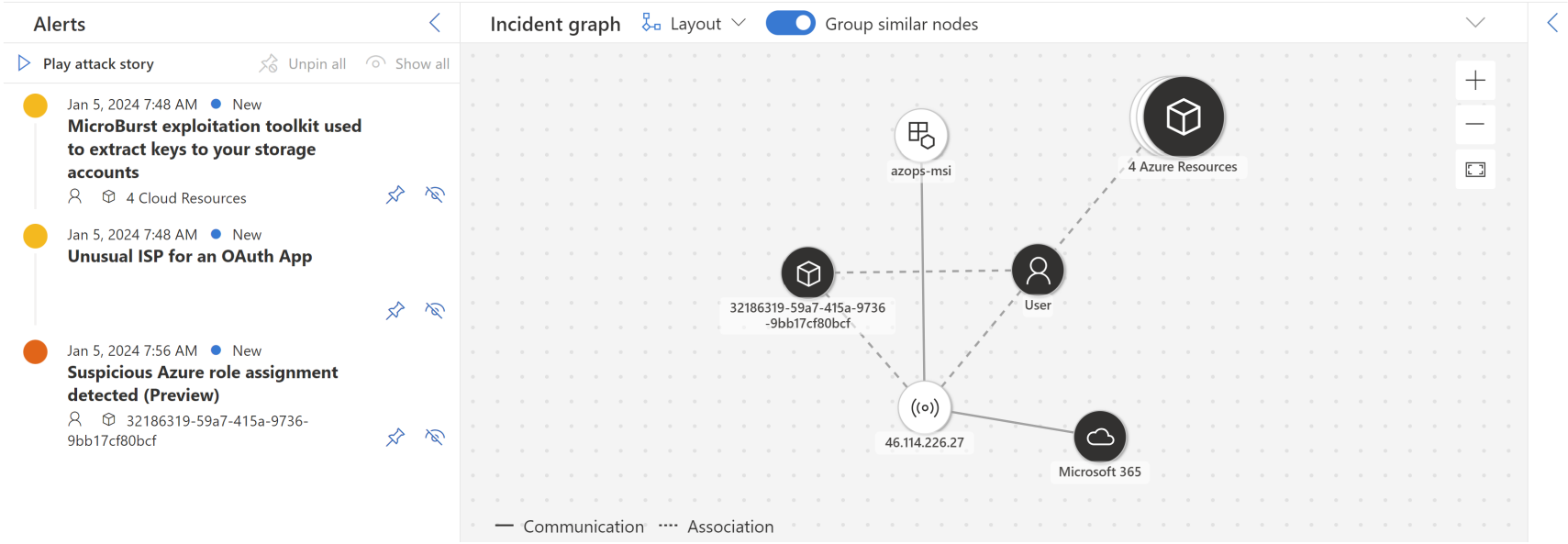
Multi-stage attacks on Azure privileges



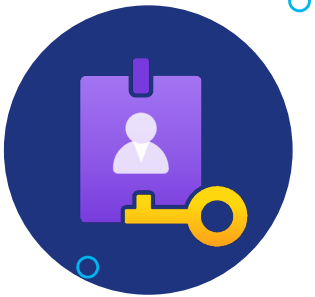
Multi-stage incidents XDR + MDC

Medium | Active | Unassigned

Attack story | Alerts (3) | Assets (7) | Investigations (0) | Evidence and Response (2) | Summary

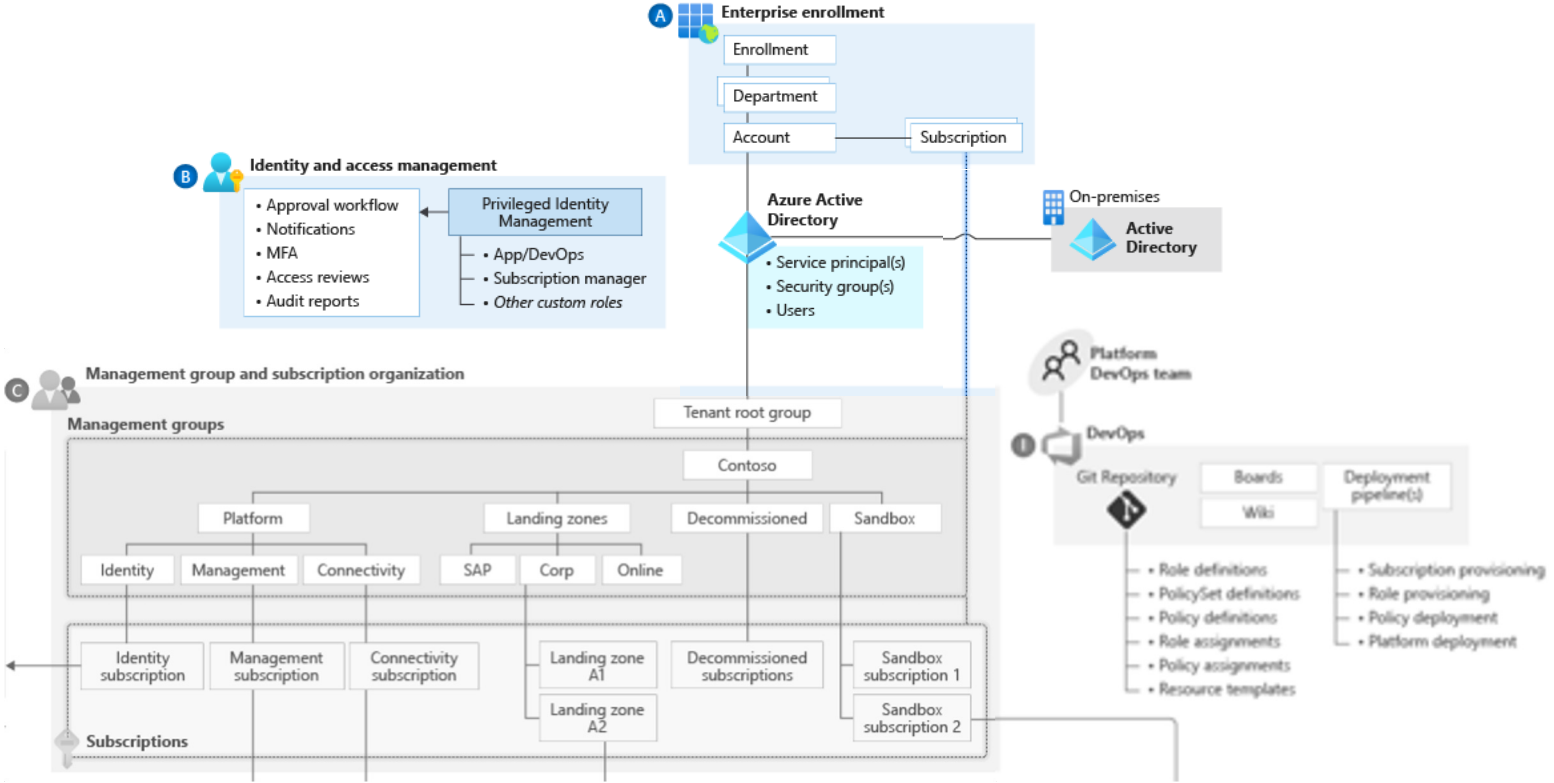


DELL Technologies | SquaredUp | infinity | INTERSTELLAR | kpn Partner Network | INSPARK | cegeka



4. Critical design areas in Identity & Access Management

Critical Design Area: Identity & Access



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

IAM for Azure Landing Zones

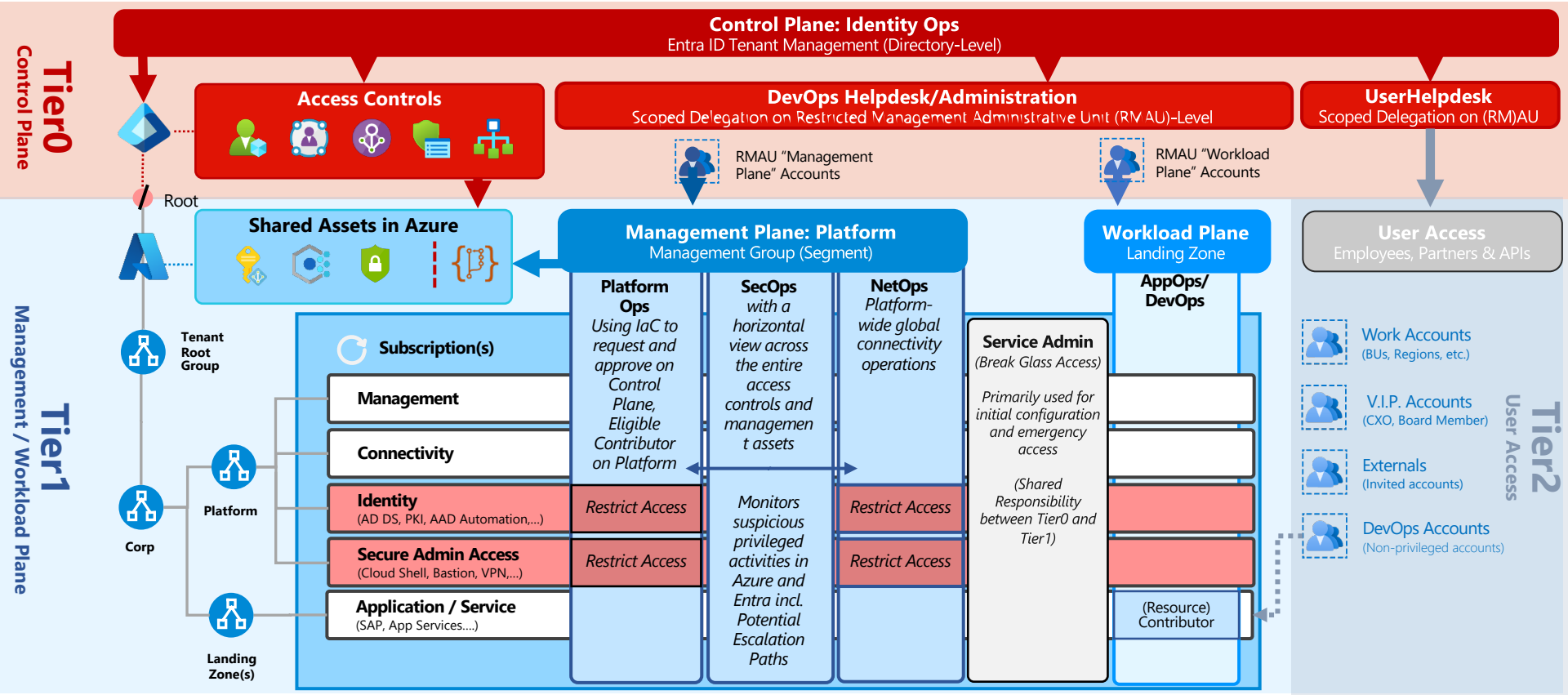
„IAM supports the ALZ design principle of subscription democratization“

„we trust application owners to know what's best for their apps“

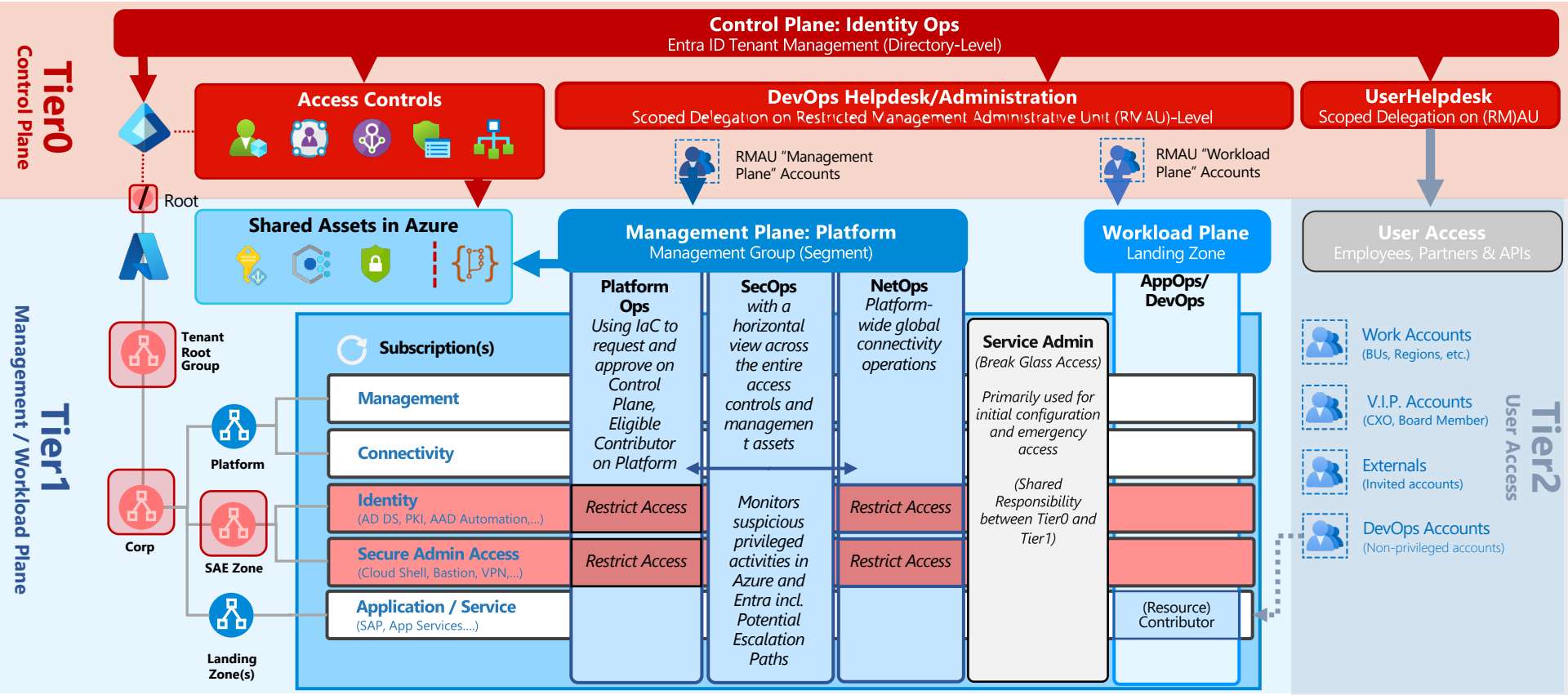
„we separate the identity and access management of every environment and every workload and avoid global permissions or reused credentials.“

Source: Refreshed Identity and Access Management CAF documentation (microsoft.com)

My Adoption of Enterprise Access Model



My Adoption of Enterprise Access Model



Example for Azure Policies related to IAM governance

- RBAC assignment only allowed for specific principals on Control Plane
- Audit usage of custom RBAC roles

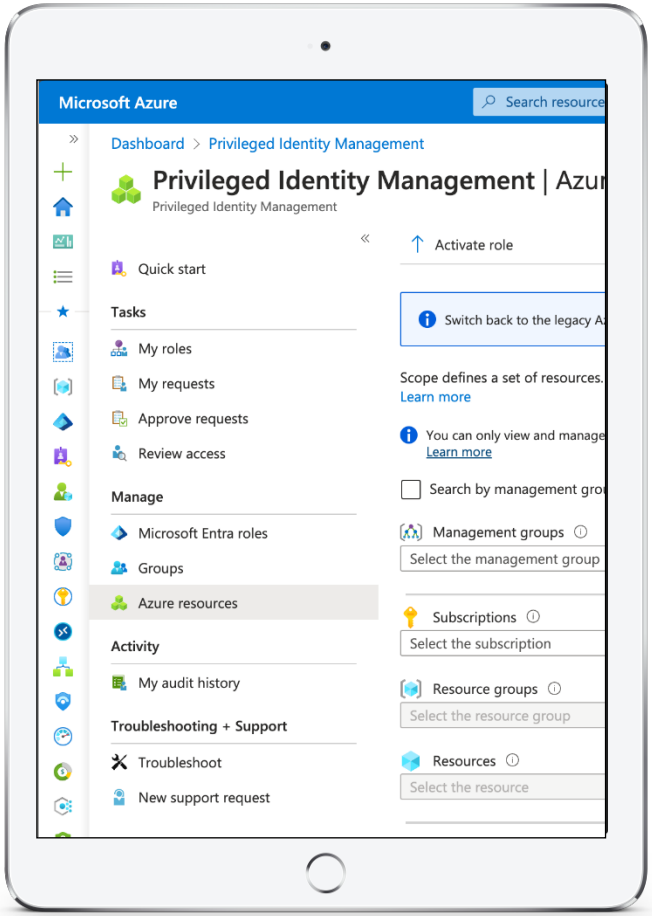
- Allow managing tenant ids to onboard through Azure Lighthouse
- Audit delegation of scopes to a managing tenant

- [Preview]: Managed Identity Federated Credentials from GitHub should be from trusted repository owners
- [Preview]: Managed Identity Federated Credentials from Azure Kubernetes should be from trusted sources
- [Preview]: Managed Identity Federated Credentials should be from allowed issuer types

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Demo

Protect and delegate privileges



DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Please evaluate this session in the App.

THANK YOU

Are there any questions?