Gregor Reimling

Thomas Naunheim

Azure Governance Best Practices and Enterprise-Scale

Start 15:25

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Gregor Reimling

Cloud Consultant
@adesso SE

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

Cyber Security Architect
@glueckkanja AG

Thomas Naunheim

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

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

1. Challenges & Best Practices in Azure Architecture

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

„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)

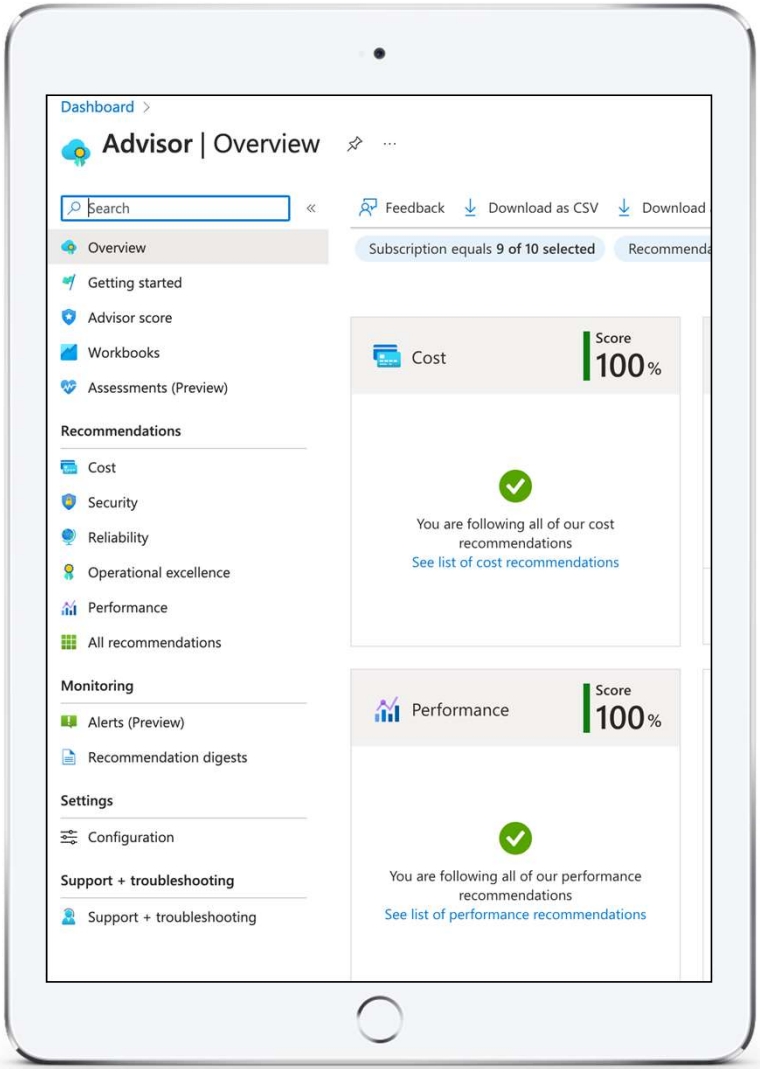
„The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey.“

Azure Well-Architected Framework (WAF)

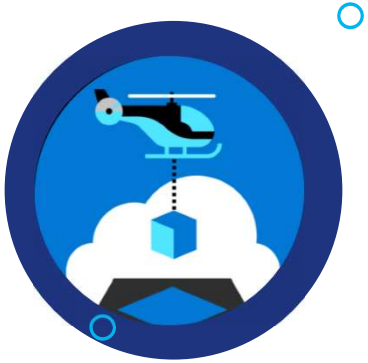
“The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload.”

Demo

Azure Advisor & FinOps

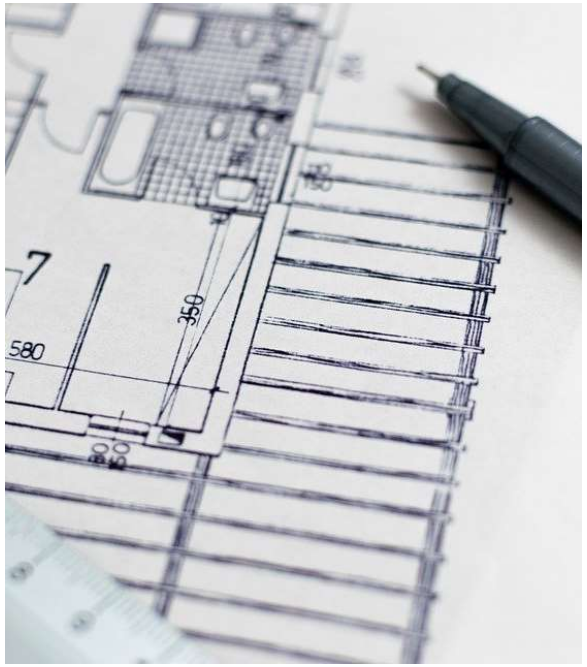


DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



2. Overview of Enterprise Scale & Landing Zones

Environment for your cloud workloads



DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

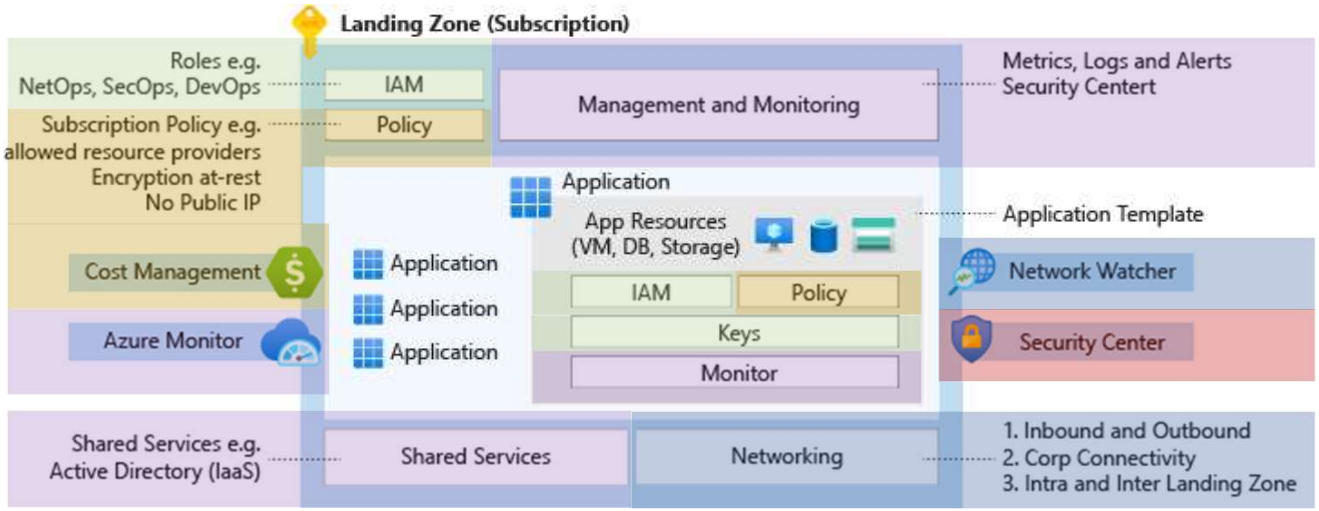
What is Enterprise-Scale?

„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

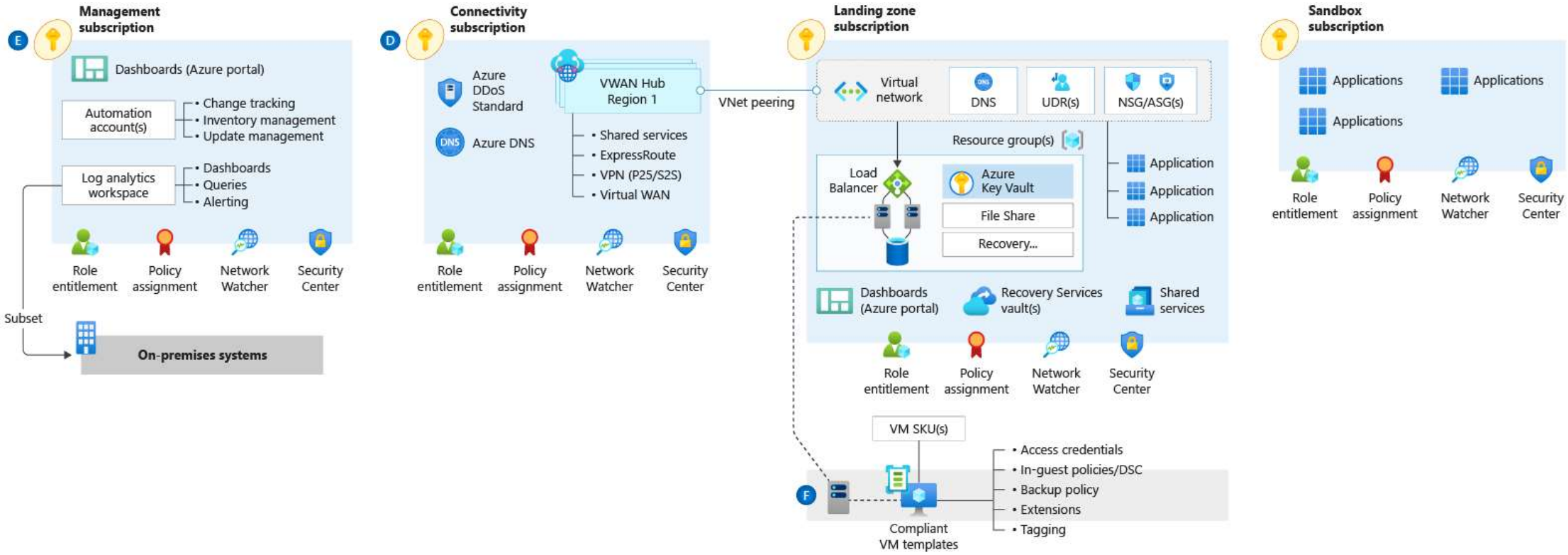
Design areas of Landing Zone(s)



Connectivity, Identity, Governance, Operations and Security

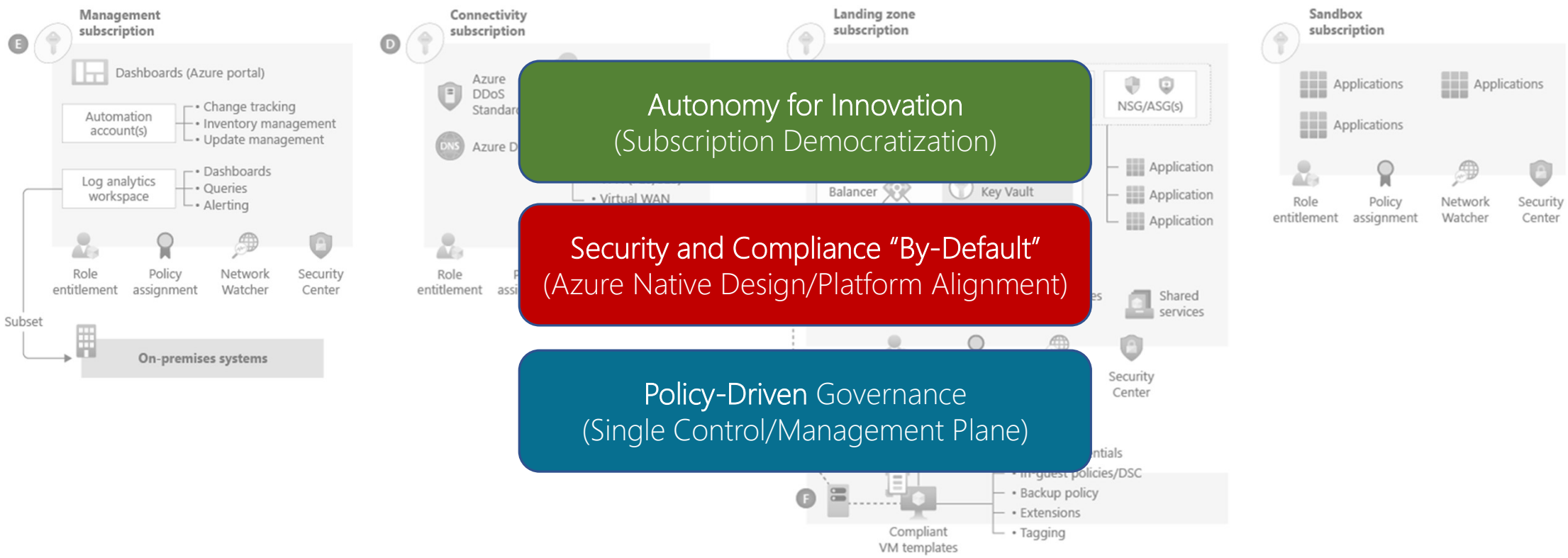
Source: Cloud Adoption Framework enterprise-scale landing zone architecture

Enterprise-Scale Design Principles



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

Enterprise-Scale Design Principles



Autonomy for Innovation
(Subscription Democratization)

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

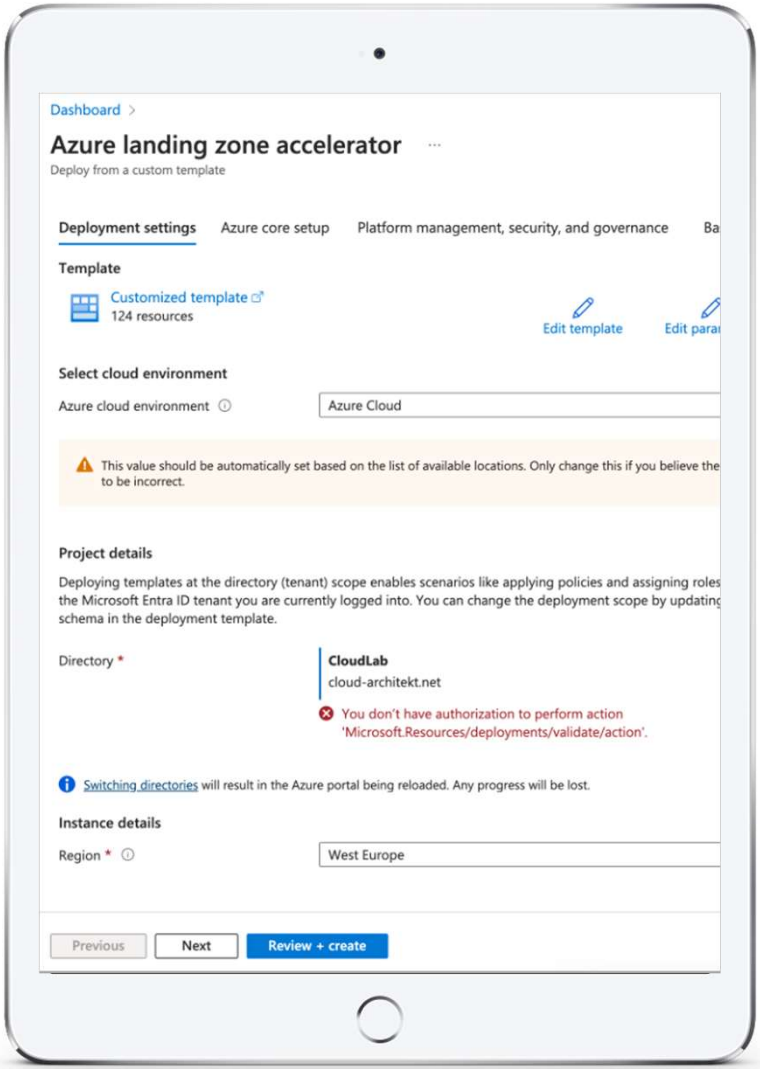
Policy-Driven Governance
(Single Control/Management Plane)

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

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

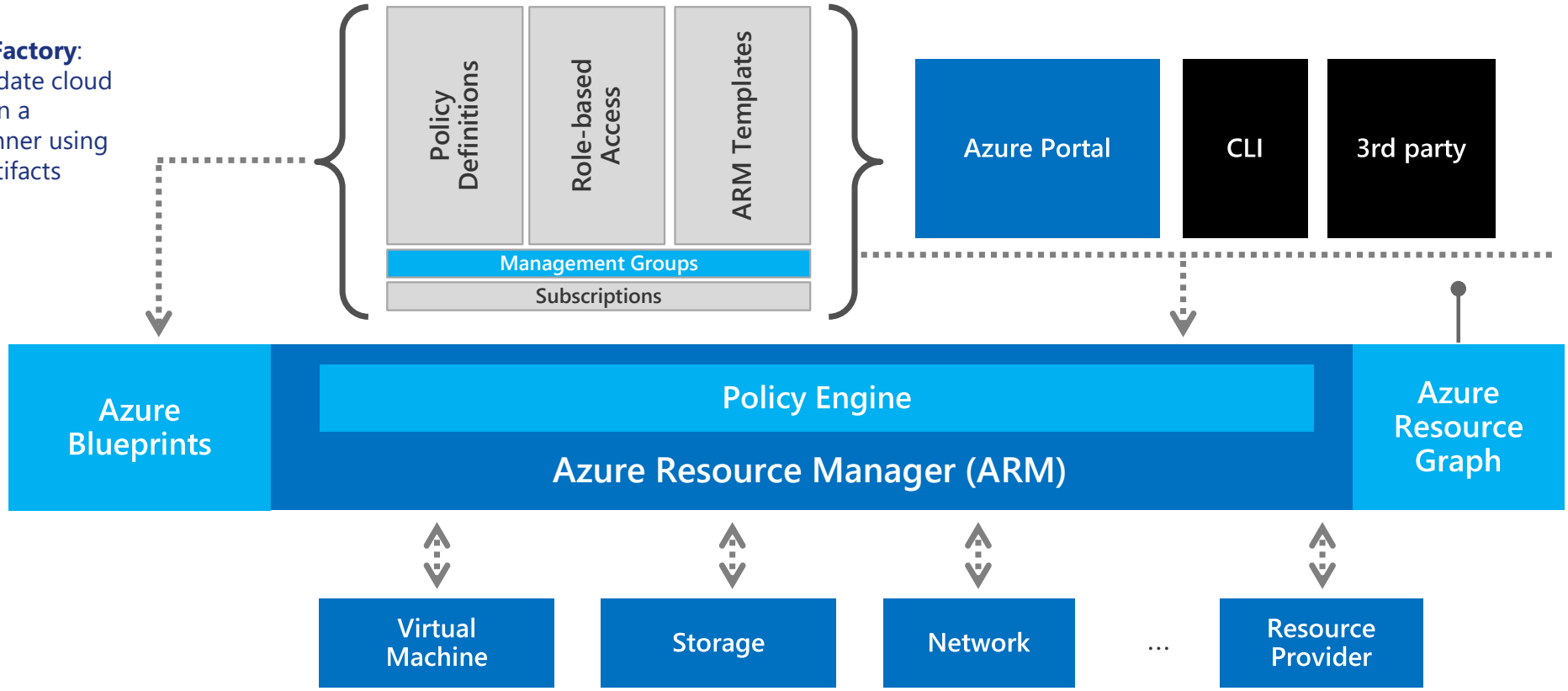
DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

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

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	Regulatory Compliance	Tags	Resource standardization	Cost
Defender for Cloud	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			

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

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

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Assign recommendations to LZ Owner

Dashboard >

Governance rules

Create governance rule | Refresh | Enable | Disable | Delete | Governance report | Guides & Feedba

Defender CSPM for GCP was released to General Availability! Learn more >

Search by name | Scope : All | Add filter

Rule name	Rule type	Environment	Scope
Notify owner by high and medium recomme...	Defender for Cloud	Azure	Platform -
Notify owner by medium or high recommend...	Defender for Cloud	Azure	Platform -

Create governance rule

General details | 2 Conditions

Impacted recommendations *

By severity: High

By specific recommendations: Select

Set owner

Owner *: By resource tag

Specifiy tag key *: owner

Set remediation timeframe

Remediation timeframe *: 7 days

Apply grace period

Set email notifications

Notify owners weekly about open and overdue tasks

Notify owner's direct manager weekly about open and overdue tasks

Email configuration day of week *: Monday

A weekly email will be sent to specified owners and their managers with all recommendations they are assigned to.

geka

Security recommendations and graph

Dashboard >

Windows servers should be configured to use secure communication protocols

Open query | View policy definition | View recommendation for all resources

Critical	vsaw-0	Overdue
Risk level	Resource	Status

Description

To protect the privacy of information communicated over the Internet, your servers should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by using security certificates to encrypt a connection between machines.

Attack Paths	Scope	Freshness
0	Platform - Iden...	30 Min
Last change date	**Owner**	**Due date**
4/2/2023	admThom0@lab.cl...	4/16/2023

Ticket ID
-

Risk factors

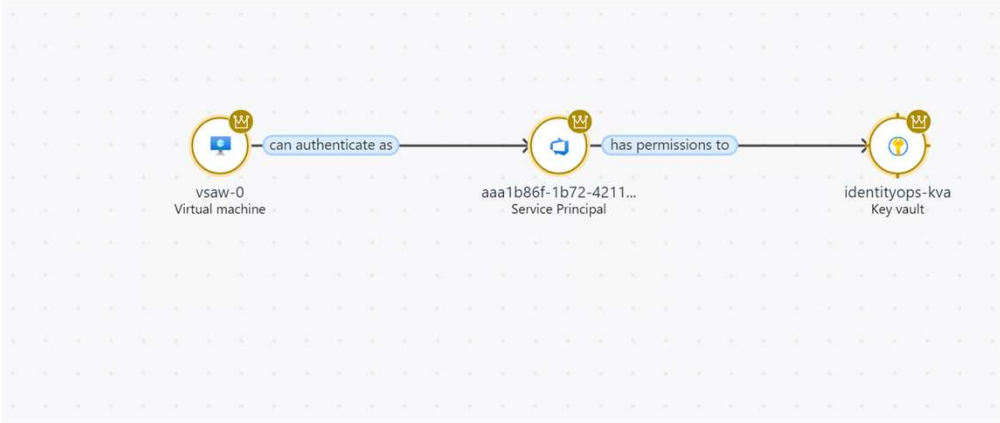
VULNERABILITIES | CRITICAL RESOURCE | SENSITIVE DATA | +1

Take action | Graph

Below you can find all attack paths and resource context that used to determine the risk level of this recommendation:

Additional context (4)

vsaw-0 (Entry point) → identityops-kva (Target)



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

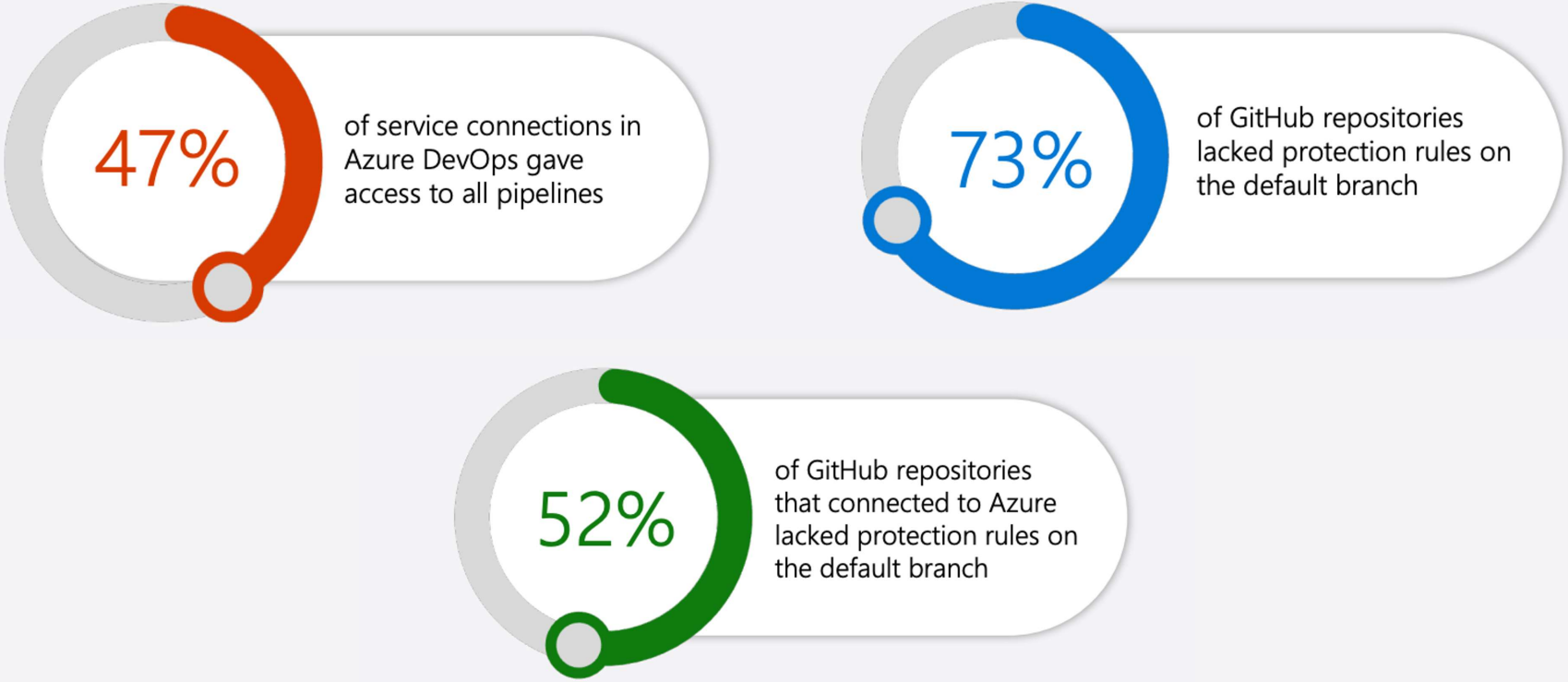
Unify your DevOps security management

- DevOps posture visibility across pipelines
- Infrastructure as Code security
- Code to cloud contextualization
- Integrated workflows & pull request annotations

Amazon Web Services | Microsoft Azure | Google Cloud Platform | On-premises

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

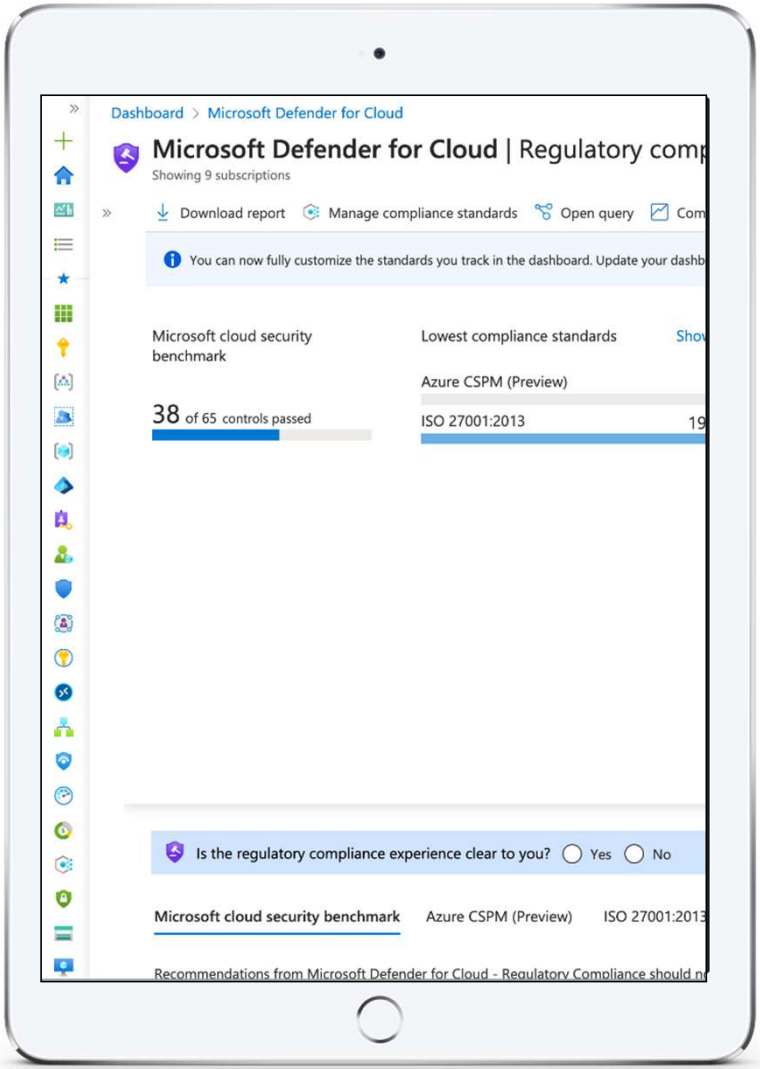
Why DevOps Security is important?



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

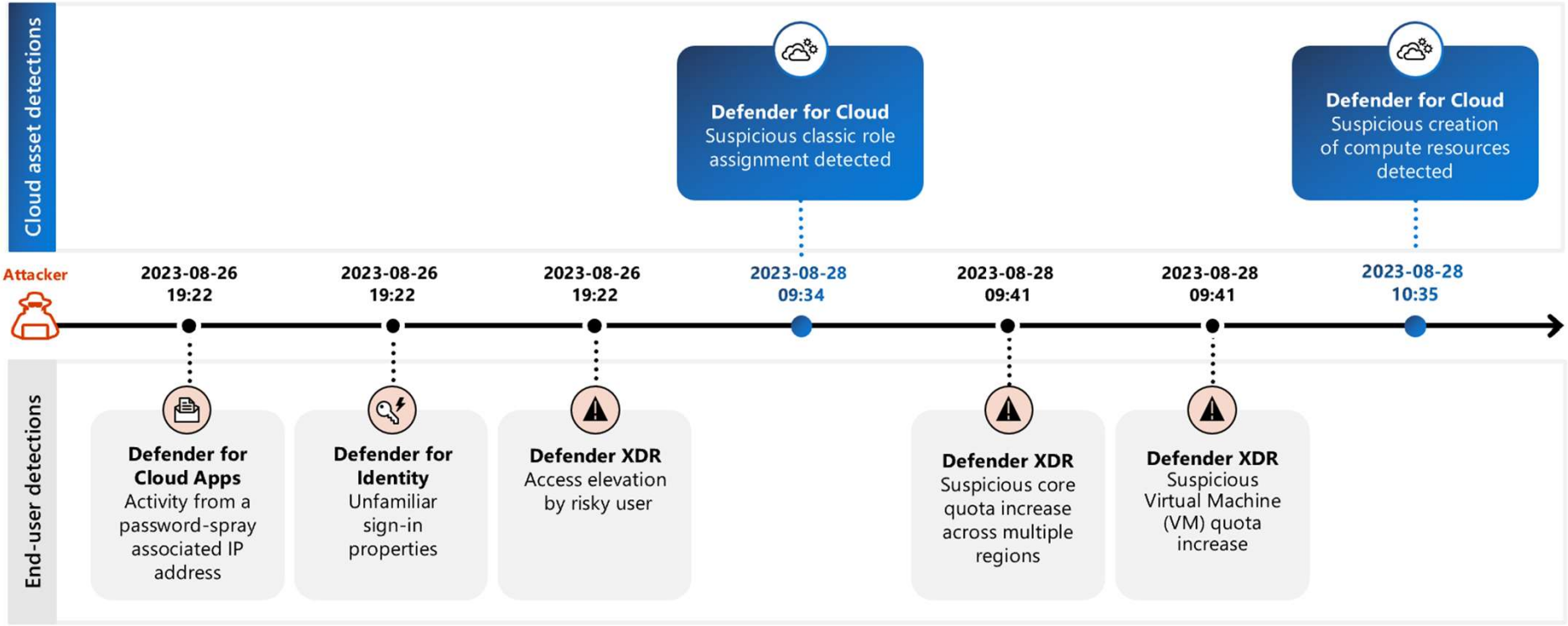
Detect threats and protect your workloads

- 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



DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Multi-stage incidents XDR + MDC

Medium | Active | Unassigned

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

Alerts

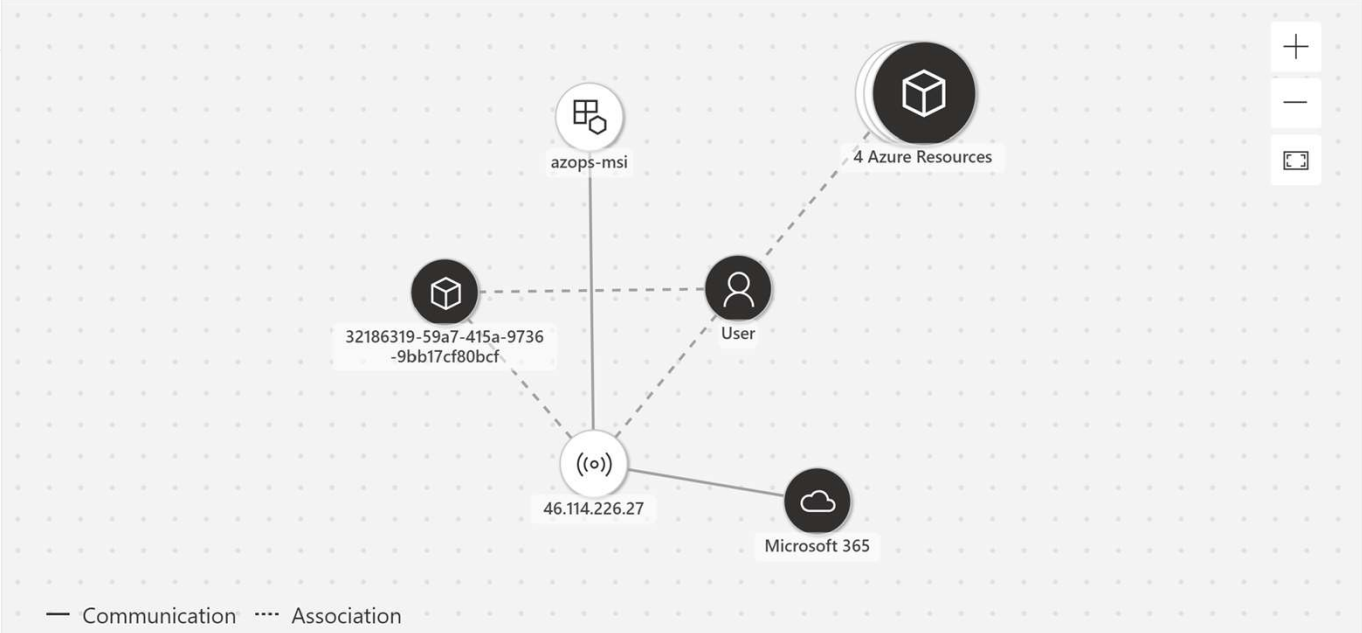
Play attack story | Unpin all | Show all

Jan 5, 2024 7:48 AM • New
MicroBurst exploitation toolkit used to extract keys to your storage accounts
4 Cloud Resources

Jan 5, 2024 7:48 AM • New
Unusual ISP for an OAuth App

Jan 5, 2024 7:56 AM • New
Suspicious Azure role assignment detected (Preview)
32186319-59a7-415a-9736-9bb17cf80bcf

Incident graph | Layout | Group similar nodes

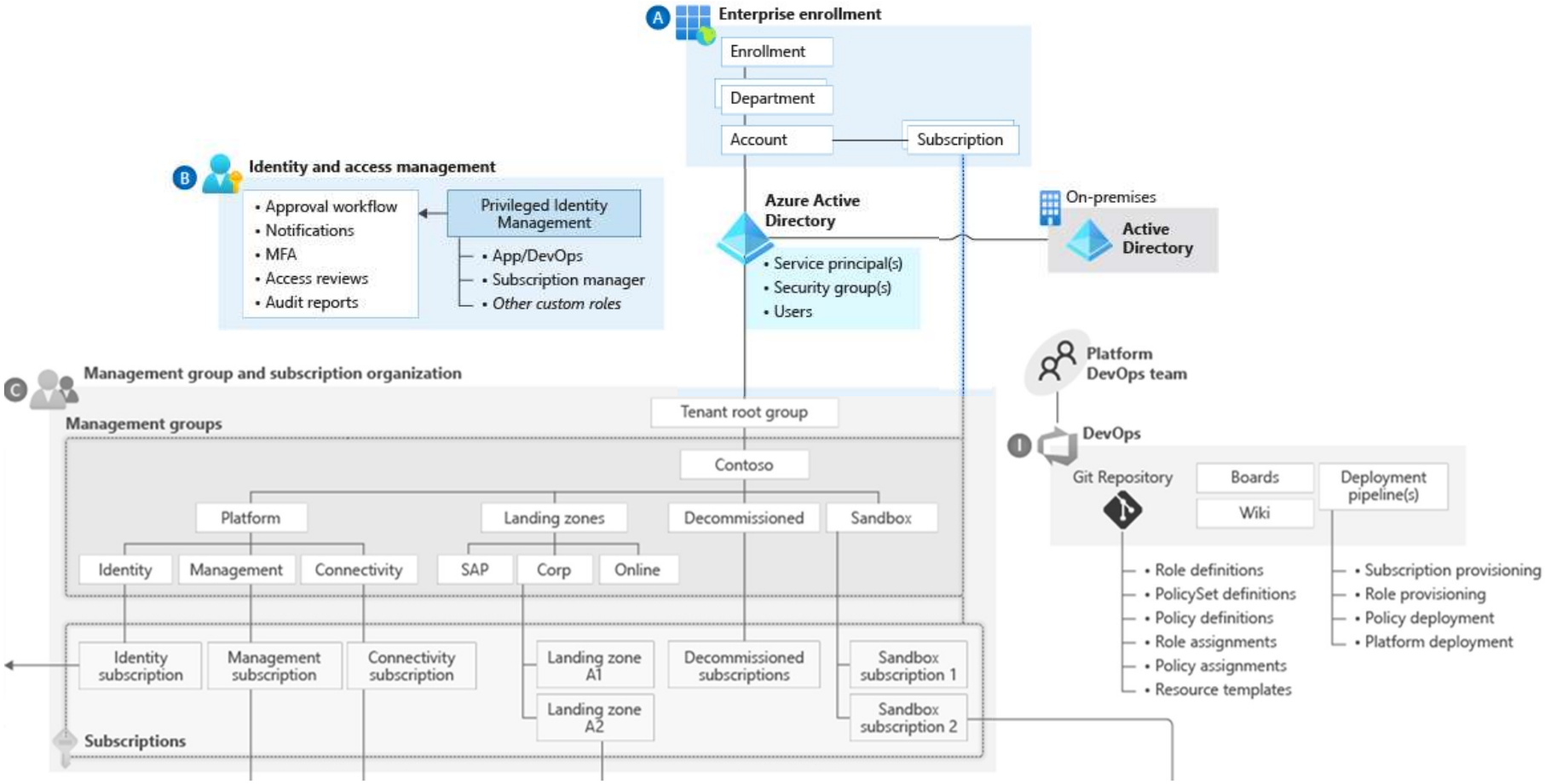


DELL Technologies | SquaredUp | infinity | INTERSTELLAR | kpn Partner Network | INSPARK | cegeka

4. Critical design areas in Identity & Access Management

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Critical Design Area: Identity & Access



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

IAM for Azure Landing Zones

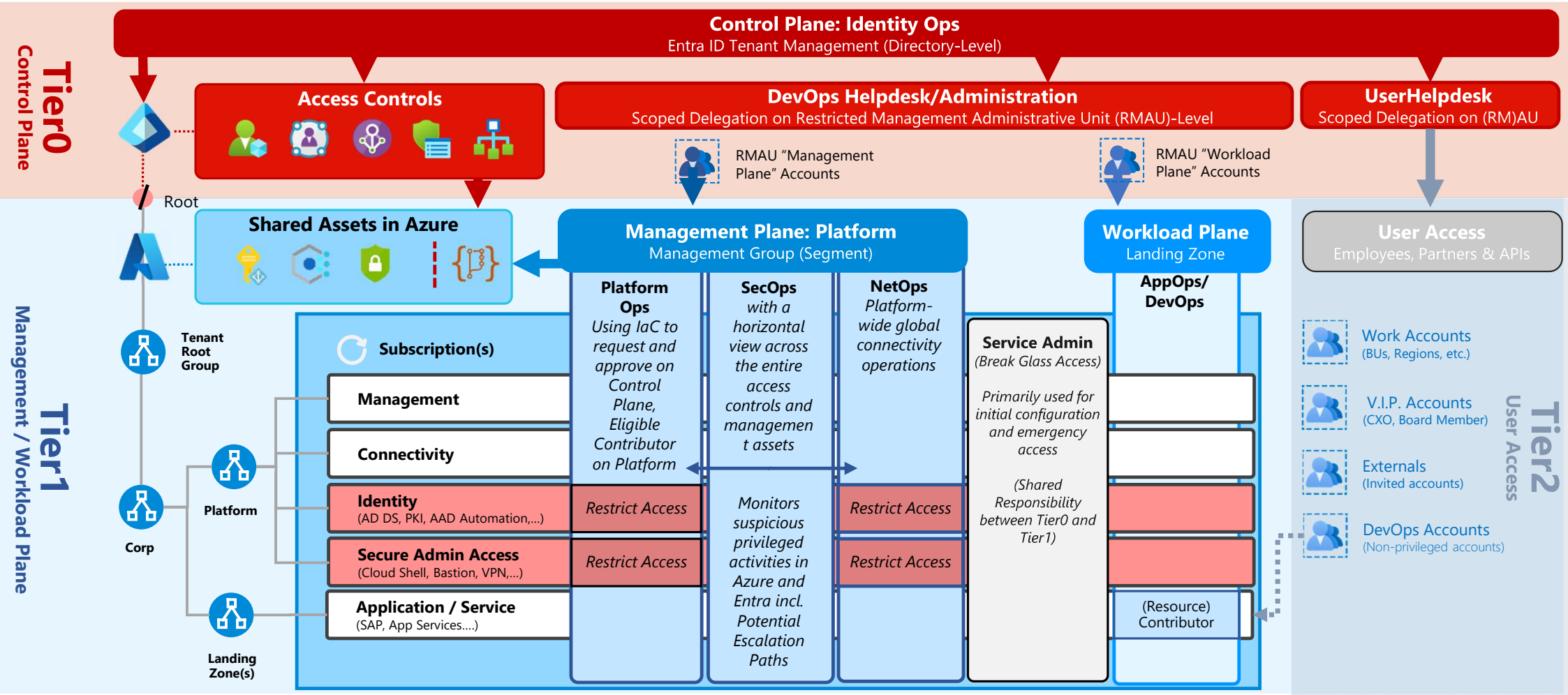
„IAM supports the ALZ design principle of subscription democratization"

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

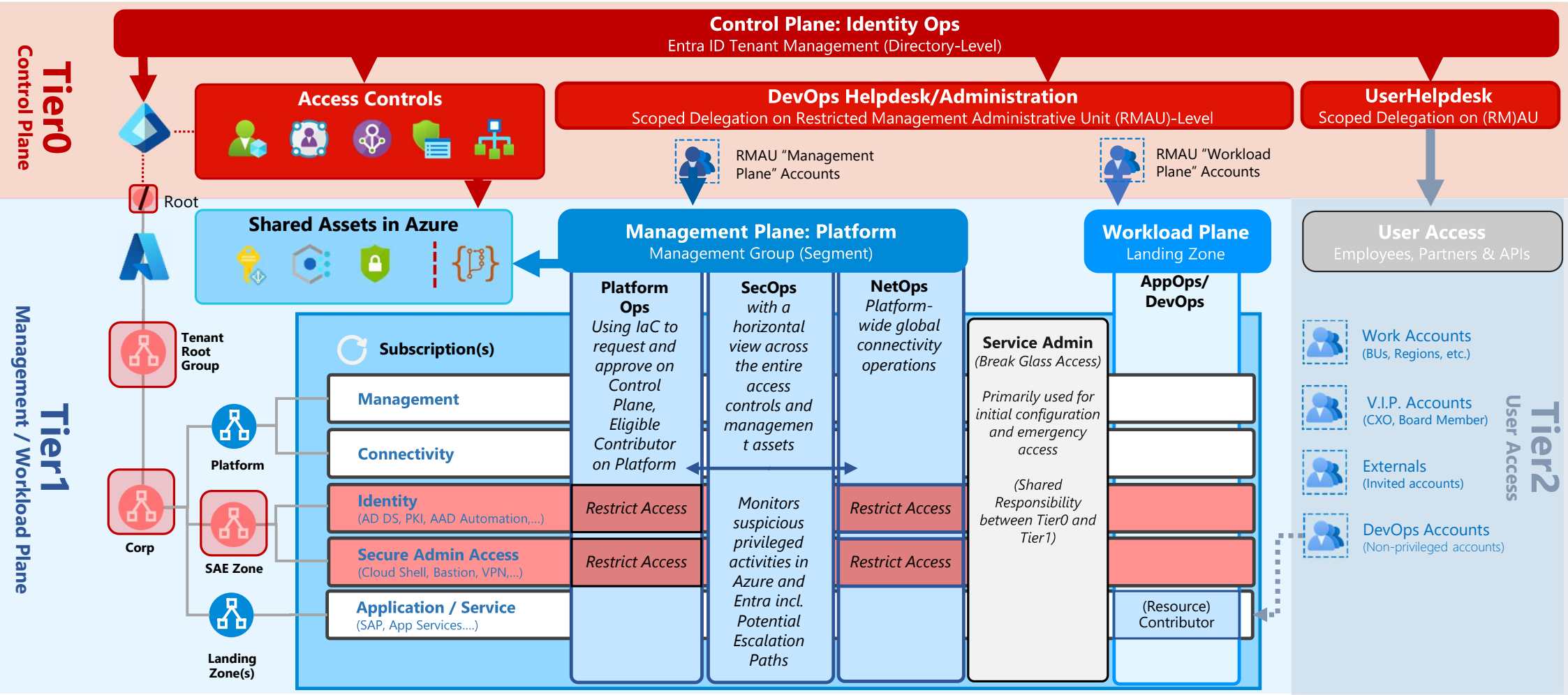
„we separate the identity and access management of every environment and every workload and avoid global permissions or reused credentials."

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

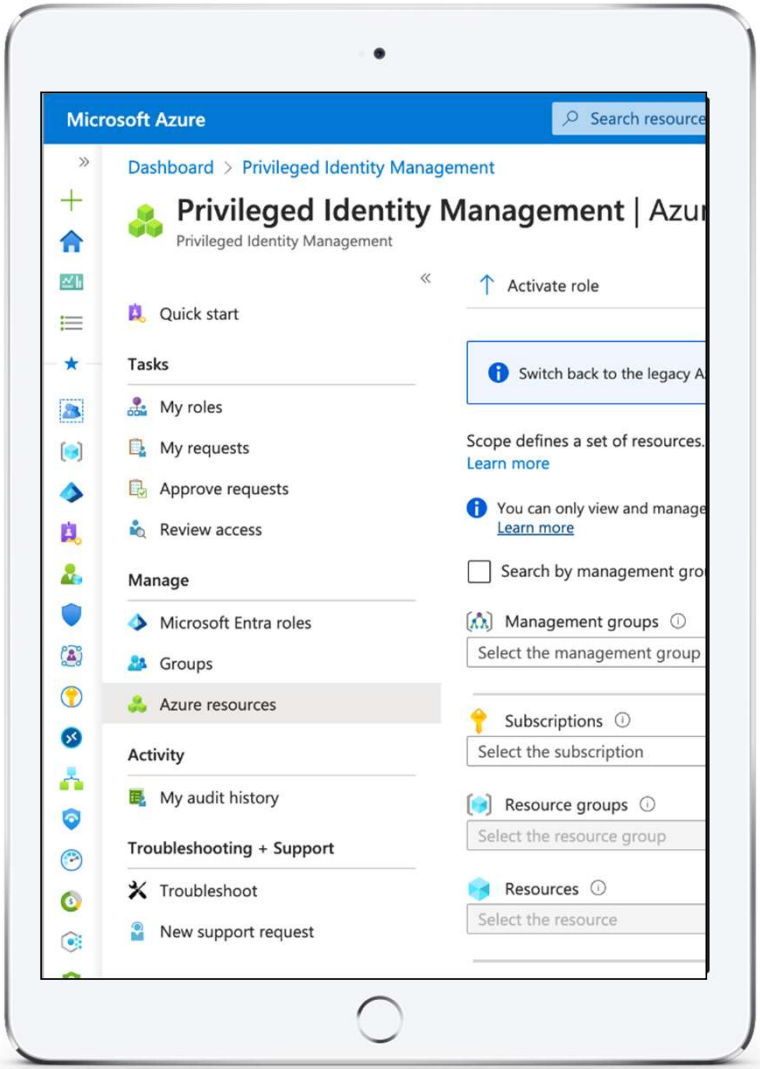
- Allow managing tenant ids to onboard through Azure Lighthouse
- Audit delegation of scopes to a managing tenant

- [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?