
ONE IDENTITY
by Quest

How do you manage access to your Azure infrastructure?

Cloud Infrastructure Entitlement Management as part of a unified identity security platform

Dr. Stephan Hausmann

Visit us at

#7-510

ONE IDENTITY by Quest

oneidentity.com

Dash to the cloud

Dash to the hybrid cloud

Dash to the hybrid multi cloud

Dash to the *secure* hybrid multi cloud

$494B market

size of the Cloud Infrastructure and Platform service market in 2025

Source: Gartner (Apr 2021)

75% of security failures

will result from **inadequate management of identities, access, and privileges** in 2023

Source: Gartner (June 2020)

Why
Cloud Infrastructure Entitlement Management (CIEM)?

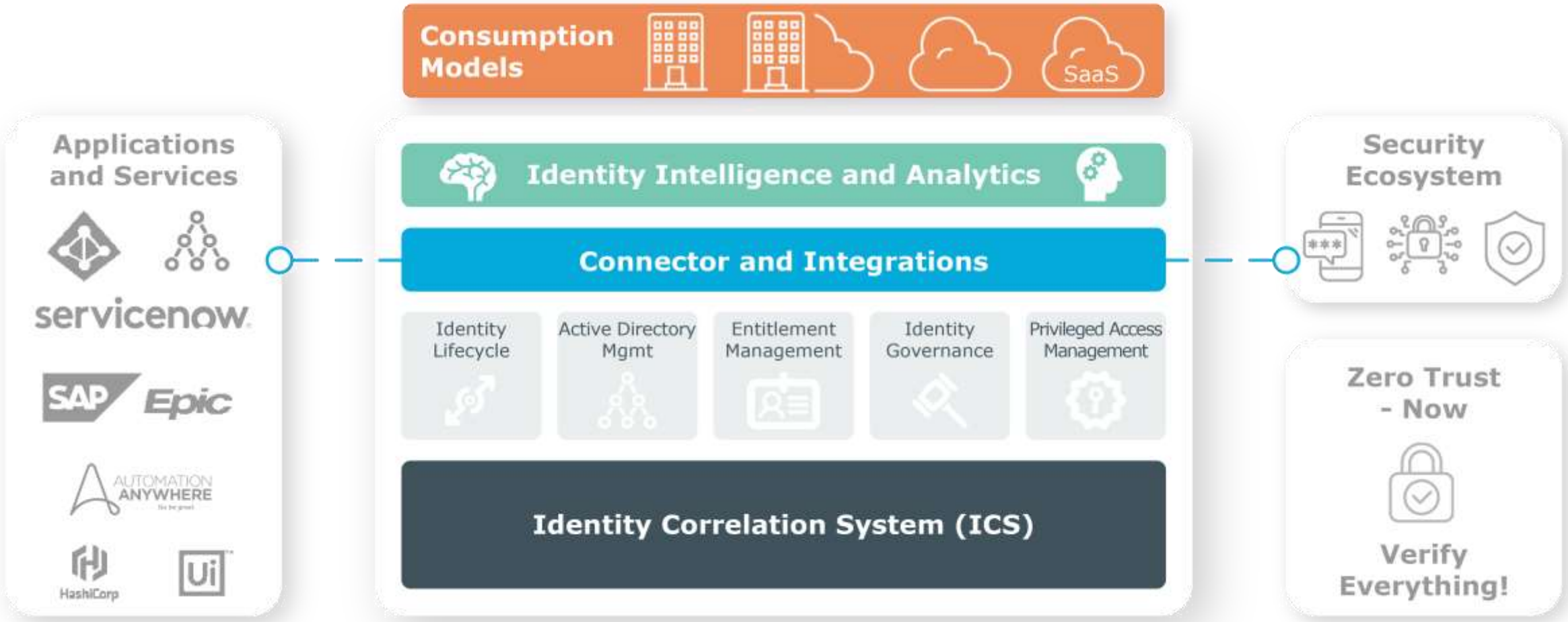
- Using the cloud is beneficial for organizations
- Everything accessible, everywhere, anytime
- Inconsistent security policies in the multi-cloud
- Excessive and long-standing privileged permissions
- cloud (usage) is dynamic
- Beyond traditional On-Premises IGA and PAM
- …

Cloud Infrastructure Entitlement Management (CIEM)

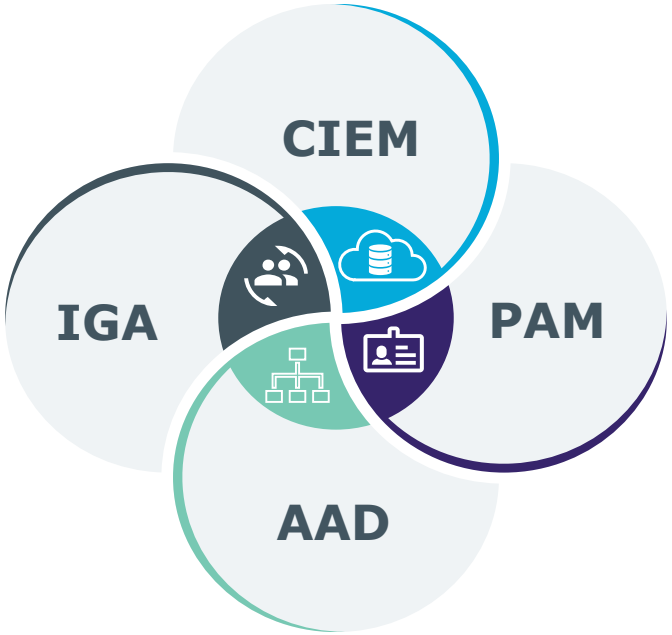
- Catalog - which entitlements exist in the cloud
  - Resources in the cloud (VMs, Containers, Serverless infrastructure, …)
  - Services in the cloud (Database, Storage, Network, Applications, …)
  - Administrative accounts in the cloud
- Managing identities and access in cloud and multi-cloud environments
  - Humans and machines
- Ensure permissions are granted appropriately, with separation of roles
- Intersection of IGA and PAM
- …

Unified identity security platform

People | Applications | Data



Our approach to CIEM....



- Use existing IGA capabilities
  - Correlation
  - Analytics and Reporting
  - Unused accounts, Peer Group Outliers, Orphan entitlements and accounts
  - Request & Attestation
- Enhance IGA
  - Visibility on infrastructure permissions
  - Integrate Cloud events and usage
  - Multi-Cloud support
  - Misc PAG workflows
- Use existing PAM capabilities
  - SSH/RDP sessions
  - Push PAM secrets to DevOps

Results

Centralize Visibility

Detect and Respond

Right Size permissions

Reduce attack surface

Breach resilience

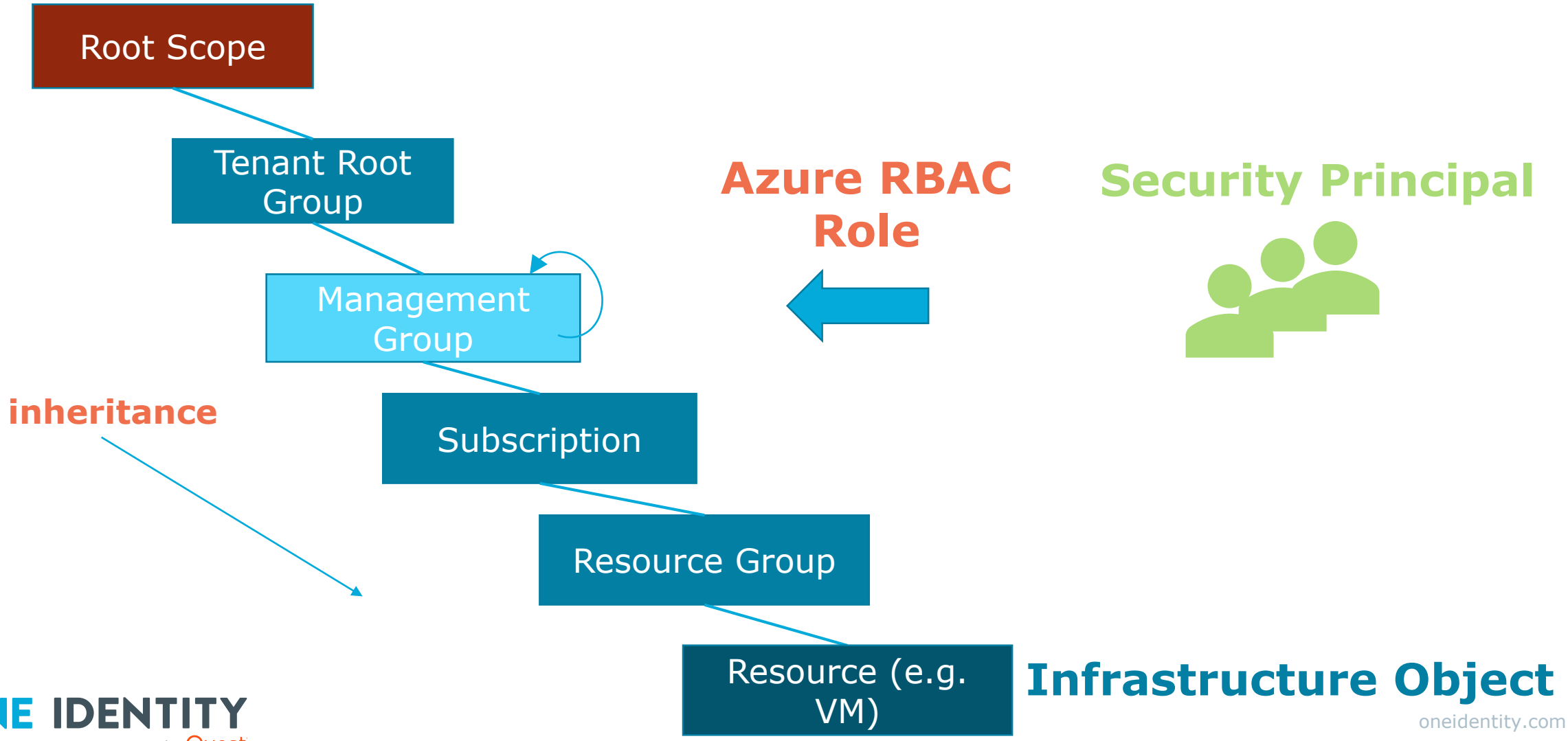
Prove Compliance

Business Confidence

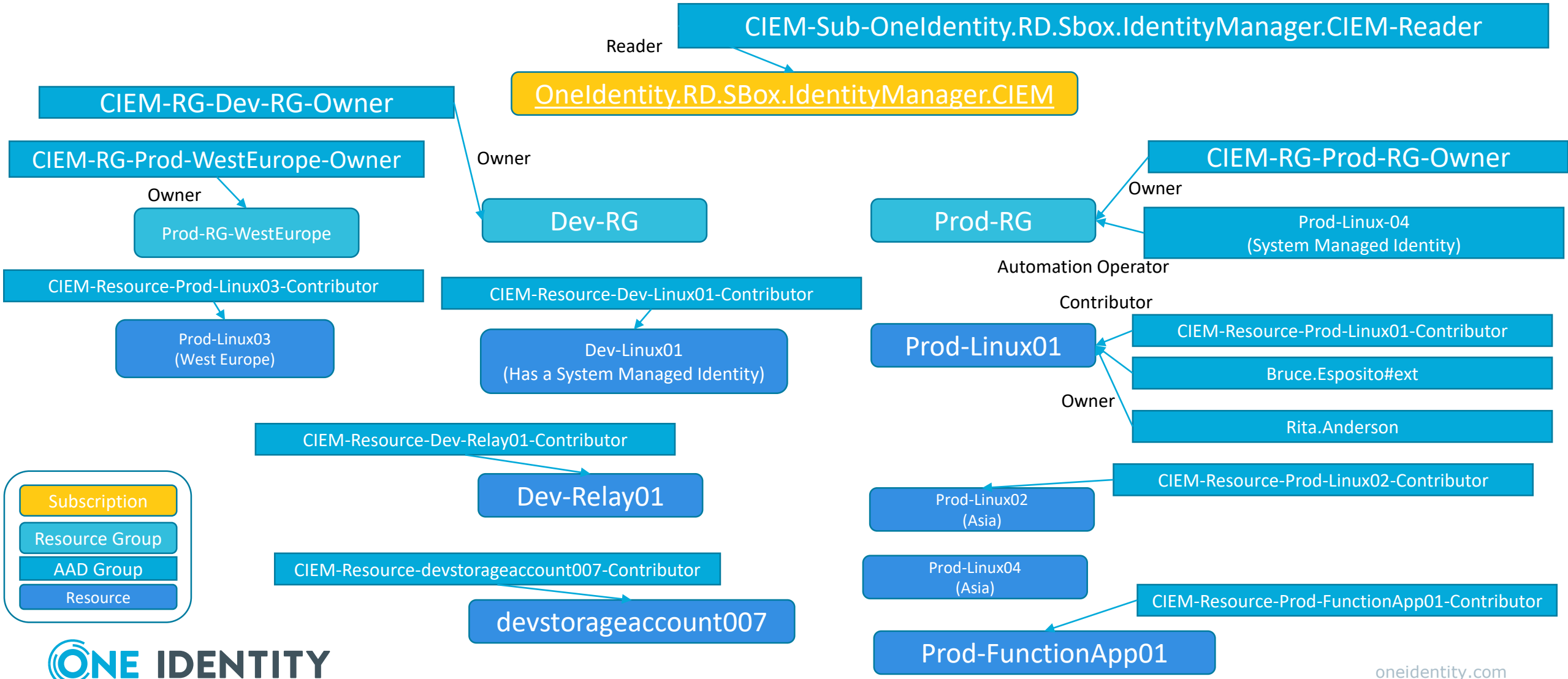
IGA Use Cases ... for Cloud Infrastructure

- Discover Cloud Infrastructure access
- Detect and Respond to anomalies in Cloud Infrastructure access
- Request for Access to Cloud Infrastructure
- Attestation of Cloud Infrastructure access
- Privilege Account Governance for Cloud Infrastructure access

Azure Infrastructure Permission Model



The reality is more complex …



ONE IDENTITY by Quest

Identity Manager CIEM Integration

From the Azure AD Module:
- Accounts
- Groups
- Service Principals (since 8.2)

Identity Manager

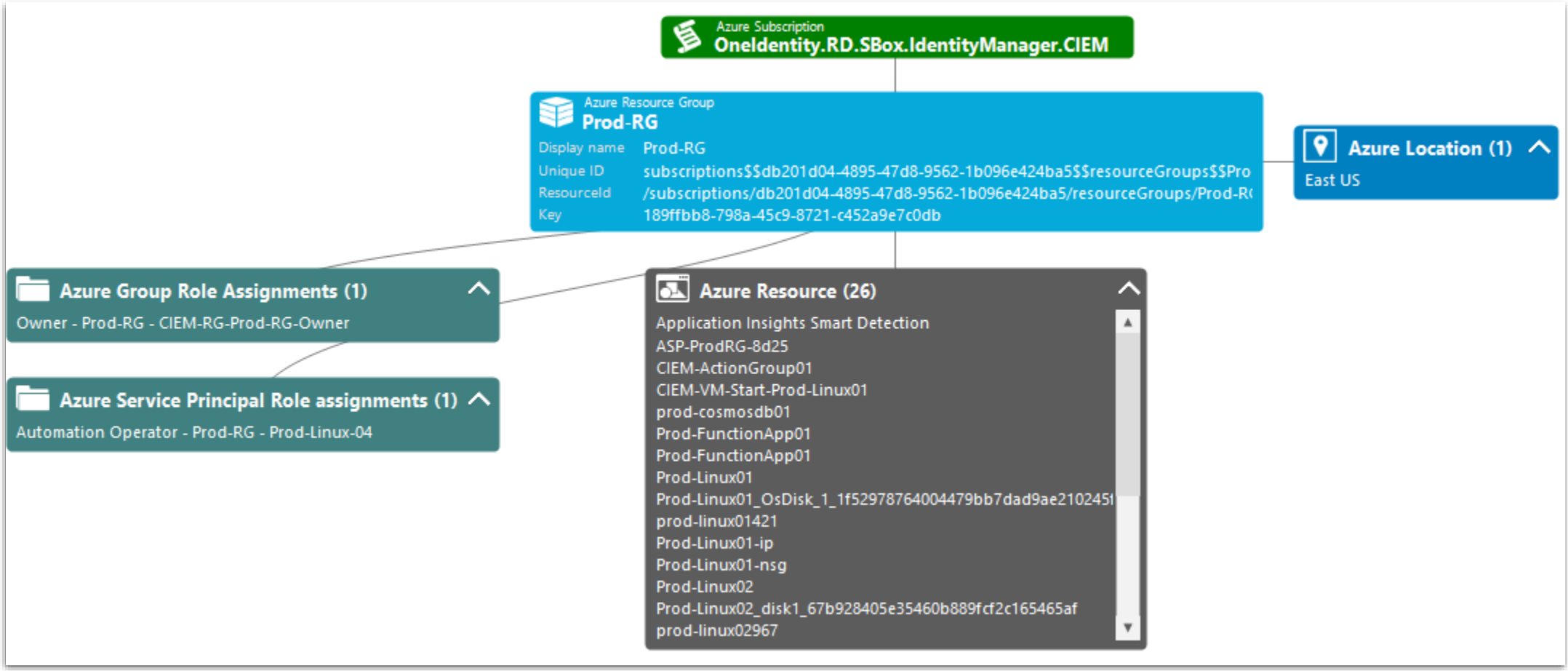
CIEM Aggregation

Azure Infrastructure Objects:
- Azure RBAC Roles
- Resources (VMs, disks, …)
- Resource Groups
- Subscriptions
- Management Groups
- Locations

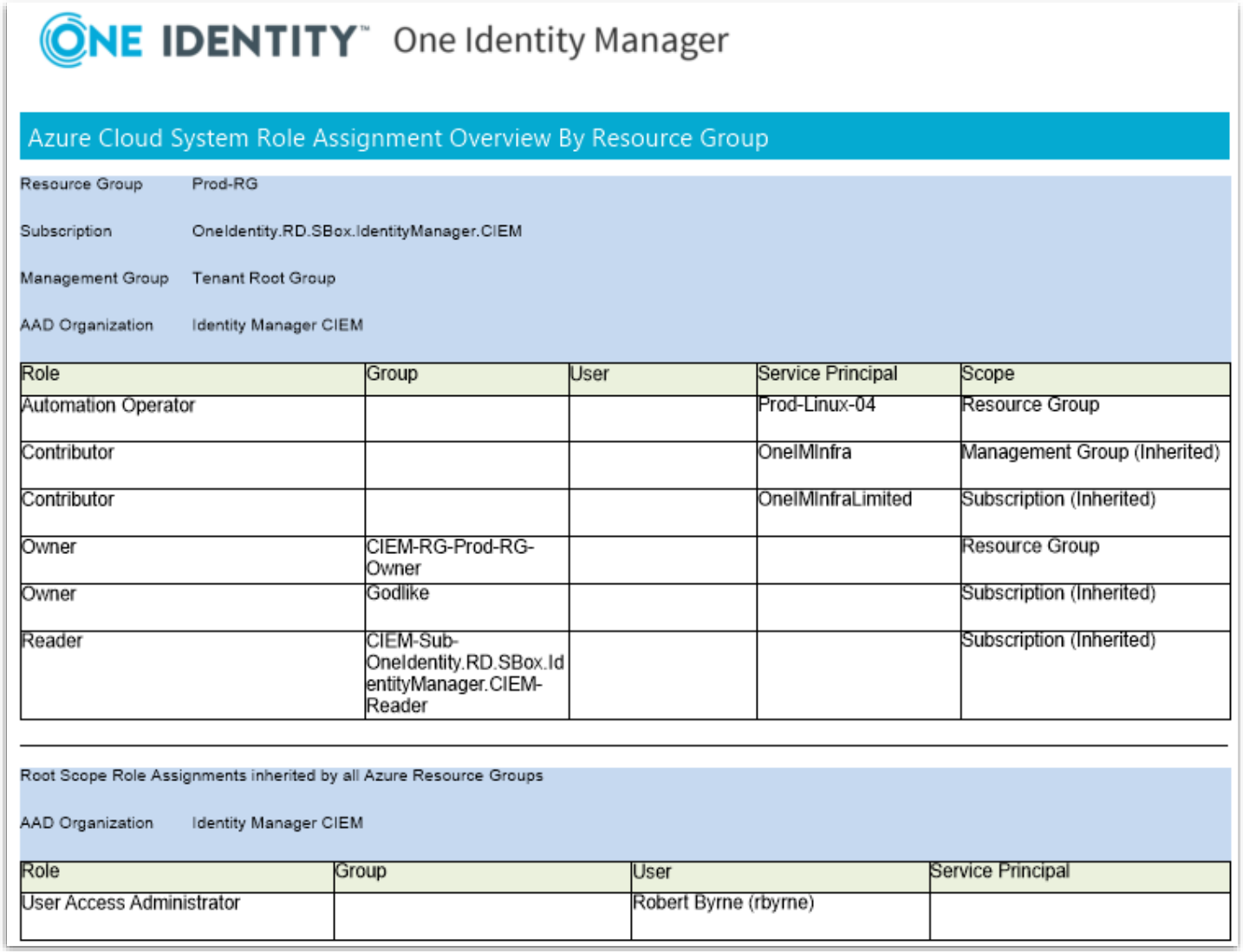
Azure AD Connector (native)

Azure Infrastructure Connector (Starling)

Visibility - Resource Group



Visibility - Resource Group Report



ONE IDENTITY One Identity Manager

Azure Cloud System Role Assignment Overview By Resource Group

Resource Group Prod-RG

Subscription OneIdentity.RD.SBox.IdentityManager.CIEM

Management Group Tenant Root Group

AAD Organization Identity Manager CIEM

Role	Group	User	Service Principal	Scope
Automation Operator			Prod-Linux-04	Resource Group
Contributor			OneIMInfra	Management Group (Inherited)
Contributor			OneIMInfraLimited	Subscription (Inherited)
Owner	CIEM-RG-Prod-RG-Owner			Resource Group
Owner	Godlike			Subscription (Inherited)
Reader	CIEM-Sub-OneIdentity.RD.SBox.IdentityManager.CIEM-Reader			Subscription (Inherited)

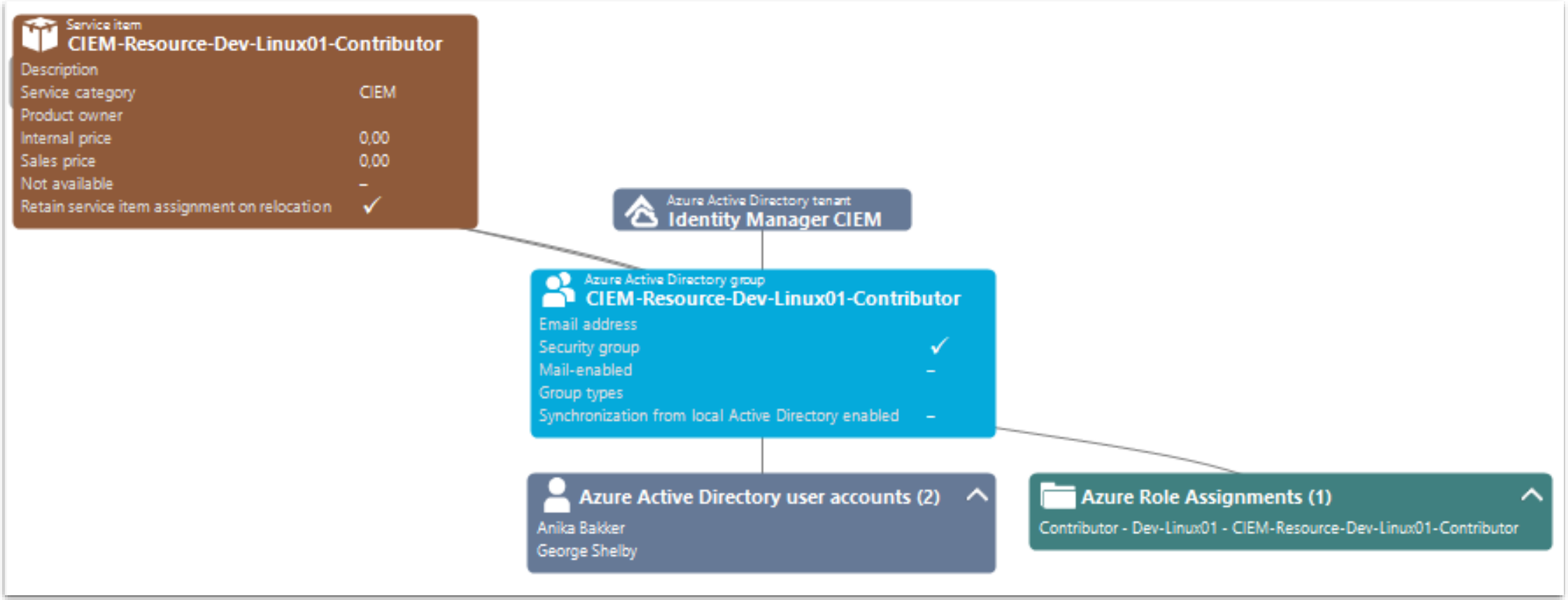
Root Scope Role Assignments inherited by all Azure Resource Groups

AAD Organization Identity Manager CIEM

Role	Group	User	Service Principal
User Access Administrator		Robert Byrne (rbyrne)	

ONE IDENTITY by Quest

Visibility - Azure AD Group granting access to a Resource



CIEM IGA Scenarios

Scenario 1 – Discovery and Visibility

- Visibility onto Infrastructure structure and objects
- Visibility onto Access – by user, by resource
- Dashboards & Reporting

Scenario 2 –Policies and Anomaly Detection

- Orphan/Dormant/Inactive accounts
- Accounts with direct access to infrastructure
- Infrastructure without owners
- Identities with inappropriate business access – geographical or role

Scenario 3 – Governance

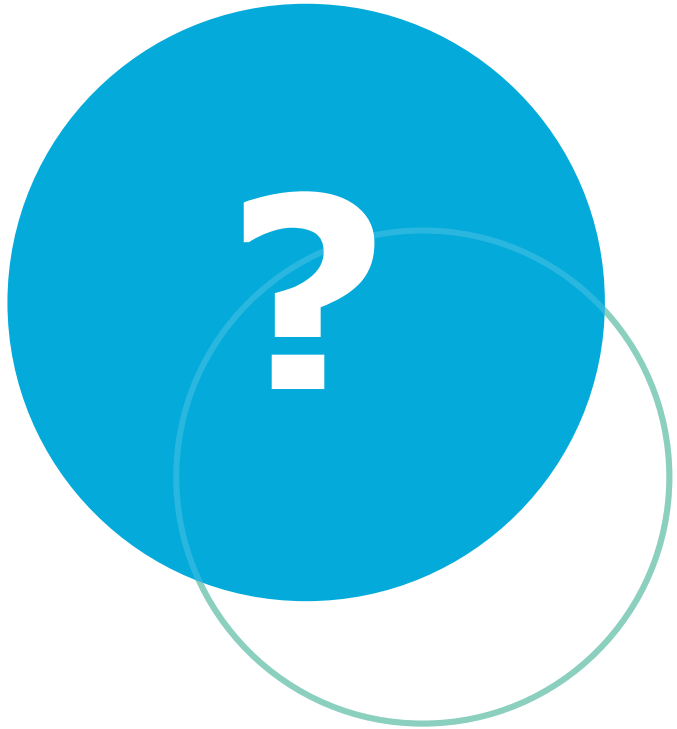
- Access Request
- Attestation/Recertification

Benefits of CIEM with Identity Manager

Extend governance

from On-Premises Applications and Cloud Applications

to Cloud infrastructure.



Questions?

#7-510


ONE IDENTITY
by Quest