



The Experts Conference

Sponsored by Quest®

Protecting Privileged User and Workload Identities in Microsoft Entra

Thomas Naunheim
Cyber Security Architect
@glueckkanja AG



**The Experts
Conference**
Sponsored by Quest®



Thomas Naunheim

Cyber Security Architect @glueckkanja AG
Microsoft Security MVP

X @Thomas_Live

 www.cloud-architekt.net

Agenda



PRIVILEGED USERS



PRIVILEGED ACCESS



PRIVILEGED ENDPOINTS

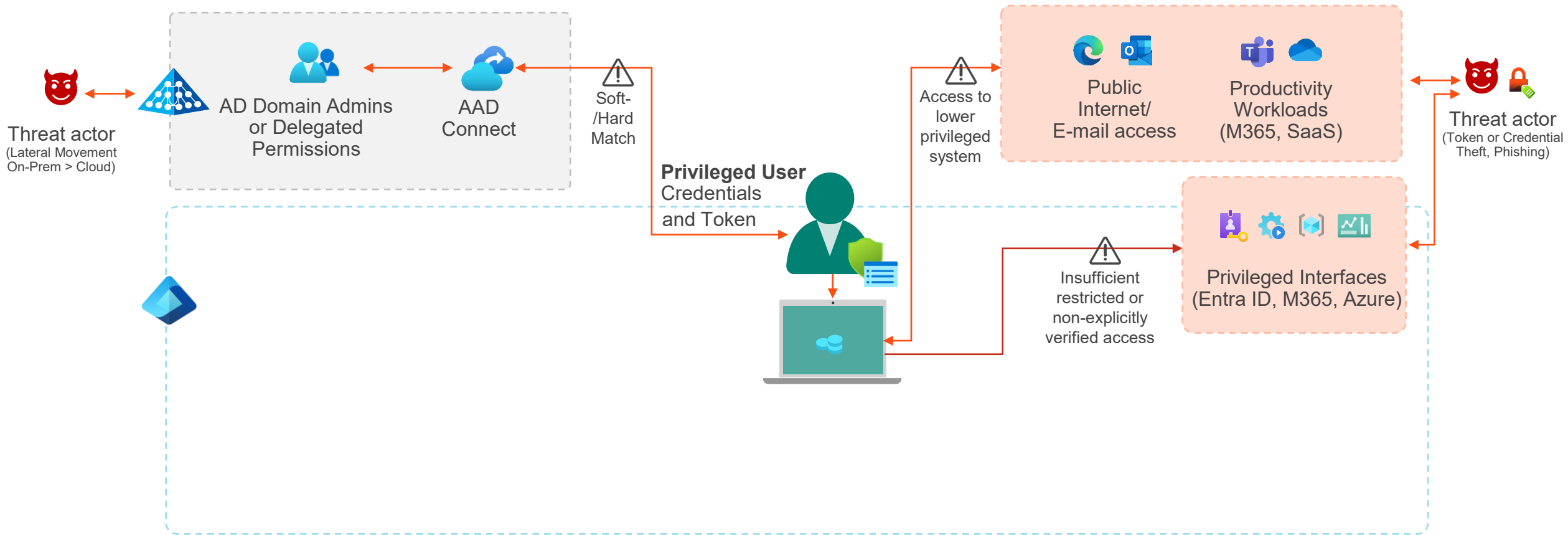


PRIVILEGED WORKLOADS

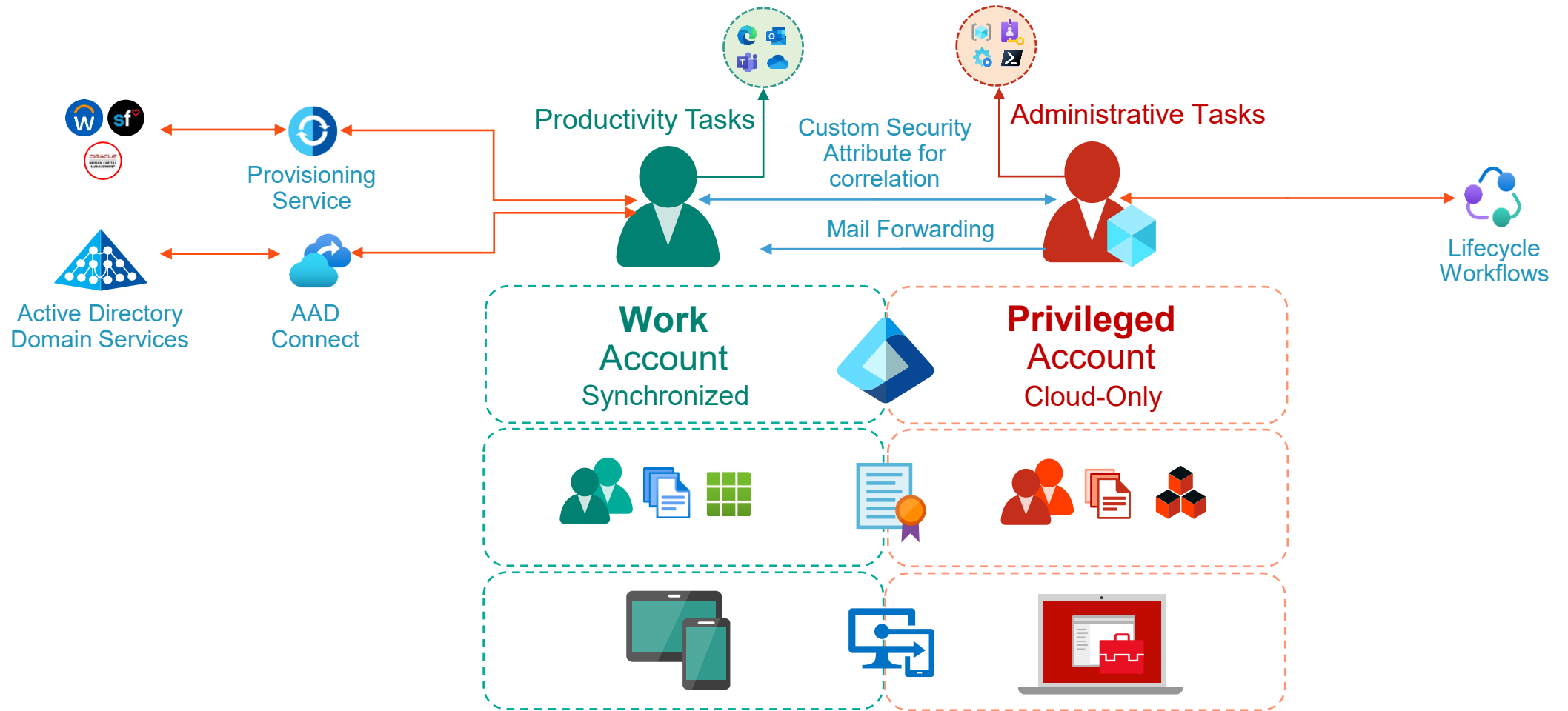
Privileged Identities

*Automated Lifecycle and
Monitoring for Privileged Accounts*

Attack paths to privileged (work) accounts



Foundation of Privileged Identities





Onboarding and of Privileged Users

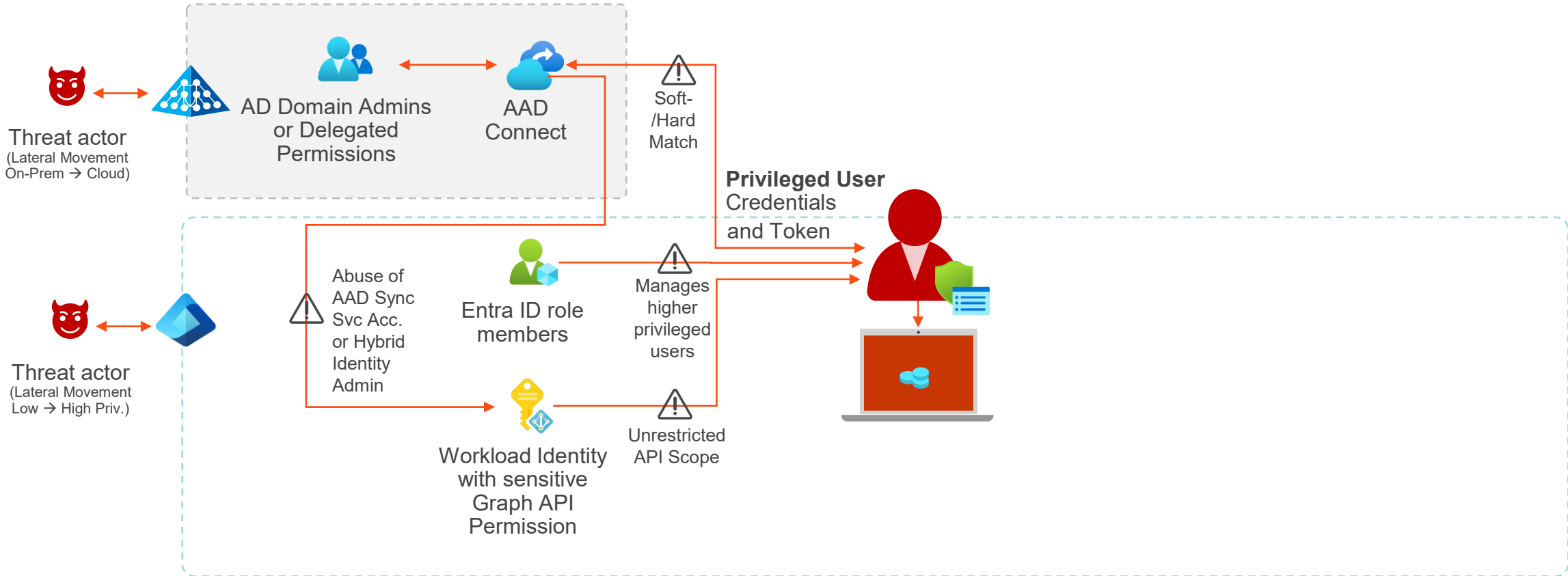


**The Experts
Conference**
Sponsored by Quest®

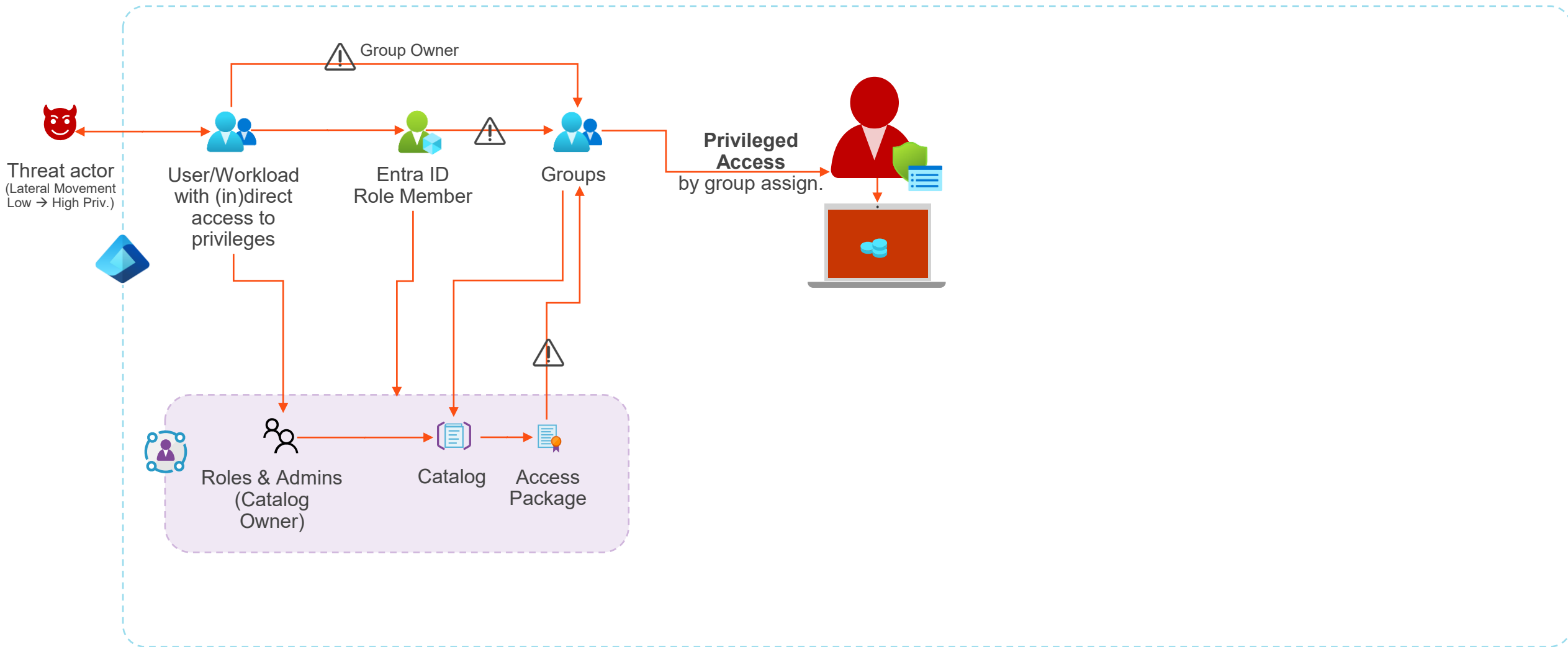
Privileged Access

*Scoped permissions on a least-privilege
and security boundary approach*

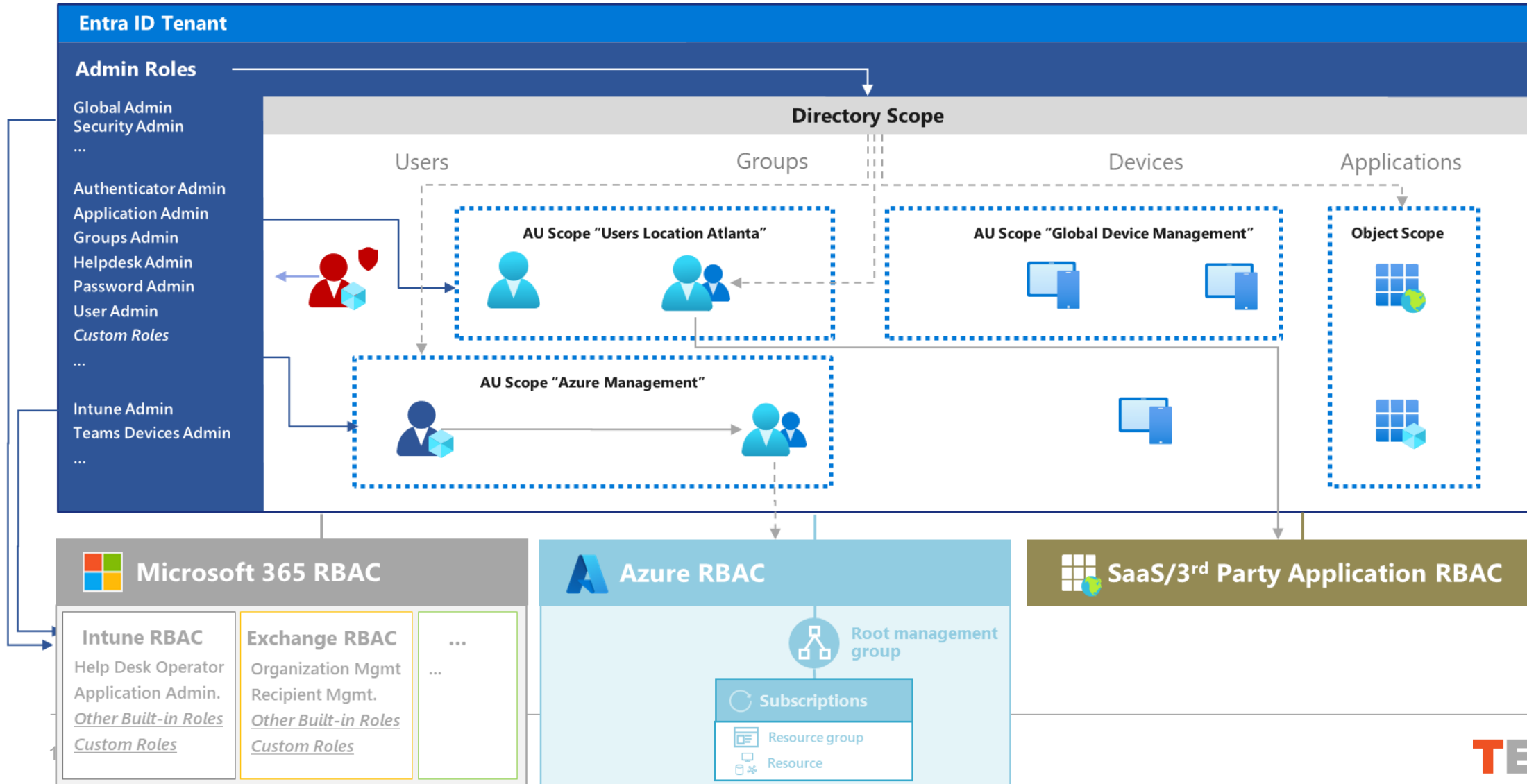
Attack paths to privileged accounts



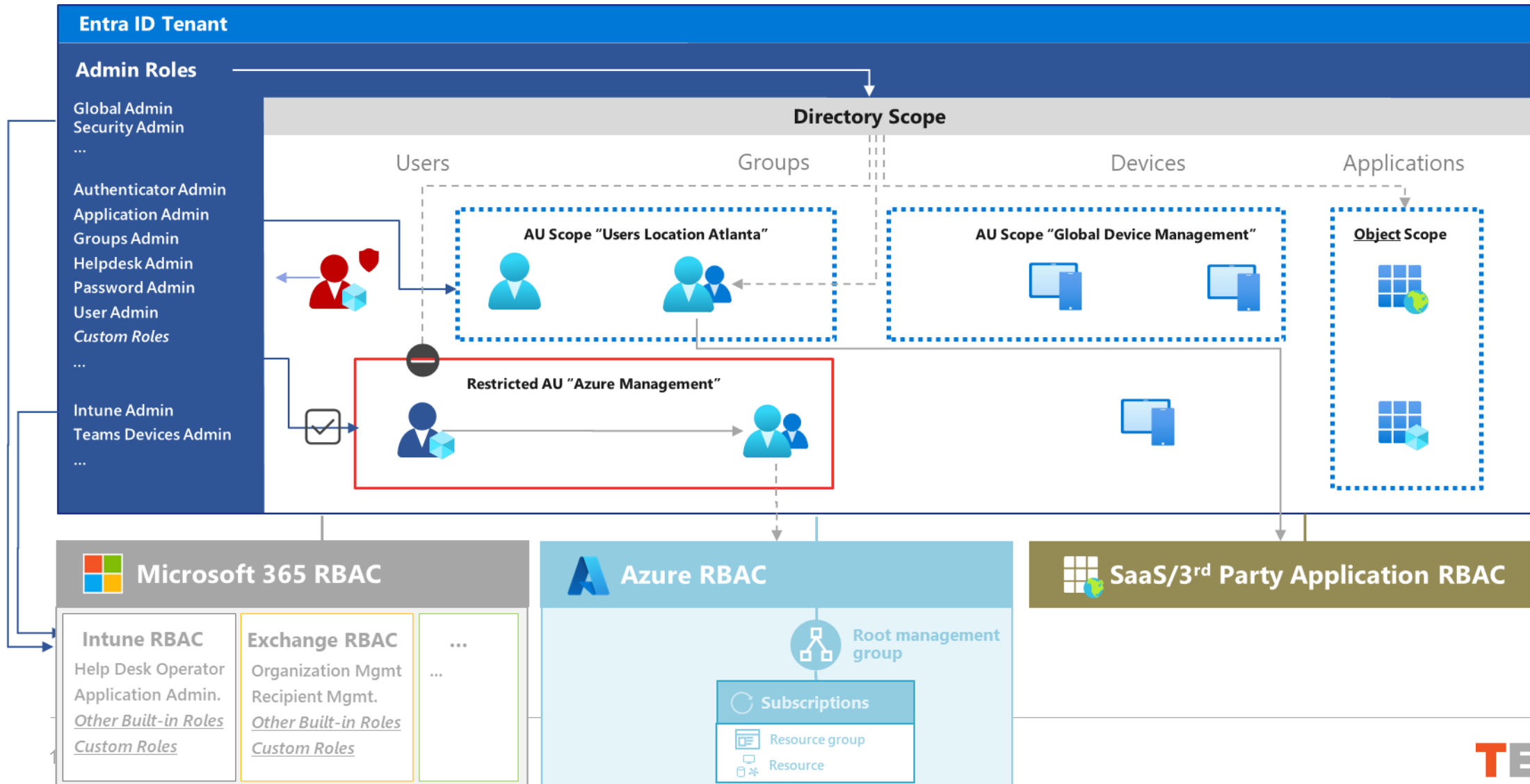
Attack paths to privileges in Entra ID



Delegation and permissions on privileged objects



Delegation and permissions on privileged objects



Different types of groups for privileged assignments

	Preferred use case/scenario	Restricted group object	Restriction applies to <u>user</u> members	Blocks AADC Soft Match
Security Groups without PIM	Non-high privileged assignments	✗ No restriction	✗ No restriction	✗ No restriction
Security Group with PIM for Groups	Just-In-Time Access outside of Azure and Entra ID RBAC	✗ No restriction	✗ No restriction	✗ No restriction
Security Groups in Restricted AU	Assignment to sensitive policies or none-PIM groups	☑ RMAU-scoped Admins	✗ No restriction	✗ No restriction
Role-Assignable Security Groups	Assigning Entra ID roles (or other high-privileges)	☑ GA, PRA and Owners	⚠ Restricted to GA and Privileged Auth. Admin when active/permanent member	⚠ Only when active or permanent assigned Entra ID role member

Identity Governance for Privileged Access



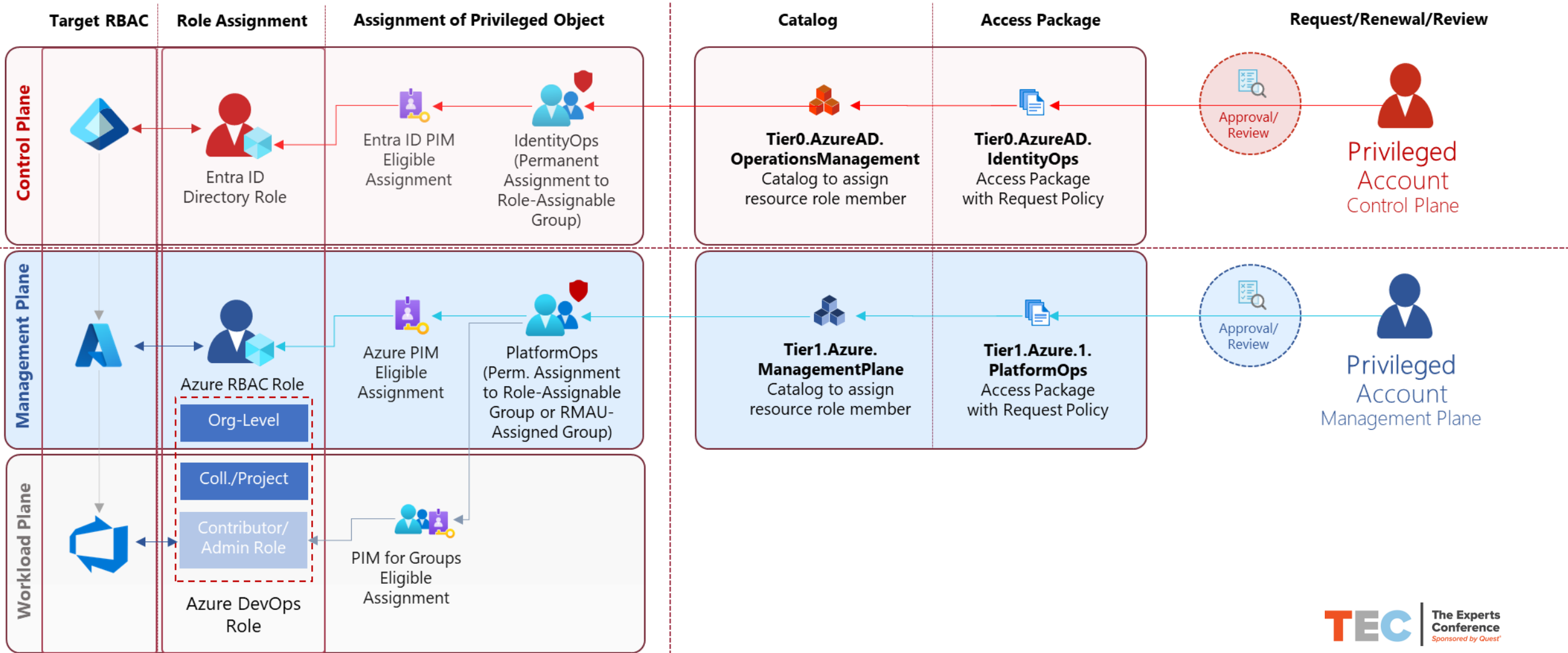
Privileged Identity Management



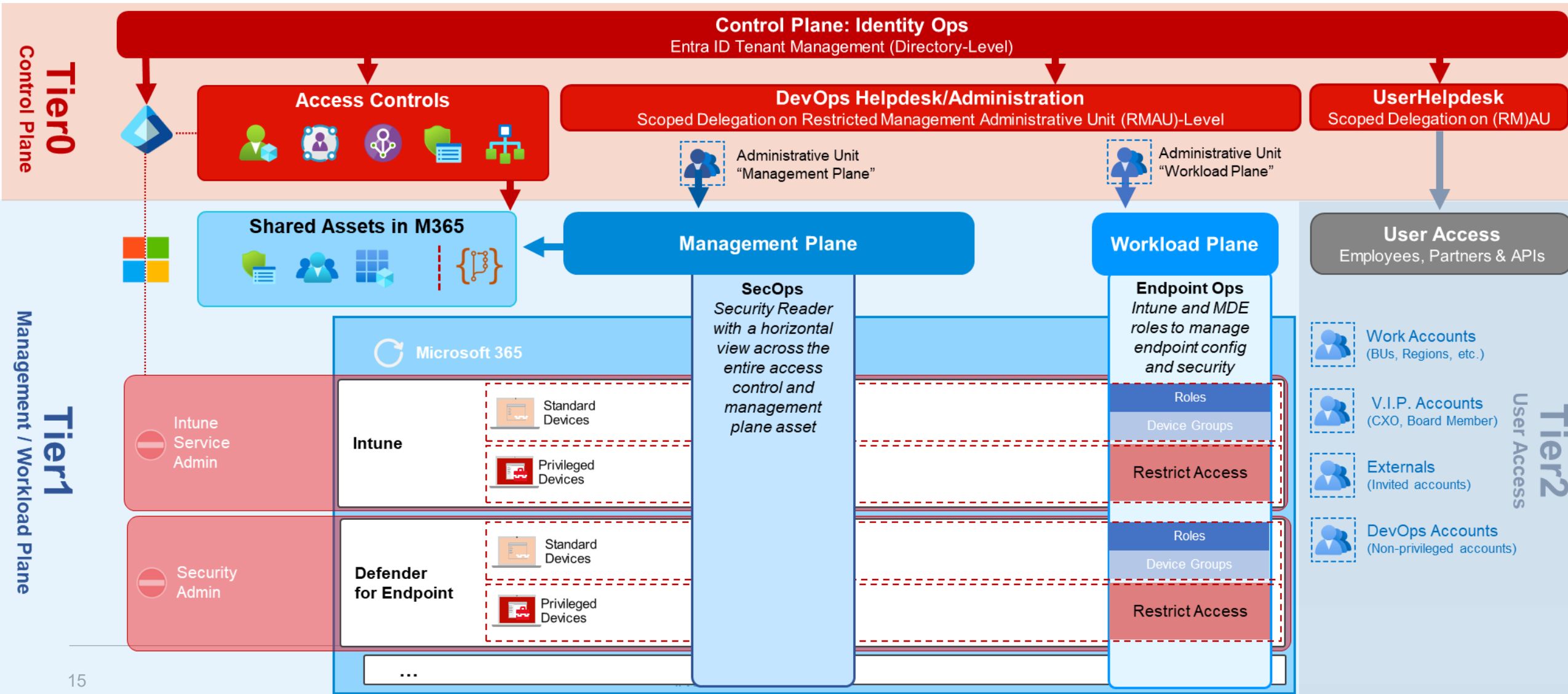
Entitlement Management



Lifecycle Workflows



Privileged Access Model for Endpoints



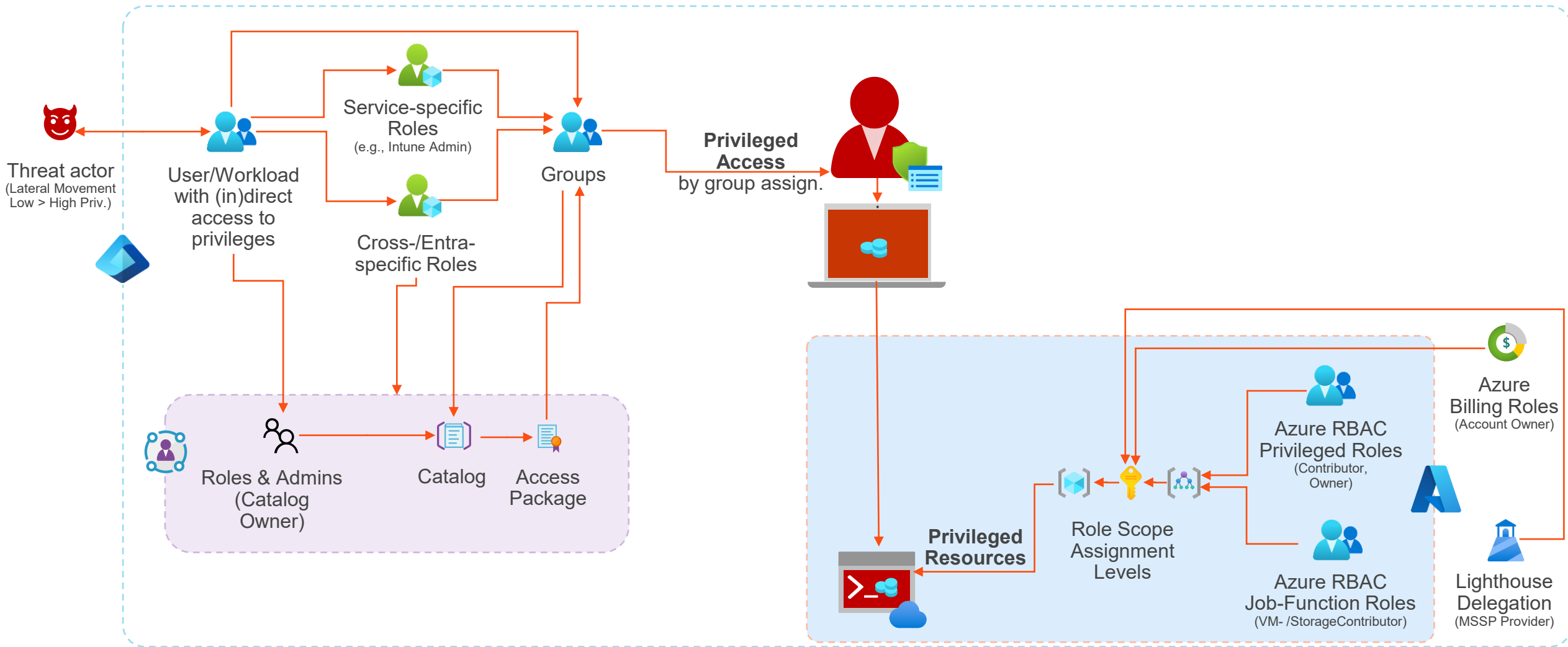


Request and assign privileged roles by Identity Governance

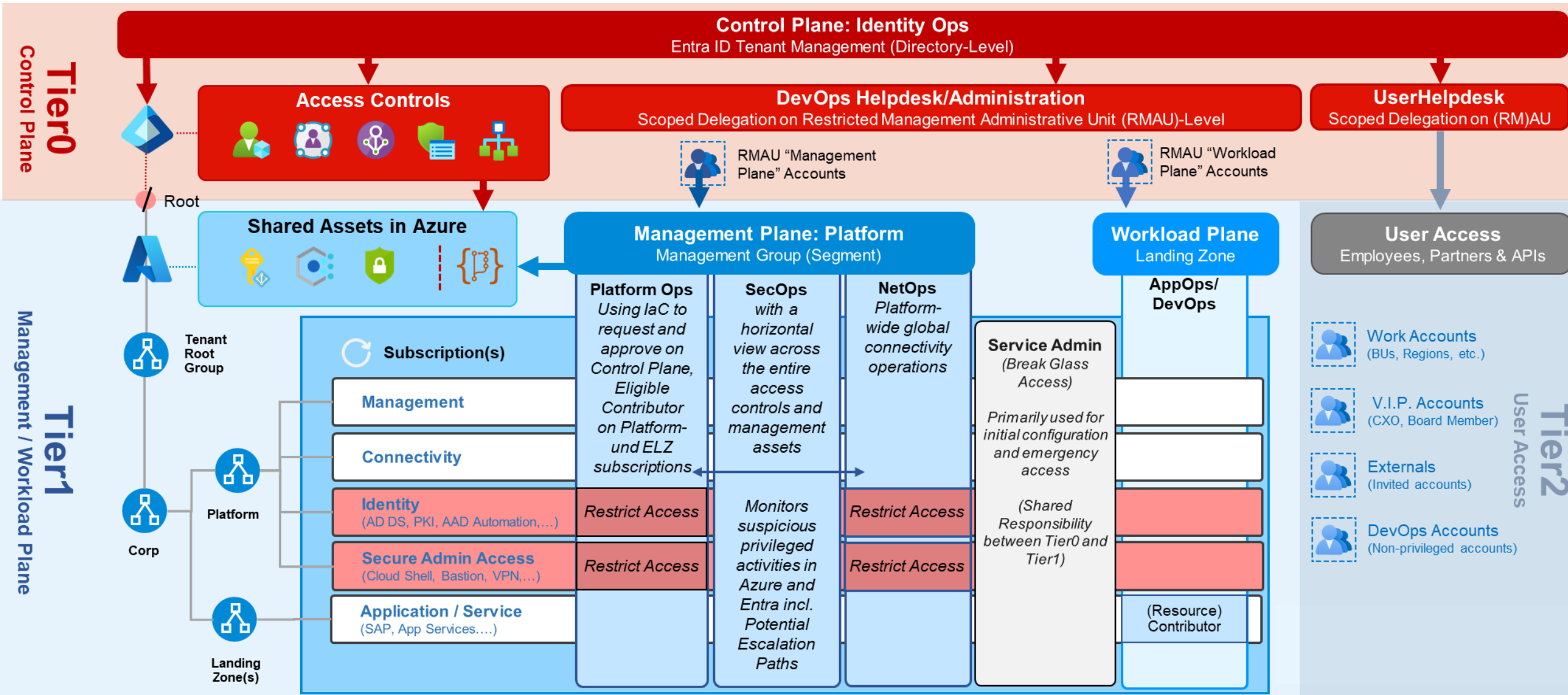


**The Experts
Conference**
Sponsored by Quest®

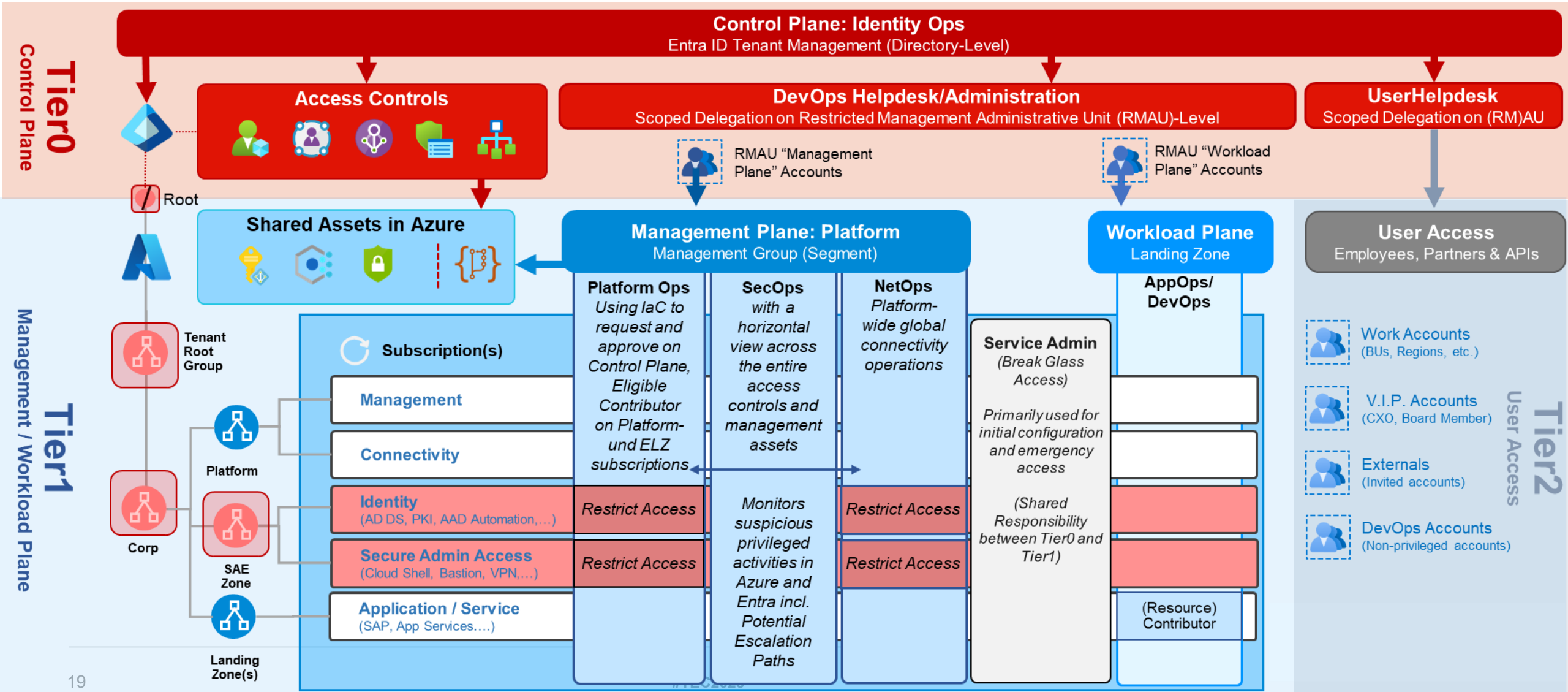
Attack paths to privileged Azure resources in Entra ID



Privileged Access Model in Microsoft Azure



Privileged Access Model in Microsoft Azure



Classification for Azure Privileged Roles

Classification of Action and Scope

```
"EAMTierLevelName": "ControlPlane",
"TierLevelDefinition": [
  {
    "Category": "Microsoft.Azure",
    "Service": "Privileged RBAC Management",
    "RoleAssignmentScopeName": [
      "/",
      "/*/*/managementGroups/lab-saezone",
      "/*/*/managementGroups/lab"
    ],
    "RoleDefinitionActions": [
      "Microsoft.Authorization/*",
      "*"
    ]
  }
]
```

Classification of Privileged Principal

```
"ObjectAdminTierLevelName": "ControlPlane",
"ObjectDisplayName": "admThom0",
"Classification": [
  {
    "AdminTierLevelName": "ControlPlane",
    "Service": "Privileged RBAC Management"
  }
]
"RoleAssignments": [
  {
    "RoleAssignmentScopeName": "/*/*/managementGroups/lab",
    "RoleAssignmentType": "Transitive",
    "TransitiveByObject": "prg_Tier0.IdentityOps",
    "RoleDefinitionName": "User Access Administrator",
    "PIMAssignmentType": "Eligible"
  }
]
```



Classification of Privileged objects in Enterprise Access Model



**The Experts
Conference**
Sponsored by Quest®

Privileged Endpoints

*Restricted access to/from privileged
and secured endpoints for privileged accounts*

Foundation of Privileged Endpoints

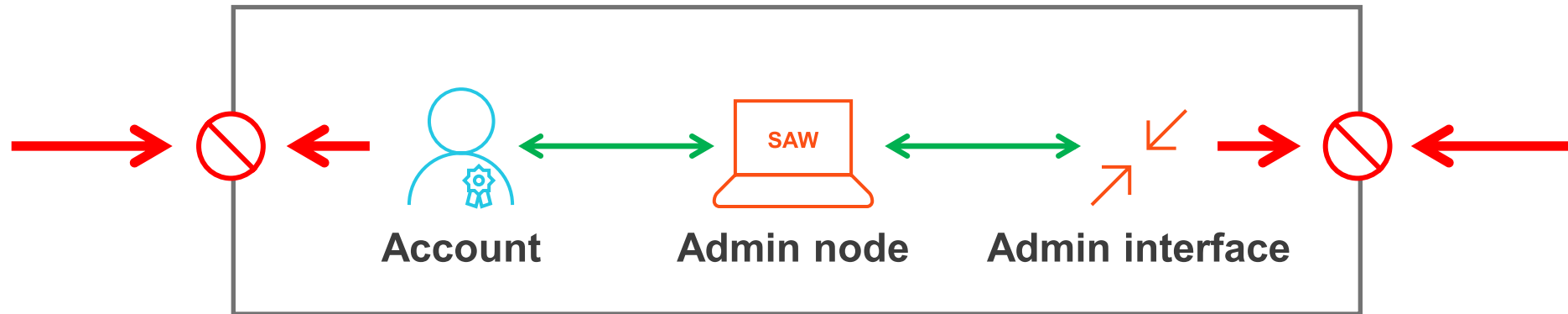
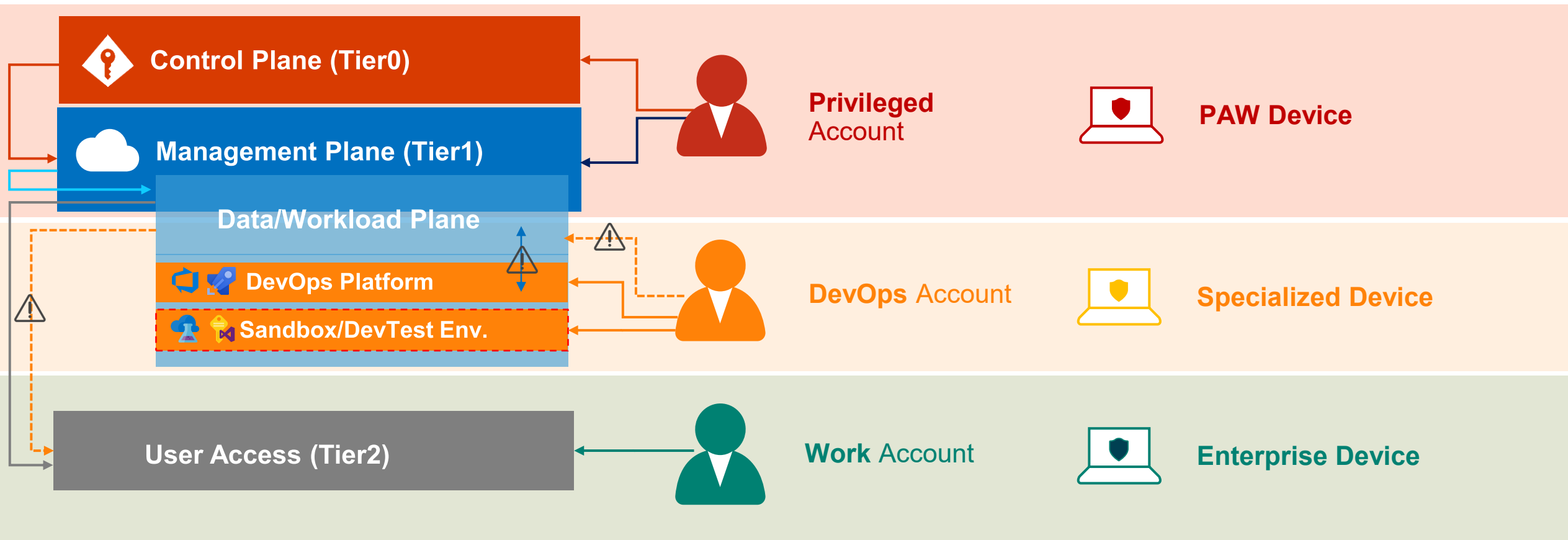
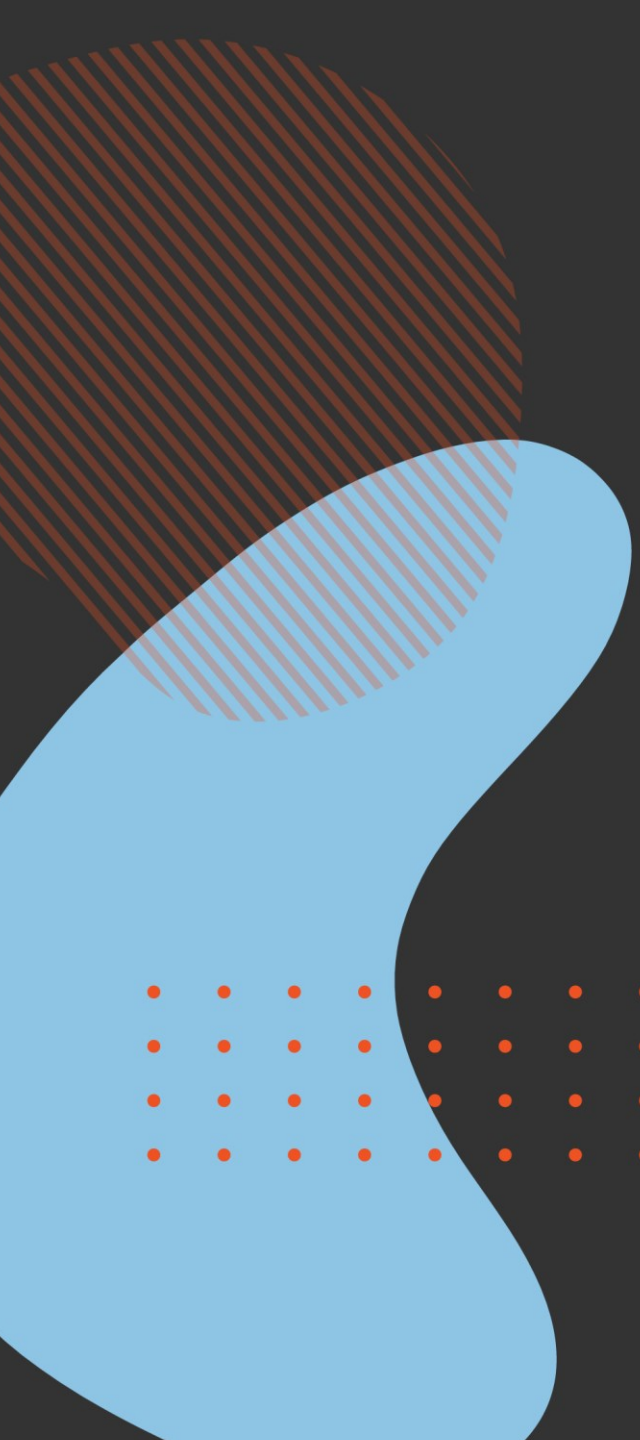


Image source: “[Microsoft CISO Workshop 4a - Threat Protection Strategy](#)”

Privileged, Specialized and Enterprise Security





Restricted access to Privileged Interfaces and Token Replay



**The Experts
Conference**
Sponsored by Quest®

Workload Identities

*Detection and monitoring of
non-human privileged identities*

Comparison Human vs. Workload Identities



HR data and processes as source of authority

Multi-factor and strong authentication
(Phishing-resistant Passwordless)

Just-in-Time access and review
by Identity Governance workflows

Support for many built-in templates
and detection capabilities



No defined lifecycle management

Risks of leaked secrets or compromised
credentials in code or automation jobs

Escalation paths by standing and overprivileged access,
limitations for fine-granted API permissions

Lack of auditing, monitoring and detections

Differences in Types of Workload Identities

	Application Identity (Key/Certificate)	Application Identity (Federated Credentials)	Azure Managed Identity (System-/User-Assigned)
Trust Relationship	Issued credential	External IdP	Azure Managed Resource
Lifecycle Management	Admin	Admin	Azure (System-Assigned), Admin (User-Assigned)
Delegation	Application/Enterprise Object, Entra ID Role	Application/Enterprise Object, Entra ID Role	Azure RBAC Role, Enterprise Object
Token Lifetime / Cache	1h (Default), 24h (CAE)	1h (Default)	24h
Entra ID Conditional Access	Yes	Yes	Not available
Entra ID Protection	Yes (Single-Tenant)	Yes (Single-Tenant)	Not available
Detection / Logging	Sign-in logs	Correlation between Entra and External IdP Logs	Limited sign-in logs



Detection and monitoring of high privileged workload identities



**The Experts
Conference**
Sponsored by Quest®

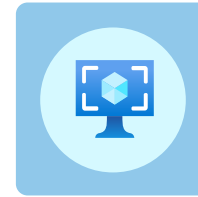
Summary | Privileged User & Workload Identities



Isolated cloud-only **privileged user** with lifecycle and relation to work account and HR processes



Established (tiered) **privileged access** model by classified, governed and scoped assignments in Entra ID Identity Governance



Explicitly verified and restricted access from **privileged endpoints** to interfaces by using secured workstations



Identified and strictly monitoring of **privileged workloads** incl. their non-human identities and security posture

Continue the conversation...

Live Q&A up next!





Questions?



**The Experts
Conference**
Sponsored by Quest®

Thank you!