Cloud Identity Governance Masterclass

Marcus Idle, Kocho

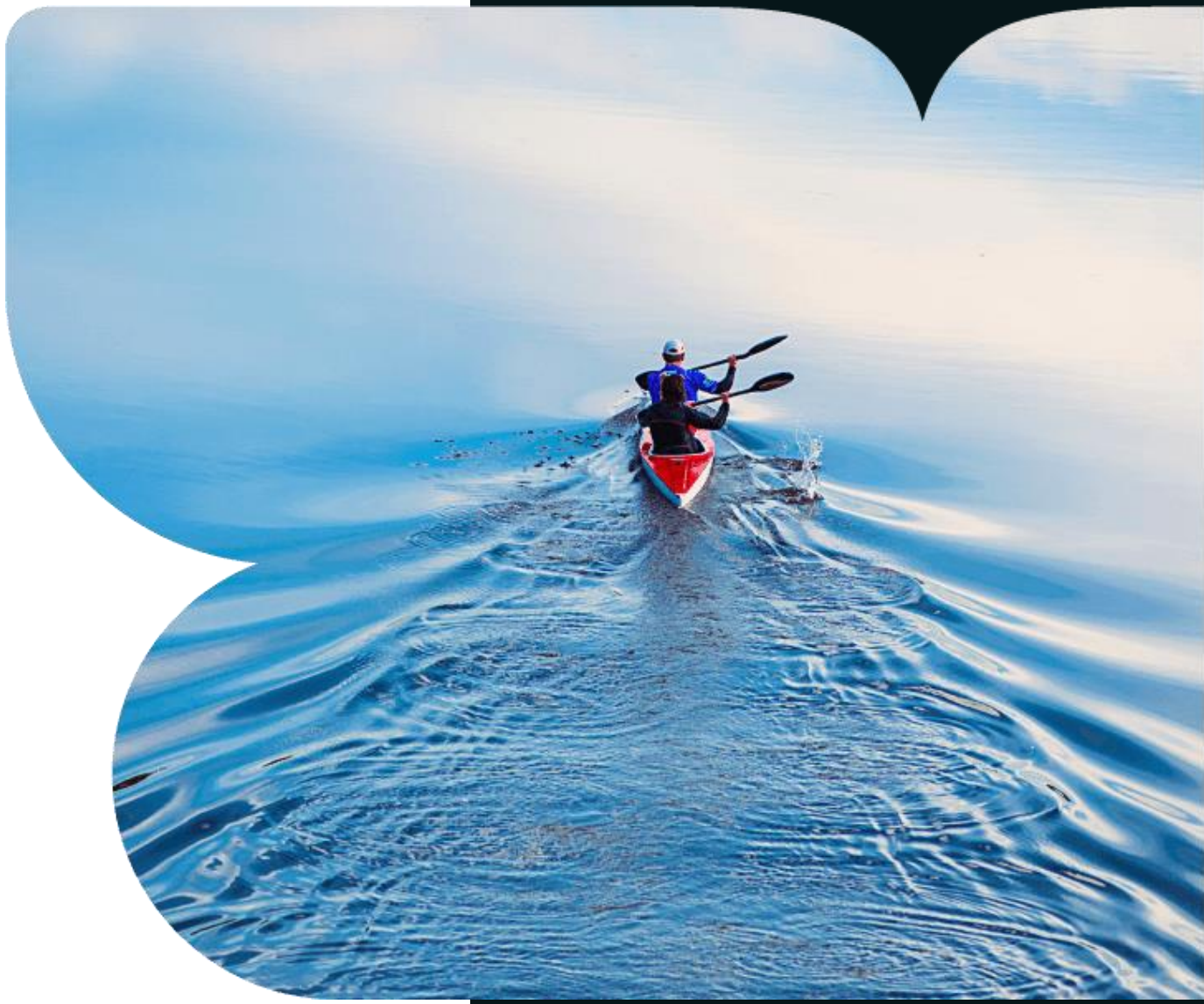
Serge Kerremans, Saviynt

Kocho

BECOME GREATER

Agenda

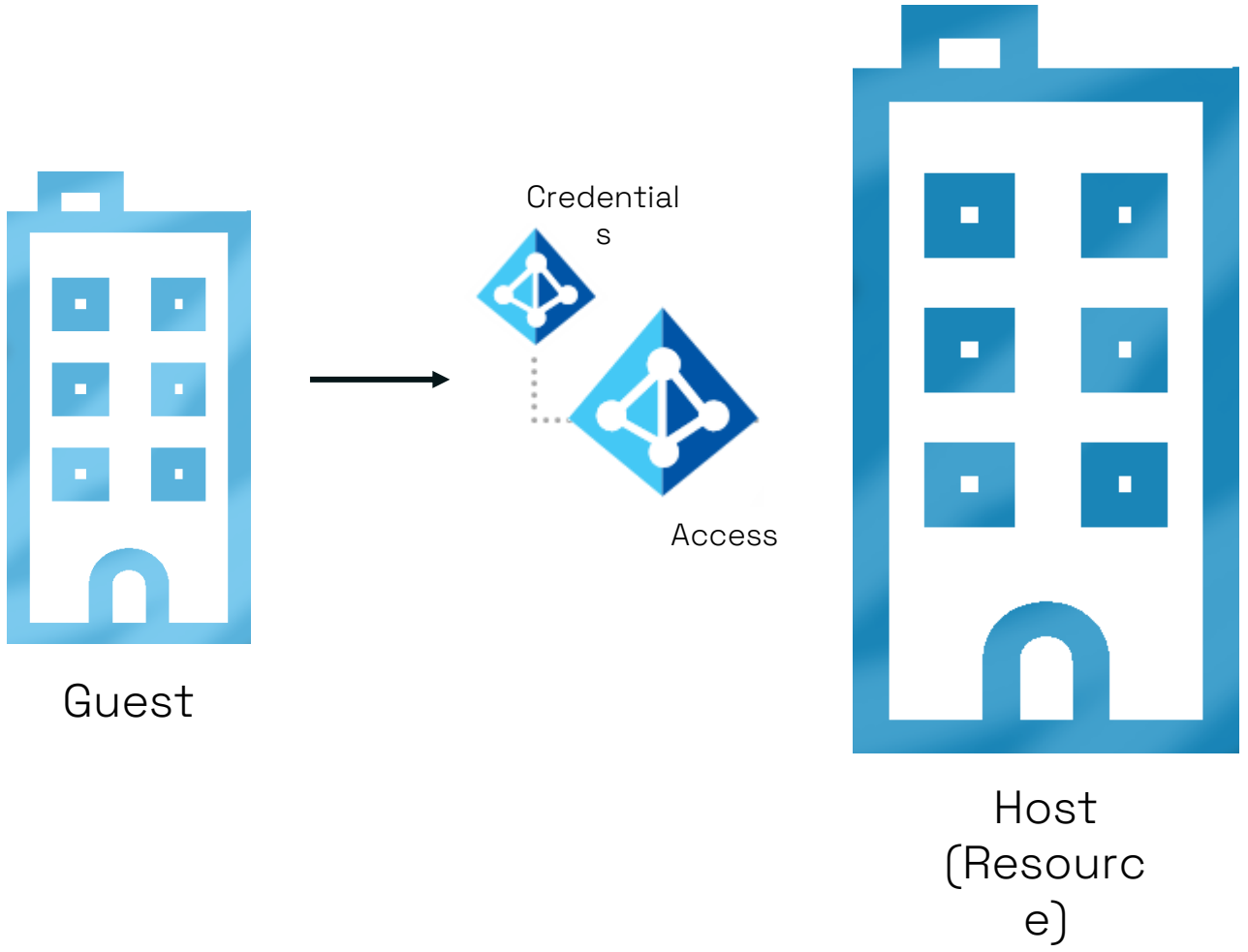
- Azure IG (30 mins)
- Saviynt (30 mins)
- Q&A (30 mins)



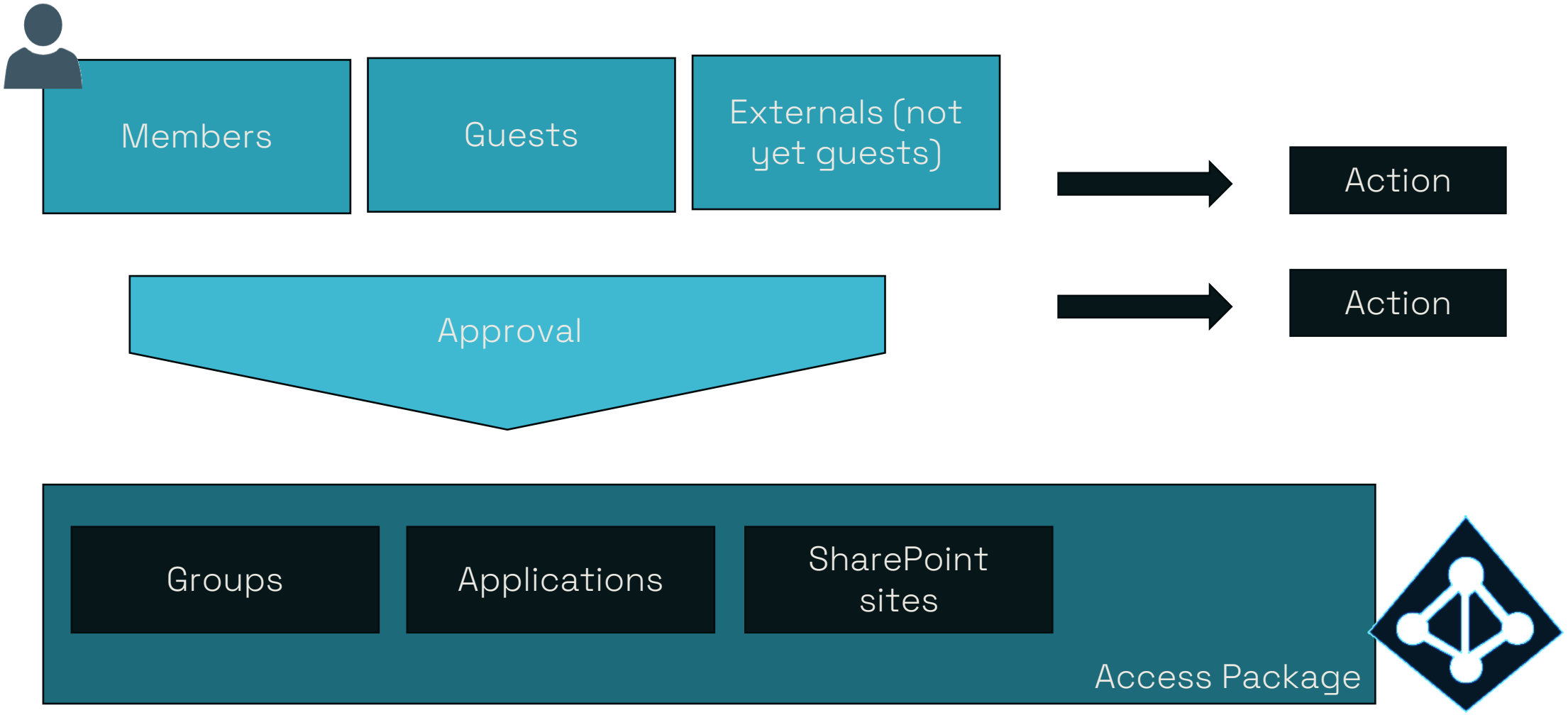
• Professional services
• £2.5m stolen
• Cause: unmanaged guest accounts

• Manufacturer
• Auditing issues
• Cause: unmanaged guest accounts

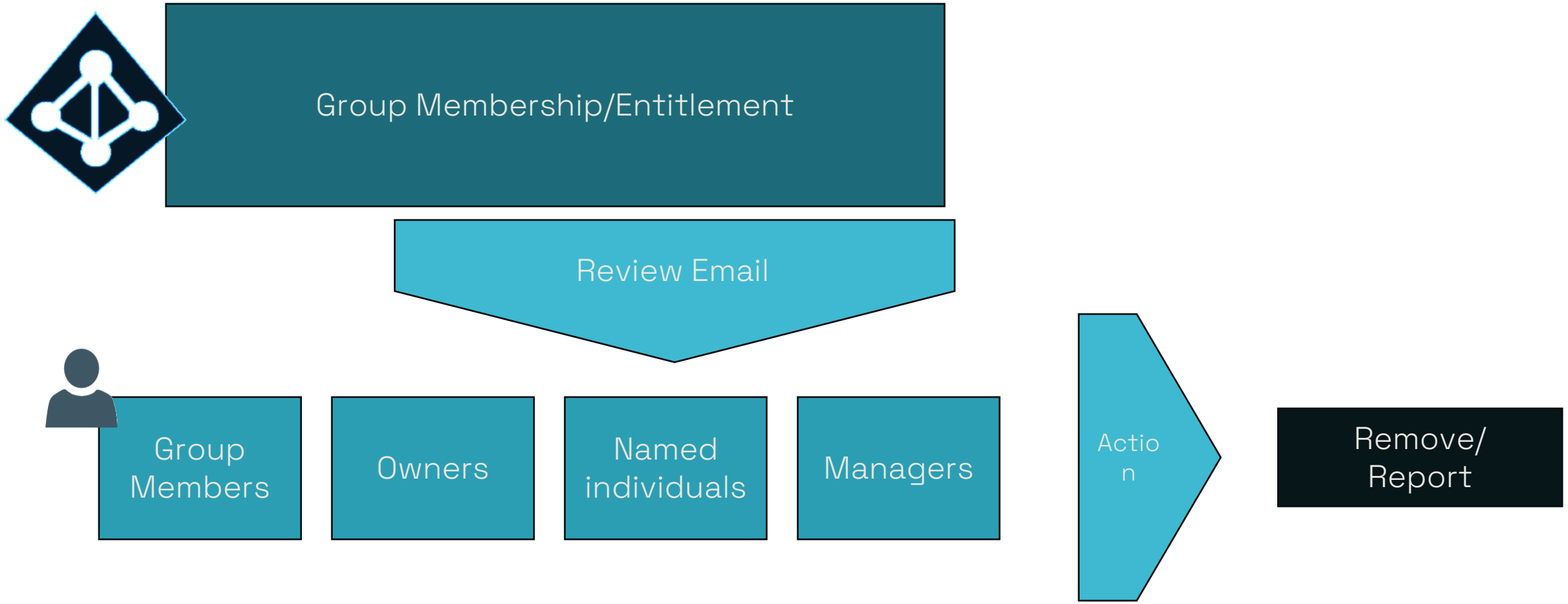
The Azure B2B Access Model

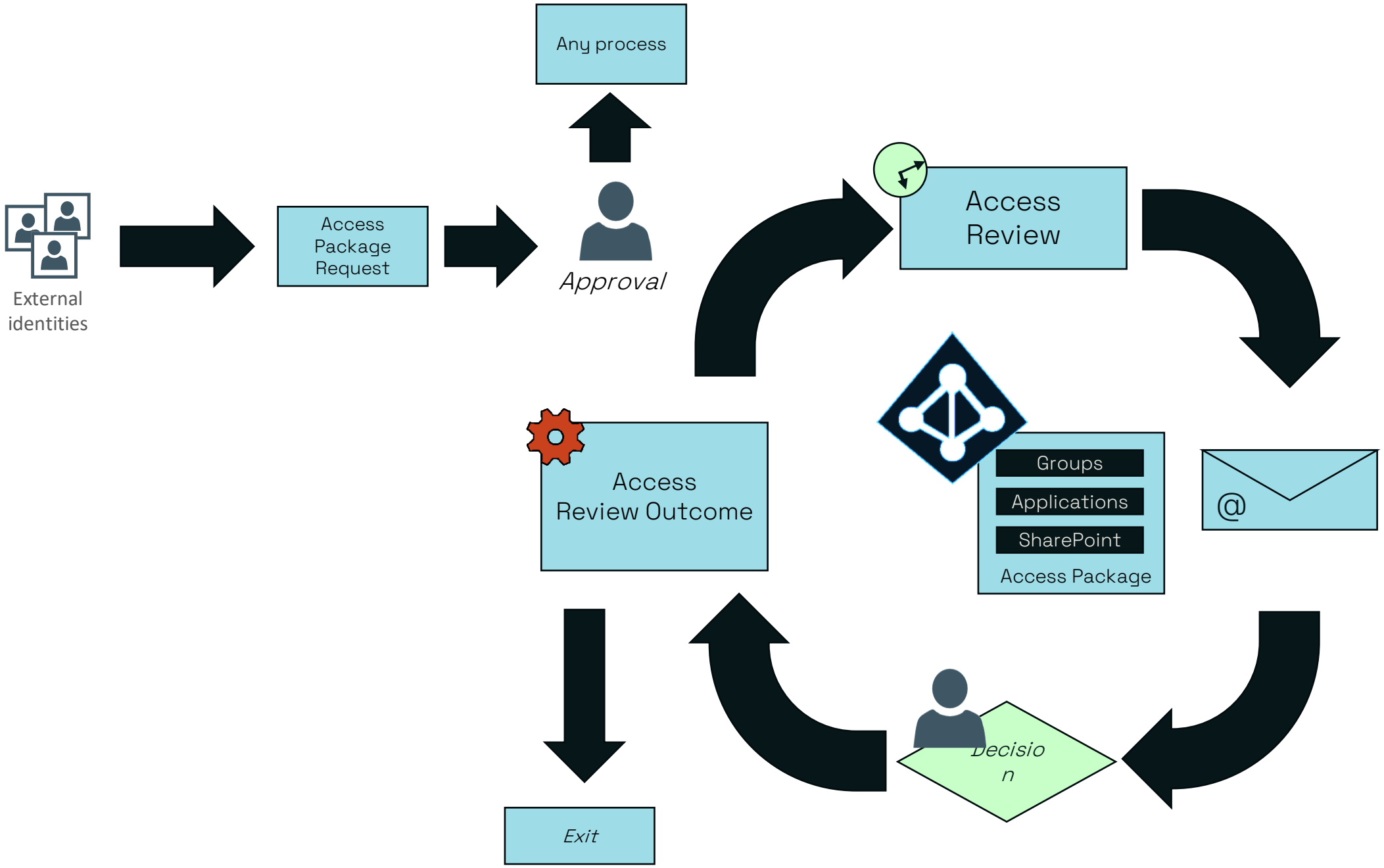


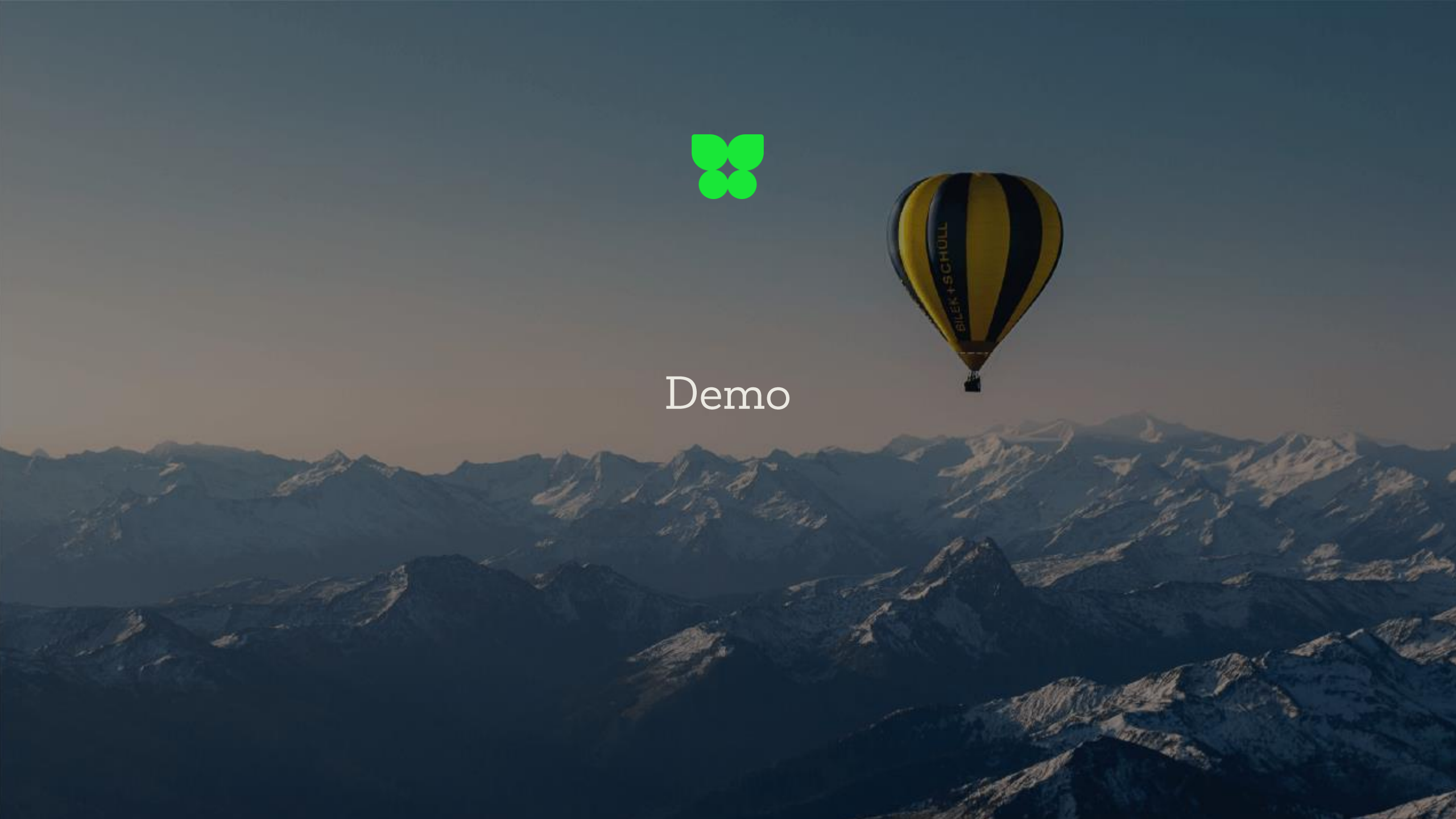
Access Packages



Access Reviews

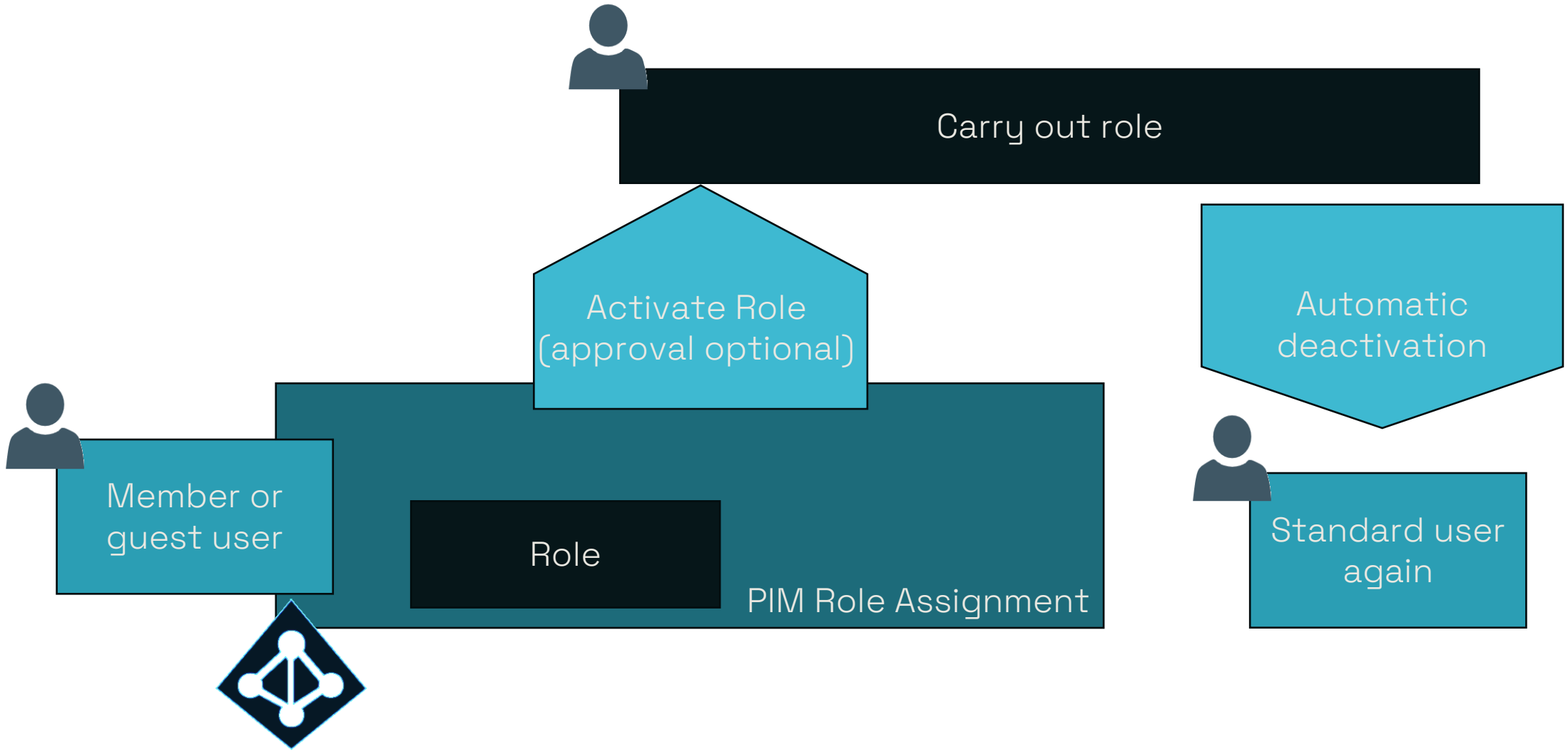



Any process
External identities
Access Package Request
Approval
Access Review
Access Review Outcome
Groups
Applications
SharePoint
Access Package
@
Decisio n
Exit



Demo

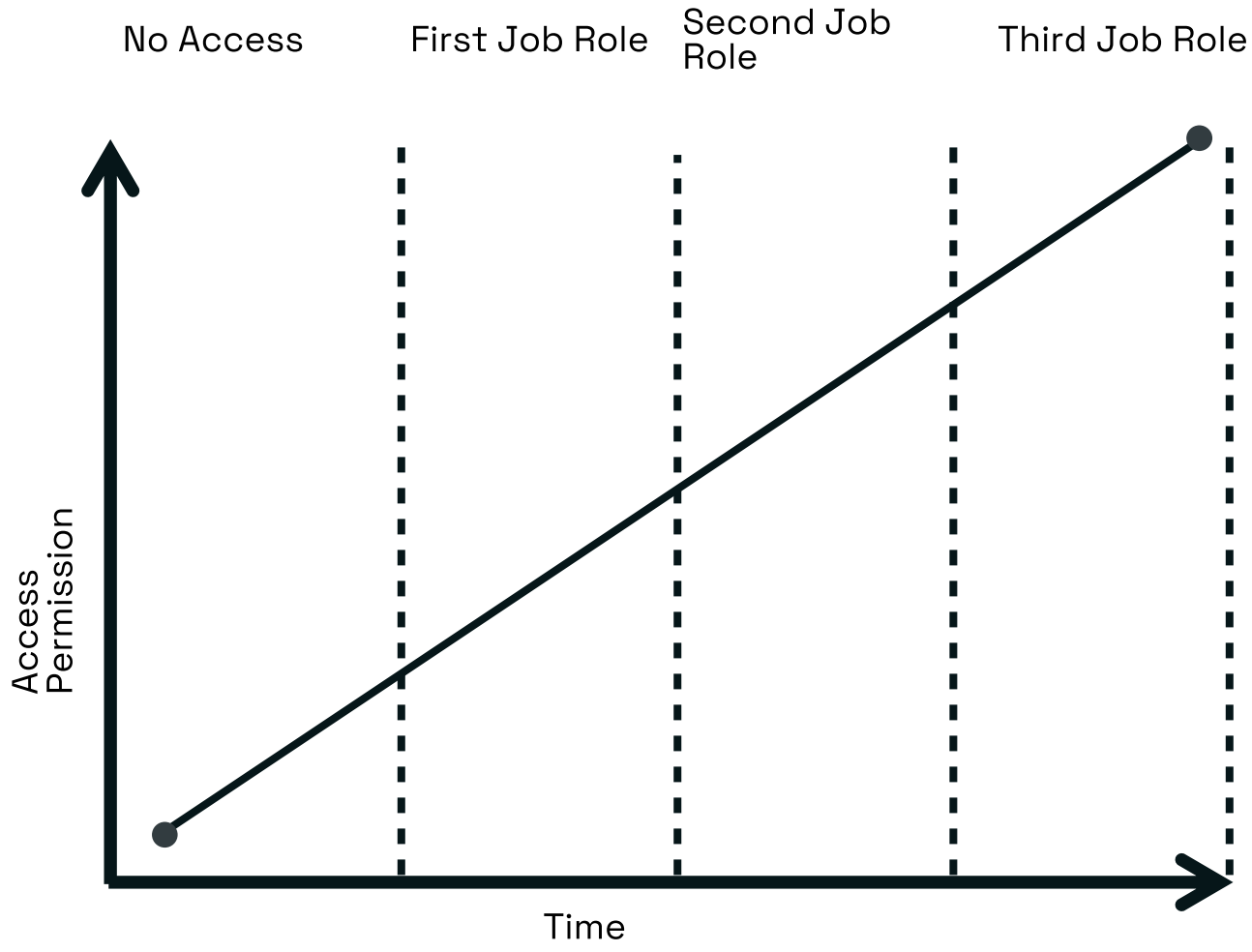
PIM


Carry out role
Activate Role
(approval optional)
Automatic
deactivation
Member or
guest user
Role
PIM Role Assignment
Standard user
again

Risk accumulates

Potential misuse of admin rights as access and responsibilities increases

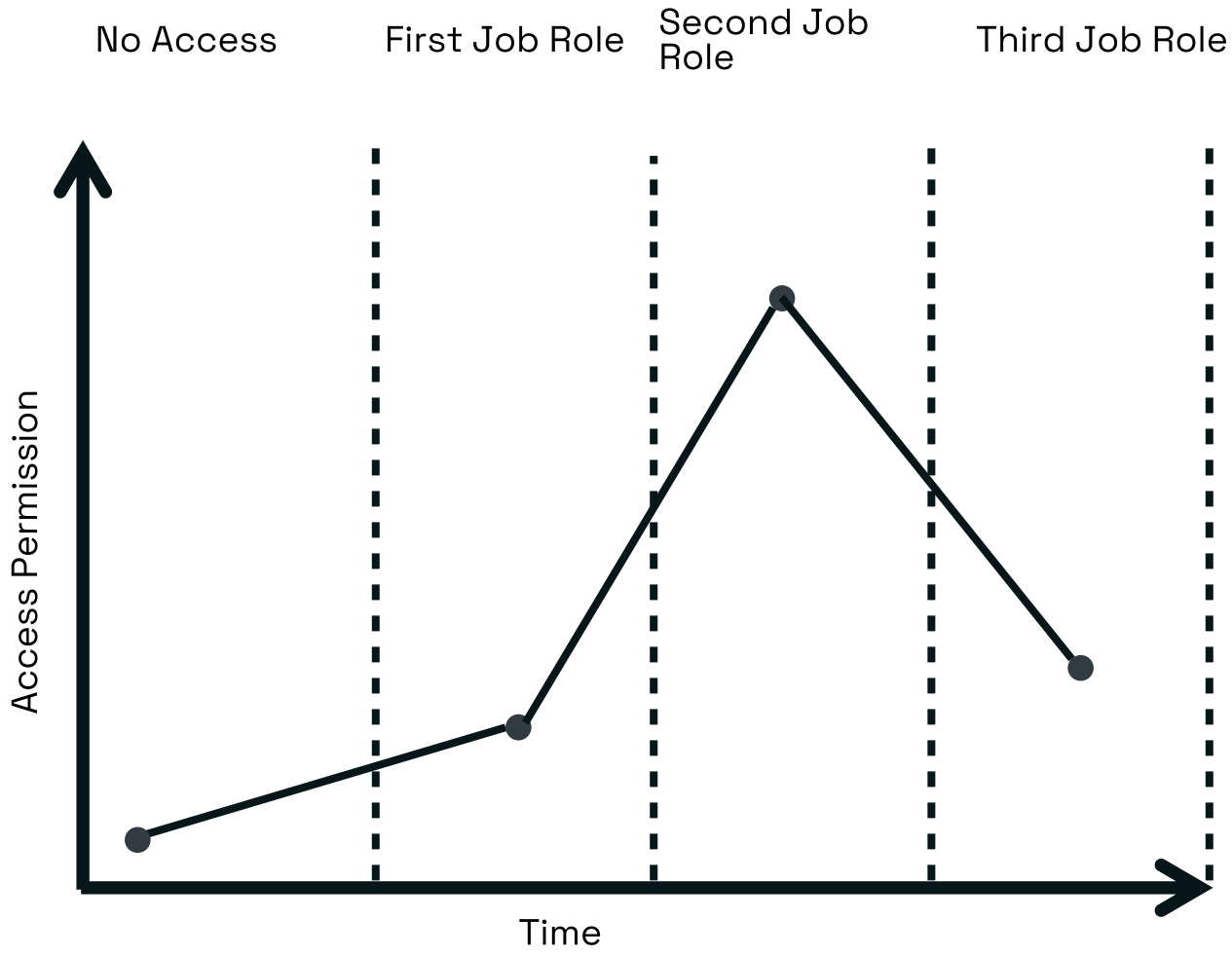
Access beyond what was initially provisioned for a user when that user's identity was created



Least privileged access

Manage access beyond what was initially provisioned for the user

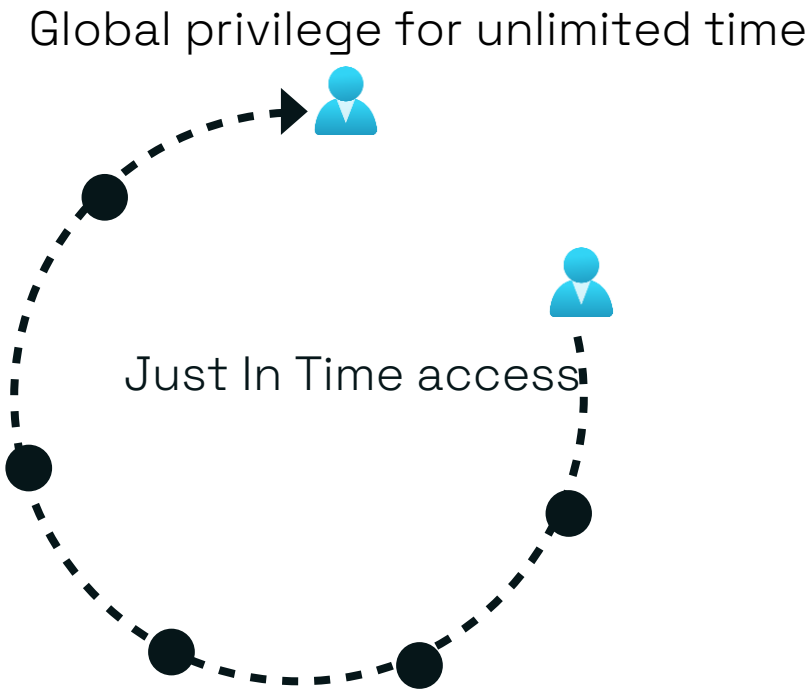
Reduce exposure to attacks while providing easy access when you need



Just-In Time privileged access

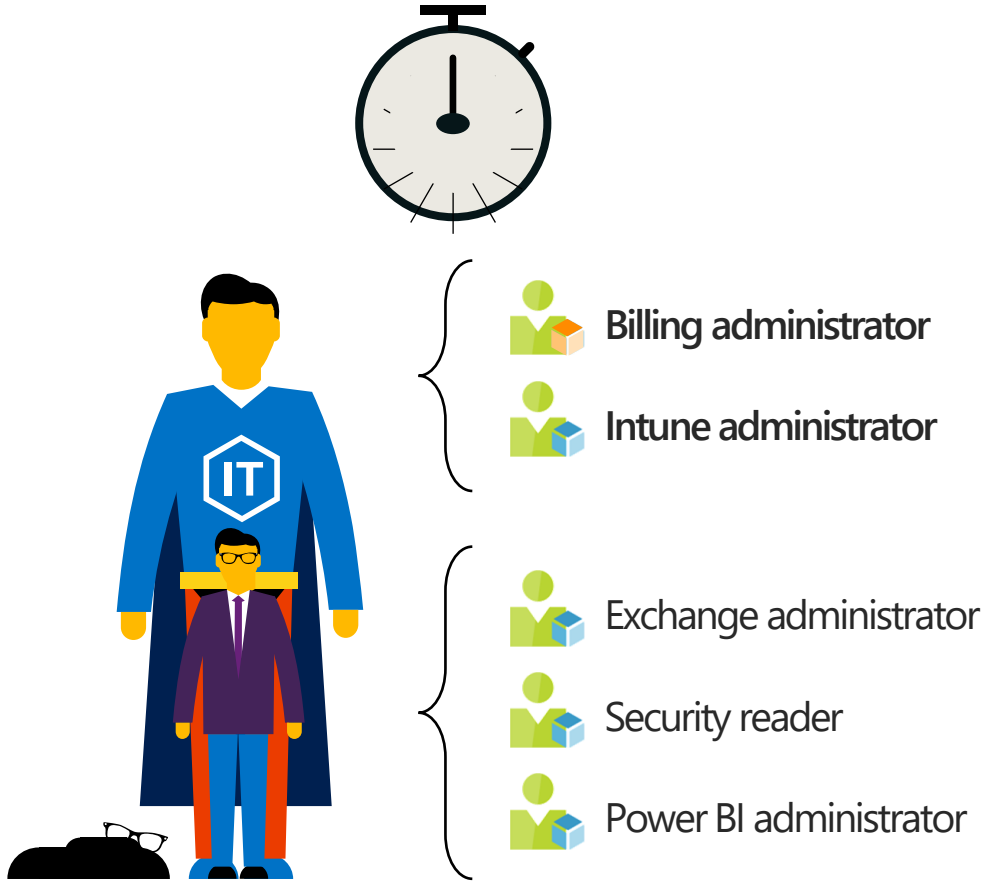
Remove unwanted standing access and reduce risk

- ✓ Reduce risk by reducing number of users with privileged roles
- ✓ Activate to just enough access (JEA) for just in time (JIT)

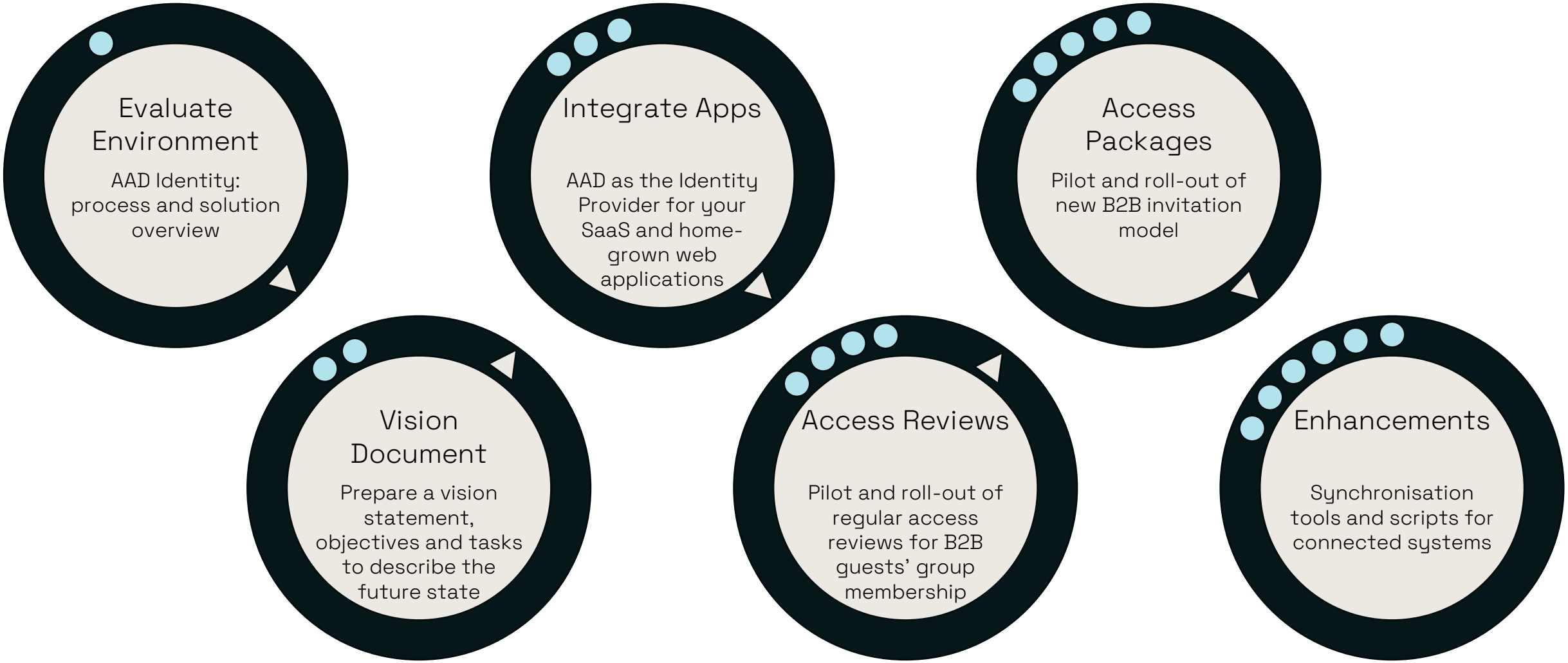


PIM – admin actions

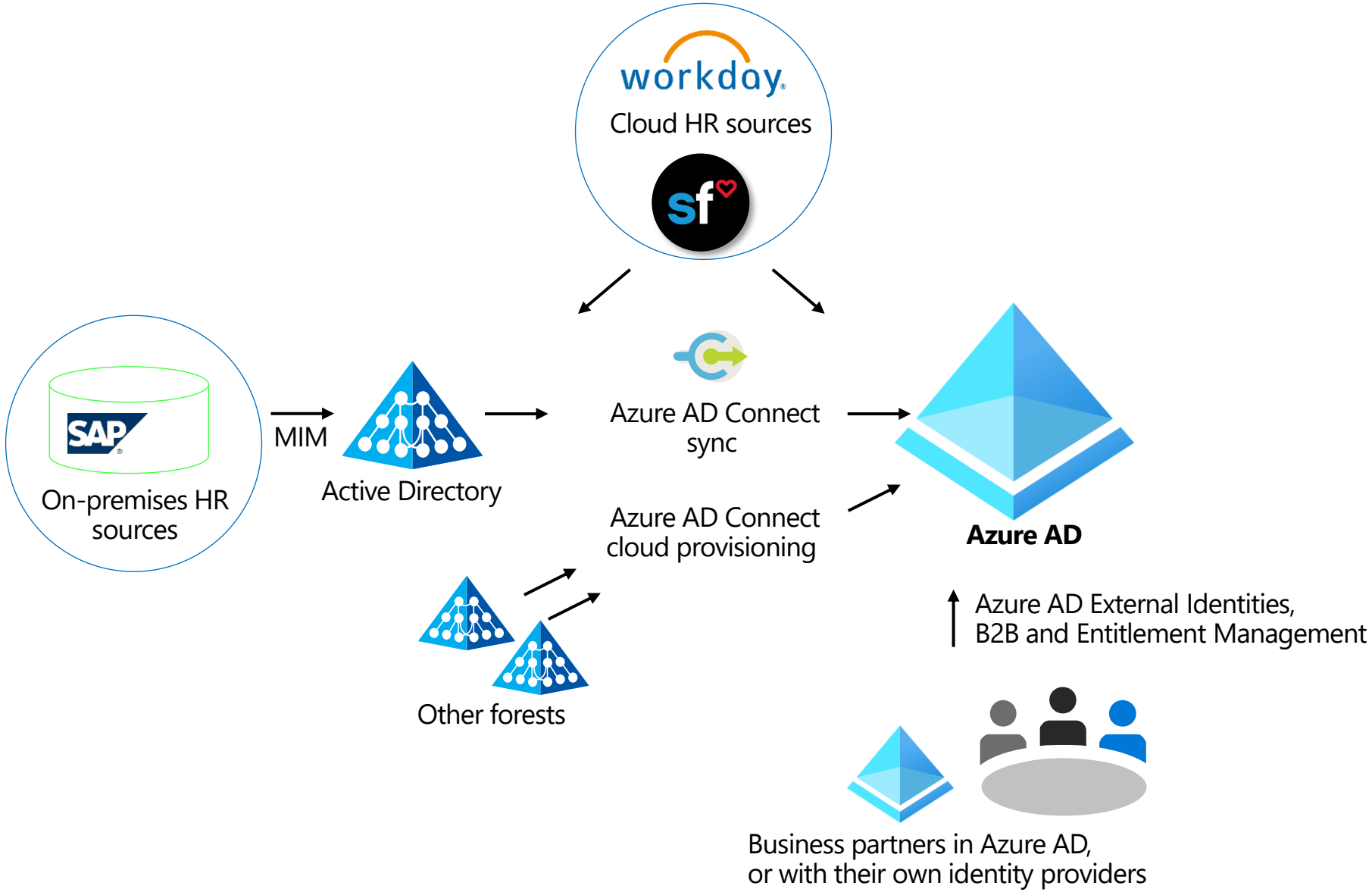
- View which users are assigned privileged roles
- Create access reviews for privileged roles
- Enable on-demand Just-in-Time & Just-Enough administrative access
- Set up approval flows for privilege activation
- Get alerts and view a history of administrator activation and actions
- Review administrative roles
- Requires users to provide justification to retain membership
- Manage built-in Azure Resource roles, as well as custom (RBAC) roles



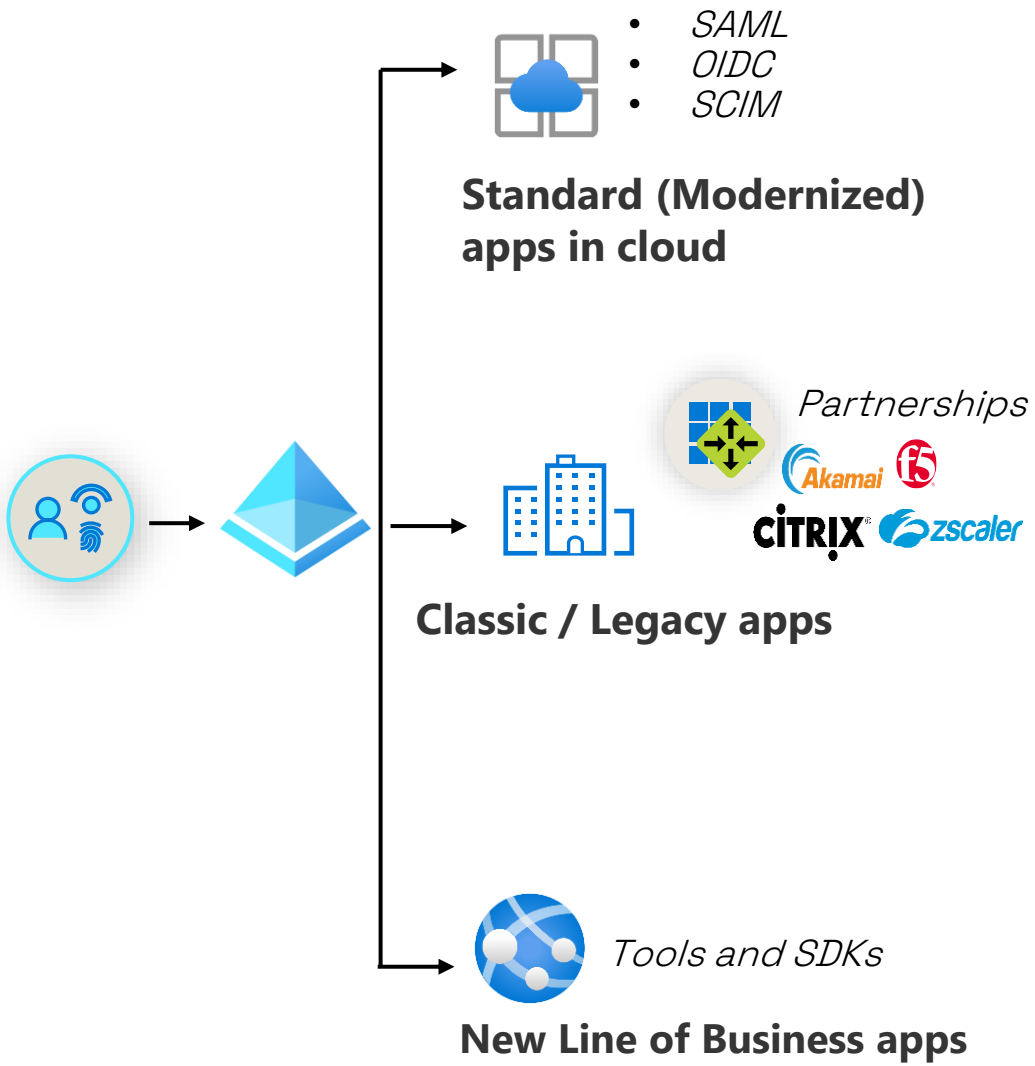
Cloud Identity Programme



Bring users into Azure Active Directory



Extend reach to any type of applications



Standards-based

- SaaS apps (Azure AD gallery)
- Apps in your organization
- Non-gallery apps

Classic/Legacy

- App Proxy access
- 3rd party integrations
- Shift to cloud (Azure AD DS)
- ADFS Migration toolkit

New Line of Business (LOB) apps

- Microsoft Identity Platform

Why Azure Identity Governance?

- Remove risk of accumulated access
- Remove risk of privileged access
- Rationalise users and groups
- Time-limited access
- Manage user lifecycles

Enterprises need a new way

MANAGE
Human and silicon identities

SECURE
Critical hybrid business and infrastructure assets

AUTOMATE
Costly & inefficient identity management processes

Saviynt is the catalyst

A single converged platform

Built for the Cloud – in the Cloud

Easy to implement. Fast to deploy.

Best-in-class enterprise solution

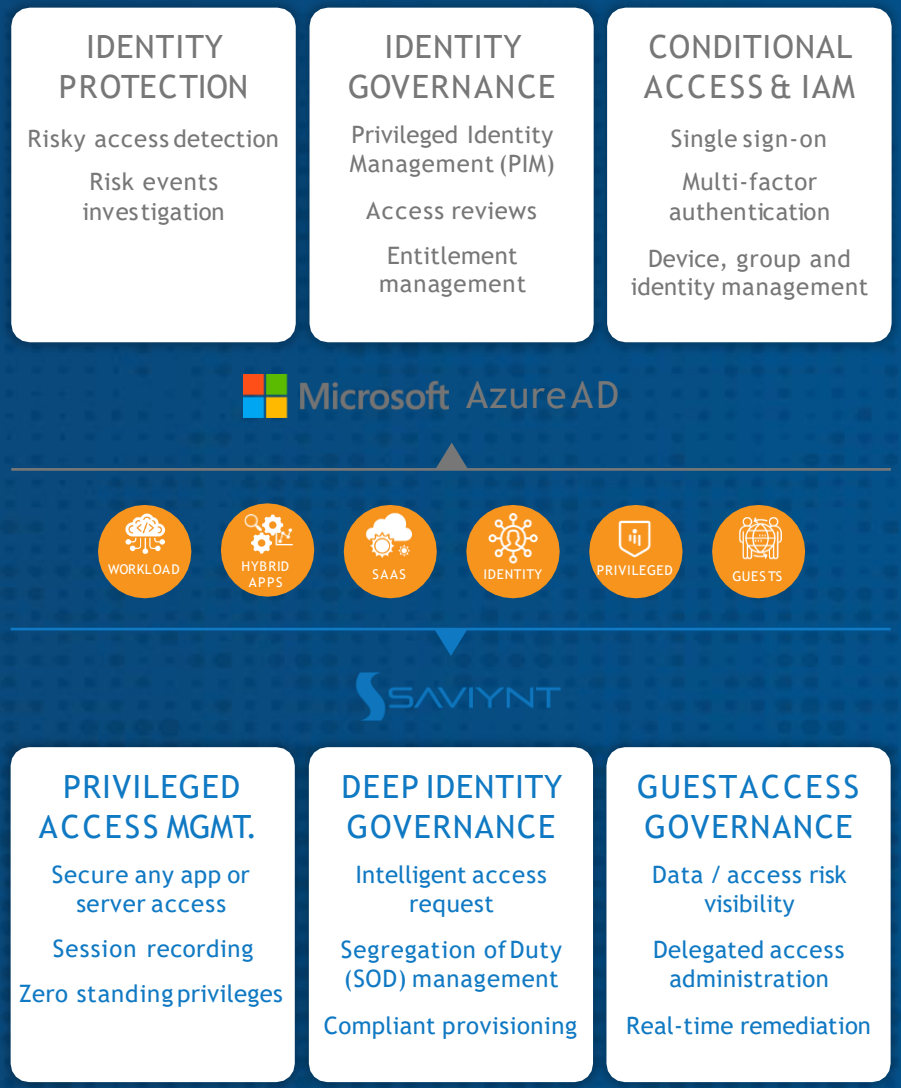
Saviynt Enterprise Identity Cloud

Any identity. Any app. Any cloud.

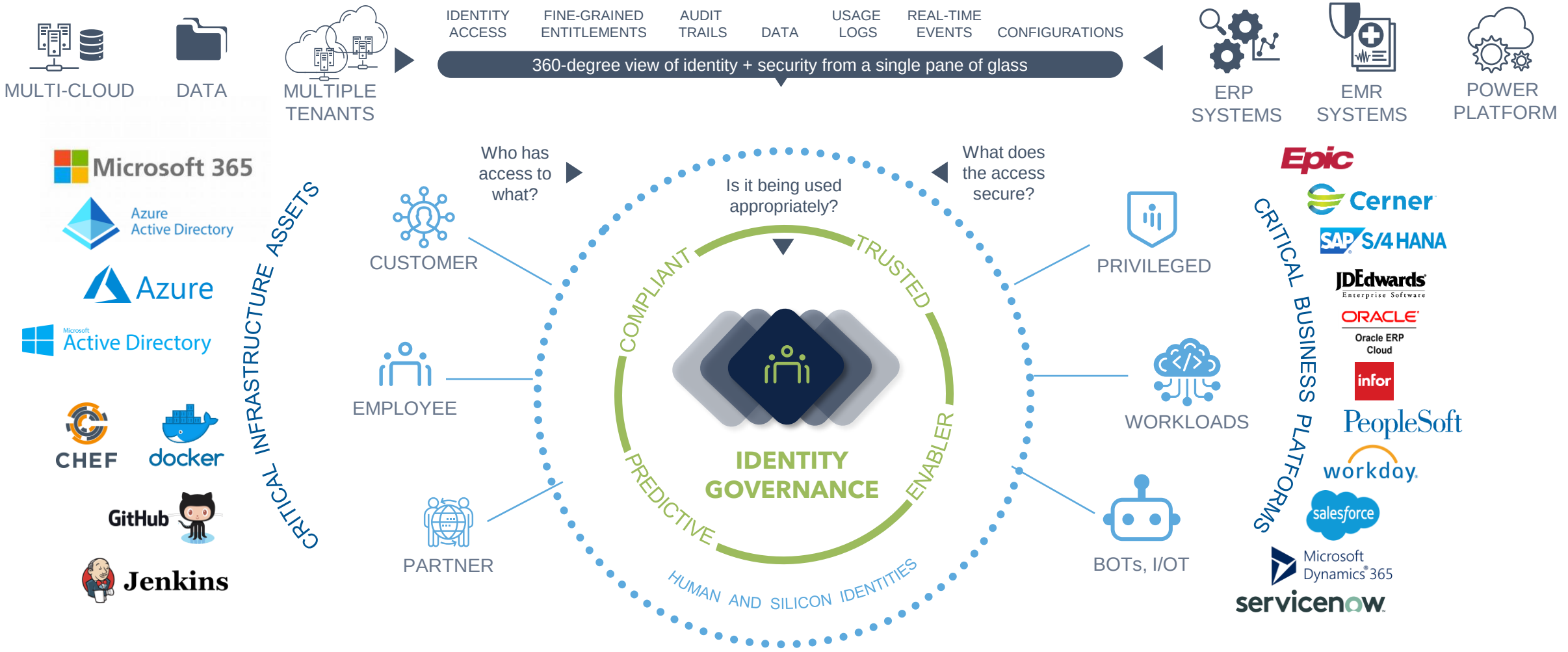
Better governance for the modern workplace

IDENTITY AND SECURITY SOLUTIONS FROM MICROSOFT AND SAVIYNT

- ZERO TRUST
- DYNAMIC RISK GOVERNANCE
- UNIFORM SECURITY & COMPLIANCE
- LOWER TCO WITH IDENTITY-AS-A-SERVICE
- FRICTIONLESS ACCESS MANAGEMENT



Governing the Hybrid Customers Enterprise

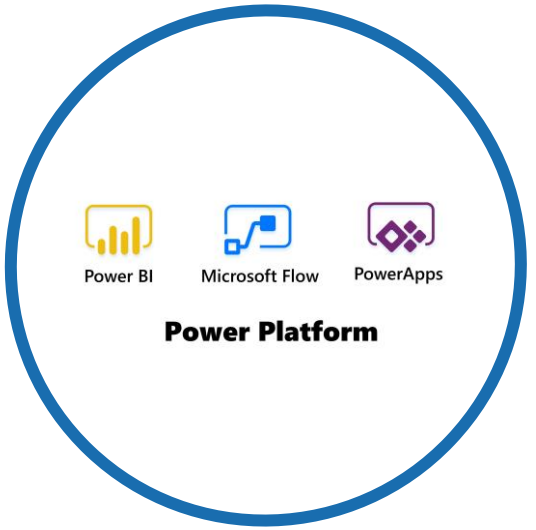


Extending Governance to Microsoft's Ecosystem

Where else is governance relevant and why?

- Continuous monitoring of Cloud Security and Operational Controls

- Securing Access to all M365 Applications
- Monitoring of shared data
- Visibility into who has access to resources

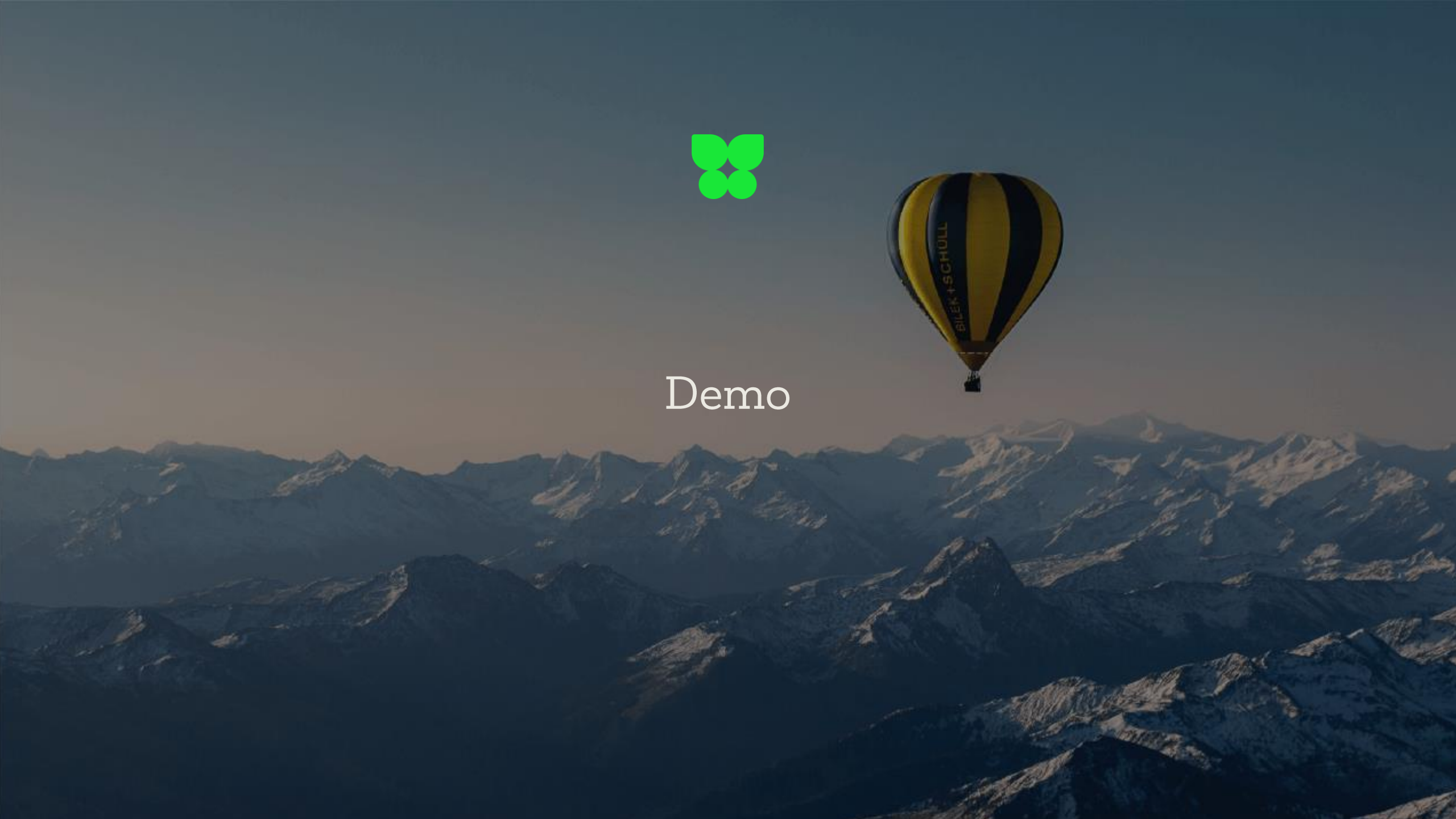


- Identity Management & Governance for custom Applications

- GRC Access Controls
- SoD Management and Mitigation

Microsoft Azure AD + Saviynt is a Complete Identity Offering

Azure AD + Saviynt	Microsoft	SAVIYNT
Single Sign-on	♦	
Conditional Access	♦	
Multi-Factor Authentication	♦	
Risk-based ID Protection	♦	
Self-Service Password Reset	♦	
Group Management	♦	✚
User Provisioning	♦	✚
Access Request	♦	✚
Workflow & Approvals	♦	✚
Compliance & Audit Reporting	♦	✚
Access Certification	♦	✚
Separation of Duties (SoD)	♦	✚
B2B Collaboration	♦	✚
Fine-Grained Entitlements		♦
Actionable Compliance Controls		♦
Entitlement and Access Risk		♦
Continuous Monitoring & Enforcement		♦



Demo

Thank you

hello@kocho.co.uk

0800 044 5009