Kill your IAM system now!
Entra ID is here

Marcel Zehner | SoftwareOne
Microsoft Cloud Architect
marcel.zehner@softwareone.com

About Marcel

- *Microsoft Cloud Architect at SoftwareOne*
- *Switzerland-based*
- *Microsoft Regional Director*
- *Microsoft Most Valuable Professional*
- *Tech Enthusiast*
- *Poker Player*
- *Piano Virtuoso*

Agenda

Agenda

- A Selection of today's IAM Challenges
- Identity Provisioning
- Access Management
- Workflow Automation
  - For Identity & Access Management

A Selection of today's IAM Challenges

Identity Challenges

- Identities can live in various places
- Platforms and applications are siloed
- Leads to complex identity processes, provisioning and management
- Complex identity protection when distributed across platforms & apps
- No centralized identity monitoring

Access Management Challenges

- Dynamic permissions requirements
  - Role changes, temporary project work etc.
- Self-service to support the business quickly
- Review access and remove if not needed anymore
- Many IAM tools & teams are slow when it comes to new requirements
- If IAM tool is compromised,

IAM Tool & Team Challenges

- IAM teams are decoupled from Microsoft identity (ADDS & Entra ID) teams
- New requirements take too long to implement
- Teams don't have up-to-date knowledge & mindsets
- IAM tools might not be part of the company's modern PAM strategy
- If IAM tool is compromised, all environments could be too – plan carefully!

Guess what?

Microsoft Entra ID addresses most of these challenges perfectly!

Identity Management

Identity Types (Microsoft perspective)

- Microsoft cloud-only (Entra ID)
- Microsoft on-premises-only (ADDS)
- Microsoft Hybrid
  - Created as on-premises identities
    - ADDS is the master
  - Synced to Entra ID
- 3rd party applications

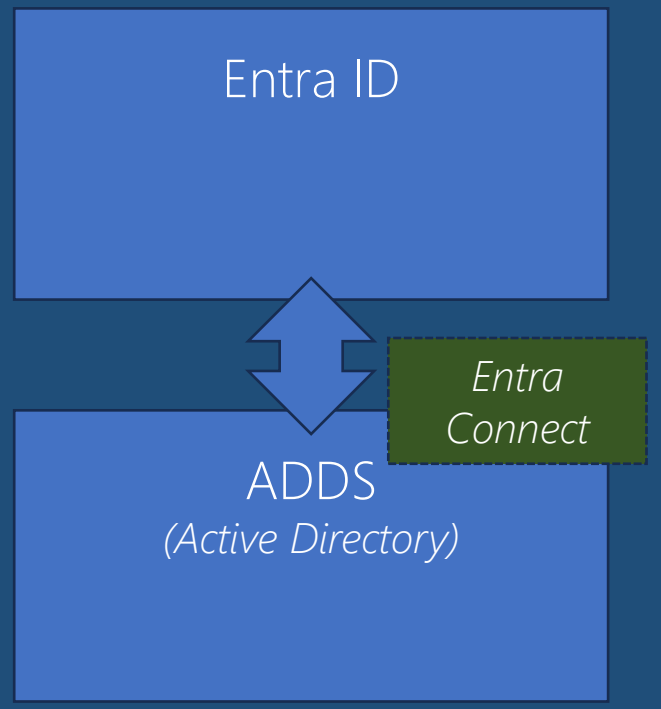
Identity Provisioning Protocols

- Directory Synchronization
- SCIM Provisioning
  - Inbound
  - Outbound

Directory Synchronization

- Entra Connect or Cloud Sync
- Synchronization of identities between ADDS and Entra ID
  - Object filtering
    - Only needed
  - Selective attributes

Directory Synchronization



SCIM Provisioning

- System for cross-domain identity management (SCIM)
- Exchange of identity information between systems
  - REST API with “Users” & “Groups” Endpoints
  - Create, update & delete objects
- Open standard
  - No individual APIs for various platforms
  - Same property names & IDs for everything
- Entra ID fully supports SCIM

Inbound SCIM Provisioning

- Provisioning inbound to the Microsoft Identity Providers
  - Microsoft Entra ID
  - Microsoft Active Directory Domain Services (ADDS)
  - Both

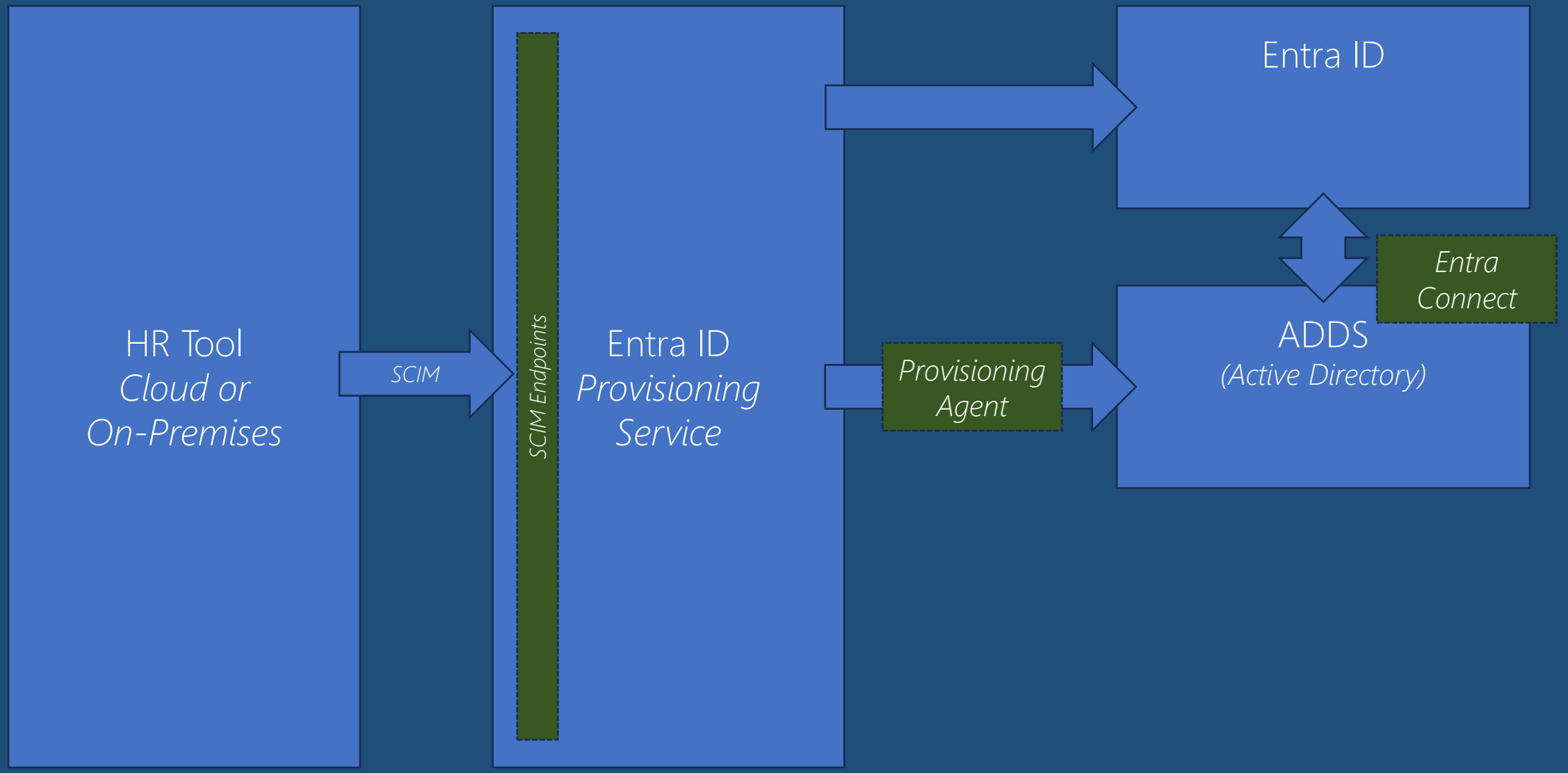
Inbound SCIM Provisioning

- Entra ID Provisioning Service API
  - Endpoints for users and groups
- Accepts creation, modification and/or deletion
- Flexible property mapping SCIM-EID
  - Hierarchical model
  - Direct, static or expression
  - Sync always or one-time

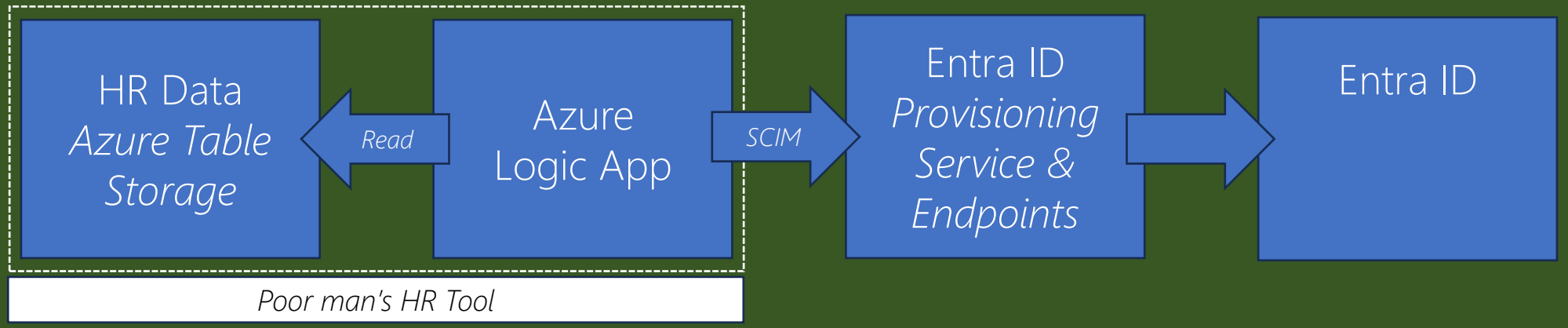
Inbound SCIM Provisioning

- When provisioning to ADDS
  - Needs Entra Cloud Sync provisioning agent
    - One or multiple agents (redundancy)
  - Executes identity creation against ADDS

Inbound SCIM Provisioning



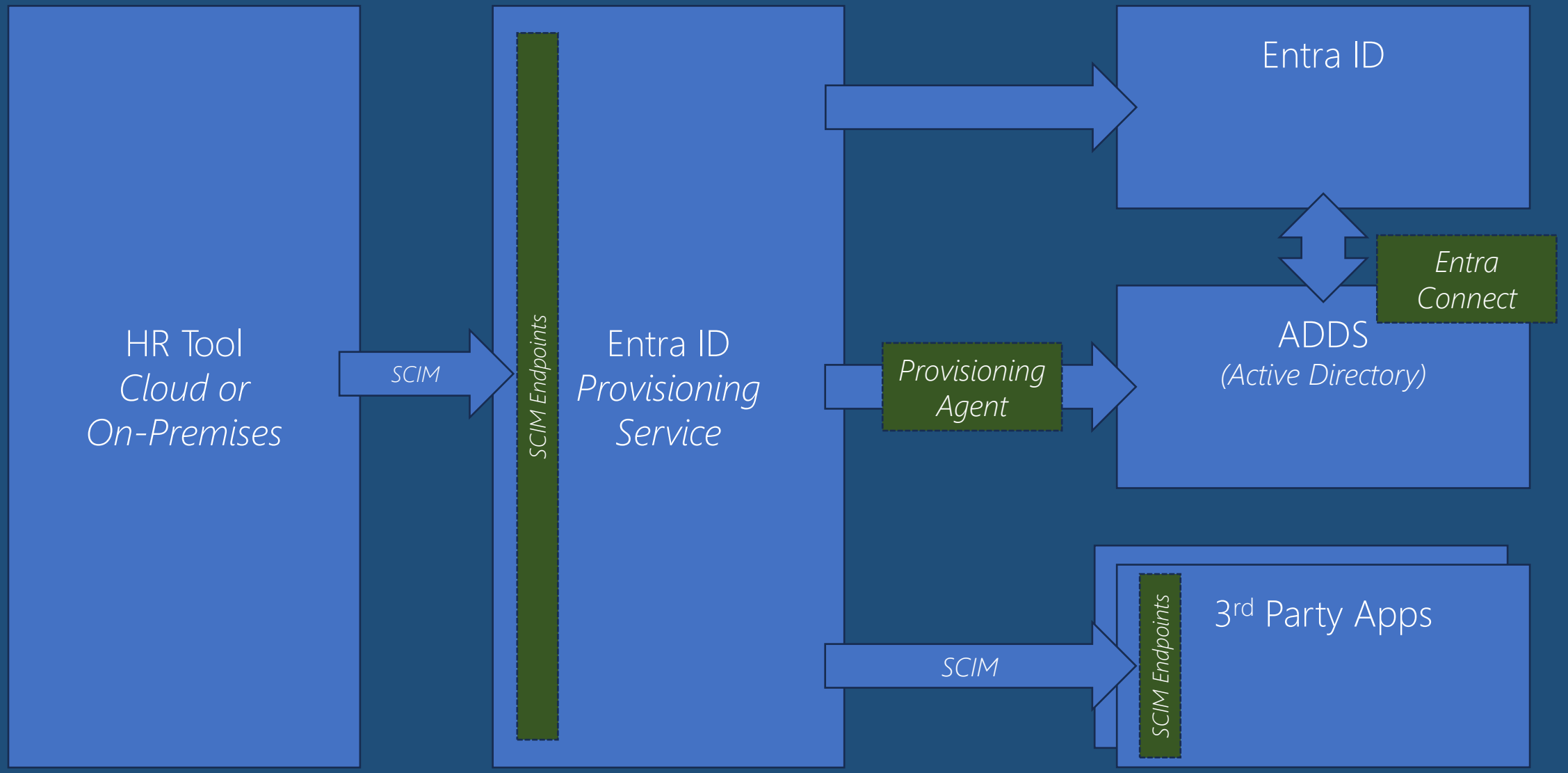
Demo 1: SCIM Inbound Provisioning



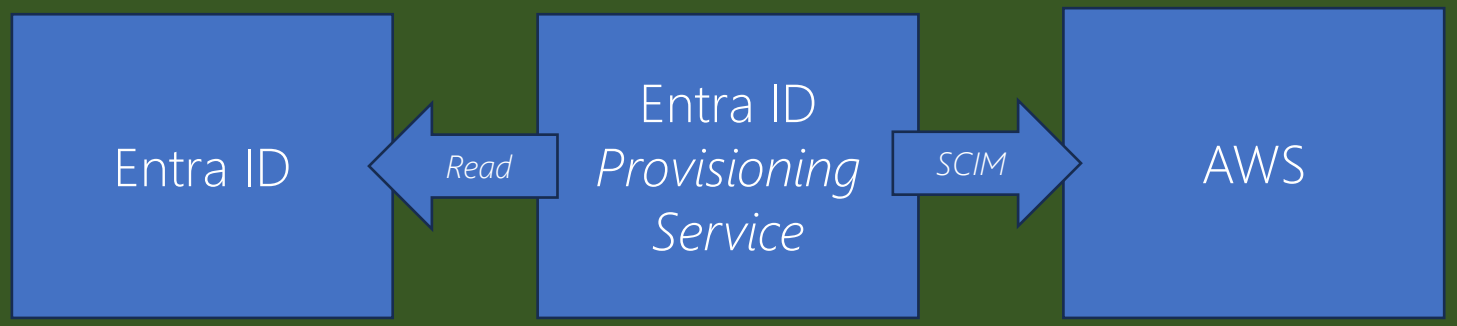
Outbound SCIM Provisioning

- Integrate app in Entra ID
  - E.g. a SaaS app
- Use SCIM provisioning to provision users and groups in 3rd party Apps
  - Automatic (40 minutes interval)
  - Manually triggered
- Outbound property mapping

Outbound SCIM Provisioning



Demo 2: SCIM Outbound Provisioning



Access Management

(Entra ID Identity Governance)

Access Packages

- Collection of permissions
- Contains one or multiple resources
  - Team, SharePoint Site, Entra ID Group etc.
- Can be assigned to users
  - Manually by admins
  - Dynamically based on user properties
    - E.g. department
  - By using self-service
  - Mix of multiple options is possible

Access Package Policies

- Defines assignment process
  - Who can request it?
    - Internal users
    - Guest users
    - No self-service (only admin assignment)
  - Approval needed? Up to three stages
  - What information to collect from requestor?
  - Expiration of assignment

Access Reviews

- Access reviews for assigned access packages
- Analyze what permissions are actively used
  - Recurring
  - Decide based on recommendations

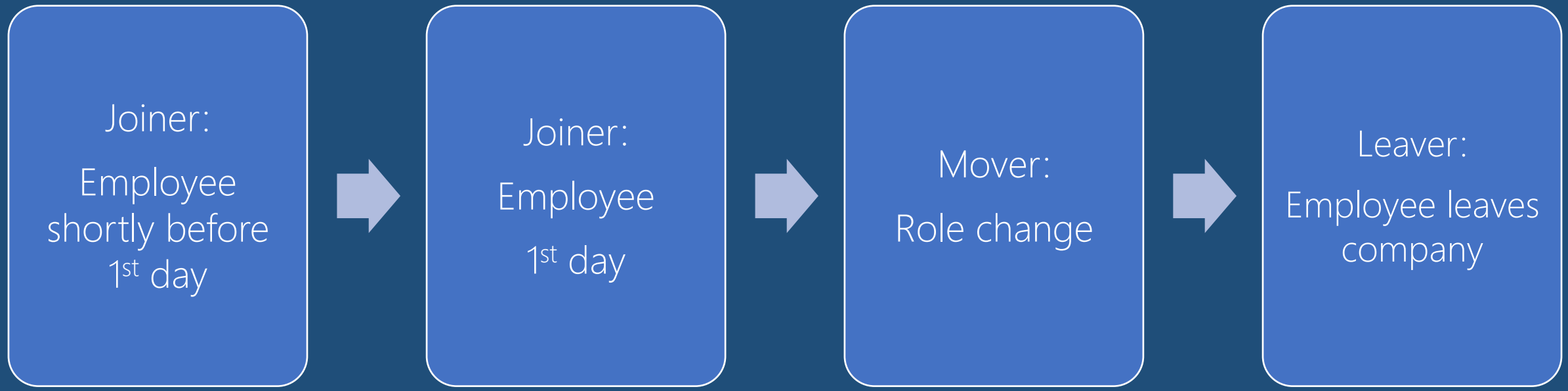
Demo 3:
Access Packages

Workflow Automation

(Entra ID Identity Governance)

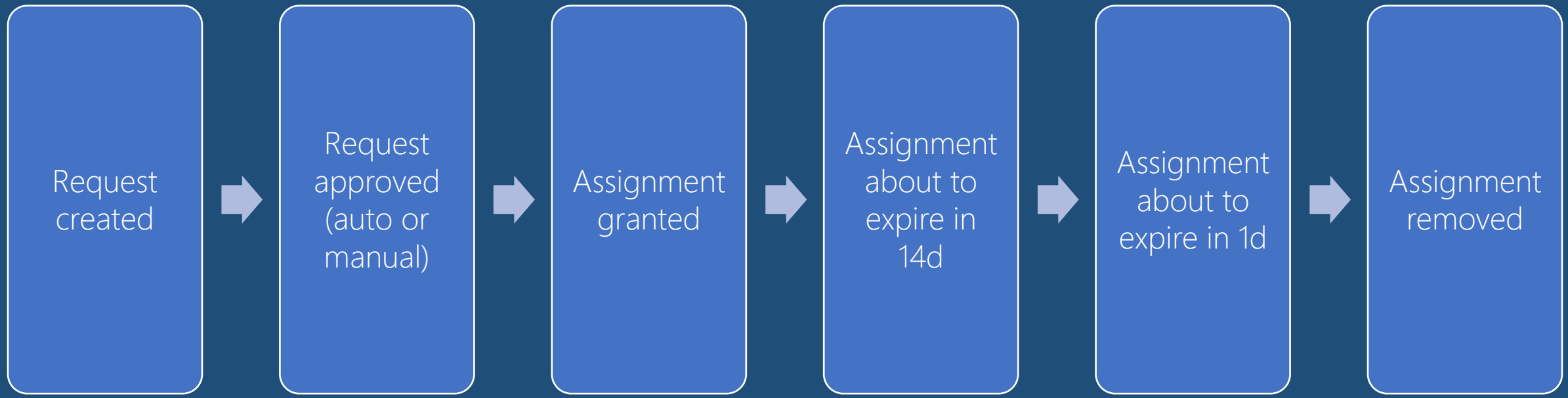
Identity Stages

- Can be used to trigger automated identity workflows
- Alternative: Trigger manually when needed



Access Package Stages

- Can be used to trigger automated workflows
- Alternative: Trigger manually when needed



Workflows Tasks

- Workflows are built with tasks
- Bulit-in Tasks (examples)
  - Enable/Disable Account
  - Create TAP
  - Send Email
- Custom Tasks (to do anything)
  - Azure Logic Apps

Demo 4: Workflows

Recap

Recap

- Entra ID comes with vast
  - Rethink concepts from the past
  - Use modern tools that are around anyway (Entra ID)
  - Remove silos and centralize IAM
- Invest some time to dig deeper, there is a lot more to discover!

Thanks to the Sponsors!

Kill your IAM system now!
Entra ID is here

Marcel Zehner | SoftwareOne
Microsoft Cloud Architect
marcel.zehner@softwareone.com