Visit us at #7-408

Least Privilege – und wie wird man Berechtigungen wieder los?

Dr. Stephan Hausmann

Visit us at #7-408

ONE IDENTITY by Quest

Least Privilege Principle

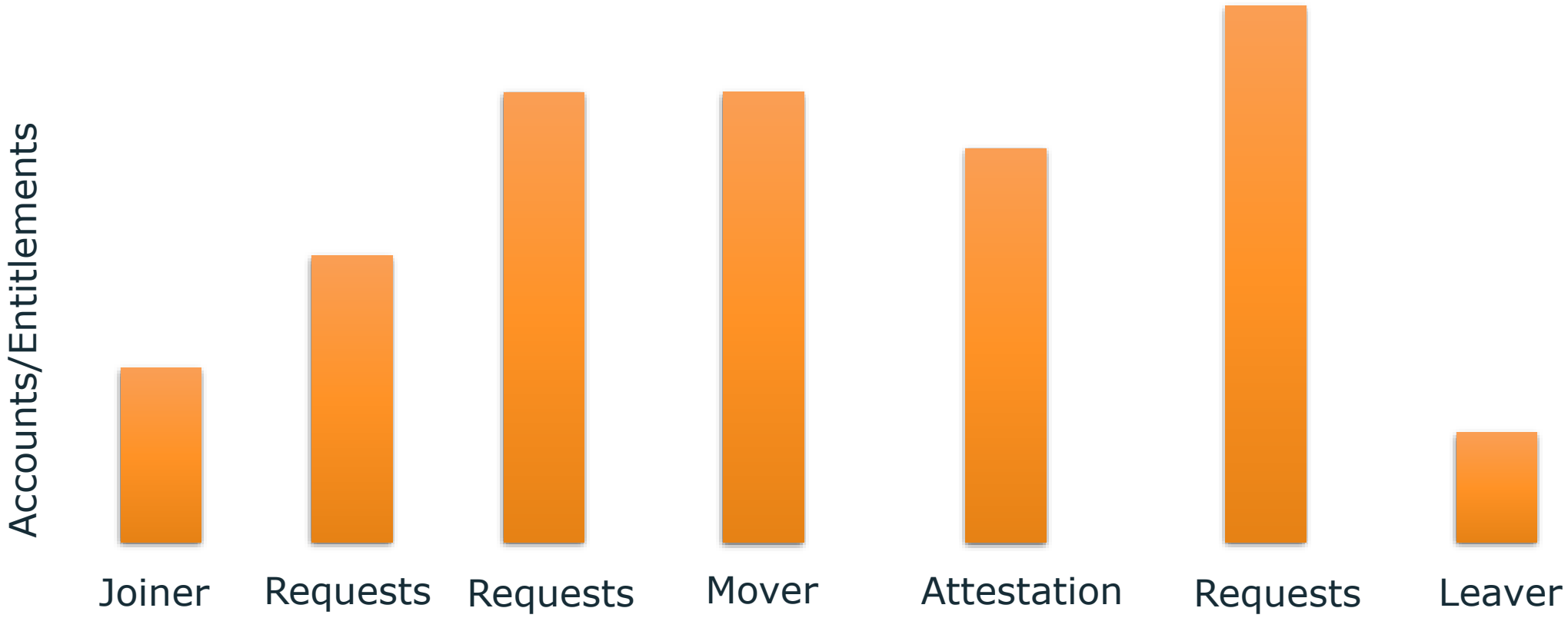
The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

https://csrc.nist.gov/glossary/term/least_privilege

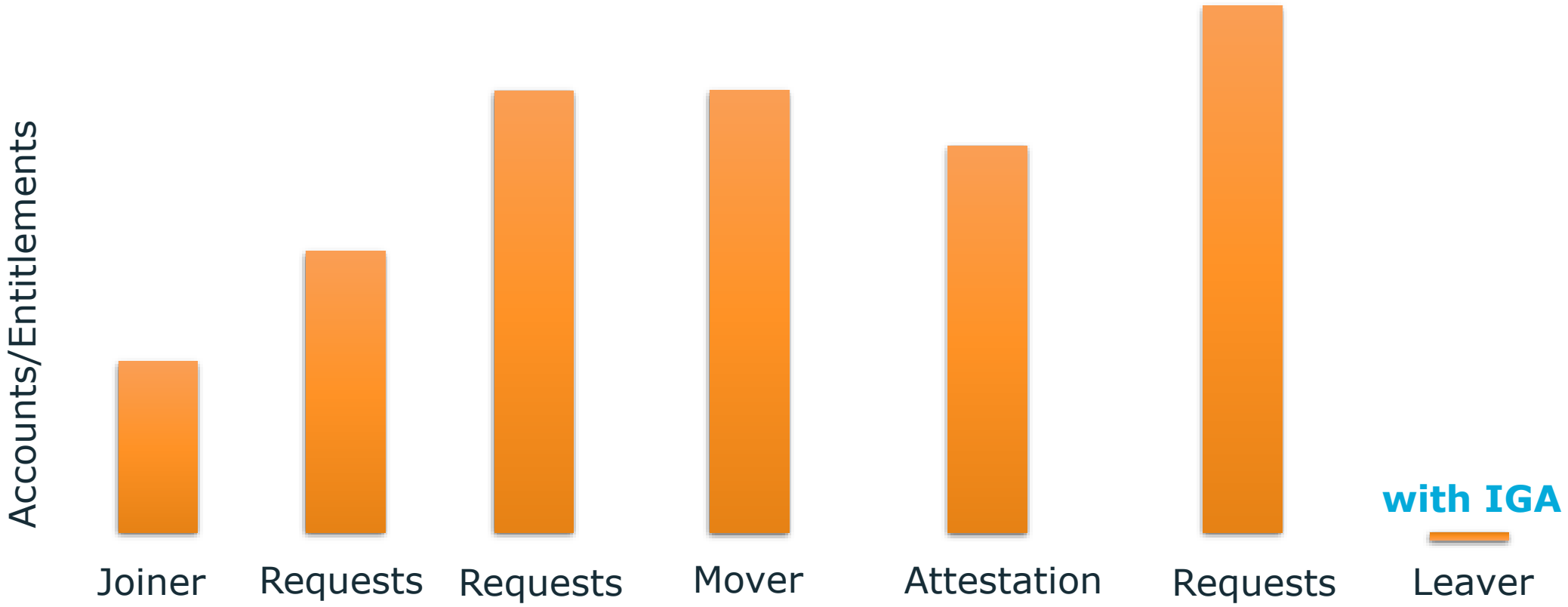
Why Least Privilege?

- Identity Security
  - Reduce the attack surface by revoking unnecessary access
  - Prevent lateral movement
- License cost
  - Remove accounts/entitlements that are not used

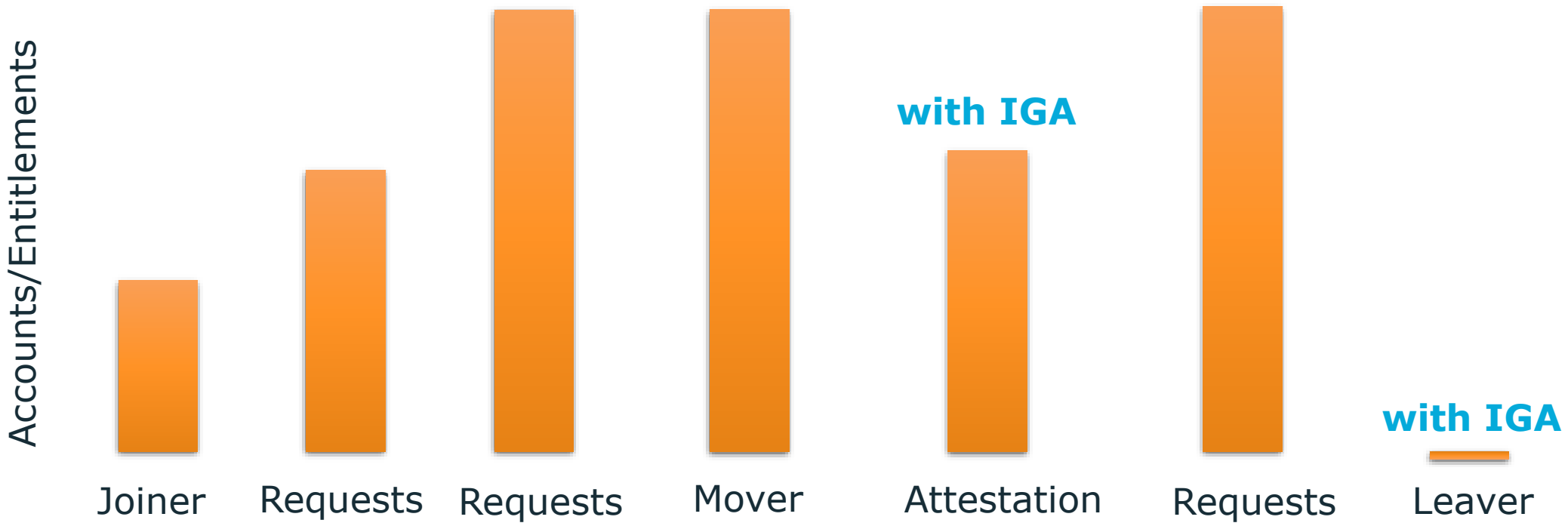
Lifecycle of an Identity



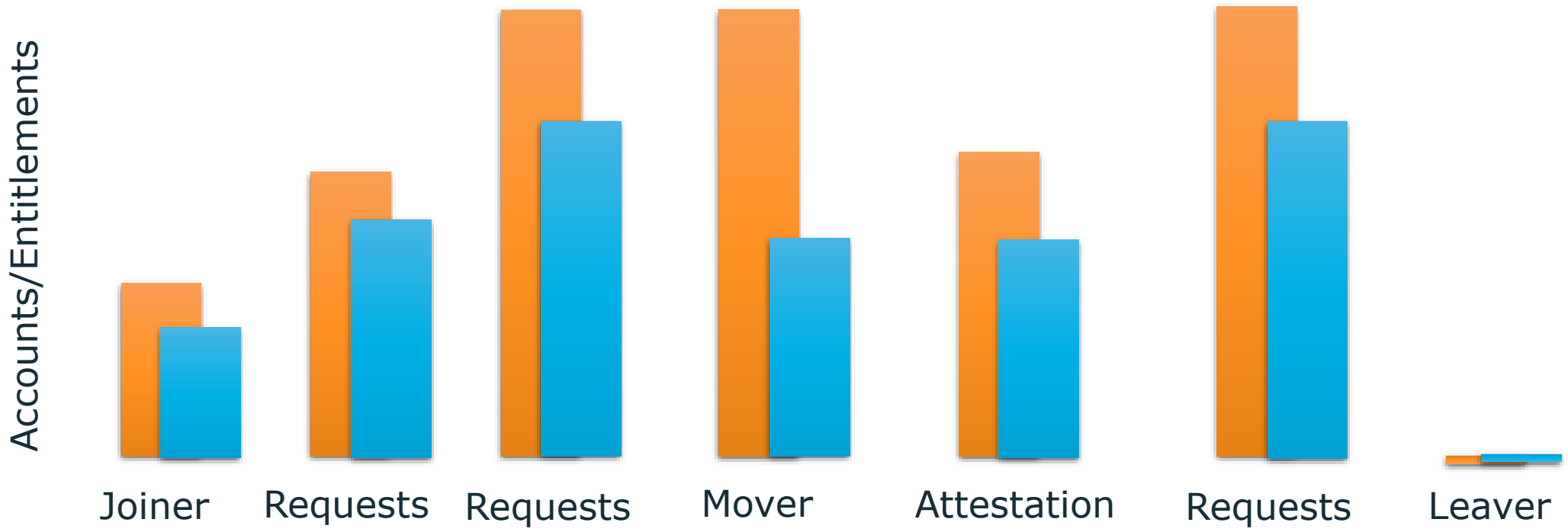
Lifecycle of an Identity



Lifecycle of an Identity



Lifecycle of an Identity – what is really needed?



ONE IDENTITY by Quest

Traditional IGA & Access Management

IGA

Governs Access

Access Management

Controls Access to Applications

The Observability Gap

IGA and Access Management are siloed

The IGA tool that controls the accounts and entitlements does not have visibility of the activity associated with that access which could support governance decisions.

Behavior Driven Governance

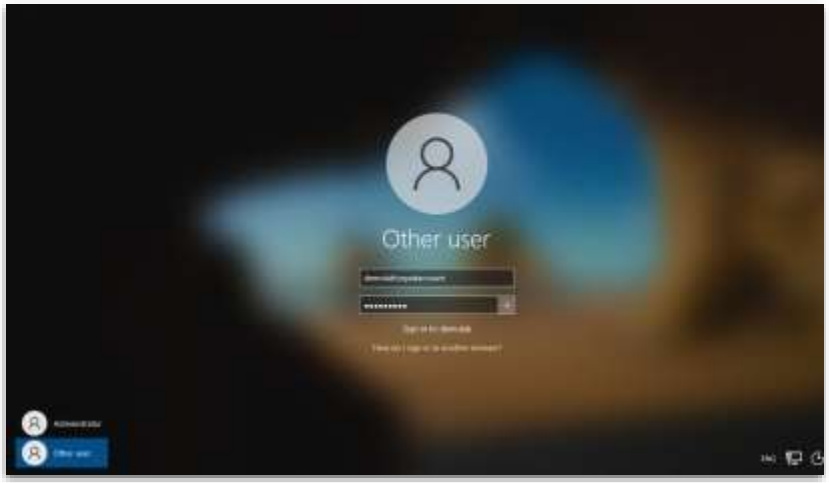
Using access insights to support governance decisions in IGA

What information is available?

- Last Login of accounts
- IdP/SSO logs/events
- Application logs/events

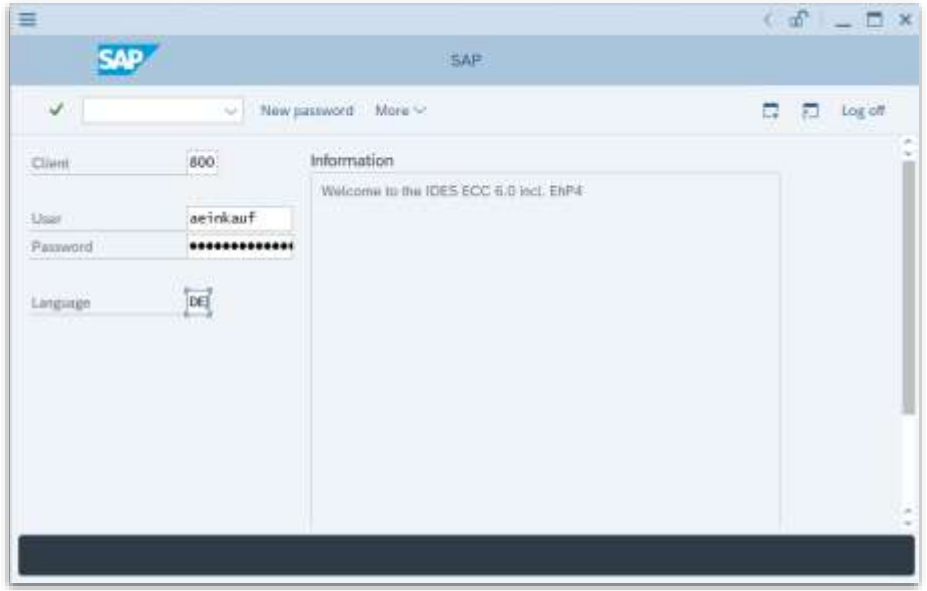
Last Login - Directory

- Active Directory, LDAP, …
- Directories are in general used by many applications
- When the Last Login is long ago
  - information reveals more likely a Leaver or a forgotten technical account



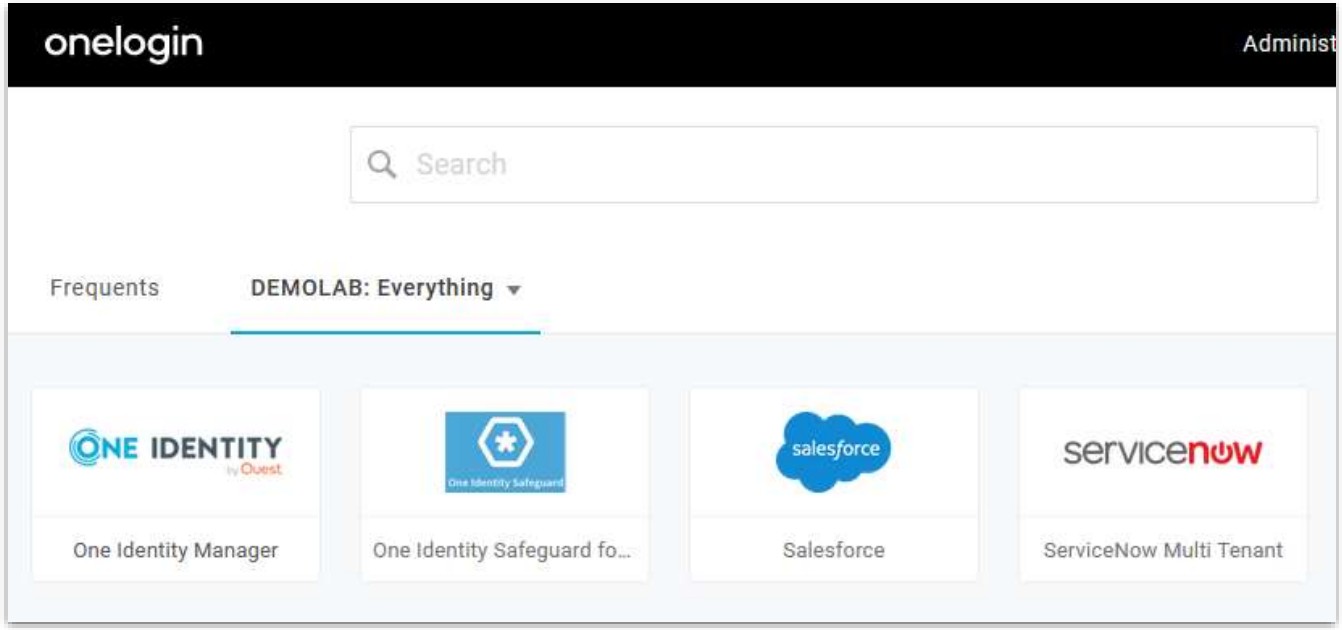
Last Login – Dedicated application

- Application with its own user store
  E.g. SAP, Safeguard, …
- When the Last Login is long ago
  - Application is unused
  - Account might be removed
- If the identity has more than one unused account this might show a Mover



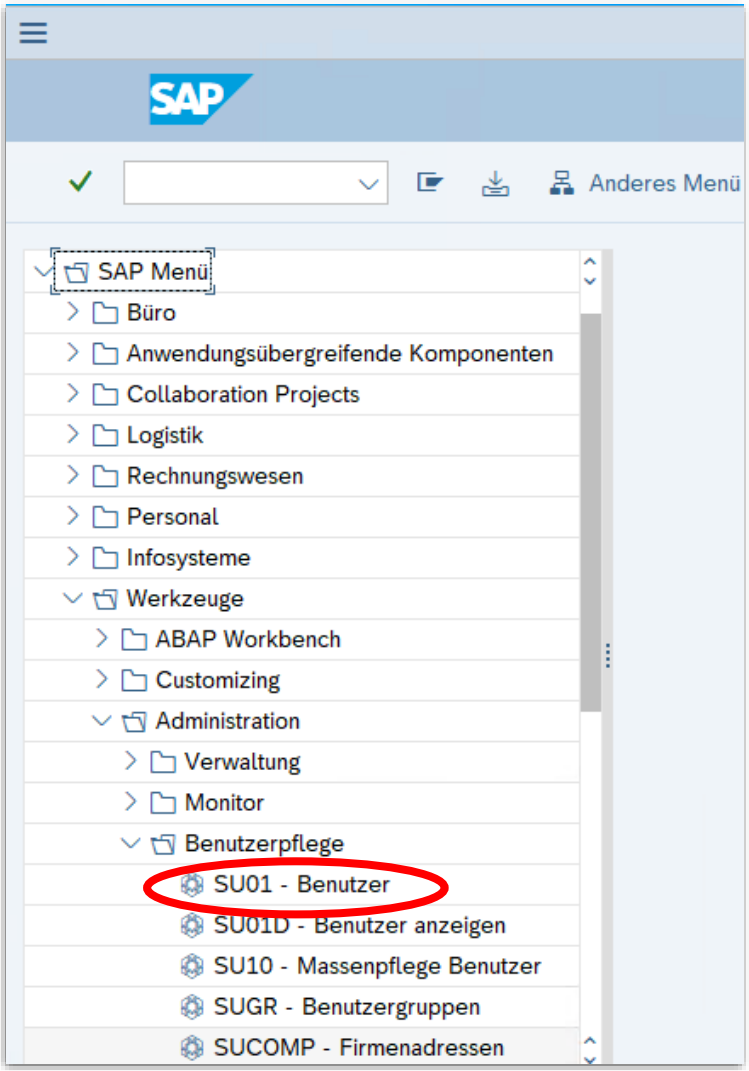
IdP/SSO

- Last Login – same as for directory
- Insight for application access
  - last access
  - frequency of application usage



Application

- Application logs allow to identify which actions have been done by a user
- Correlation between action and entitlement needs to be available



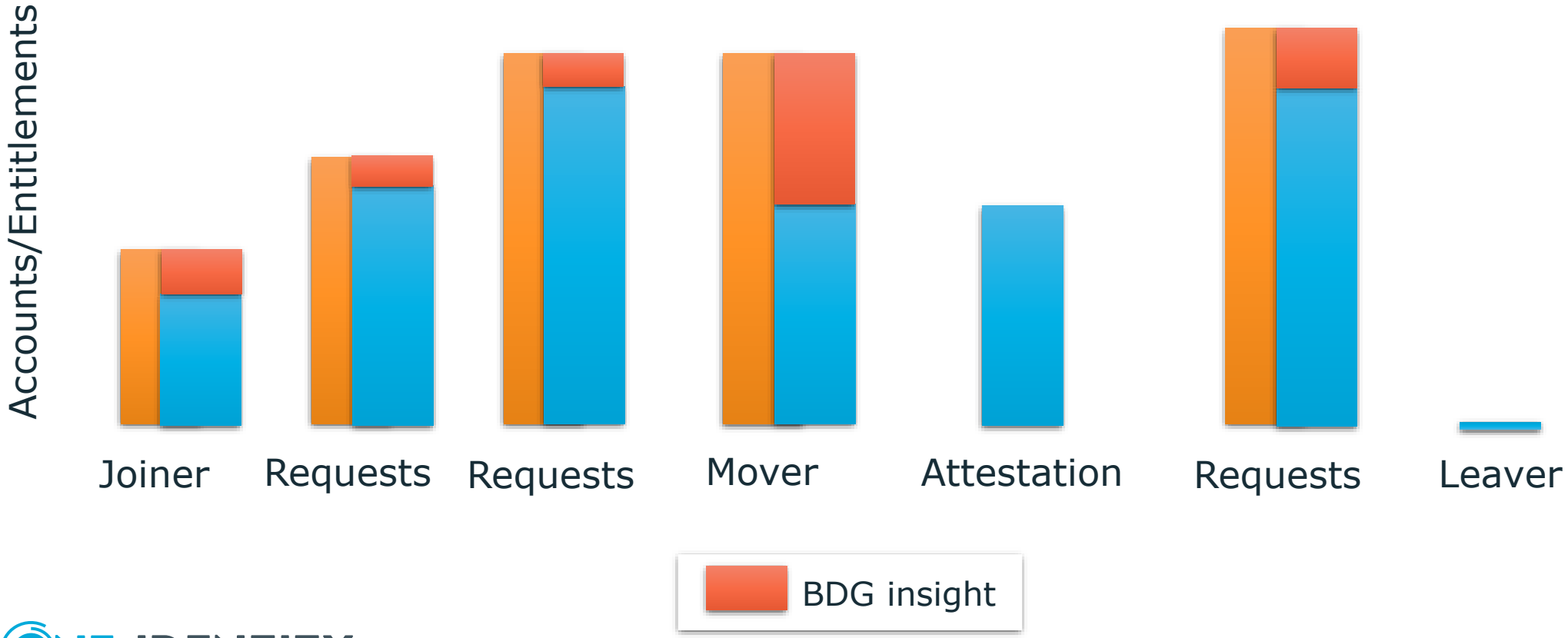
How to support the decision makers

- Make Behavior Driven Governance insights available within IGA

- Define Policies that show unused
  - accounts
  - applications (for an account)
  - entitlements (of an account)

- provide usage insights to support attestation decisions

Lifecycle with Behavior Driven Governance



Summary

- Behavior Driven Governance provides insights which accounts/entitlements are not used by an identity during daily work
- Not used = Not needed!
- A path to reach the Least Privilege Principle

Unified Identity Platform

To close the cybersecurity exposure gap, security executives need to shift from a fragmented to a **unified approach to identity security.**

Visit us at #7-408

ONE IDENTITY by Quest

Visit us at #7-408