SailPoint®

The core of identity security

Roles – What? Why? and How?

Steve Toole CISSP – Principal Solution Consultant

Agenda

Why roles?

Different approaches to building roles

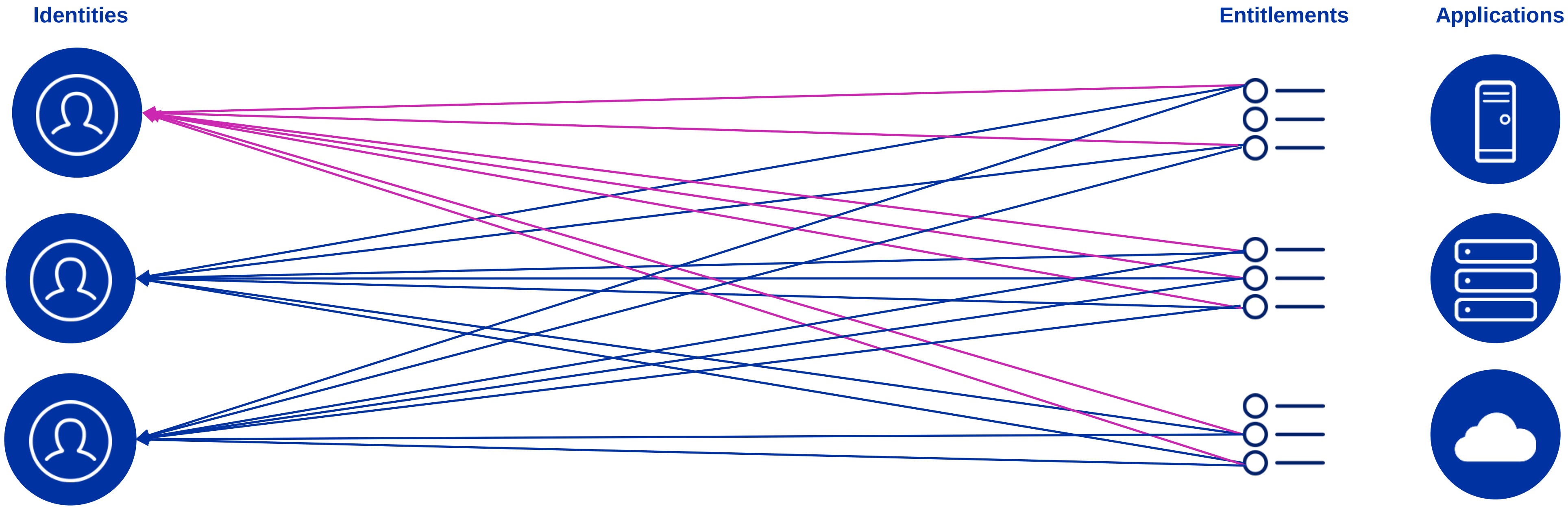
Traditional role design project

Best practices

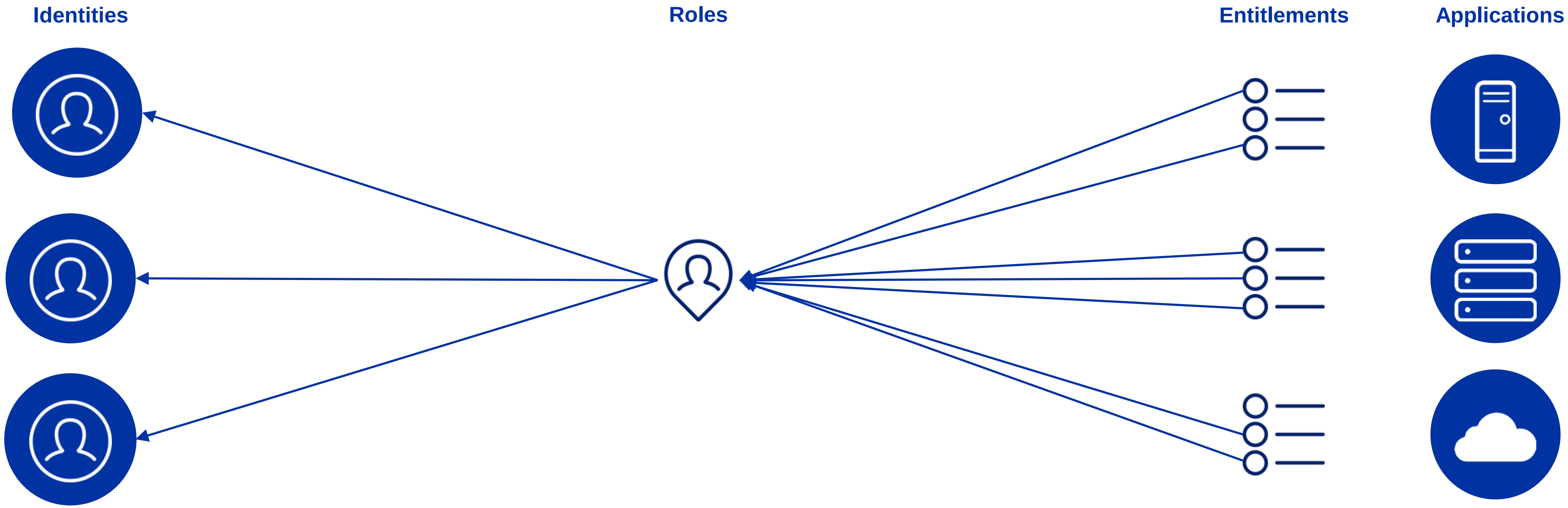
How SailPoint can help

Why Roles ?

Why Roles ?



Why Roles ?



Why Roles?

Productivity

- Day 1 Access
- Increase User satisfaction
- Simplify access certifications

Reduce Overhead

- Reduce manual effort
- Reduce end-user confusion
- Simplify your access
- Automation

Increase Security

- Least-privileged access
- Access changes throughout a user’s life cycle
- Automation of Joiner / Mover / Leaver events

The Need for Roles – Provisioning

Roles ensure users have the right access to do their job automatically.

JOB TITLE
DEPARTMENT
LOCATION

The Need for Roles - Compliance

Do you **KNOW** who has access to what and

if it is **APPROPRIATE**

And can you **PROVE** it?

Roles enable better & more efficient

governance reviews

Different Approaches

Different Approaches to Roles

Enterprise

Business roles based on organisational hierarchies

RBAC strategy

Use Case

Project scoped

Project aligned

RBAC not a goal

Targeted

Bundles of access, groups of identities

Focus on targeted groups / areas

RBAC not the goal, at least initially

Enterprise Approach

Typical goals

Define roles for every job/position/worker in the company

Cover 100% of all access they need

Advantages

- all access is assigned automatically based on identity attributes – have everything they need from hour 1 in the job
- Supports joiners, movers, leavers
- Significantly reduce certifications

Constraints

- Takes a long time to accomplish
- End up with more roles than actual workers!
- Companies are moving targets – imagine updating all those roles for every re-org, M&A, applications added /removed

Use Case Approach

Typical goals

Support a particular use case, i.e., assigning common birthright access as part of a joiner/new hire process

Advantages

- Required access is assigned automatically
- Supports some differentiation (e.g., employees vs contractors)
- Workers get the foundational access they need from hour 1 in the job

Constraints

- It only covers birthright access unless you combine it with another approach
- Need to request additional access

Targeted Approach

Typical goals

Define roles for a few specific groups with high turnover and high standardization (e.g., hotel clerks, cashiers at a store)

Cover 100% of all access they need

Advantages

- When it's done, all access is assigned automatically based on identity attributes – have everything they need from hour 1 in the job
- Enforces standardization

Constraints

- It only covers certain groups unless you combine it with another approach

Traditional Role Design

Role Design

Role design is the practice of strategically designing roles to improve the performance, efficiency, manageability and security of the organization

- **Job analysis** is the systematic analysis access required to complete the job function – what exactly does the job entails and the tasks it performs
- **Role definition** is concerned with defining the purpose and objectives of the role – automation, certification, birthright access, additional access
- **Qualification criteria** for assigning a role

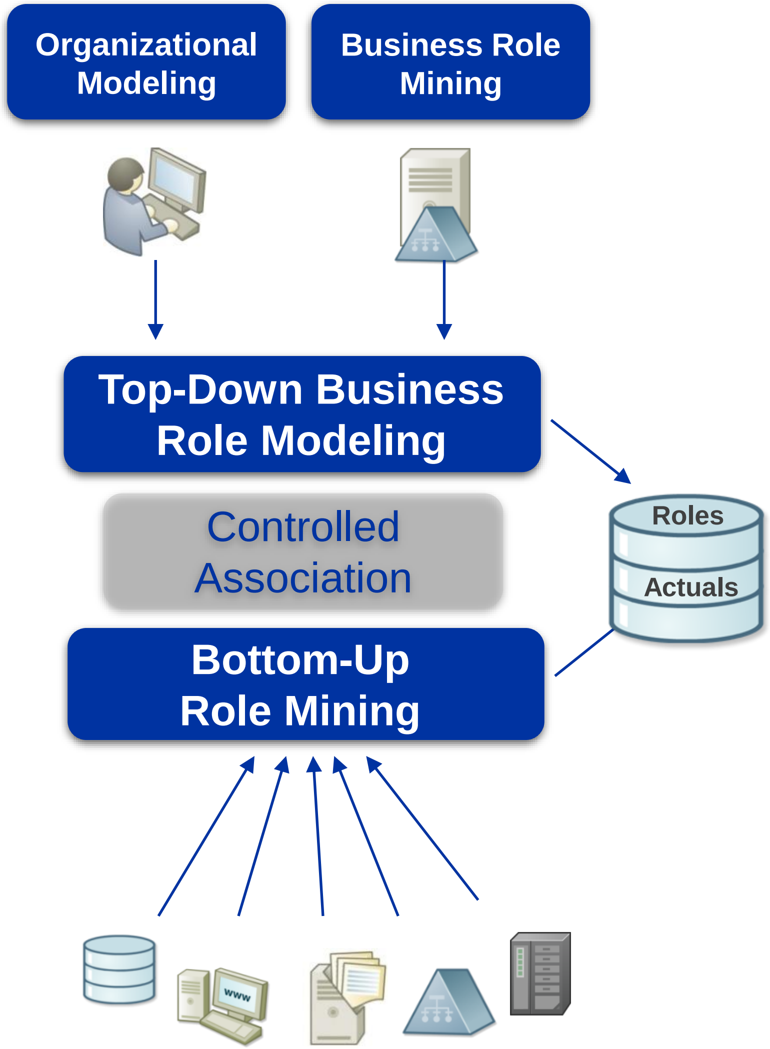
Role Design Process

Top-Down Business Role Modeling

- Capture via business analysis and organizational modeling

Bottom-Up IT Role Modeling

- Driven by analysis and analytics-focused processes



Top Down Analysis

- What business functions does each job perform?

- Which applications are required? What type of access is required for each application?

- How are accounts and access assigned for each application?

- Review HR job architecture, interview job holders, managers and application owners, conduct surveys, and observe people at work.

Bottom Up Analysis

- Create a list of user access permissions for each application
- Start with a cleanup!
- Compare and group users together for each type of application access
- Compare and group user access across applications
- Identify common elements between users who have the same or similar access
- Provides better defined roles but more time consuming process

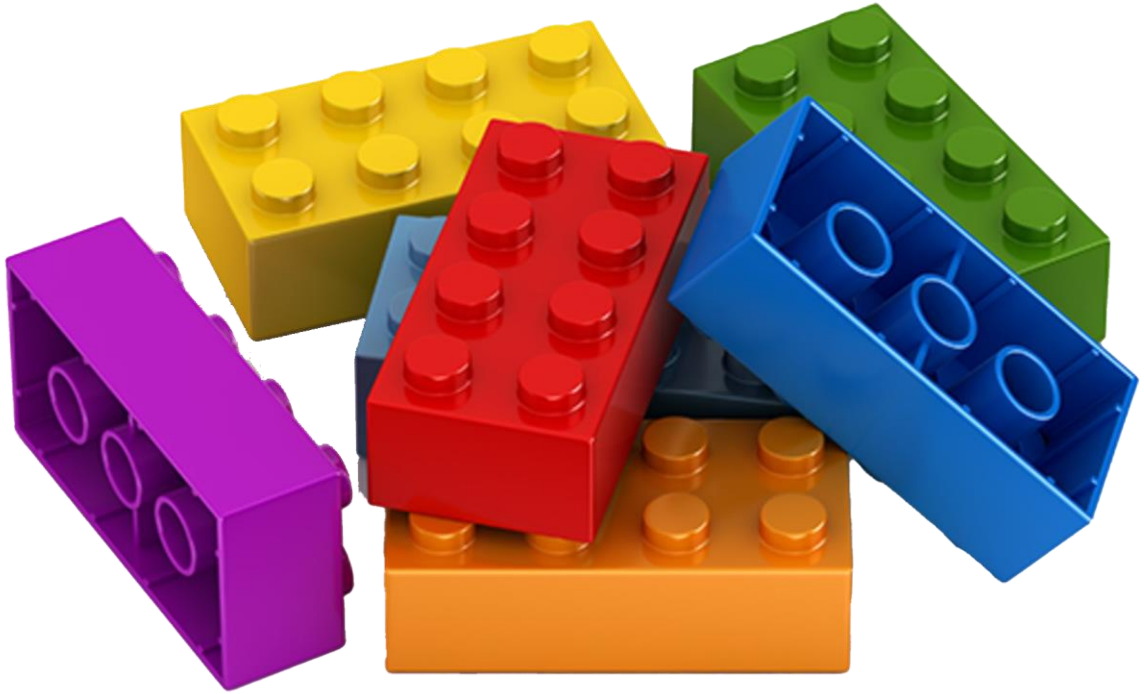
Role Design Process

Step 1: Define Geographic Organization Structure

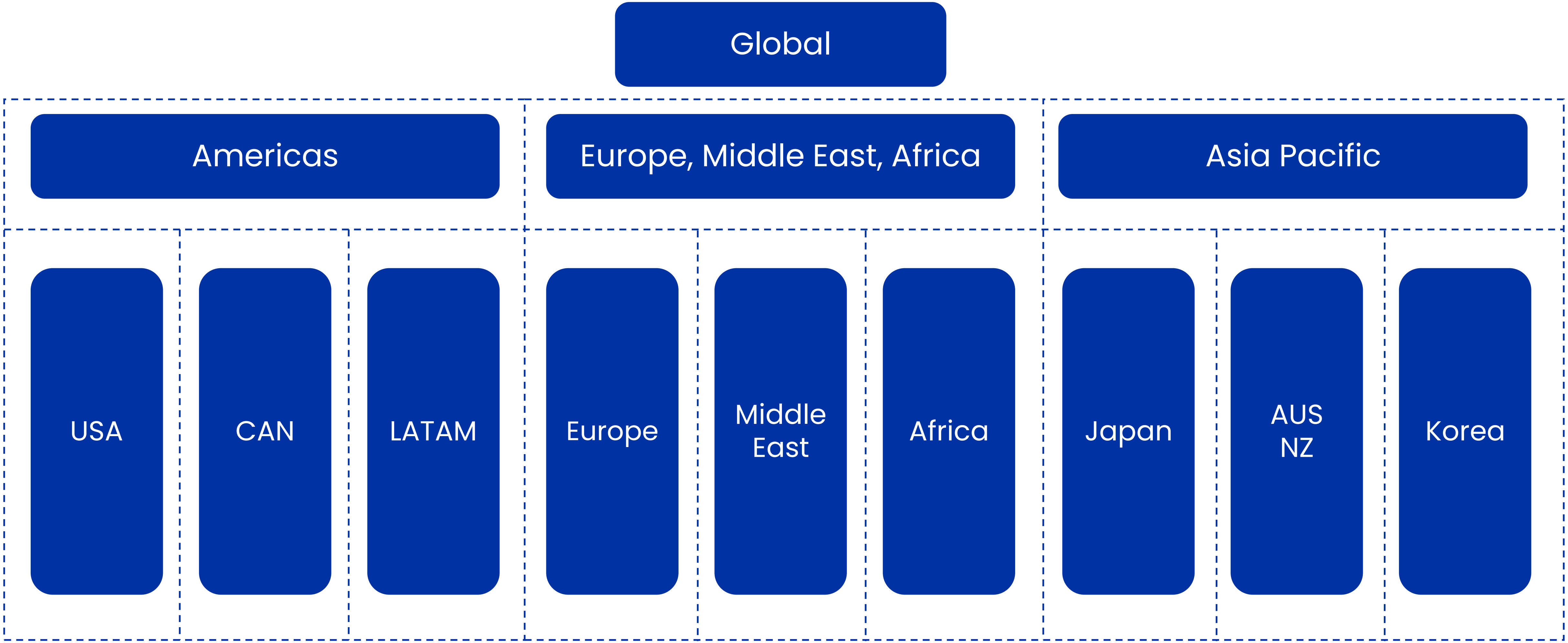
Step 2: Define Business Organization Structure

Step 3: Design Roles

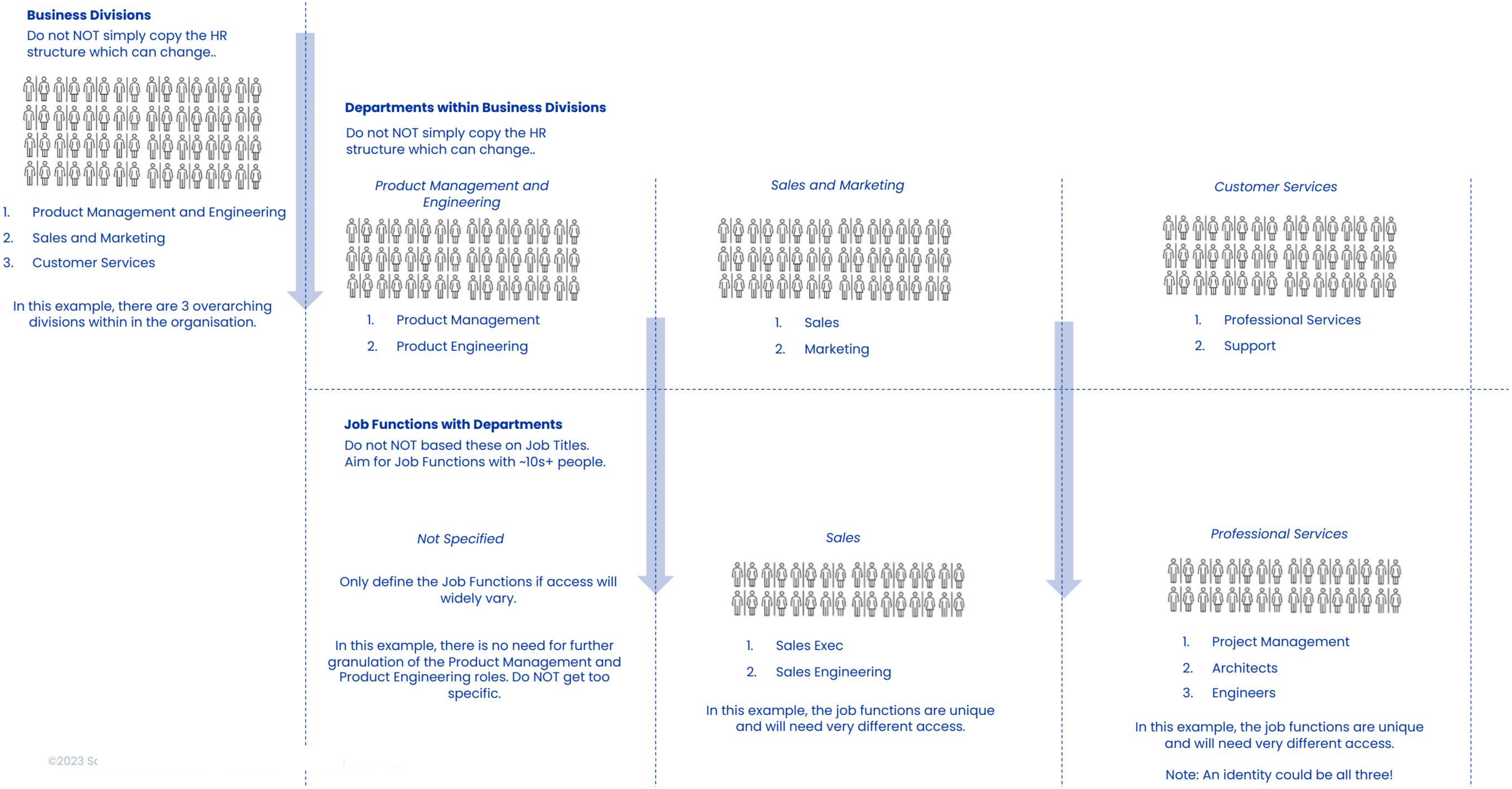
Step 4: Implementation



Step 1 – Define Org Structure by Access



Step 2 –Define Organization Structure



Business Divisions

Do not NOT simply copy the HR structure which can change..

1. Product Management and Engineering
2. Sales and Marketing
3. Customer Services

In this example, there are 3 overarching divisions within in the organisation.

Departments within Business Divisions

Do not NOT simply copy the HR structure which can change..

Product Management and Engineering

1. Product Management
2. Product Engineering

Sales and Marketing

1. Sales
2. Marketing

Customer Services

1. Professional Services
2. Support

Job Functions with Departments

Do not NOT based these on Job Titles.
Aim for Job Functions with ~10s+ people.

Not Specified

Only define the Job Functions if access will widely vary.

In this example, there is no need for further granulation of the Product Management and Product Engineering roles. Do NOT get too specific.

Sales

1. Sales Exec
2. Sales Engineering

In this example, the job functions are unique and will need very different access.

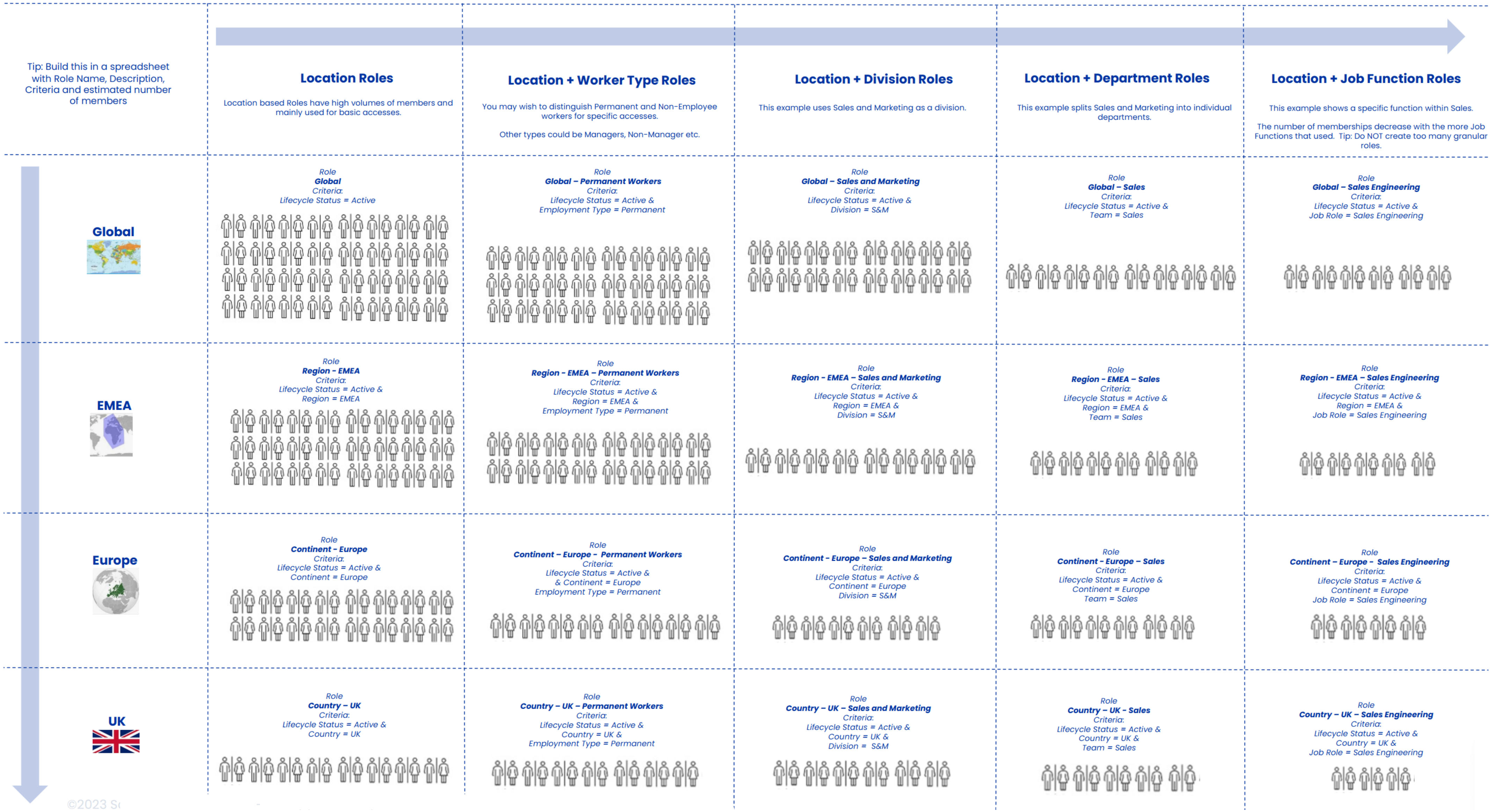
Professional Services

1. Project Management
2. Architects
3. Engineers

In this example, the job functions are unique and will need very different access.

Note: An identity could be all three!

Step 3 –Create Roles based on Geo & Business



Tip: Build this in a spreadsheet with Role Name, Description, Criteria and estimated number of members	**Location Roles** Location based Roles have high volumes of members and mainly used for basic accesses.	**Location + Worker Type Roles** You may wish to distinguish Permanent and Non-Employee workers for specific accesses. Other types could be Managers, Non-Manager etc.	**Location + Division Roles** This example uses Sales and Marketing as a division.	**Location + Department Roles** This example splits Sales and Marketing into individual departments.	**Location + Job Function Roles** This example shows a specific function within Sales. The number of memberships decrease with the more Job Functions that used. Tip: Do NOT create too many granular roles.
Global	*Role* ***Global*** *Criteria:* *Lifecycle Status = Active*	*Role* ***Global – Permanent Workers*** *Criteria:* *Lifecycle Status = Active &* *Employment Type = Permanent*	*Role* ***Global – Sales and Marketing*** *Criteria:* *Lifecycle Status = Active &* *Division = S&M*	*Role* ***Global – Sales*** *Criteria:* *Lifecycle Status = Active &* *Team = Sales*	*Role* ***Global – Sales Engineering*** *Criteria:* *Lifecycle Status = Active &* *Job Role = Sales Engineering*
EMEA	*Role* ***Region - EMEA*** *Criteria:* *Lifecycle Status = Active &* *Region = EMEA*	*Role* ***Region - EMEA – Permanent Workers*** *Criteria:* *Lifecycle Status = Active &* *Region = EMEA &* *Employment Type = Permanent*	*Role* ***Region - EMEA – Sales and Marketing*** *Criteria:* *Lifecycle Status = Active &* *Region = EMEA &* *Division = S&M*	*Role* ***Region - EMEA – Sales*** *Criteria:* *Lifecycle Status = Active &* *Region = EMEA &* *Team = Sales*	*Role* ***Region - EMEA – Sales Engineering*** *Criteria:* *Lifecycle Status = Active &* *Region = EMEA &* *Job Role = Sales Engineering*
Europe	*Role* ***Continent - Europe*** *Criteria:* *Lifecycle Status = Active &* *Continent = Europe*	*Role* ***Continent – Europe - Permanent Workers*** *Criteria:* *Lifecycle Status = Active &* *& Continent = Europe* *Employment Type = Permanent*	*Role* ***Continent - Europe – Sales and Marketing*** *Criteria:* *Lifecycle Status = Active &* *Continent = Europe* *Division = S&M*	*Role* ***Continent - Europe – Sales*** *Criteria:* *Lifecycle Status = Active &* *Continent = Europe* *Team = Sales*	*Role* ***Continent – Europe - Sales Engineering*** *Criteria:* *Lifecycle Status = Active &* *Continent = Europe* *Job Role = Sales Engineering*
UK	*Role* ***Country – UK*** *Criteria:* *Lifecycle Status = Active &* *Country = UK*	*Role* ***Country – UK – Permanent Workers*** *Criteria:* *Lifecycle Status = Active &* *Country = UK &* *Employment Type = Permanent*	*Role* ***Country – UK – Sales and Marketing*** *Criteria:* *Lifecycle Status = Active &* *Country = UK &* *Division = S&M*	*Role* ***Country – UK - Sales*** *Criteria:* *Lifecycle Status = Active &* *Country = UK &* *Team = Sales*	*Role* ***Country – UK – Sales Engineering*** *Criteria:* *Lifecycle Status = Active &* *Country = UK &* *Job Role = Sales Engineering*

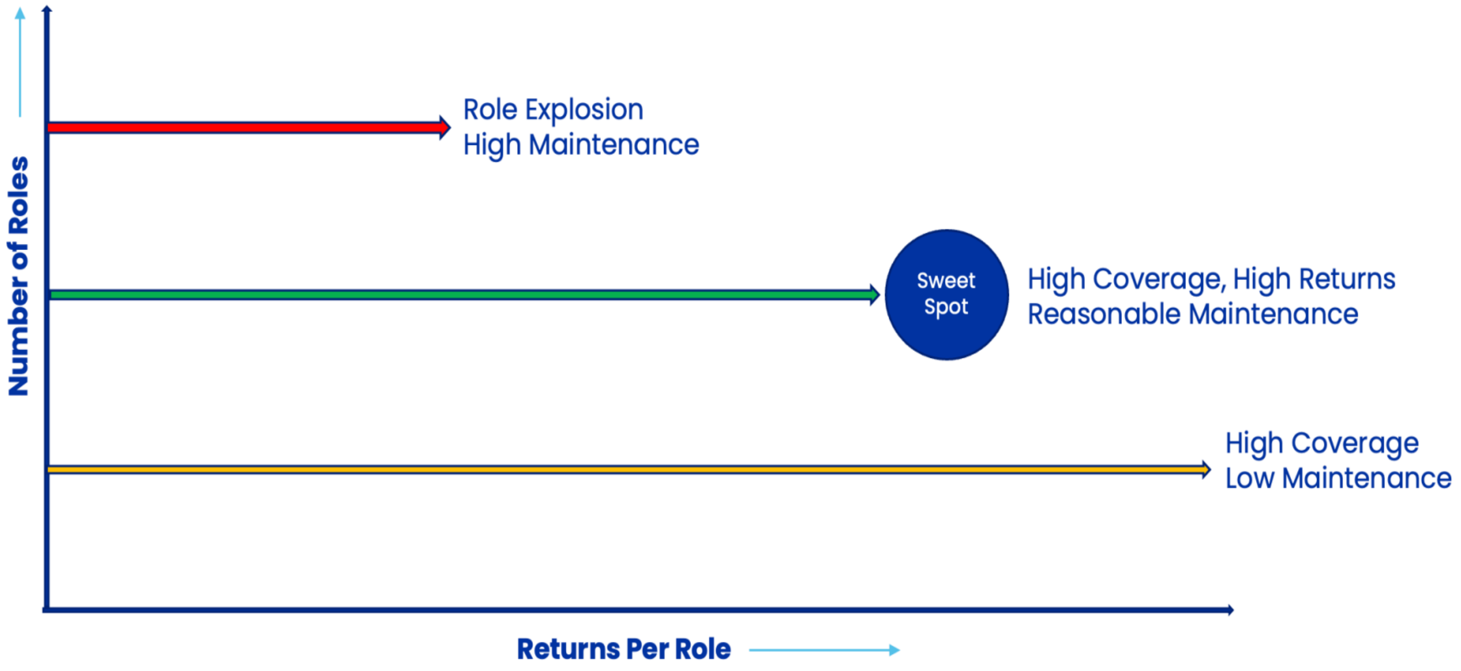
Step 4 - Implementation

1. Review and approval of role composition – criteria and access
2. Create roles without entitlements to test automation and volumes
3. Attach entitlements to roles in a controlled rollout - monitor outcomes and adapt

Best Practices

Role Design Best Practices

- Avoid creating too many roles, especially where role membership is low
- More roles results in more maintenance
- Design roles for business functions
  - Span multiple systems
  - Avoid ‘Business Title Roles’



Role Project Best Practices

General

- Look for groupings of user types
- Prevent role proliferation
- Enforce least privilege
- Define roles that are reusable

High turnover or high use roles are a good way to start

- Bank tellers, seasonal employees, employee vs. contractor
- Don’t attempt to “boil the ocean”

Know your scope

- Simplify certifications? Access requests?
- Involve SME’s who know the business

Role Project Best Practices (cont.)

Build Roles Following Data Cleanup where possible

- HR Cleanup
- Active Directory Cleanup
- ERP Cleanup

Every business approaches roles differently

Roles are a program, not a project

- Too big, too fast is how role projects fail
- Roles have a lifecycle and should evolve
- Start small and familiar
- Can give key managers the capability to suggest roles as needed

Before inventing your own, consider default role models to start

SailPoint Automated Role Design

Barriers to Building Better Roles

We don’t have the expertise to build a role program.

Building roles is a time-intensive, manual effort.

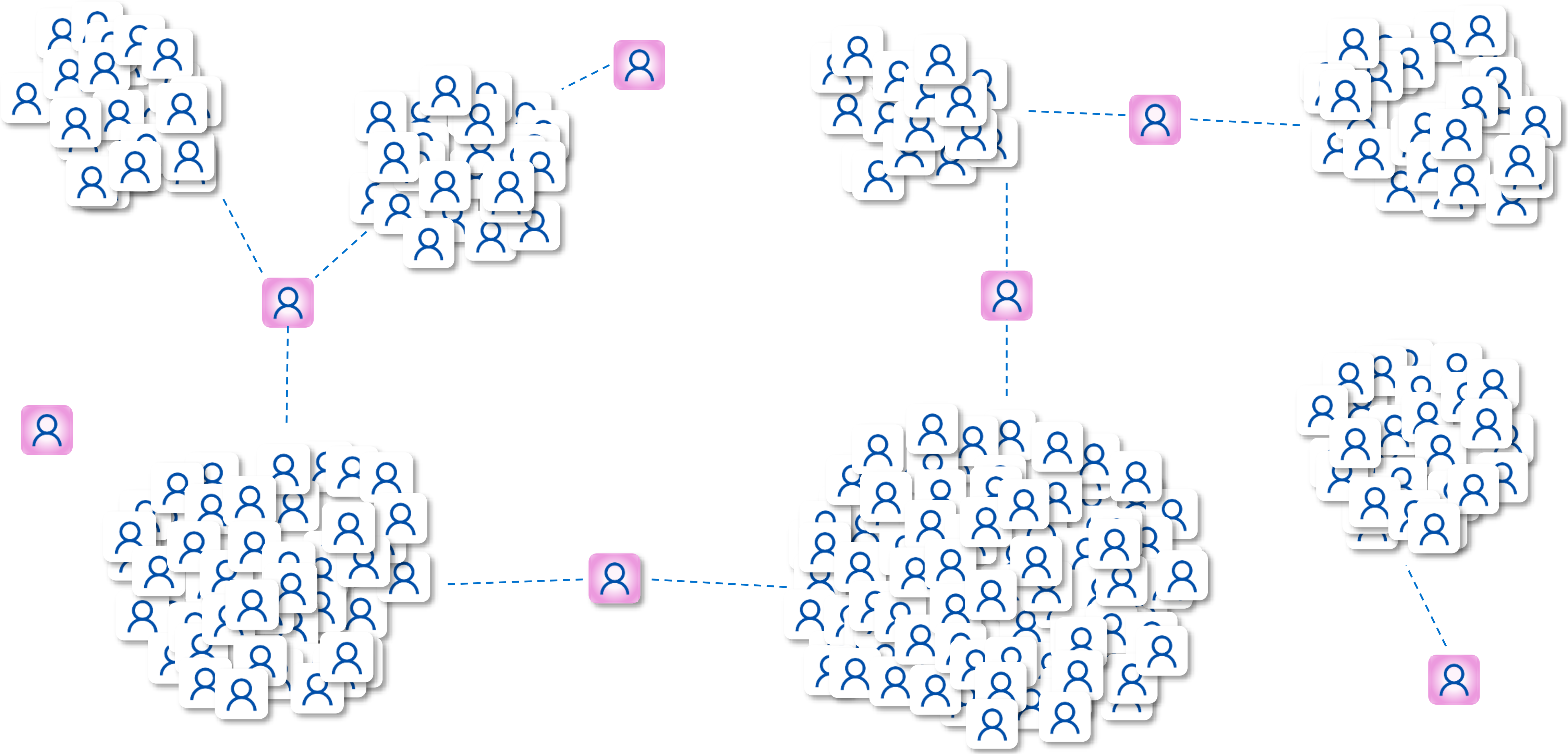
We can’t provide the right-sized access and security for our users.

SailPoint

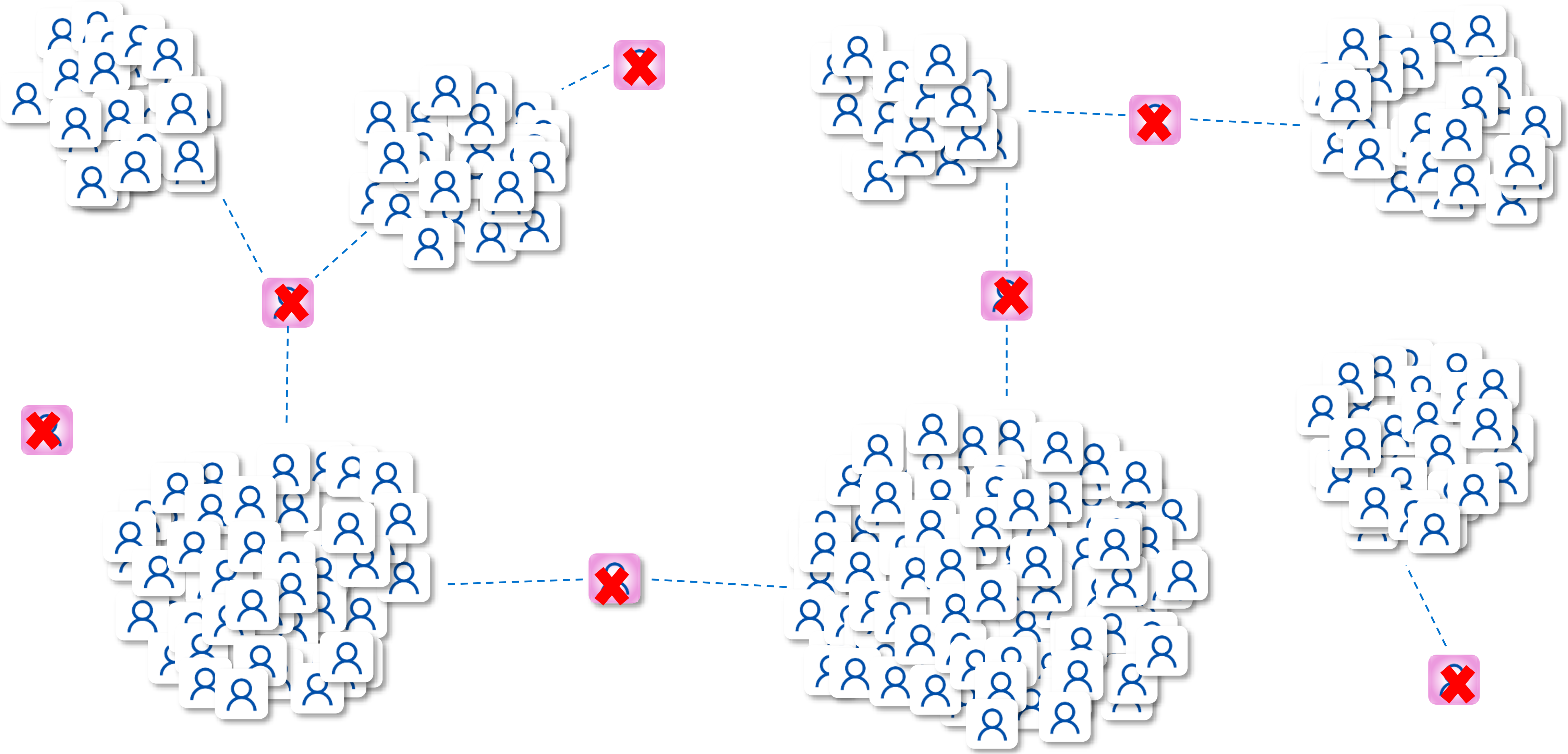
Where do you start ?

Proactively highlight anomalous access

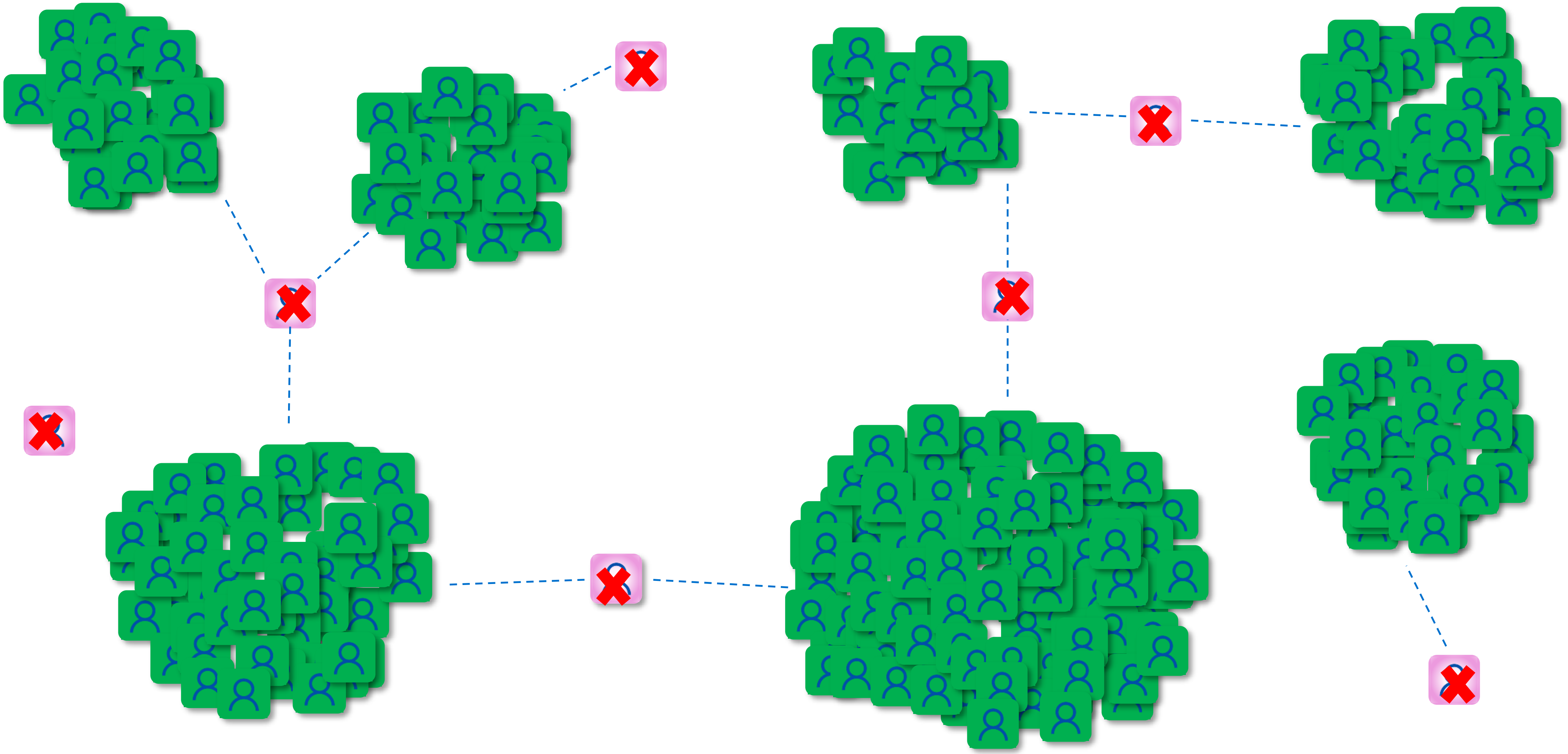
Peer groups are key for identifying outliers



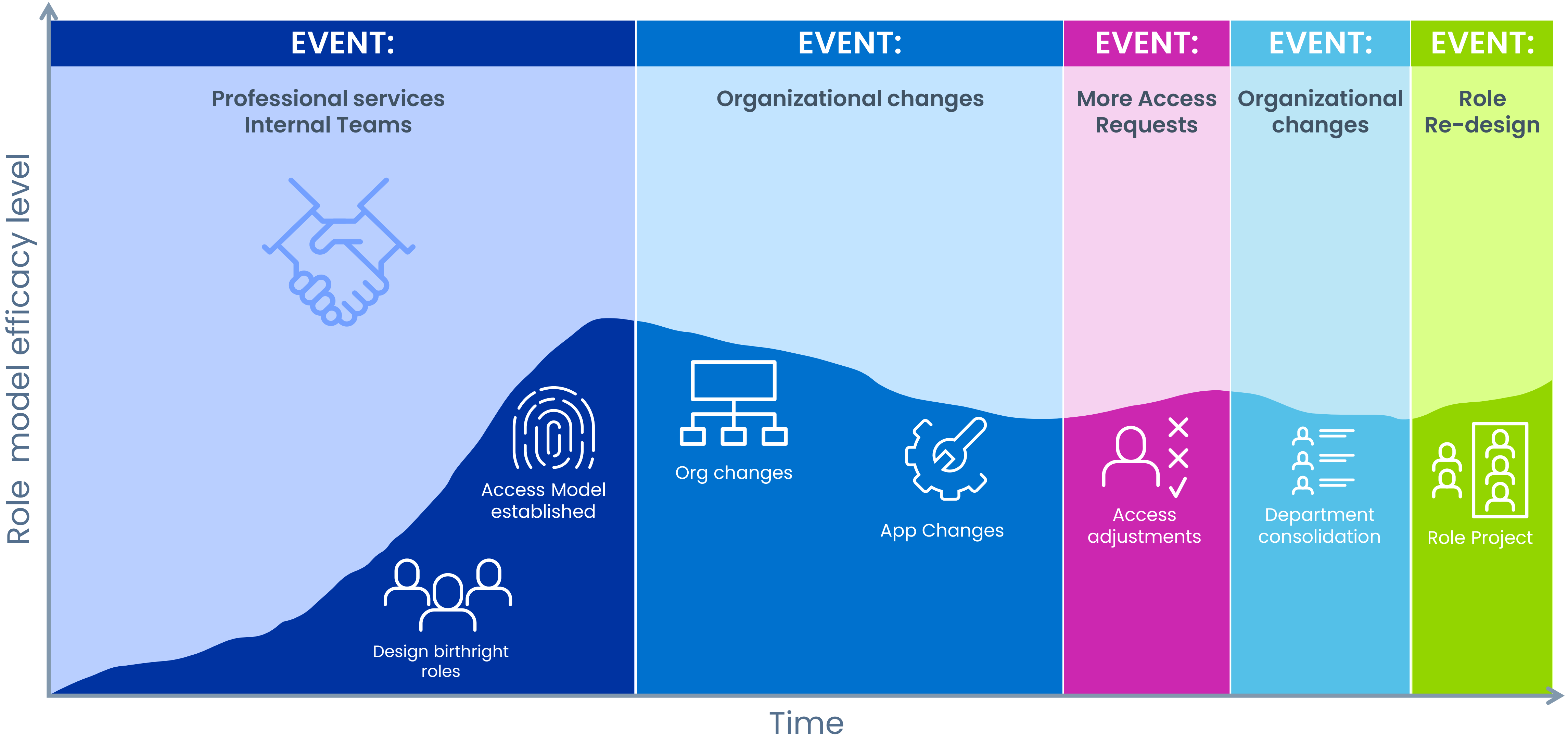
Clean Up Outliers !!!!



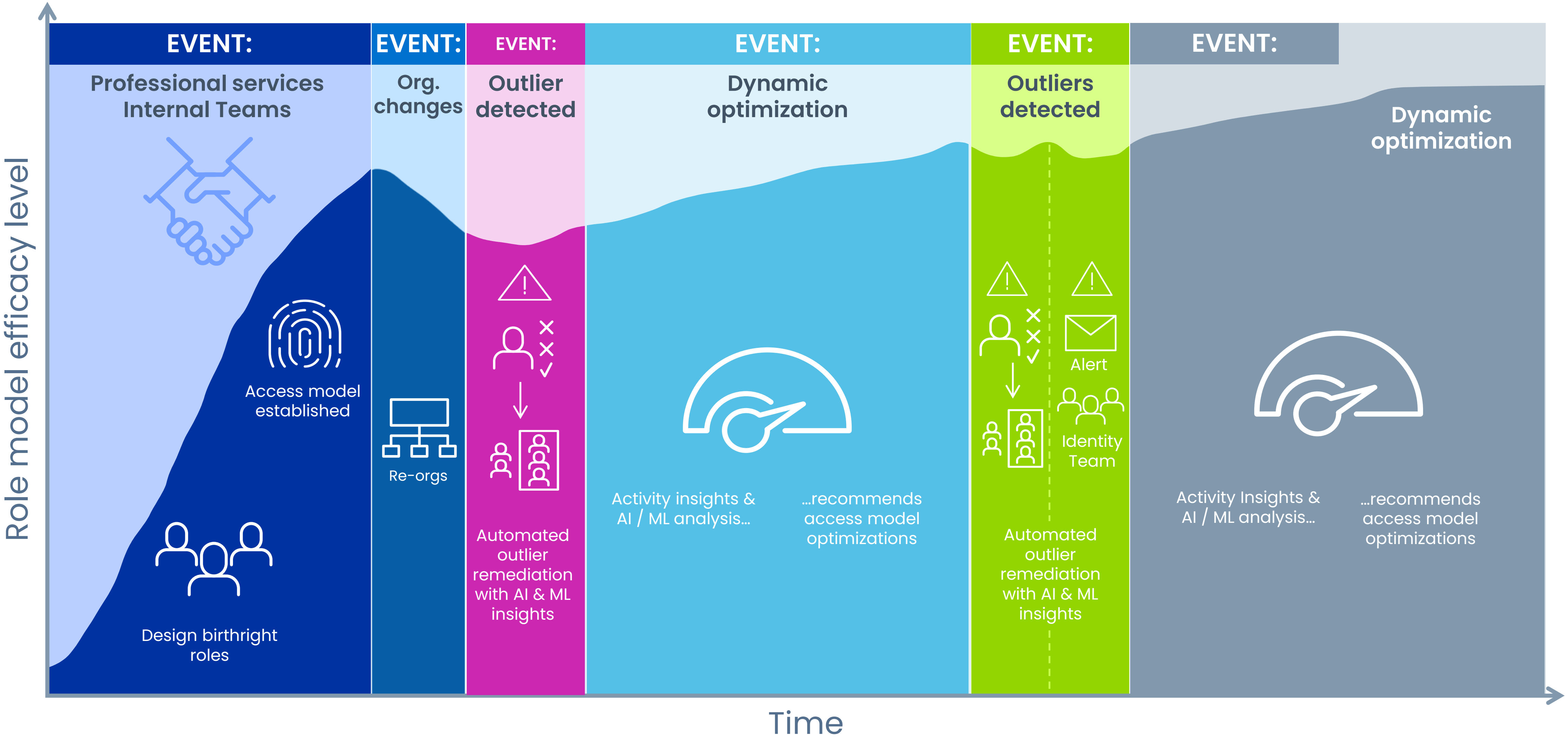
Build Roles Automatically (and keep them up do date)



Traditional Role Design



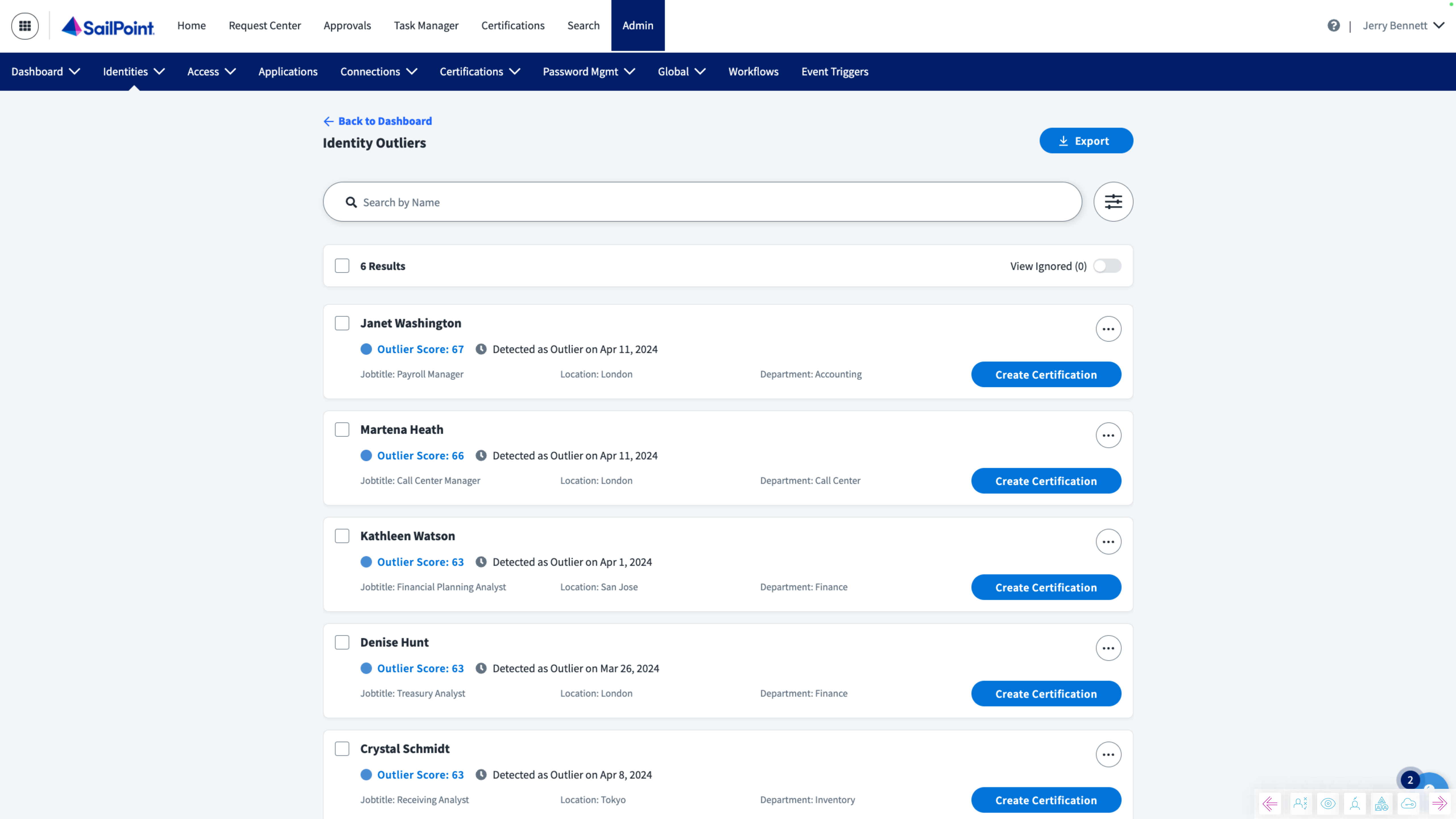
Autonomous Identity Role Modeling


EVENT:
Professional services Internal Teams
Access model established
Design birthright roles
EVENT:
Org. changes
Re-orgs
EVENT:
Outlier detected
Automated outlier remediation with AI & ML insights
EVENT:
Dynamic optimization
Activity insights & AI / ML analysis...
...recommends access model optimizations
EVENT:
Outliers detected
Alert
Identity Team
Automated outlier remediation with AI & ML insights
EVENT:
Dynamic optimization
Activity Insights & AI / ML analysis...
...recommends access model optimizations
Role model efficacy level
Time

Advanced Identity Capabilities

Insights

- Access History
- Identity Outliers
- Access Intelligence Center



Identity Outliers

□ **6 Results**

□ **Janet Washington**
● Outlier Score: 67 — Detected as Outlier on Apr 11, 2024
Jobtitle: Payroll Manager — Location: London — Department: Accounting

□ **Martena Heath**
● Outlier Score: 66 — Detected as Outlier on Apr 11, 2024
Jobtitle: Call Center Manager — Location: London — Department: Call Center

□ **Kathleen Watson**
● Outlier Score: 63 — Detected as Outlier on Apr 1, 2024
Jobtitle: Financial Planning Analyst — Location: San Jose — Department: Finance

□ **Denise Hunt**
● Outlier Score: 63 — Detected as Outlier on Mar 26, 2024
Jobtitle: Treasury Analyst — Location: London — Department: Finance

□ **Crystal Schmidt**
● Outlier Score: 63 — Detected as Outlier on Apr 8, 2024
Jobtitle: Receiving Analyst — Location: Tokyo — Department: Inventory

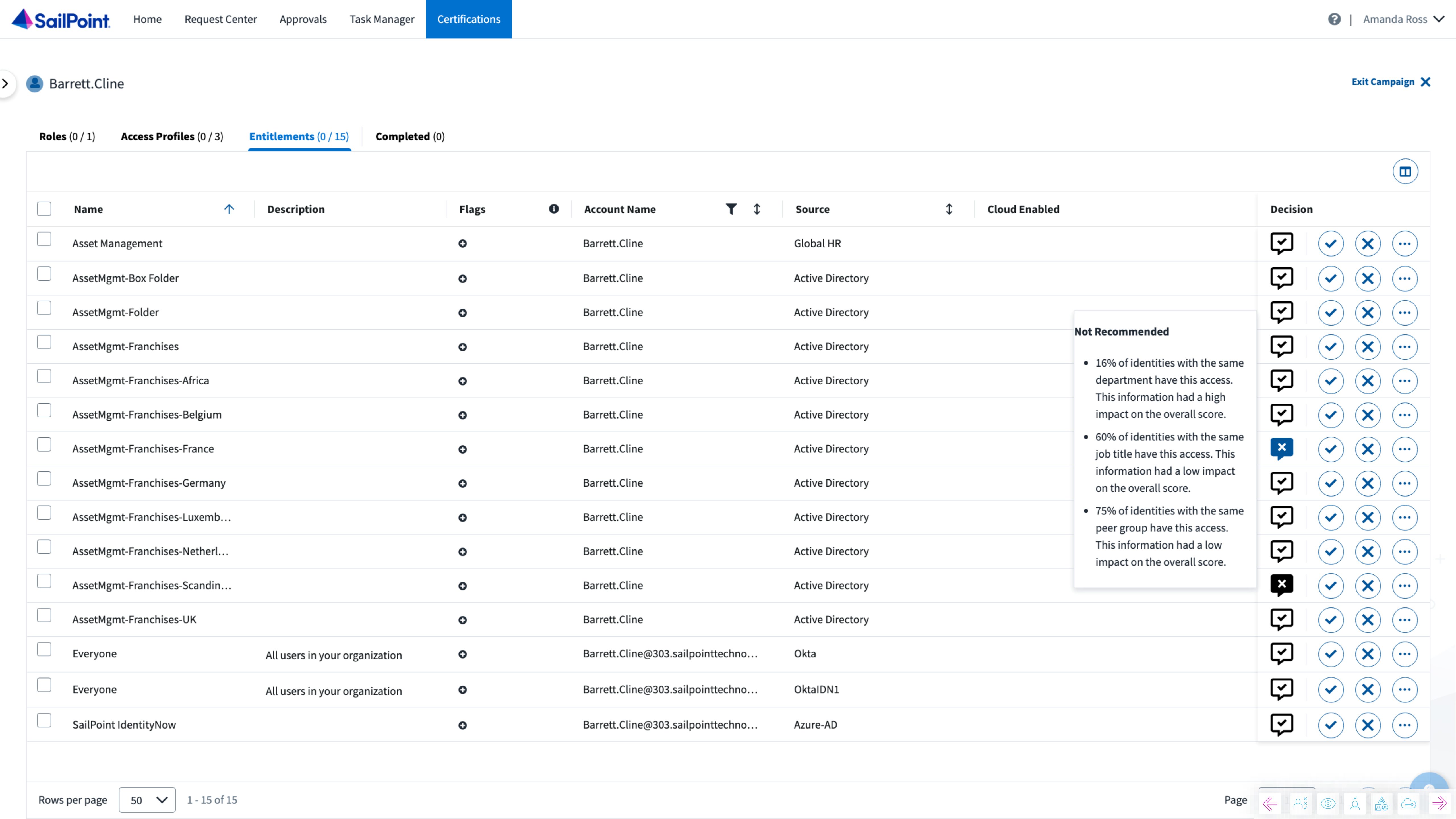
Advanced Identity Capabilities

Insights

- Access History
- Identity Outliers
- Access Intelligence Center

Recommendations

- Access Requests
- Certification
- Streamline access requests



SailPoint Home Request Center Approvals Task Manager **Certifications** Amanda Ross

Barrett.Cline

Exit Campaign ✕

Roles (0 / 1) **Access Profiles** (0 / 3) **Entitlements (0 / 15)** **Completed** (0)

□	Name	Description	Flags	Account Name	Source	Cloud Enabled	Decision
□	Asset Management		⊕	Barrett.Cline	Global HR		✓ ✓ ✕ ⋯
□	AssetMgmt-Box Folder		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Folder		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Franchises		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Franchises-Africa		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Franchises-Belgium		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Franchises-France		⊕	Barrett.Cline	Active Directory		✕ ✓ ✕ ⋯
□	AssetMgmt-Franchises-Germany		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Franchises-Luxemb…		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Franchises-Netherl…		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	AssetMgmt-Franchises-Scandin…		⊕	Barrett.Cline	Active Directory		✕ ✓ ✕ ⋯
□	AssetMgmt-Franchises-UK		⊕	Barrett.Cline	Active Directory		✓ ✓ ✕ ⋯
□	Everyone	All users in your organization	⊕	Barrett.Cline@303.sailpointtechno…	Okta		✓ ✓ ✕ ⋯
□	Everyone	All users in your organization	⊕	Barrett.Cline@303.sailpointtechno…	OktaIDN1		✓ ✓ ✕ ⋯
□	SailPoint IdentityNow		⊕	Barrett.Cline@303.sailpointtechno…	Azure-AD		✓ ✓ ✕ ⋯

Not Recommended

- 16% of identities with the same department have this access. This information had a high impact on the overall score.
- 60% of identities with the same job title have this access. This information had a low impact on the overall score.
- 75% of identities with the same peer group have this access. This information had a low impact on the overall score.

Rows per page 50 1 - 15 of 15 Page

Advanced Identity Capabilities

Insights

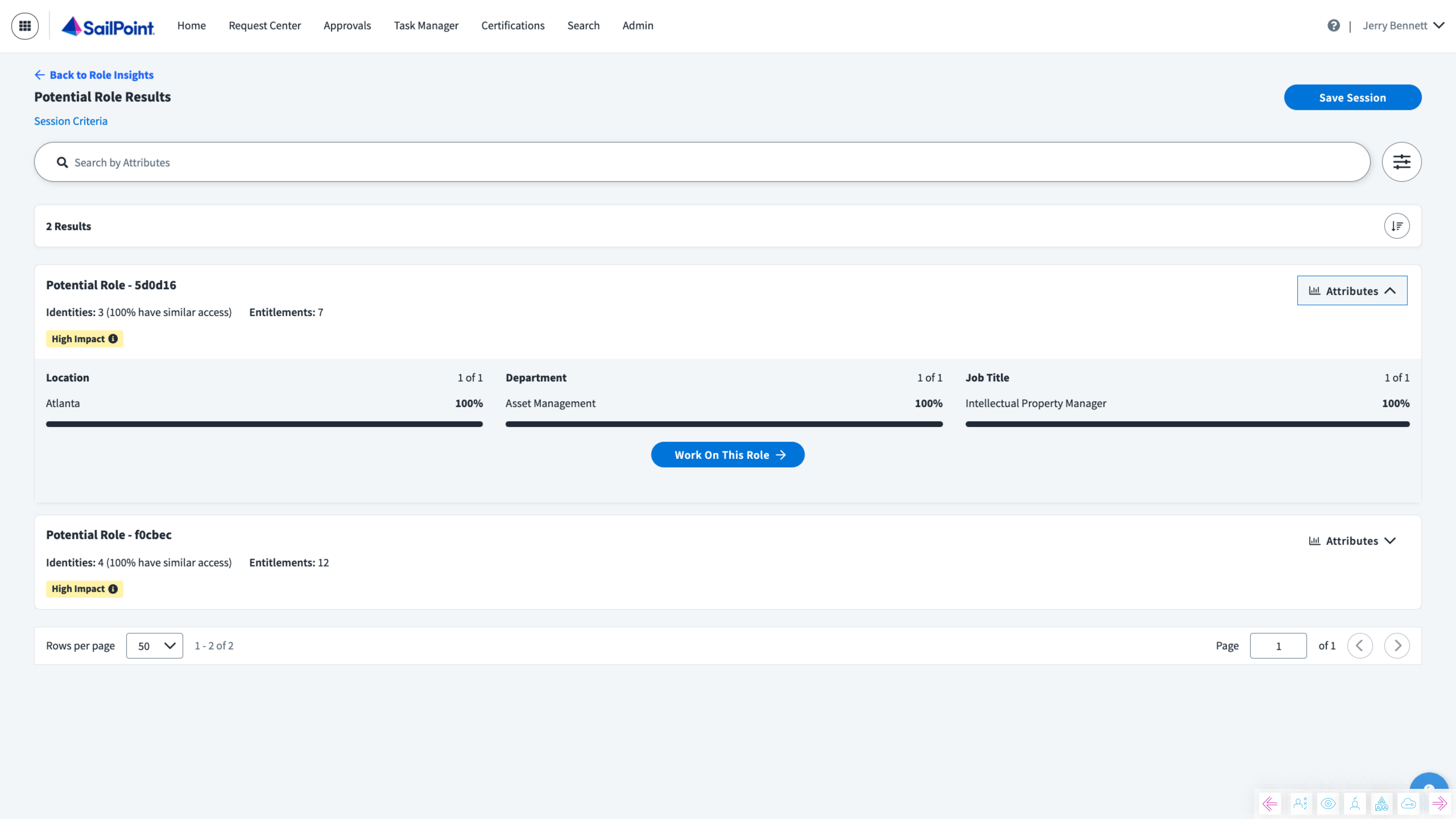
- Access History
- Identity Outliers
- Access Intelligence Center

Access Modeling

- Discover Common Access
- Discover Roles (RBAC)
- Role Insights

Recommendations

- Access Requests
- Certification
- Streamline access requests



Potential Role Results

2 Results

Potential Role - 5d0d16

Identities: 3 (100% have similar access) **Entitlements:** 7

High Impact

Location	1 of 1	**Department**	1 of 1	**Job Title**	1 of 1
Atlanta	**100%**	Asset Management	**100%**	Intellectual Property Manager	**100%**

Potential Role - f0cbec

Identities: 4 (100% have similar access) **Entitlements:** 12

High Impact

Advanced Identity Capabilities

Insights

- Access History
- Identity Outliers
- Access Intelligence Center

Access Modeling

- Discover Common Access
- Discover Roles (RBAC)
- Role Insights

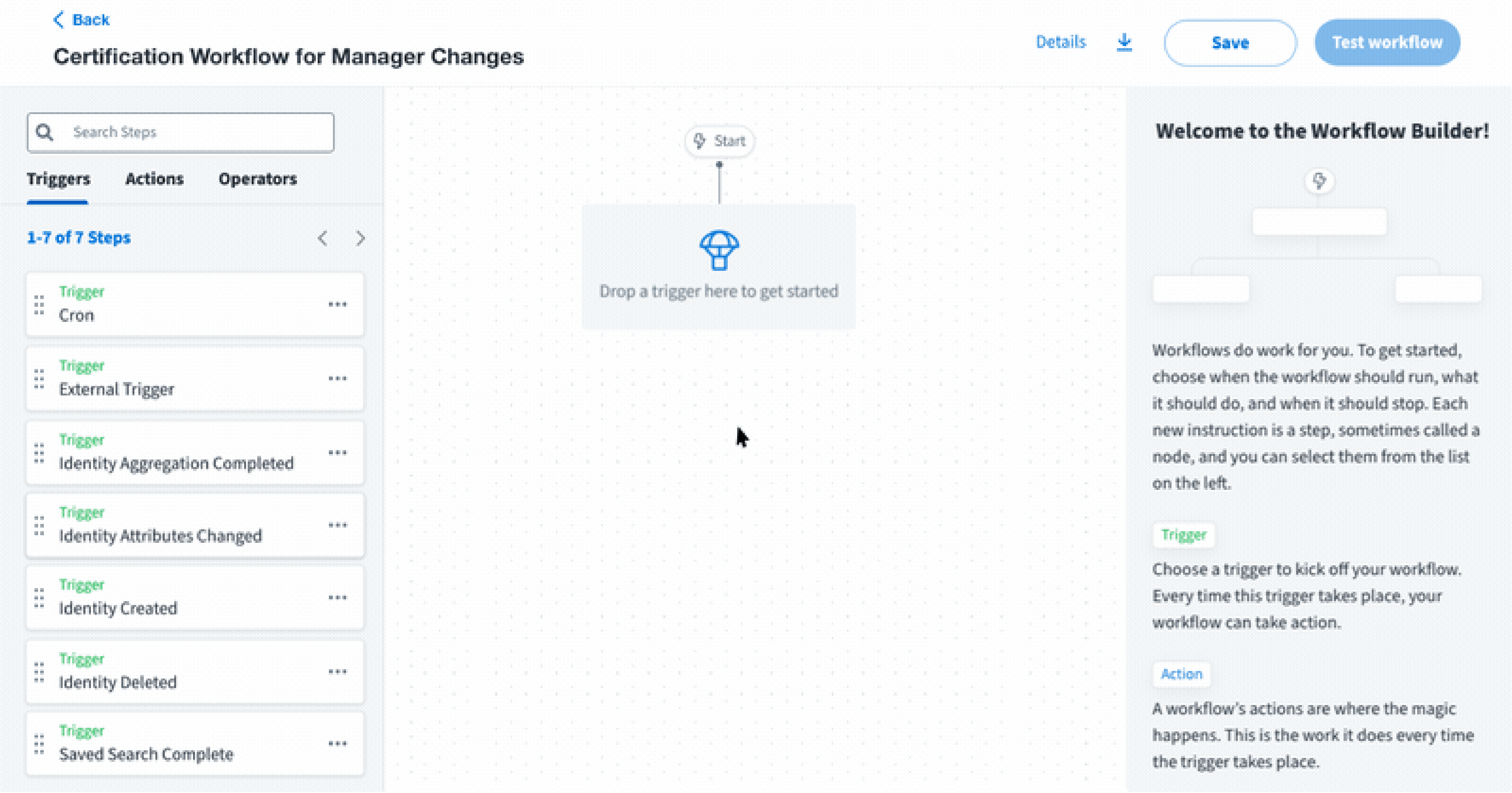
Recommendations

- Access Requests
- Certification
- Streamline access requests

Workflow

- Extensibility
- Customization
- Automated Orchestration

Workflow Builder



Certification Workflow for Manager Changes

Trigger
Cron

Trigger
External Trigger

Trigger
Identity Aggregation Completed

Trigger
Identity Attributes Changed

Trigger
Identity Created

Trigger
Identity Deleted

Trigger
Saved Search Complete

Drop a trigger here to get started

Welcome to the Workflow Builder!

Workflows do work for you. To get started, choose when the workflow should run, what it should do, and when it should stop. Each new instruction is a step, sometimes called a node, and you can select them from the list on the left.

Trigger

Choose a trigger to kick off your workflow. Every time this trigger takes place, your workflow can take action.

Action

A workflow's actions are where the magic happens. This is the work it does every time the trigger takes place.

Advanced Identity Capabilities

Insights

- Access History
- Identity Outliers
- Access Intelligence Center

Access Modeling

- Discover Common Access
- Discover Roles (RBAC)
- Role Insights

Recommendations

- Access Requests
- Certification
- Streamline access requests

Workflow

- Extensibility
- Customization
- Automated Orchestration

SailPoint®

Thank you!