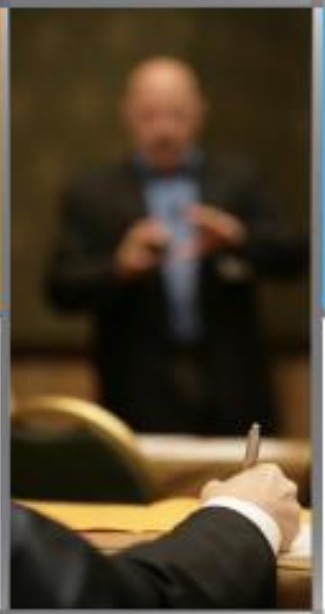
@CSOevents
#CSO50

CSO50 CONFERENCE+AWARDS

Aligning Proactive Security with Modern Threats



May 1-3, 2017

The Scottsdale Resort
Scottsdale, Arizona

PRODUCED BY
CSO
FROM IDG

CSO 50 CONFERENCE +AWARDS

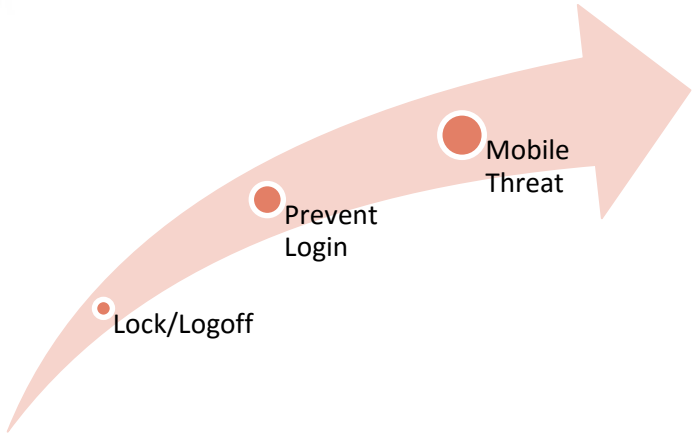
Providing Comprehensive Identity Management Across Multiple Business Units

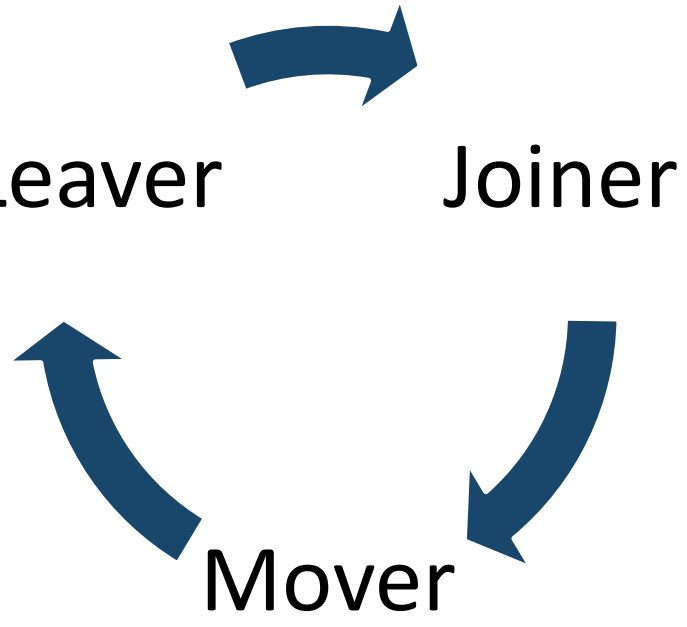
Patrick Landry
IT Technical Director
USAA
@PatrickDLandry

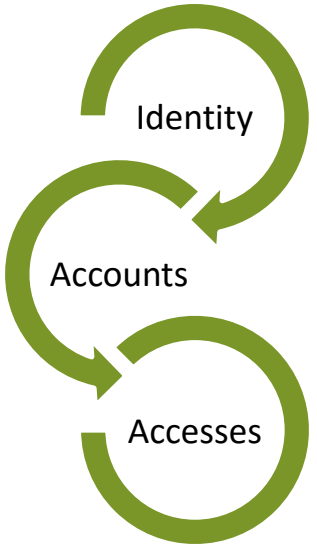
Identity Proofing

- First level of assurance
- Background checks
- Standards based (BYOI)
- If wrong, all efforts are at risk

Identity life cycle fundamentals





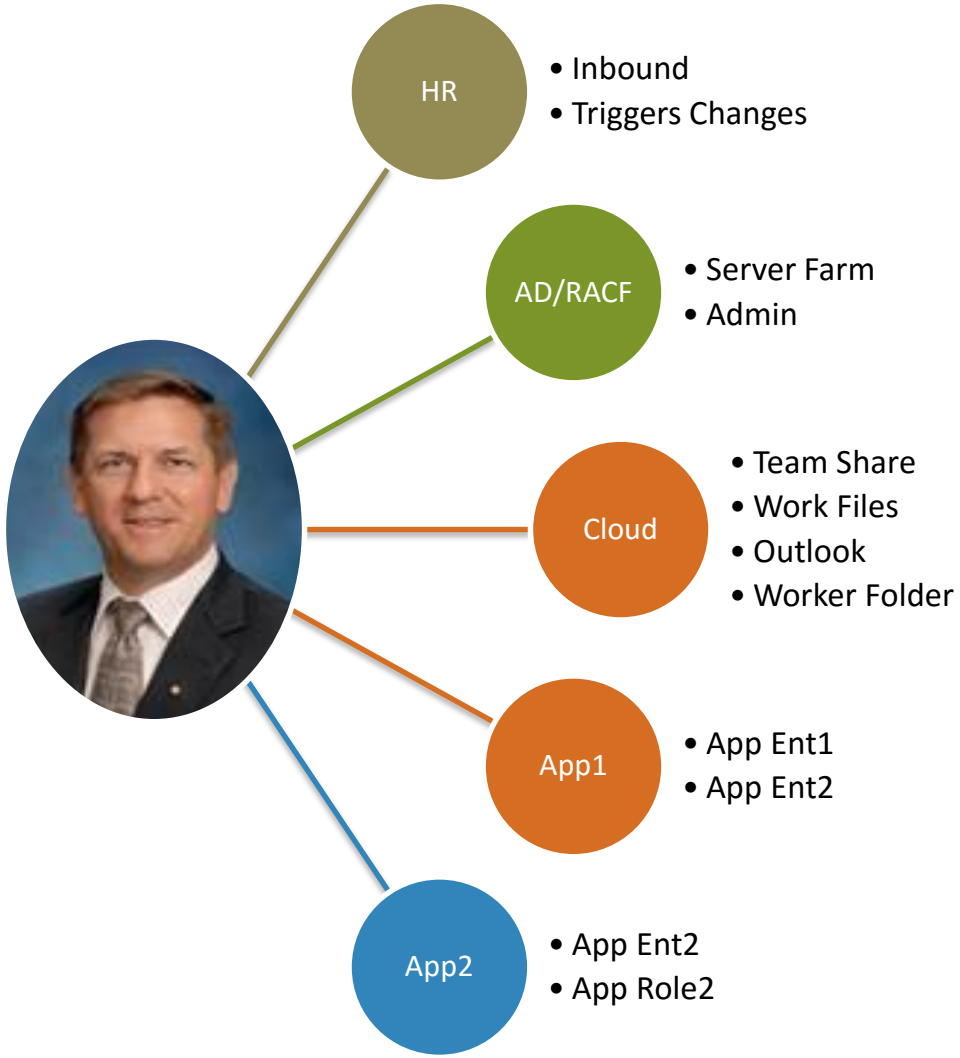


Joiner - One Identity…Many Accounts

Zero Day

Birthright

Request Based



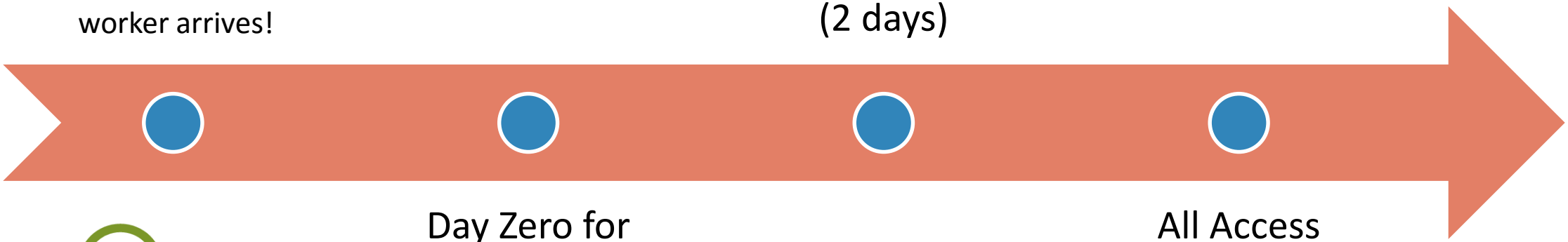
What it looked like for us

Total time from acceptance to productivity =10 days
5 workers over an 8 day cycle

Onboarding (5 days)

- Started before worker arrives!

Access Request (2 days)

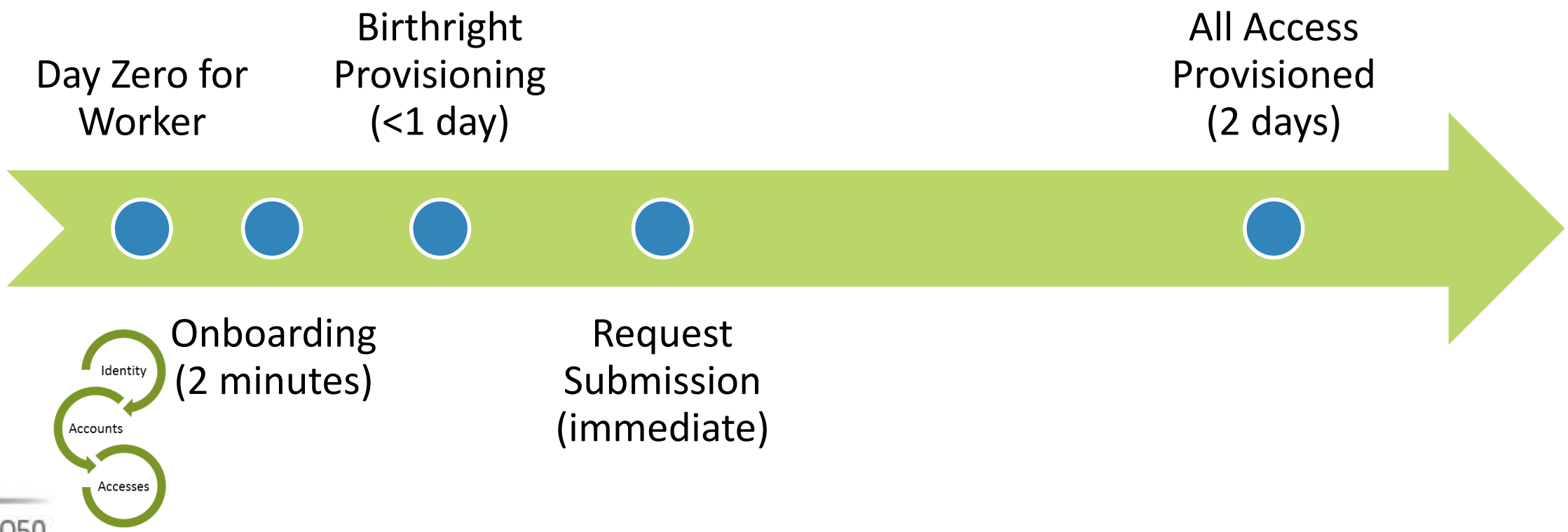


Day Zero for Worker

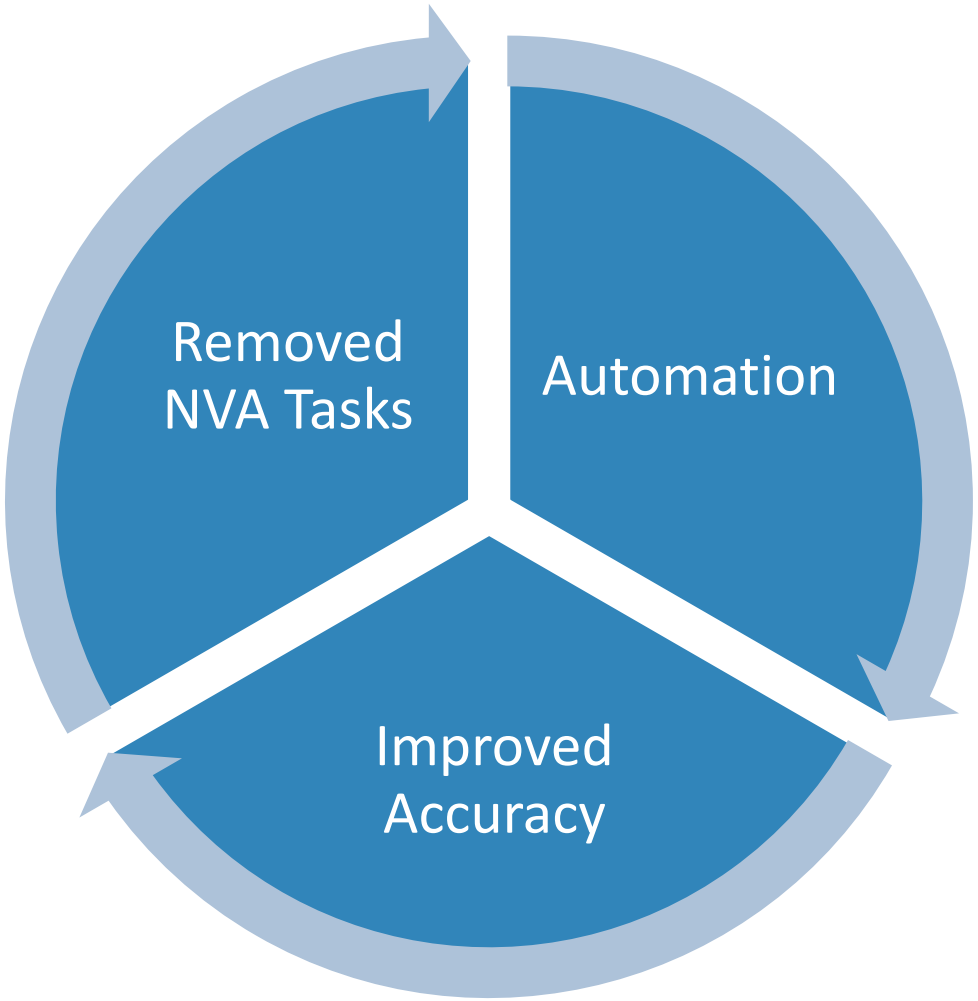
All Access Provisioned (3 days)

What it looks like now

Total time from acceptance to productivity = 2 days
1 worker for <30 minutes



Joiner - What did we do?



Mover – Where the Risk hits the Road

- Automatically remove privileged administrative access
- What about high-risk business access?
- Segregation of Duties
- Access Certification

- But…I need {worker} to keep their old accesses until I can backfill them

Privileged Access Removal

- Administrative Entitlements
  - Remove highest risk roles/entitlements
  - Key risk control! – measure it
- High Risk Business Applications
  - Business partners love this option
  - Separate process

Remove Elevated → Certify Remaining → Remove Revoked

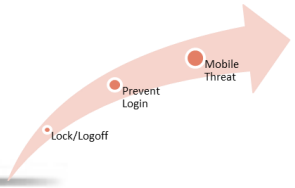
Event Driven Certifications

- Review all remaining roles/entitlements
  - Direct manager accountability
  - Exempt rules provisioning
- Limit time for review (2 weeks)
- Set workload expectations
- Must have ‘teeth’ to be effective

Leaver – Should be easy, but…

- Real-Time considerations
- Scheduled terminations
- Close all the gaps!

- Don’t forget mobile



Great risk if not complete

- Scan the network for logins/remove them
- Real-Time and Scheduled options
- Watch those external applications
  - ESSO closes the gap

- Mobile Device Management Considerations

Key Takeaways

- Identity functions are integral to all insider threat possibilities
- Partner with the business owners early in the process
- Control partners and regulators will have lots of questions
- IDaaS has a way to go yet

Determining What to Manage

- Know your portfolio
- Objectively rank it
- Determine “High Risk”

- Work with Control Partners