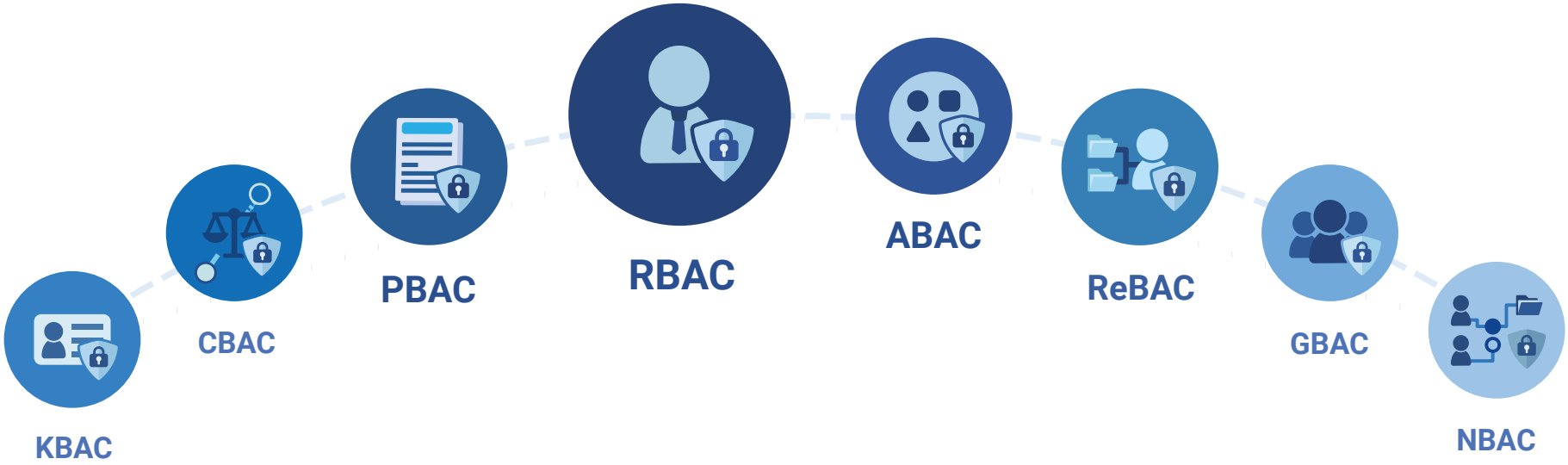
Navigating the Access Control Maze

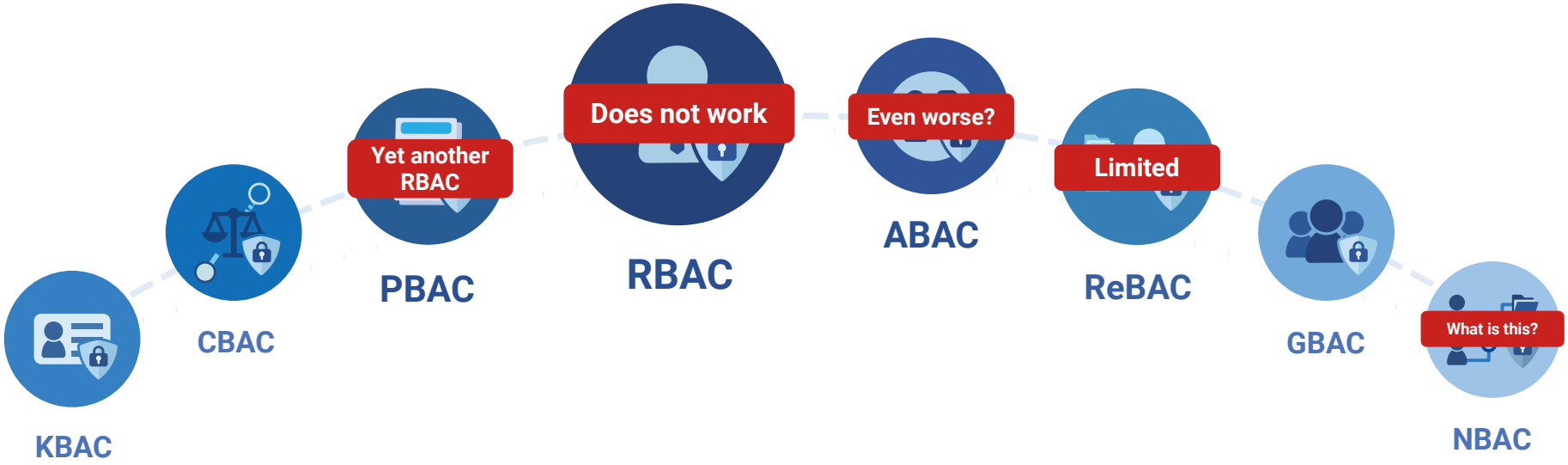
Radovan Semančík, December 2023
Co-Founder and Software Architect

Access Control ZOO



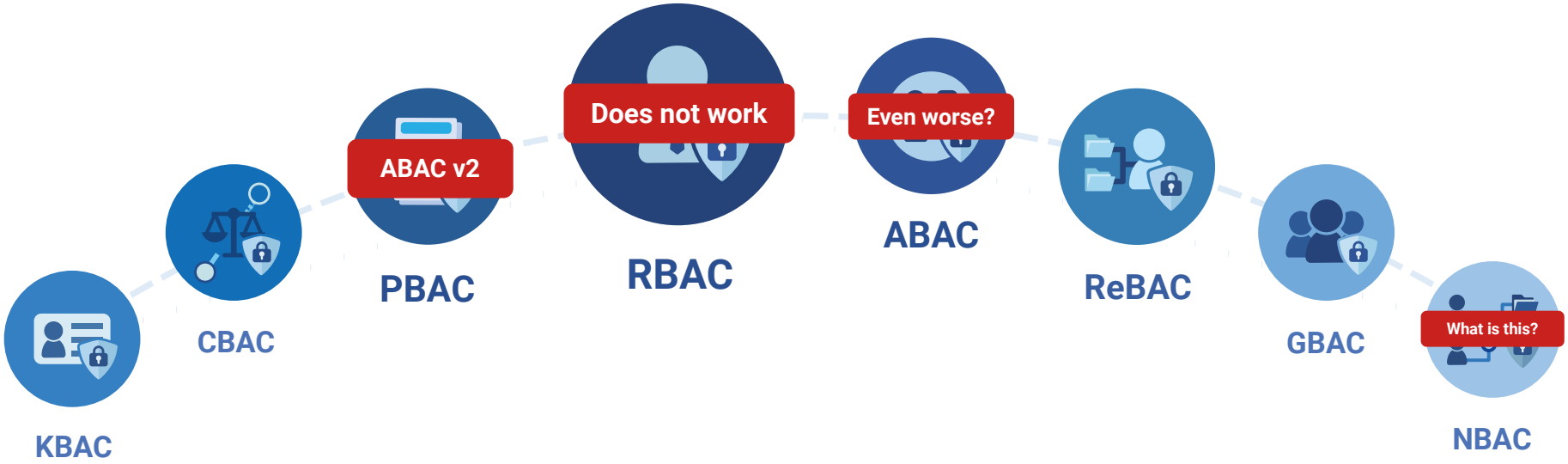
Evolveum

Access Control ZOO



Evolveum

Access Control ZOO



What can we do?

Evolveum

Traditional RBAC

- NIST (ANSI/INCITS 359-2004, INCITS 359-2012)
- Static – no policy
- Already outdated
- Still the king of access control

Evolveum

RBAC Does Not Work

- Overuse of application roles
- Access request frenzy
- Role explosion
- Huge certification effort
- Business role duplication
- Role decay

Evolveum

PBAC/ABAC Do Not Work Either

- Public secret #1:
  Nobody knows what access employees should have
- We need an exact, complete, understandable, and up-to-date policy in a machine-executable form
- How realistic is this?

Evolveum

PBAC/ABAC Do Not Work Either

- Public secret #2:
  Your **data are wrong** (and incomplete)
- Garbage in, garbage out
- You do not even know that your data are wrong
- You ain’t going to know until you try to enforce the policy
- Many things can go very wrong very quickly

Evolveum

PBAC/ABAC Do Not Work Either

- Public secret #3:
  There is an **exception** to every rule (even policy)
- Policy exceptions have to be part of the policy
- The policy gets very complicated
- Need to re-certify the policy
- Need to re-certify the data
- Exception tracking?

Evolveum

PBAC/ABAC Do Not Work Either

- PBAC is supposed to be dynamic
- **Policy maintenance** is a nightmare
- One big global policy is not going to work
- Missing: simulations, impact analysis, tooling
- How quickly can we change the policy?
  Weeks? Months?
- Is business going to wait?

Evolveum

What Can Work?

- A bottom-up approach
- From data to policy
- Data mining, AI/ML
- Work around data errors and exceptions
- Divide and conquer:
  split policy into manageable pieces

Evolveum

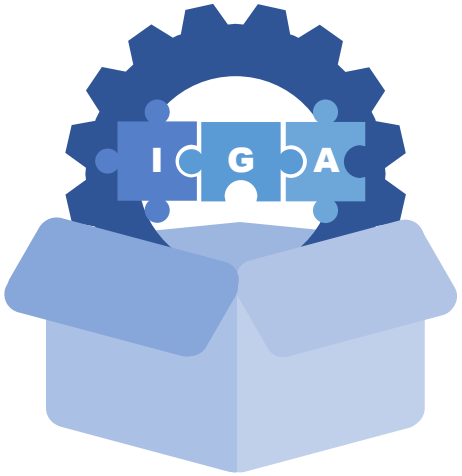
What Can Work?

- Heavily extended PBAC
  - Request-approval process, exceptions, manageable policy, compliance management, great tooling
- Dynamic RBAC
  - RBAC with policy

Evolveum

Evolveum's MidPoint

- MidPoint: an open source identity governance and administration (IGA) platform
- Appreciated by customers, recognized by analysts
- Evolveum: professional development and maintenance of midPoint
- More than a decade of continuous innovation



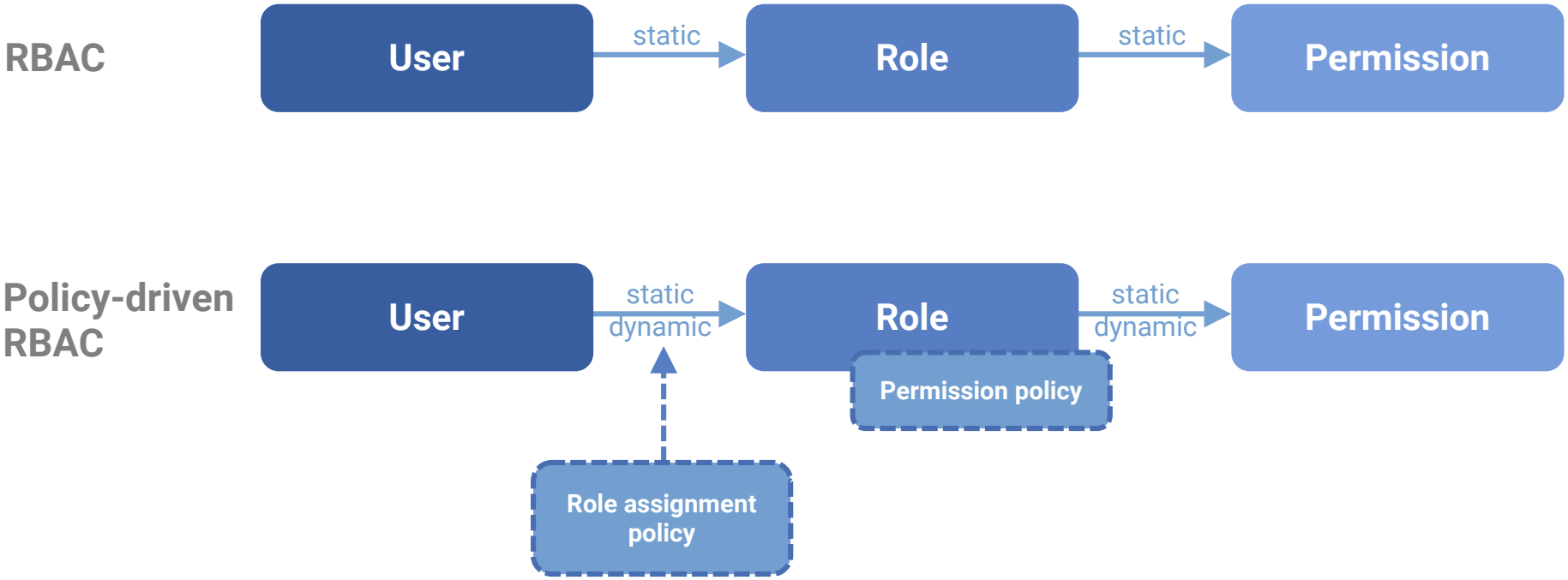
Evolveum

How Do We Do It

- RBAC is not going away anytime soon
- Dynamic RBAC: policy in the roles
- A bottom-up approach: from roles to policy
- AI-assisted mechanisms
- A practical solution, available today (midPoint 4.8)

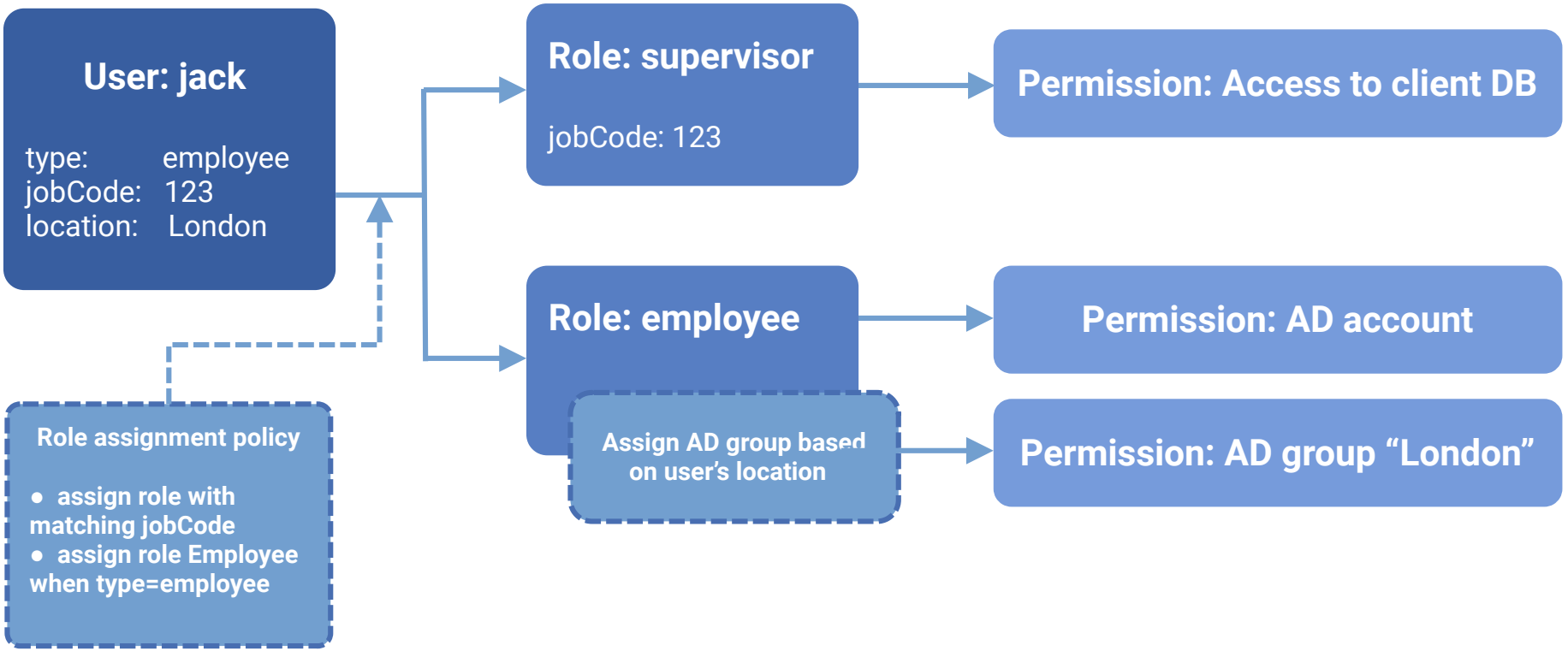
Evolveum

Policy-Driven RBAC



Evolveum

Policy-Driven RBAC



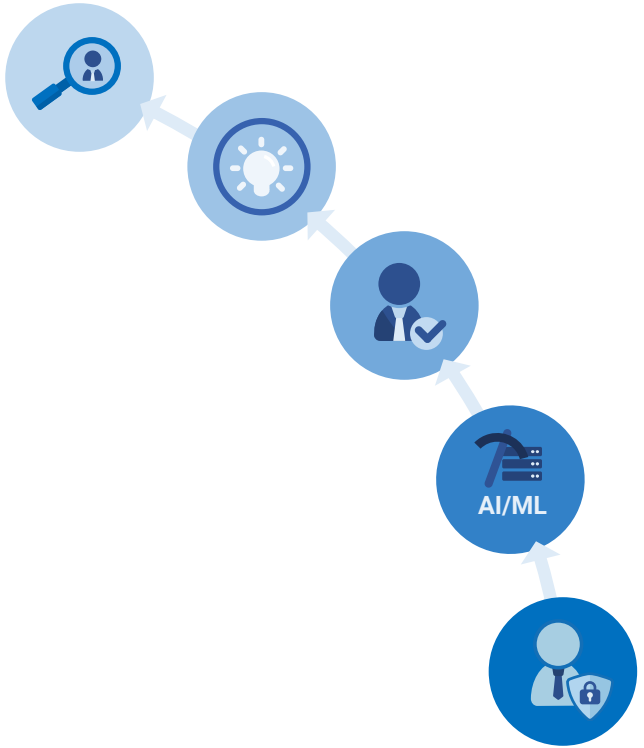
Evolveum

Bottom-Up Approach

1) Start with ordinary RBAC
2) Mine business roles (AI/ML)
3) Assign business roles automatically
4) Make smarter roles
5) Review/decommission old roles

Repeat as necessary

Future: policy mining



Evolveum

MidPoint 4.8

- A powerful IGA platform
- Policy-driven RBAC
- Organizational structure
- Simulations
- Role mining
- … and much more

Evolveum

Benefits of Policy-Driven RBAC

- Practical, available today (midPoint 4.8)
- Iterative and incremental
- It works, even if the policy is unknown
- A safe approach (simulations)
- Policy encapsulated into manageable pieces (roles)
- Long-term sustainability

Evolveum

Conclusion

- Both RBAC and PBAC/ABAC fail
- A combined approach is necessary
- Policy-driven RBAC
- A bottom-up approach assisted by AI/ML
- Available in midPoint today

Evolveum

Thank you for your attention

Do you have any **questions**? Feel free to contact us at **info@evolveum.com**.

Follow us on social media or **join us** on GitHub or Gitter!

 /Evolveum

 @Evolveum

 /Evolveum

 /Evolveum

 /Evolveum

 /Evolveum

Evolveum