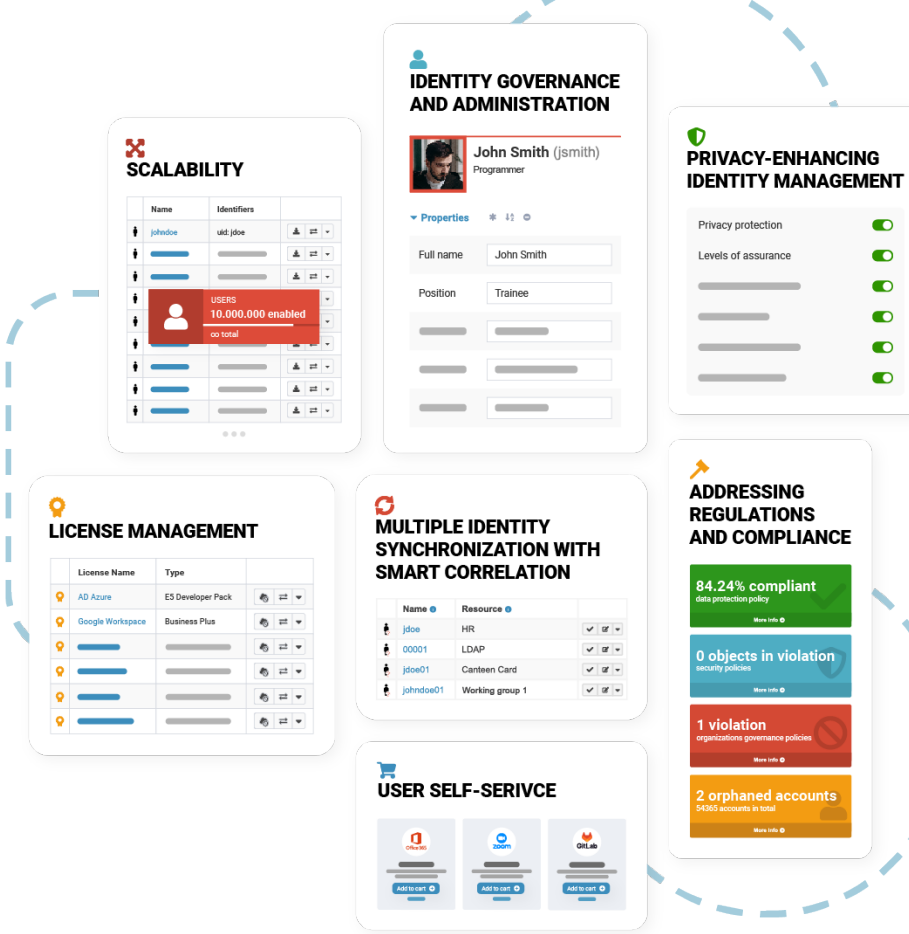
Advancing MidPoint With IGA Principles

Slavek Licehammer / December 2022

MidPoint

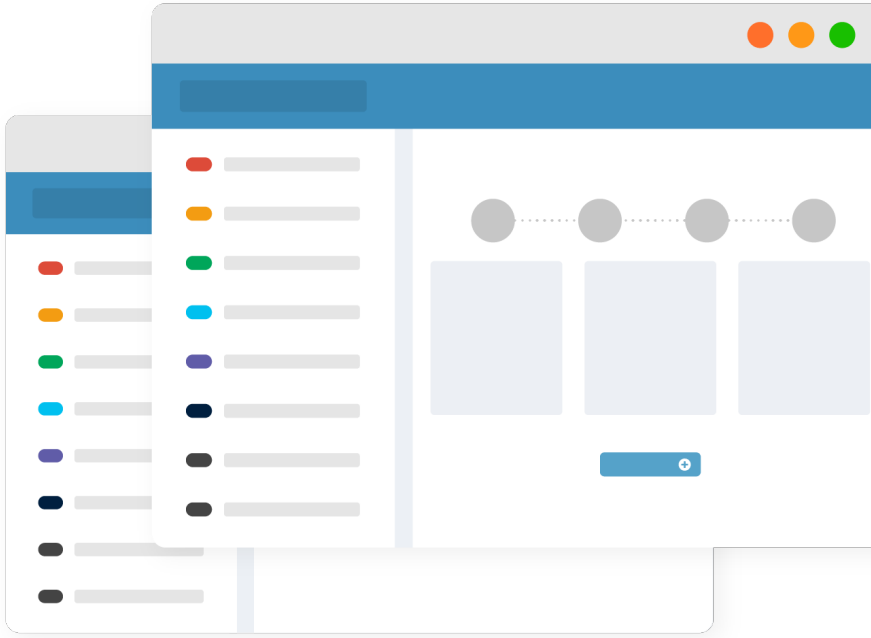
- Open source IdM and IGA platform
- Flexible and customizable solution
- Strongly influenced by academia
- One of Trusted Access Platform components



Evolveum

MidPoint - News

- GUI improvements
  - Customization
- Smart correlation
  - ID Match integration
- Open ID Connect support
- Axiom query language improvement
- Request access wizard
- Resource definition wizard
- Better containers and Kubernetes support



Evolveum

IGA

Identity Governance and Administration

Principles

- Focus on „business“ users
  - Shift from engineers
- Visibility
- Delegation of responsibilities
- Processes
- Automation
- Security

Evolveum

Motivation

- Empower users
- Remove burden from technical staff
- Speed up organizational processes
- Maintain order
- Reduce costs
- Digital transformation

Evolveum

Motivation

- Empower users
- Remove burden from technical staff
- Speed up organizational processes
- Maintain order
- Reduce costs
- Digital transformation

Evolveum

Areas

- Visibility
  - For non-technical users
  - Reports, audits
  - Risk analysis
- Policies
  - Security
  - Automation
  - Compliance

Evolveum

Visibility

- „Who has access where and why“
- Understanding for non-technical users
  - Understanding own accesses
- Business, technical, application roles
- Concept of application
  - Member of AD Group vs access to WiFi
- Manual access rights management
  - Utilization of organizational structure

Evolveum

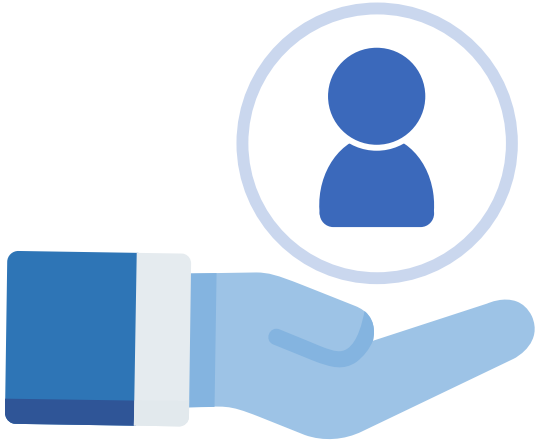
Reporting, Dashboards

- Overview on any level
- Easier debugging, monitoring
  - Notifications
- Audits
- Security
- Compliance
- Risk analysis

Evolveum

Role Request

- Self-service
- Fast and easy
- Empower end users
- User understand what role is needed
- Combination with other processes
  - Approvals, certification, expiration
  - Role mining



Evolveum

Role Engineering

- Preparing roles for role request
- Requires application and IdM experts
- Long term process (day)
- Can be automated
  - Application inventory
- Separate it from role assignments/requests

Evolveum

Approvals

- Approval for selected actions
  - Triggered by self service
  - Triggered by other events (e.g. adding user to role or group)
- Multistage approvals
- Deputies
- Escalation
- Don‘t overuse it
  - Notification

Evolveum

Access Certification

- Check manually added rights
- Crucial for maintaining order
- Scheduled campaign
- Lightweight process
  - Easy for reviewers

Evolveum

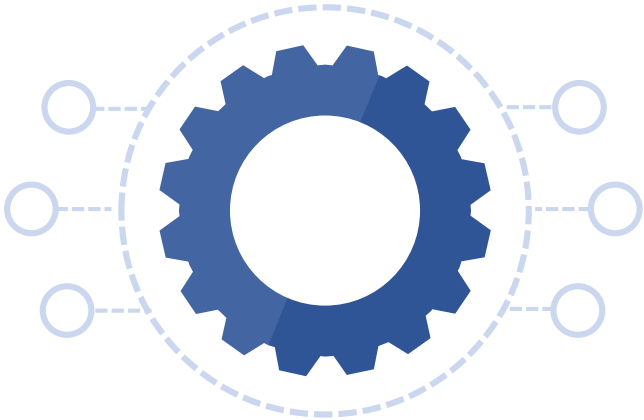
Policies

- Enforce policies within IdM
  - Segregation of duties, approvals, compliance, lifecycles
- Reporting
- Policy remediation
- Compliance
- Risk analysis

Evolveum

Global Integration and Processes

- MidPoint can work with any identity object
  - Objects/identities are created outside IGA
  - IGA responsible for: relations, rights
- Application catalog
- Identity of devices
- Entitlement management
- Organization wide workflows



Evolveum

Where Are We With MidPoint?

- Focusing on visibility
- Self-service – done
- Approvals – done
- Access certification – done
- Policies – partialy done
- Processes – partially done
- Notifications, reports, dashboards – done

Evolveum

Conclusion

- Visibility and policies
  - „Who has access where and why“
- IGA is complex
- IGA bring lot of benefits
- midPoint is IGA platform
- New IGA-related features in midPoint 4.7

Evolveum

Thank you for attention

If any questions occur, feel free to ask at **slavek@evolveum.com**

Also **follow us** on our social media for further information!

 /Evolveum

 /Evolveum

 /Evolveum

 @Evolveum

 /Evolveum

Evolveum