2nd Annual

MidPoint Community Meetup

# Privacy, Identity, and AI

May 2026

Evolveum

Martin Špánik
CISO & Compliance

Radovan Semančík
Software Architect

# AI Everywhere

- GenAI is everywhere
- It is transforming the world around us,
  for better or worse
- We may love it, we may hate it,
  but we cannot ignore it

## AI Everywhere

## versus

## Security, Privacy, Reliability, Fairness, ...

- GenAI is everywhere
- It is transforming the world around us, for better or worse
- We may love it, we may hate it, but we cannot ignore it

- Who has my data?
- How are my data used?
- How reliable are AI results?
- Does AI really make us more efficient?
- What do the machines know about me?
- Can AI be subverted to harm me or others?
- What can AI agent do on my computers?

## AI Everywhere

## versus

## Security, Privacy, Reliability, Fairness, ...

- GenAI is everywhere
- It is transforming the world around us, for better or worse
- We may love it, we may hate it, but we cannot ignore it

- Who has my data?
- How are my data used?
- How reliable are AI results?
- Does AI really make us more efficient?
- What do the machines know about me?
- Can AI be subverted to harm me or others?
- What can AI agent do on my computers?

**Is AI helping us or destroying us?**

# Privacy, Identity, and AI
## Comedy in Five Acts

**Dramatis Personæ**

**Martin Špánik**
manager – devil's advocate
AI proponent

**Radovan Semančík**
old grumpy engineer
AI opponent

# Prologue: Golem of Prague

- Jewish legend from 16th century
- Rabbi Yehuda Löw ben Bezalel a.k.a. *Maharal*
- Golem created out of clay from the Vltava river, to protect Prague ghetto from pogroms
- Brought to life using magic *shem*
- The golem went rampant
- Rabbi Löw removed the *shem*, deactivating golem


Illustration by Philippe Semeria (CC:BY)

אמת
emet (truth)

מת
mēt (death)

# Act I: Benefits of AI

- Efficiency boost
- Individuals report huge efficiency increase
- Produce ‘good enough’ results quickly
- Good for research, routine communication
- Bad for where ‘good enough’ is not sufficient
- AI is cheaper than people

- Slop, hallucinations
- Companies see almost no efficiency increase
- Redirecting workload (reviews)
- Good for brainstorming
- Disaster for precision work
- Social and environmental impact

# Act II: AI in the Clouds

- Low cost to start - no infrastructure investments necessary
- Great in internal knowledge - summarize long documents in seconds, prepares emails
- Using Office 365 – Microsoft already has the data

- AI hyperscalers:
  too big, too powerful, too unhinged
- Massive data sharing
  Data centralization in few big companies
- No transparency, no oversight
  How exactly are they using the data?

Evolveum

2nd Annual
MidPoint Community Meetup

# Act III: AI in Cybersecurity

- AI can detect attacks
- AI can detect vulnerabilities
- Fighting fire with fire –
  can't bring a knife to a gunfight
- Levels the chances for small teams
- Fast response, fast remediation

- AI helps attackers much more than defenders
- False positives → alarm fatigue
- We are not wining
- False sense of security
- Treatment of symptoms rather than cure:
  cybersecurity is much more than "no vulnerabilities"

# Act IV: AI Coding

- AI can produce a lot of code very quickly
- Vibe coding: enabler – providing results
- Good results for smaller components (connectors)
- Shorten development time dramatically
- Teams with AI will outpace teams without it

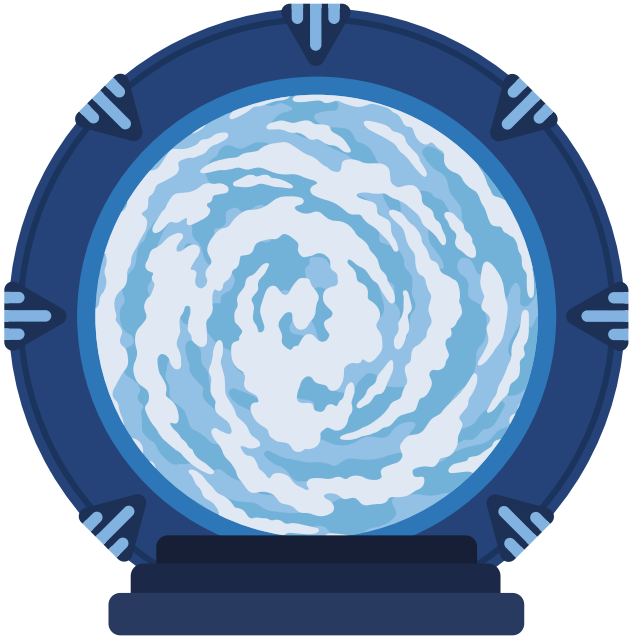
- Is it *good* code though?
- Vibe coding: cybersecurity disaster
- Still requires experienced people in the team
- Short-term advantage, long-term catastrophe
- Bottlenecks move:
  review, architecture, security, decisions

Evolveum

2nd Annual
MidPoint Community Meetup

# Intermezzo: midPilot

- AI assistant for rapid application onboarding: quickly connect a system (resource) to midPoint
  - Create connector (REST, SCIM, DB)
  - Suggest configuration (mappings, correlation, etc.)
- Using AI to produce *configuration* rather than code (whenever possible)
- Human review at every (risky) step
- Clear marking of AI suggestions
- LLM model hosted by Evolveum (or local)



# Act V: AI Agents

- Agents make AI immensely powerful
- Can work across tools – in the ecosystem
- Useful for repetitive operations
- Best as junior assistants
- Reducing boring tasks

- Agents make AI way too powerful
- The more tools agent can use, the larger attack surface.
- Current AI agents can be malware loaders
- Acting with full permissions
- Insufficient constraints (sandbox, guardrails)
- No mature solution for agent security yet

Evolveum

2nd Annual MidPoint Community Meetup

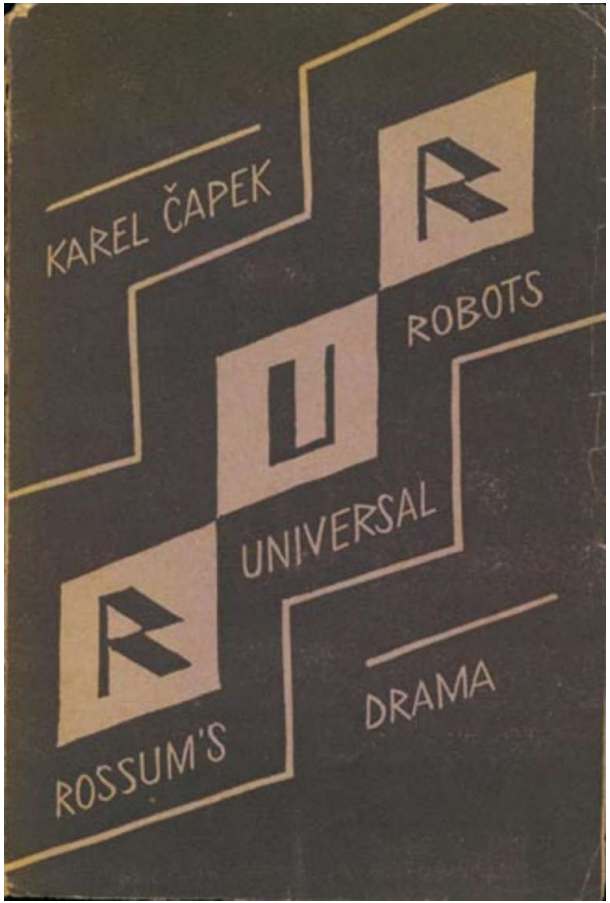
# Conclusion

- Use AI locally for sensitive data
  - Avoid uncontrolled data sharing
    (seems to be cheaper anyway)
- Check AI outputs
  - Always check AI output when you make decisions
    (where “good enough” is not enough)
- Beware AI agents
  - They are efficient, but learn to use them safely
    (chatbots are mostly safe)
- AI requires skilled people in the loop
  - AI is not going to replace experts anytime soon,
    it may make them more efficient (if used well)

# Epilogue: R.U.R.

- Karel Čapek (1890-1938)
- Rossum's Universal Robots (1921)
- Introduced the word "robot",
  invented by Josef Čapek
- Exploring interaction of robots and humans

- MidPoint 4.11 "Čapek"



# THE END

Evolveum

# Thank you for your attention

**Feel free to ask your questions now!**

2nd Annual MidPoint Community Meetup