GOVERN ROVO BEFORE IT GOVERNS YOU

A practical guide

viadee
IT-Unternehmensberatung

Successful AI Adoption

Strategic

Goals and Vision

Boards

Budget

Tool Selection

Out-of-the-Box vs. Custom

Processes / Use Cases

Opeartional

Data

Integration

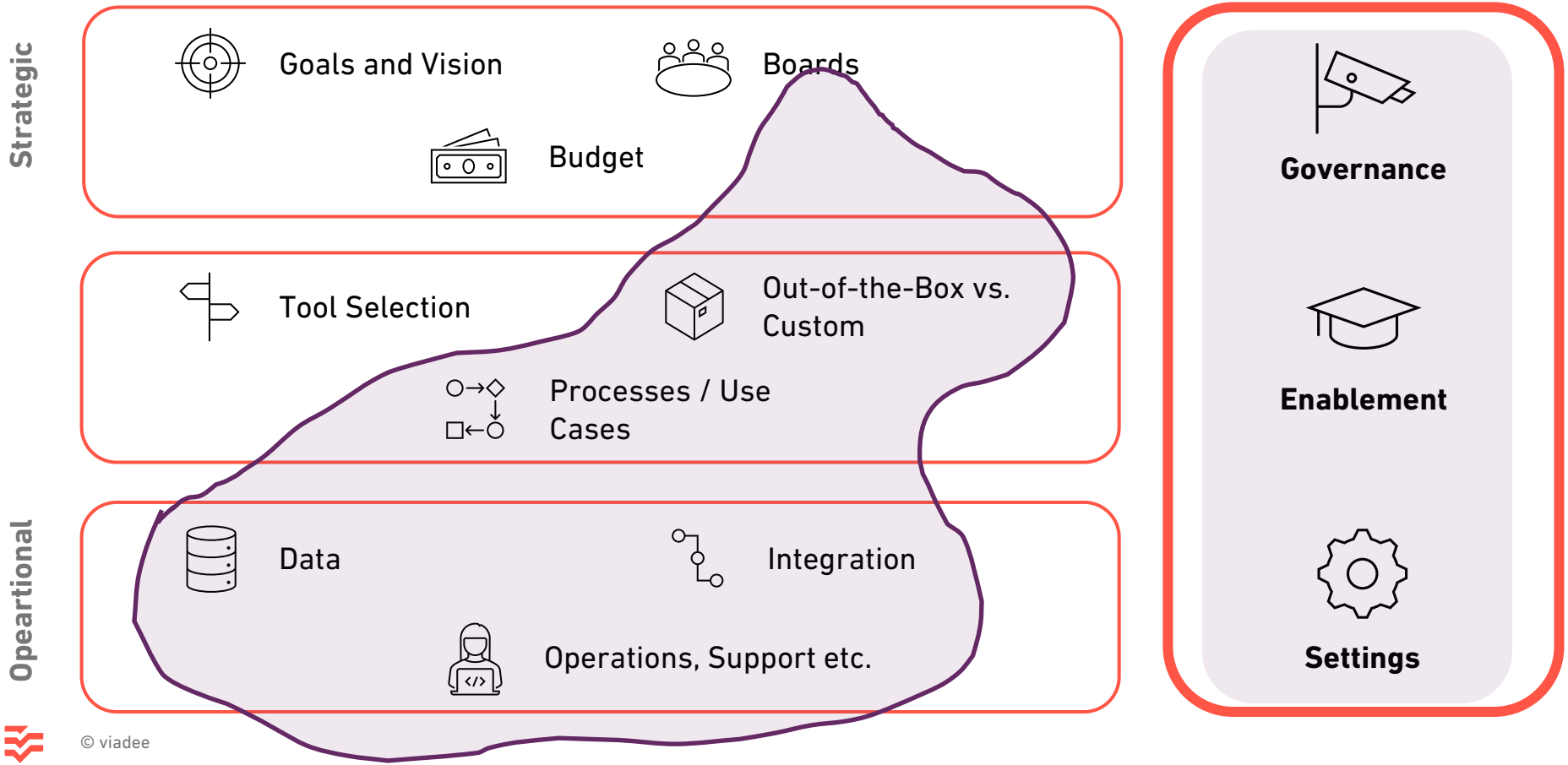
Operations, Support etc.

Governance

Enablement

Settings

Successful AI Adoption



viadee

More than 250 Consultants in Münster, Köln & Dortmund, that develope Software, Process and Organisations with Empathy, Curiosity and Pragmatism.


BPM & Prozessautomatisierung


Quality Engineering


Projektmanagement


Organisationsentwicklung


IT-Sicherheit


Data & AI


Cloud-Architekturen & -Plattformen


Business Analyse


Softwareentwicklung & -architektur

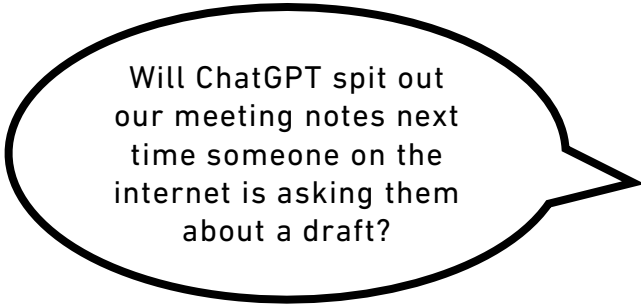

Atlassian Beratung

Meet Grumpy George

Everyone has at least one George in their company.

Will ChatGPT spit out our meeting notes next time someone on the internet is asking them about a draft?

What Atlassian does



- 3rd Party LLMs are not trained with Company data

AI Trust | Atlassian

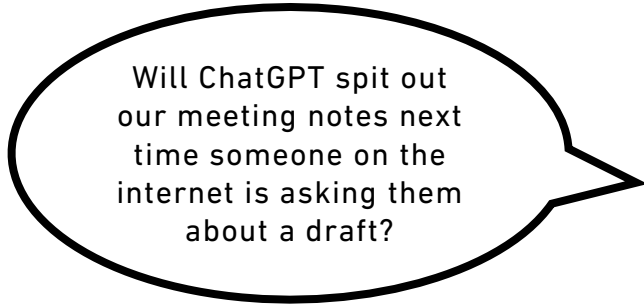
- EAP (Enterprise and US only) for Atlassian-hosted LLMs

Atlassian-hosted LLMs | Atlassian Support

- Data Contribution Policy: Data is used to improve Products and AI services

Data practices built for responsible AI | Atlassian

What you need to do



- Accept it.

- Inform Users

Will Bob see my private content in Rovo?

What Atlassian does

- Rovo Search & Chat respect User Permissions
- Rovo Agents in Chat respect User Permissions
- Agents in Automations run with specific Account permissions

Agent Accounts in EAP

What you need to do

- Inform about risk

- Limit Automation creation

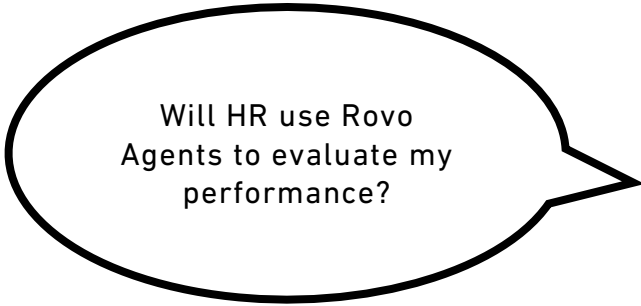
Permissions required to manage automation flows | Cloud automation Cloud | Atlassian Support
Manage who can create in Studio | Rovo Studio | Atlassian Support

- Only Agent Owners are allowed to add Agents to Automations

- Use Agent Accounts when available and appropriate

Will HR use Rovo Agents to evaluate my performance?

What Atlassian does



- LLM system prompts

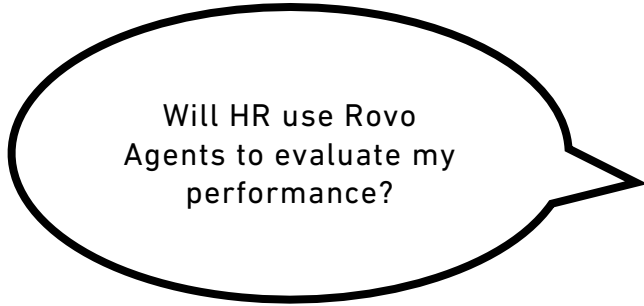
- Atlassian system prompt respects EU AI Act

Atlassian's proactive approach to EU AI Act compliance | Atlassian

- Agent Creation Permissions & Agent Verification

Verify Rovo agents in your organization | Rovo | Atlassian Support

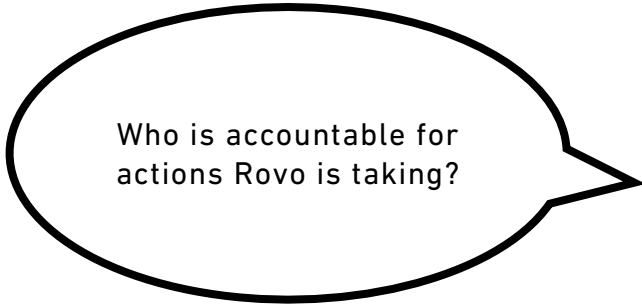
What you need to do



- Prohibit certain practices
- Approval process for Agents
- Regularly check Use Cases & double check Agents created

Who is accountable for actions Rovo is taking?

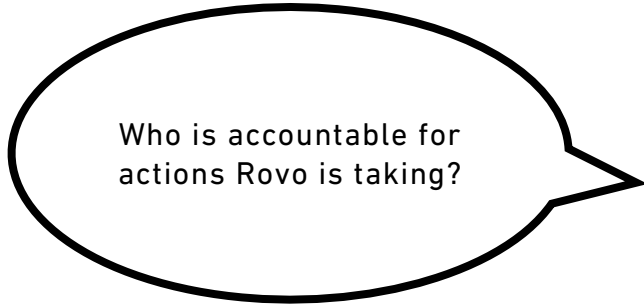
What Atlassian does



- Acts as User when Human in the Loop

- Agent Accounts in EAP

What you need to do



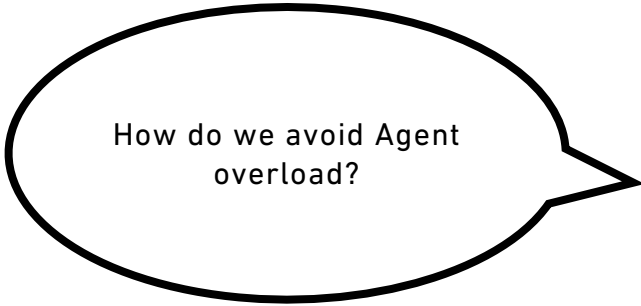
- Define Accountability

- Emphasize validity checks

- Use Agent Accounts when available and appropriate

How do we avoid Agent overload?

What Atlassian does



- „Verified“ Agents

  Verify Rovo agents in your organization | Rovo | Atlassian Support

- User Permissions in Agents

  Rovo agent permissions and governance | Rovo | Atlassian Support

- Agent Insights

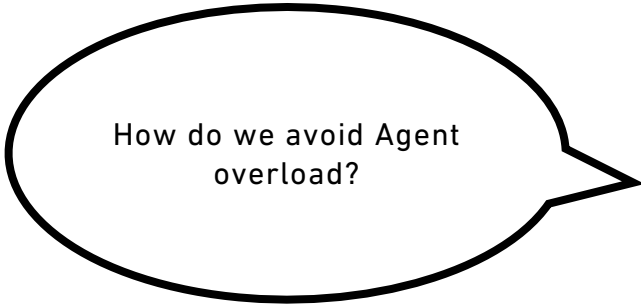
  Track how often a Rovo agent is used | Rovo | Atlassian Support

What you need to do

- Define Verification Process and criteria

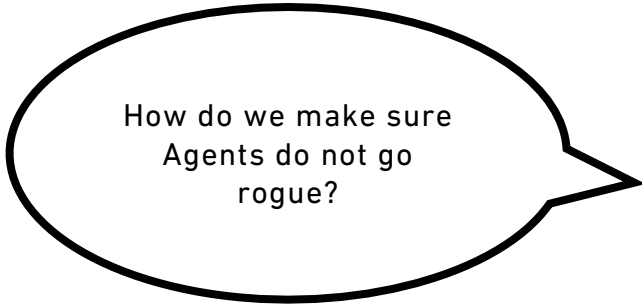
- Agent Best Practice: Limit Users

- Regularly check Agent usage



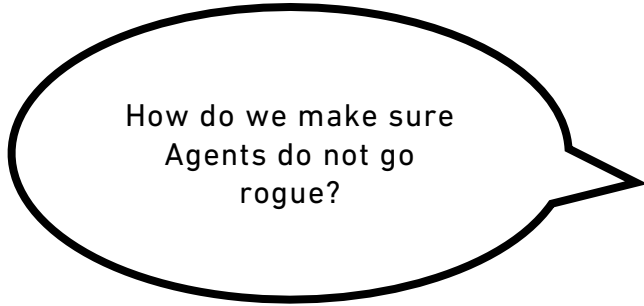
How do we make sure
Agents do not go rogue?

What Atlassian does



- Human in the Loop
- Agent Accounts & Permissions
- Announced: Autonomous Agents in Automations

What you need to do



- Agent Best Practice: Least Privilege

Rovo agent tools | Rovo | Atlassian Support

- Agent Best Practice: Sandbox & Shadow Mode

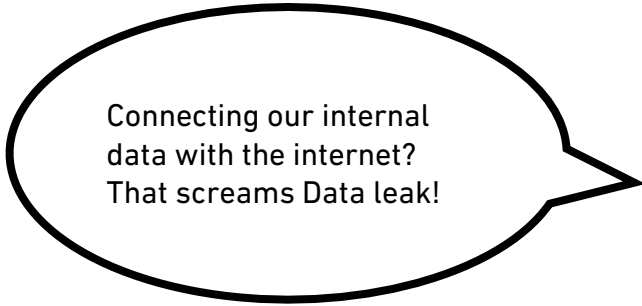
- Human in the Loop where sensible

- Limit MCP/CLI access

Configure Atlassian Rovo MCP server permission | Atlassian Support

Connecting our internal data with the internet? That screams Data leak!

What Atlassian does



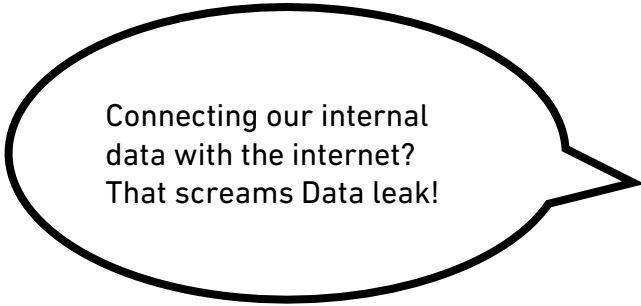
- Disable Websearch

Manage a web search option for Rovo | Atlassian Support

What you need to do

- Option 1: Disable

- Option 2: Inform



I keep getting Ads for the Browser Extension but it requests access to everything!

What Atlassian does

- Push users to install it

What you need to do

- Option 1: Disable centrally in Edge/Chrome settings

- Option 2: Inform

- Option 3: Ignore

Rovo keeps asking me to connect my OneDrive but I am not allowed to.
Finally a useful feature, and I can't use it?!

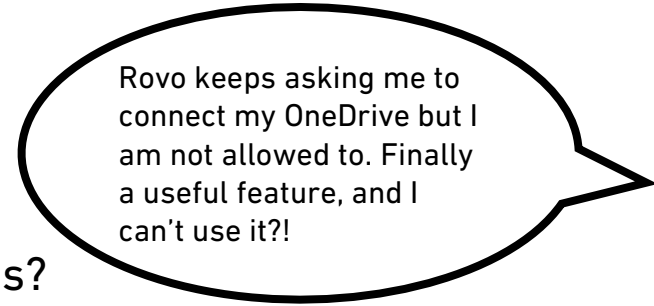
What Atlassian does

- Various Rovo Connectors
  Available Rovo Connectors | Atlassian

- Respect User Permisssions (or use a technical User Account)

- All Connectors down to Admin settings

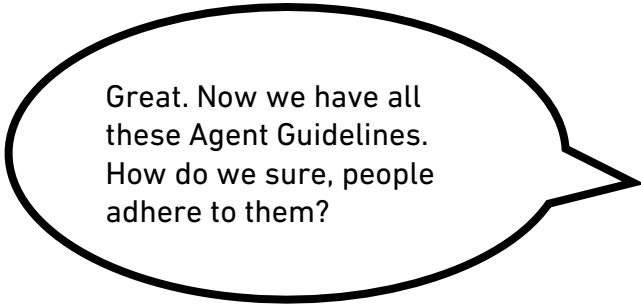
What you need to do



- Risk assessment: Duplicate Data in multiple systems?
- Try to set some Standards in the AI Tool jungle
- Only add connectors that have value > risk

Great. Now we have all these Agent Guidelines. How do we sure, people adhere to them?

What Atlassian does



- Rovo Studio Permissions

  Manage who can create in Studio | Rovo Studio | Atlassian Support

- Feature Request/Announced: Overview of Agents incl. Instructions

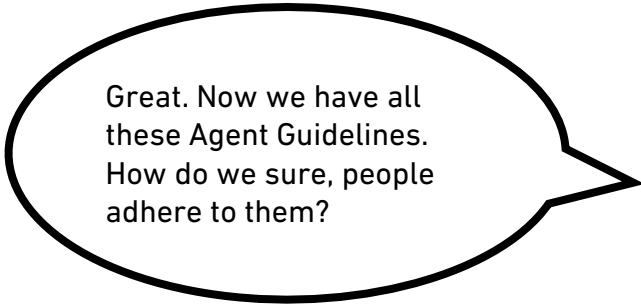
- Announcement: Guard Detect in Rovo Chat

What you need to do

- Make Policy mandatory to acknowledge

- Restrict Agent creation

- Regularly check Compliance



Successful AI Adoption

Strategic


Goals and Vision


Boards


Budget


Tool Selection


Out-of-the-Box vs. Custom

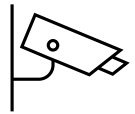

Processes / Use Cases

Opeartional


Data


Integration


Operations, Support etc.


Governance


Enablement


Settings

To sum it up

While Atlassian is lacking major Governance controls on a technical level,
a good **Usage Policy** is the only way to

Govern Rovo before it Governs you.

Stay connected

Rebekka Heilmann

Head of Atlassian Consulting

rebekka.heilmann@viadee.de

+49 162 608 9938

https://www.linkedin.com/in/rebekka-heilmann/

viadee

IT-Unternehmensberatung