Your AI acted. Who authorised it?

AI access is being solved. Authority is not.

AI tools now read your code, query your data and call your internal systems. Your logs may show what happened. **They may not show why it was allowed.** And an action can be permitted without ever being intended.

66% of developers use AI assistants or agents at work.

24% say their organisation provides approved AI tools and guidance.

Stack Overflow, 2026 ↗

◆ THE EXECUTIVE PROOF TEST

FORWARD TO PLATFORM, SECURITY AND RISK

Could you prove this tomorrow?

Your approved coding agent reads a hidden instruction in a repository. It then calls an internal tool, using permissions you gave it. The call succeeds. Was that meant to happen? Can your teams show:

1. **Who** started it, and on whose authority?
2. **What** it tried to do, and to what?
3. **Which** rule was checked *before* it ran?
4. **Which** model or tool ran, and what happened?
5. **Can** you rebuild the whole story from records you own?

Permission is not the same as authority. If you're not sure, find out before your next AI rollout.

"BUT WE ALREADY HAVE…"

YOU HAVE	IT MAY NOT TELL YOU
Access control	Who was behind an agent's action
Model gateway	Whether the agent's tool use was allowed
Vendor logs	The full story, in records you own
AI policy	Whether it was applied to this request

These may all exist. The question is whether they link into one chain you can prove.

THE NEXT STEP

Get the answer in two weeks.

Pick one real AI workflow: an agent, its model and the tools it can call. We trace it end to end against the five questions.

- A written gap report
- Fixes, in priority order
- A target architecture

BOOK A 20-MINUTE CALL →

WHY PARAKLETOS



Jason Southgate
FOUNDER

Almost 30 years building production systems where failure is expensive. University of Cambridge programme in data science, ML and AI.

EXPERIENCE INCLUDES

A tier-one Nordic financial services company

A premier German automotive group

A premier Nordic retail group

A tier-one cloud managed services provider

WE BUILD IT, TOO

Built, not just theorised. **Governator**, our AI control plane, links identity, policy checks, model and tool access, and evidence you own.

Prior work led by Jason, described by sector. No endorsement implied.