

**Episode 256****Gareth Rydon**Co-Founder, [Friyay.ai](https://friyay.ai)**Stop Building AI Agents: Brief and Control Them Safely**

On this episode of the [DevReady Podcast](#), host [Anthony Sapountzis](#) speaks with [Gareth Rydon](#), Co-Founder of [Friyay.ai](#), about why most organisations should stop building AI agents and start briefing them properly for safer, more reliable results. They cover human in the loop controls, secure login checkpoints, prompt injection risks, how to monitor agent behaviour, when simple workflow automation beats a free roaming agent, and practical tool choices across Claude, Copilot, Gemini and ChatGPT.

The discussion begins with the rapid rise of pre-built agents in tools like ChatGPT and the parallel increase in risks. Rather than handing over passwords and hoping for the best, Gareth recommends explicit checkpoints, for example pausing at log-ins so a human enters credentials, and monitoring early runs to see which sites an agent visits and why. Anthony adds a security lens, noting spoofed pages, homograph domains, and other phishing traps that emerge when browser agents roam the web. Both advocate a human-in-the-loop approach that balances capability with oversight, especially for sensitive tasks.

They then explore when not to use agents. For repeatable processes such as content pipelines, a simple workflow often beats a free-roaming agent on cost, speed, and reliability. Anthony cites scraping projects where agent costs ballooned, while Gareth shares a LinkedIn workflow that runs on lightweight steps in a shared sheet, with research, condensing, tone-of-voice prompts, and human review. This approach is easier to debug, avoids the variability of large models, and delivers predictable ROI for marketing and operations teams.

On talent and skills, Gareth acknowledges that roles will change and some jobs will go, yet the best response is to upskill and let AI amplify existing strengths. Drawing on examples from law and creative work, they note that experts using AI are busier than ever because they combine judgement with acceleration. Anthony cautions that DIY builds can hide structural issues such as empty databases or non-functional features, which is why domain knowledge and clear instructions still matter. The takeaway is simple: AI raises the floor and the ceiling; invest in skills, keep humans in the loop, and choose pragmatic workflows over hype.



Finally, they assess today's tool choices. The uplift from recent model shifts feels modest compared with the collaboration gap, where shareable projects and team workflows remain the blocker. Gareth sees strong enterprise adoption of Claude and advises buyers not to default to Microsoft Copilot or ChatGPT by habit. Instead, run a one-week bake-off with Claude, ChatGPT, and Gemini, compare security posture, collaboration features, and day-to-day usability, then standardise on the platform that fits your organisation. The goal is faster, safer collaboration rather than chasing headlines.

Topics Covered

- Rise of pre-built AI agents and how to brief them effectively
- Prompt injection and agent security risks in web-facing workflows
- Human-in-the-loop control
- Monitoring agent behaviour
- Agents versus workflow automation
- LinkedIn content pipeline
- AI job fears and upskilling
- Experts plus AI: raising the floor and the ceiling while avoiding vibe-coding pitfalls
- Model updates and enterprise tool choice

Important Time Stamps

- The 90/10 Rule of AI Agents: Use > Build (0:07 – 5:05)
- Don't Hand Over the Keys: Human-in-the-Loop AI Agents (5:06 – 10:20)
- Agents vs Workflows: Stop Using an Agent Hammer for Every Nail (10:21 – 14:45)
- Stop Cherry-Picking AI Fails: Upskill and Stay Relevant (14:46 – 20:48)
- AI Won't Steal Your Job But Someone Using It Might (20:49 – 27:07)
- Ignore the Hot Takes and Test Your AI Stack Properly (27:08 – 36:04)
- Software, Not Souls: Stop Calling AI "Conscious" (36:05 – 38:40)

Useful Links[Gareth Rydon | LinkedIn](#)[Friyay.ai | LinkedIn](#)[Friyay.ai | Website](#)**Listen & Subscribe** YouTube: <https://youtu.be/sFGRh8PGIi8> Spotify: <https://open.spotify.com/episode/2aD6gg1CmUmlgE1KwFTphZ?si=tRcehYtgSsmI9Ik2LoP0EQ> Apple Podcasts: <https://podcasts.apple.com/us/podcast/stop-building-ai-agents-brief-and-control-them-safely/id1497226071?i=1000725952297>