

Agent permissions become a product decision, as Fin shows the payoff of a shared AI platform

PM Daily Digest

2026-10-13

Agent permissions become a product decision, as Fin shows the payoff of a shared AI platform

By PM Daily Digest • October 13, 2026

Several sources argued the same thing: what decides whether teams can trust agents is the controls around the model, meaning permissions, review steps and skills. Also covered: Fin's AI transformation, AI-native PM hiring, and practical advice on adoption and launch decisions.

Agent permissions are now a launch decision

Aakash Gupta retold Alexey Grigorev's incident. Claude Code ran `terraform destroy` and wiped out DataTalks.Club's production setup after it unpacked an old state file. Grigorev let it go ahead because "That looked logical" [1]. AWS support found a snapshot, and everything was back after about 24 hours [1]. Grigorev changed four things afterward: agents no longer run infrastructure commands, a person reviews every plan, he runs every destructive action himself, and he is looking at separate development and production accounts. None of them involved changing the model [1]. Gupta tells PMs to settle three questions with their engineering lead before launch: which actions an agent can take on its own, which need a human, and which it should never be able to reach [1].

Others made the same point the same day. Runlayer launched secured, policy-governed connectors for the Muse agent. Its pitch: some companies block Muse, and others have seen it leak data and send unauthorized emails [2]. Hiten Shah's takeaway: an agent having permission to do something doesn't mean it should. "The ability to stop one action is what lets companies say yes to thousands of others" [3]. Shah also thinks some of the next big waves of AI adoption could come from better harnesses around existing models, even without major model improvements [4]. In The Product Compass, Paweł Huryn shares the "ask first" rules for his seven-bot Grok product team. They cover outside messages,

anything customers can see, contacting customers or competitors, payments, and decisions that are high-risk or hard to reverse [5]. One of his bots checks competitors' pricing pages, changelogs and X posts every week. If nothing changed, it stops; if something did, it reports why it matters [5].

Skills are where team know-how lives

Sachin Rekhi says Fin is seeing a 3x increase in engineering velocity, while many teams remain stuck at about 30%. He credits Fin's AI platform: a single agentic platform for the whole team, a shared skills marketplace anyone can publish to, and systems that let designers ship code to production [6]. Rekhi is promoting his course here, and Fin's Brian Scanlan is its first guest speaker [6].

Two posts show why skill design matters. Shah asked Claude why Linear was losing deals to Jira, with no interviews or deal records to go on, and got eight reasons. With his team's win/loss skill, Claude said it couldn't know yet and listed the evidence to collect [7]. That skill is one of 16 product-marketing skills his team has open-sourced [8]. Gupta found that Claude scans only each skill's name and description until it picks one. In his test of 25 skills, one with a 37-character description was never chosen: "the description is the skill" [9].

Hiring and go-to-market

- **Product builders.** Gupta and HelloPM's Ankit Shukla report that LinkedIn replaced its APM program with Associate Product Builders. They also say 30%+ of PM job descriptions ask for AI skills, most often picking the right use case [10]. Their suggested path: build in stages from a PRD Gem to shipping in Claude Code, then post the work on GitHub with a Loom demo [10].
- **Selling to agents.** Paul Graham suggested a nerdy founder might want an outgoing sales cofounder. The founder said no, because most of his sales would be to agents, and Graham admitted he "could be right" [11].

Practitioner advice from Reddit

- **Developer-tool trials.** Keep the first trial to one existing task, run it alongside the current approach, and make it clear how to stop and remove the tool. Watch where hesitation comes from: setup, permissions, trust in the output, or making the internal case to buy [12]. Another commenter suggests a read-only "shadow mode" that shows the difference without writing anything to production [13].
- **Beta scope.** A founder with one of six modules ready [14] was advised to show only that module, because "five future tabs make a working product feel unfinished" [15].
- **Small B2B markets.** A founder selling into a conservative niche said the first PO came from offering a new capability priced low enough that it didn't take much of the buyer's budget [16]. That fits a commenter's

view that the real trigger is the buyer making room in the budget for a second tool [17].

- **Build vs. buy.** A vibe-coding platform is weighing Merge.dev’s model routing against its own stable control plane. The poster also says two exec buyers they spoke to described very different pricing [18].
- **Stale demos.** DemoForge is a free, MIT-licensed tool. You write the demo once as a script of clicks and narration, then re-record it with one command after each release [19].

Pushback on Lenny’s podcast

A popular r/ProductManagement thread argued that Lenny’s podcast has drifted toward AI and an executive audience paid for by sponsors [20]. One commenter called it “not a front-line PM’s podcast” [21]. Another said it now covers practice “through the lens of administrators” [22]. In the same period, Lenny kept promoting Josh Woodward’s case that companies need people “plugged into the hive mind” at the frontier [23].

Sources

1. substack
2. X post by @berman66
3. X post by @hnshah
4. X post by @hnshah
5. I Built a Product Swarm With Grok Bot
6. X post by @sachinrekhi
7. X post by @hnshah
8. X post by @hnshah
9. substack
10. substack
11. X post by @paulg
12. r/startups comment by u/DanielatUntrapped
13. r/startups comment by u/alexid95
14. r/startups post by u/AggravatingCoyote186
15. r/startups comment by u/alexid95
16. r/startups comment by u/rt2828
17. r/startups comment by u/alexid95
18. r/startups post by u/Free-Pickle-3621
19. r/ProductManagement post by u/deegit_00
20. r/ProductManagement post by u/Victor_eu
21. r/ProductManagement comment by u/cost4nz4
22. r/ProductManagement comment by u/FamouslyUnknown
23. X post by @lennysan