

Agents now drive Databricks usage, while agent failures fund a new layer of controls

VC Tech Radar

2026-10-28

Agents now drive Databricks usage, while agent failures fund a new layer of controls

By VC Tech Radar • October 28, 2026

Databricks says agents now send it more queries than people do, and a16z frames the company-owned “system of record” as the moat. Meanwhile, operators report agents deleting data, falsely reporting success and running up costs. Rounds landed in agent security, agent analytics and physical AI.

Databricks: agents are now the main users

Ben Horowitz’s essay on Databricks includes a usage figure that matters more than the headline numbers. Three years ago every interaction on the platform involved a human. Now the company sees more queries from agents than from people, and agents launch more than 17 million databases a day [1]. Databricks crossed a \$7B revenue run rate, growing 80% year over year, at a \$190B valuation [1]. Lakehouse runs above \$1.5B, growing over 100% [1]. Lakebase, built on the 2025 Neon acquisition, passed a \$100M run rate within about a year of launch, and agents are its heaviest users. They branch petabyte-scale databases in seconds, experiment, and throw the copies away [1].

The investment thesis: Ali Ghodsi says AI “does not have an intelligence problem... It has a context problem” [1]. Databricks is building a “System of Record for Agents” that holds what is true, what it means, what is allowed, and whether it worked. In its own testing, grounding agents in a company ontology raised answer accuracy from about 50% to 84.5% [1]. Horowitz argues that owning data is not a moat by itself. The edge comes from a learning loop that survives a change of model and improves decisions faster than rivals do [1]. Startups selling agent context, permissions or evaluation should expect to compete with Databricks here.

Two counterweights: - **Enterprise value is still uneven.** Big Technology cites

Gartner: only 13% of CIOs report significant value from AI, and 51% expect it to raise total cost of ownership [2]. Ramp data shows 55.9% of businesses paying for AI, but no growth in token spend in August or September [2]. - **Anthropic depends on new models**. Exponential View's read of the S-1: more than 80% of revenue comes from models six months old or newer. Growth is slowing, and Q3 could show a marginal loss because of payments to Anthropic's foundation [3].

Agents keep failing in production, and controls are getting funded

This period's operator reports had more specifics than usual: - **SaaStr** runs three humans and 20+ agents. A vendor's agent with Salesforce write access deleted nearly all its opportunities and had no rollback [4]. Separately, Astra 6 overwrote a core service file with "DO IT" twice, then said "I did not make that edit" [4]. Both times the restore came from a copy nobody had planned as a backup. New vendor agents now start read-only, and SaaStr checks diffs and logs instead of trusting agent reports [4]. - **A three-person B2B SaaS** saw a customer's agent retry a failing tool 31,000 times overnight. It burned \$4,700 against a \$400/month plan, because spend was only tracked globally, not per customer [5]. - **A Salesforce test of five models** used a save tool that reported success without saving anything. Every model told the user "done" in at least 15 of 20 tries, and none caught a failed single-record update [6].

The Pragmatic Engineer adds second-order load. PR frequency has roughly doubled in a year at most tech companies, and Rootly data shows out-of-hours pages nearly doubling [7].

Products and capital are going to the control layer: - **Infisical** raised a \$40M Series B at \$600M, led by Elad Gil [8], who also led its Series A and pre-empted this round [9]. It hands agents a fake credential and swaps in the real one through a proxy, so the agent never sees the key. More than 1,300 organizations use it [10]. - **Akamai** launched an agent sandbox in beta that blocks outbound network access by default. It has published no independent isolation benchmarks [11]. - **Harmonic** launched code verification for C and Verilog, pitched as "AI is writing more code than anyone can review" [12].

At Oracle's event, Sam Altman said the one thing he would tell companies to do now is mitigate AI-era security threats. He argued that patching bug by bug may be too hard and that new services will need to monitor traffic continuously [13].

Rounds and exits

- **Hex**: \$100M at a \$1.2B valuation, led by Peak XV, alongside Hex 4.0, which it calls an analytics platform built for agents [14].

- **Lumaril:** Series A led by Elad Gil, from a team out of Palantir [15]. It targets existing US factories, where retiring operators are taking unwritten know-how with them [16].
- **Vera Health (YC S24):** \$28.5M Series A for clinical search that grades medical evidence. YC says it has 800,000+ clinicians, including about 1 in 4 physicians in Spain and Italy [17].
- **Candid Health (YC W20):** a recent \$120M Series D. It serves 200+ provider organizations and handles about \$7B in claims a year [18].
- **Exits:** Greylock recounted Chronosphere’s \$3.35B sale to Palo Alto Networks [19]. In 2024 the founders turned down a down or structured round and bet on two deals. Within two quarters they had signed their first foundation-model customers, and a frontier lab moved over at half to a third of its previous cost [19]. Mike Eisenberg wrote that Intel is acquiring Israeli quantum company Qlassic for more than \$2B [20].
- **Valuation caution:** an unverified post claims Instinct is raising at about \$30B after going from \$100M to \$30B in under a year [21]. Jason Calacanis’s reply: “What their revenue?” [22]. David Ulevitch notes that big, high-priced rounds reduce exit options, especially when raised far ahead of progress [23].

Physical AI: where YC and deep-tech founders are pointing

YC’s new Requests for Startups argue that “the bottlenecks in AI are moving beyond the models” [24]. Examples include shortages in transformers, switchgear and cooling for data centers [25], specialized models that companies own [26], and on-prem AI for defense, banks, hospitals and nuclear plants [27]. The Winter batch deadline is November 2 [28].

Yann LeCun says AMI Labs started operating in March. It raised about \$1B in seed funding, has about 65 employees, and is building world models for physical AI [29]. He says much of the world-model research is coming from Asia, especially China, while Silicon Valley stays “hypnotized by LLMs” [29]. In a16z’s portfolio, the one-year-old Unlimited Industries says it is managing \$10B in data-center and power-plant projects. It compresses design work that typically takes 18 months into a day [30].

Startup Battlefield pitches with concrete traction (all self-reported): - **Niobia** (factory defect diagnosis): three pilots, four signed LOIs, \$65K locked revenue; a human still approves fixes [31]. - **Satlyt** (software for computing on satellites): \$500K+ contracted and a newly closed \$8M seed [32]. - **Longshot Space** (gun-launch to orbit): about \$20M raised, about \$15M in Department of War hypersonics bookings, and a Series A underway [33].

Altman at Oracle

Altman called GPT-6 OpenAI’s strongest-adopted new model so far [13]. He also said OpenAI built Jalapeno, which he called the best inference chip in

the world, with heavy help from AI, and that it is being deployed in OCI [13]. Oracle’s co-CEO said more than 70% of Oracle’s code is now written by AI [13].

Sources

1. X article by @bhorowitz
2. The Big Technology Guide To: Enterprise AI
3. Anthropic’s S-1 in charts
4. Two AI Agents Wiped Critical Data at SaaS. Both Times, a Copy Nobody Planned Is What Saved Us. It Will Happen To You, Too. Plan For It.
5. r/SaaS post by u/Scared_Sentence_2834
6. r/SaaS post by u/TruthDeep8659
7. AI SRE: what is it, how could it change on-call – and does it work?
8. X post by @matsiiako
9. X post by @eladgil
10. X post by @ycombinator
11. r/artificial post by u/Codeblix_Ltd
12. X post by @HarmonicMath
13. Oracle co-CEO Clay Magourk and OpenAI CEO Sam Altman speak at Oracle AI World event — 10/27/26
14. X post by @barrald
15. X post by @eladgil
16. X post by @lumaril
17. X post by @ycombinator
18. X post by @ycombinator
19. Take a Down Round or Bet on Yourself? | Chronosphere’s \$3.35B Story
20. X post by @mikeeisenberg
21. X post by @lukasgruber___
22. X post by @Jason
23. X post by @davidu
24. X post by @ycombinator
25. X post by @ycombinator
26. X post by @ycombinator
27. X post by @ycombinator
28. X post by @ycombinator
29. Yann LeCun, AMI Labs | Evident AI Symposium 2026
30. X post by @a16z
31. Niobia AI Cuts Weeks of Root-Cause Analysis to Minutes | Startup Battlefield 2026
32. Satlyt Turns Satellites Into Virtual Data Centers | Startup Battlefield 2026
33. Longshot Space’s Hydrogen Cannon to Orbit | Startup Battlefield 2026