

AI security turns urgent as the eMudhra CA breach lands, while capital moves toward physical AI and agent infrastructure

VC Tech Radar

2026-10-21

AI security turns urgent as the eMudhra CA breach lands, while capital moves toward physical AI and agent infrastructure

By VC Tech Radar • October 21, 2026

This period's AI security failures, OpenAI's safety hire, new funding rounds in manufacturing, robotics and agent infrastructure, Google's compute constraints, and falling AI costs.

Security is now a basic assumption

A new case for the “vulnpocalypse” thesis arrived this period. Sarah Guo reports that eMudhra's intermediate CA private keys were tiny numbers like 4 and 56. Anyone could recover them in seconds and mint a trusted certificate for any site. Browsers have already blocked the bad certificates, but many servers, containers and devices still trust them. She traces the problem to a single bad key-generation script from 2025, which is now forcing a “Heartbleed-scale cleanup” [1]. Asked what share of token use will go to security in 2027, Guo relayed @dok2001's answer: “>50%” [2].

Leadership moves point the same way: - **Aleksander Madry is back at OpenAI** after what he now calls a sabbatical. He joins @merettm because, in his words, getting safety and security right “has to become a central priority” [3]. - **Dario Amodei** defended Anthropic's “race to the top” strategy. He said Anthropic had Mythos-class models in February but held general availability until June, when stronger cyber safeguards were ready, and probably gave up “a significant chunk of a several-month model lead.” He also said competitors sell against Anthropic by pointing to its strict bio classifiers [4]. - **Clem Delangue** said the Netflix documentary on the OpenAI agent attack on Hugging Face left

out the lack of agent containment and the fact that closed-model safeguards blocked Hugging Face’s defense. Hugging Face defended itself with an open model [5]. This continues the guardrail-refusal story from earlier briefs.

Market sizing angle: Vanta CEO Christina Cacioppo says AI attackers mostly chain many low-severity weaknesses rather than find zero-days. That pushes defenders toward fixing at machine speed [6]. She sees a constant pentest-and-patch product for customers who won’t pay \$150K for Wiz but “very well could pay 40 or 50” [6]. Separately, Vanta is absorbing token costs rather than marking them up. About 25% of its customers use the agent flow, and it is aiming for 75% [6].

Where capital went

- **Arda** (Bob McGrew) launched publicly with a \$160M Series A at a \$1.5B valuation. It has spent a year building with Anduril as its design partner. Today it helps manufacturers run manual assembly lines; next it plans re-configurable automated lines aimed at products now made by large workforces in Asia [7].
- **Daytona** raised a \$60M Series B at \$1B for its “Agent Cloud,” led by First-Mark. Angels include Patrick Collison, Tobi Lütke and Aravind Srinivas. The team has 35 people [8].
- **Eka Robotics:** a16z led the Series A. Eka builds a Vision-Force-Action model co-designed with its own robotic hands. The founders are Pulkrit Agrawal (MIT CSAIL) and Tuomas Haarnoja (formerly Google DeepMind) [9].
- **OpenAI acquired Orchestra Bio**, a drug-development coordination platform, to build on its Rosalind life-sciences models [10].
- **Salesforce is buying Braze** for about \$5.66B EV, a 58% premium [11]. Six weeks earlier, Braze’s stock fell 25% after a beat-and-raise quarter with 26% growth. SaaStr’s takeaway: companies growing in the 20s with little AI revenue may get their best price from a strategic acquirer, not a next-round lead [11].
- **Workday is acquiring C1.ai**, which governs access for both employees and AI agents under one lifecycle and audit trail [12].

Founder flows seem to agree with these rounds. One widely shared observation says smart young builders are moving from vertical agents into data/RL environments, physical AI, and wet-lab drug discovery [13]. Nathan Benaich replied “that checks” (anecdotal).

Physical AI: design gets easy, atoms stay slow

a16z argues AI will soon become a superhuman hardware *designer*, but building, testing and iterating will remain bottlenecks [14]. It names opportunities in simulation (Navier, Inviscid, Lanyon) and in suppliers and test software (Hadrian, Cofactr, Instrumental, Revel) [14]. Pat Gelsinger gave a chip example: AI

could produce a design in three months, but silicon processing takes nine [15]. On robot data, Mecka’s Josh Gao says the field is now at millions of hours, still “many orders of magnitude” short of autonomous driving [16]. He expects pick-and-place and packaging tasks on assembly lines within one to two years [16].

Compute and cost

Sundar Pichai says Gemini 4 Argon processed nearly 25T tokens in its first 72 hours, about 3x Gemini 3.0, and is capacity-constrained [17]. Google gives DeepMind first call on compute, and its cloud business is forgoing short-term revenue as a result [17]. Customer requests for 2027 compute are “incredibly difficult” to fill [17]. He grants that an overbuild could happen if any of roughly 2,000 components becomes a constraint [17]. Internally, Google reports 30% more code changes and about one-third fewer rollbacks in Argon’s first four weeks [17]. SF Compute’s compute market is still thin: 5% of its capacity is on the order book [18].

Prices keep falling. OpenAI’s Karan Singhal says GPT-6 Luna beats the model that was OpenAI’s best a month ago on its health benchmark, at 34x lower cost [19]. Among the companies The Pragmatic Engineer surveyed, AI spend on API plans has roughly halved since June–July peaks, helped by moves to open models. Some subsidized subscriptions are ending, though, and those bills could rise 5–10x [20].

Open models and policy

The DHS order bars DeepSeek, both the company and its models, from federal civilian procurement. It is unclear how the order applies to fine-tunes or to models trained on DeepSeek outputs [21]. DeepSeek then open-sourced DeepInfer, its internal inference stack; one estimate puts DeepSeek’s token gross margin as high as 90% [21]. China’s MOFCOM proposed, but has not enacted, pre-approval for sharing frontier AI abroad, with automatic approval for open-source [21].

Local and sovereign deployment also moved forward. Perplexity Computer now runs fully on a Mac, with both the model and the agent on-device [22]. Mistral’s Voxtral 3 adds speech recognition, text-to-speech and a voice-agent SDK, available through its API or on customer infrastructure [23].

Agent infrastructure

Ramp tested several off-the-shelf agent harnesses before building its own model-agnostic one, Laminar [24]. LangChain packaged the pieces its internal agents kept needing into Managed Deep Agents: per-user identity, scoped memory, sandboxed code execution, and scheduled runs [25].

Briefly

- Waymo reports 0.01 serious-injury crashes per million miles versus 0.21 for human drivers, across 271M miles. Semafor reports Waymo plans to grow from about 4,000 to 20,000 cars by end-2027, funded by a \$5B loan [26].
 - Microsoft exited Nscale’s £2bn Essex data center after its grid connection slipped to the 2030s. Nscale says it will still build [27].
 - An NBER paper estimates California’s billionaire tax would raise about \$30B but have a mean net present value of −\$39B once departures are counted [28].
-

Sources

1. X post by @saranormous
2. X post by @saranormous
3. X post by @aleks_madry
4. X post by @DarioAmodei
5. X post by @ClementDelangue
6. How AI Is Repricing Every Software Company
7. X post by @bobmcgrewai
8. X post by @ivanburazin
9. X post by @a16z
10. X post by @OpenAI
11. 5 Interesting Learnings from Braze at \$910 Million in Revenue: A \$5.66B Sale to Salesforce, 26% Growth, and Operating Expenses Up Just 6%
12. r/artificial post by u/Dapper-Tale-4021
13. X post by @goodhartproof
14. X article by @pronounced_kyle
15. X post by @a16z
16. Inside the Robot Data Factory: Mecka’s Josh Gao on Sensorizing Humans to Train Robots
17. Sundar Pichai: Google’s Frontier Imperative, Compute Scarcity Dilemmas, Future AI Products and Businesses
18. The Programmable Data Center — Evan Conrad, SF Compute
19. X post by @a16z
20. What’s the ROI of software engineers’ spending on AI?
21. Latest open artifacts (#25): DeepSeek V4.1 Flash 1017, American-made models, and new regulatory controls in the US & China
22. X post by @perplexity_ai
23. X post by @GuillaumeLample
24. X post by @kir_lev
25. X post by @caspar_br
26. r/Futurology post by u/mawcopolow
27. r/Futurology post by u/lughnasadh

28. X post by @nberpubs