Prosper AI's Series A, Gray Swan's Security Stack, and Open Agents Tighten the Market

VC Tech Radar

2026-06-23

Prosper AI's Series A, Gray Swan's Security Stack, and Open Agents Tighten the Market

By VC Tech Radar • June 23, 2026

Prosper AI's $30M Series A is the clearest funding signal in this batch, while Gray Swan, Recursive, and MacroData Labs point to investable themes in AI-native security, automated research, open-agent infrastructure, and robotics data plumbing. The brief also tracks market signals around open-model pricing pressure and AI data-center cooling economics.

1) Funding & Deals

- **Prosper AI: a16z backs end-to-end clinic automation with real commercial proof.** Prosper AI raised a $30M Series A led by a16z. The product is positioned as an AI-native platform for voice-heavy clinic operations, covering appointment scheduling, eligibility and benefits verification, patient billing, and the broader patient journey. Reported traction is unusually strong for this stage: 5x growth in six months, support for 150k+ healthcare providers across 60+ organizations, and athenahealth as a customer. Founders Xavier DeGracia and Josep Mingot bring medical practice, call-center operations, and insurance distribution experience [1, 2].
- **Gray Swan: Series A behind an AI-specific security stack.** Gray Swan was discussed as having a Series A, with Snowflake as one of its investors. The company's view is that LLMs and agents have their own vulnerability surface, so enterprises need dedicated red teaming and guardrails rather than conventional software security alone. Its current stack spans the Arena community, the Shade automated red-teaming model, and the Cygnal guardrail model [3].

2) Emerging Teams

- **MacroData Labs: a data-refinery thesis for robotics.** MacroData Labs is building data infrastructure for robotics, with the core argument that robots need a specialized data refinery. The timing matters because robotics teams are moving from model experimentation to scale-stage bottlenecks in storage, sampling, deduplication, QA, and annotation [4, 5, 6, 7].
- **Recursive: a newly founded research startup already pairing thesis with results.** Recursive says its automated AI research system proposes ideas, implements them, runs experiments, validates results, and iterates toward a target objective. It has already posted new state-of-the-art results on NanoChat Autoresearch, NanoGPT Speedrun, and SOL-ExecBench [8].
- **Openference: lightweight infra capturing early open-model demand.** Openference is a one-person project offering a single OpenAI-compatible API across models such as GLM-5.2, DeepSeek V4 Pro, and Kimi 2.6, with stable routing and automatic failover. The founder says paid subscriptions launched within days and new users are signing up daily [9].
- **Jettson: a clear wedge on agent runtime persistence.** Jettson is building a durable runtime for production AI agents, centered on persistent workspaces, browser state, shell access, memory, and crash recovery. The founder is explicitly testing whether persistence and recovery are a broad SaaS pain point or still mostly an infrastructure-niche concern [10, 11].

3) AI & Tech Breakthroughs

- **Recursive's automated research loop is one of the clearest early RSI signals in this batch.** The system automates the sequence of proposing an idea, implementing it, running an experiment, validating the result, and selecting the next experiment. The reported wins span small-model training under compute constraints, training speed, and GPU kernel optimization — all domains where goals are well-defined and fast to evaluate [8].

  > "These results are an early sign that our system can push the frontier on AI training and infrastructure tasks, especially when the goal is well-defined, measurable, and quick enough to evaluate many times." [8]

- **Gray Swan's security stack suggests safety tooling is becoming its own model category.** Shade is described as an automated red-teaming model that now outperforms human red teamers at breaking frontier models and agents. Cygnal is a separate filter model placed between users,

models, and tool calls to enforce policy on untrusted data and agent actions [3].

- **GLM-5.2 looks like a step-change for open agents, not just another open model release.** Interconnects argues it is the first open-weight model that feels credible as a general agent in coding harnesses, with community benchmarks placing it alongside leading OpenAI and Anthropic systems on agent leaderboards. The model is also appearing quickly in developer tooling: Openference already lists GLM-5.2 among its supported models [12, 9].

4) Market Signals

- **Open models are starting to create both pricing pressure and immediate infrastructure demand.** Interconnects argues GLM-5.2 is a major inflection for the open-model economy, naming inference and fine-tuning providers such as Fireworks, Together, and Prime Intellect as likely beneficiaries. The same piece frames the current open/closed gap at roughly 6.8 months, while Aravind Srinivas argues GLM passes blind tests on median production-grade knowledge-work tasks and says more multi-trillion-parameter open-source models are coming soon. Ground-level demand is already showing up in projects like Openference, whose founder says new users are subscribing daily [12, 13, 14, 9].

- **Robotics is moving from model tinkering to data plumbing.** Notes from the MacroData orbit point to a shift from demo-stage experimentation to questions about raw sensor storage, alignment strategy, sampling, deduplication, QA, and scalable labeling of instructions, subtasks, and failures. The same thread highlights Zurich talent across student groups, frontier labs, and integrators, and argues Europe may be better positioned in robotics than in LLMs [7].

- **AI-native security may grow into an insurance and compliance workflow, not just a testing product.** Gray Swan's framing of prompt-injection risk centers on the combination of untrusted external data, private data, and possible exfiltration. Zico Kolter also describes a future in which risk can be assessed with tools like Shade and mitigated with tools like Cygnal, pairing security tooling with insurability decisions [3].

- **Liquid cooling is materially changing the water-footprint discussion around AI data centers.** One cited figure puts data centers at 0.2% of U.S. daily water usage, and argues that 45°C liquid cooling can cut facility cooling water from roughly 2.6 million gallons per MW per year to near zero in favorable climates. A separate comment stresses that the marginal water consumption of properly implemented liquid cooling is almost zero, distinct from water used by power plants supplying the electricity [15, 16].

5) Worth Your Time

- **Latent Space: Gray Swan** — best starting point here on AI-specific security, especially the link between red teaming, guardrails, and insurer/compliance workflows [3].
- **Import AI 462** — concise framing of Recursive's automated research results and the bigger question of whether recursive self-improvement can move beyond tightly measured tasks [8].
- **GLM-5.2 is the step change for open agents** — useful because the key claim is market-relevant: open weights are becoming credible general agents in coding workflows, with downstream pressure on closed-model pricing and open-model infra demand [12].
- **MacroData Labs pre-seed announcement** — a short thesis read on why robotics teams may need a dedicated data-refinery layer as scaling bottlenecks shift away from model experimentation [5, 4, 7].
- **Prosper AI founder thread** — the cleanest primary source in this batch for vertical-AI healthcare traction, including the product scope and the 5x-in-six-months growth claim [2].

Sources

1. X post by @a16z
2. X post by @XDeGracia
3. Red-Teaming after Mythos — Zico Kolter & Matt Fredrikson, Gray Swan
4. X post by @nathanbenaich
5. X post by @nathanbenaich
6. X post by @nathanbenaich
7. X post by @HKydlicek
8. Import AI 462: Superpersuasion; self-sustaining AI; paths to ASI
9. r/SideProject post by u/Anh-DT
10. r/SideProject post by u/r2werks
11. r/SaaS post by u/r2werks
12. GLM-5.2 is the step change for open agents
13. X post by @AravSrinivas
14. X post by @AravSrinivas
15. X post by @nvidia
16. X post by @AravSrinivas