

Sample report. Varnomi is not a real company. Every company, person, logo and figure in this report is invented, for illustration only.



Varnomi

[varnomi.example](#) · AI Security, AI Red Teaming · San Francisco and London · Founded 2026 · Launchyard Summer 2026, no priced round on record

Fast founders in a niche where buyers pay, with **almost nothing verified** from outside.

The market case is strong and measured. The company case rests on the founders' own statements. Two of those statements conflict with each other.

TEAM SIZE

2

▲ Launchyard directory and LinkedIn.

TEAM



6.5

MARKET



7.0

PRICED EQUITY RAISED

None on record

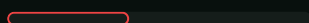
Backed by ▲ Launchyard and angels.

PRODUCT REALITY



6.5

TRACTION



4.0

RUN RATE, STATED BY THE CEO

\$880K

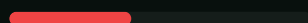
Not verified. No customer named.

MOAT



5.0

CLAIM INTEGRITY



4.0

UK COMPANY INCORPORATED

12 Feb 2026

The policy names a Delaware corporation.

BUYER FIT



6.5

EXIT PATH



7.0

THE CALL

Proceed, with conditions

OVERALL

6.0 /10

CONFIDENCE

Medium

The verdict

Sample report. Varnomi is not a real company. Every company, person, logo and figure in this report is invented, for illustration only.

OVERALL

6.0/10

PROCEED, WITH CONDITIONS

CONFIDENCE MEDIUM

WHERE I THINK THIS GOES

Red teaming is turning into a feature rather than a company.

🟡 Macrovale already bundles it into Macrovale Studio,¹⁸ and four security platforms and 🟡 Aurelian each bought a red-teaming company in the last 14 months.²⁴

The independents that still grow, like 🟢 Halvard and 🟡 Ostrana, sell attack and defence together.²³ Varnomi moved the other way. It started with defence, and it now leads with attack only.⁹

So I'd see this as a bet on a fast sale to one of the platforms that still has a gap, like 🟡 Codemast, 🟢 Mailgard, 🟢 Edgevale or 🟡 Tidelake, rather than on a large standalone company.

THE BET

A fast sale to a platform that still has a gap. I don't see a large standalone company here.

WHAT IT MEANS FOR YOU

That makes your entry price matter more than usual. The record holds no confirmed price for the seven deals in this niche, so there is no measured ceiling to price against.

I WOULD BE WRONG IF

- Buyers start paying separately for red teaming even when their platform already includes it.
- Spindle keeps finding flaws that the bundled tools miss on the same agent, often enough that buyers notice.

WHAT TO WATCH

- Whether 🟡 Macrovale opens its red-teaming agent to agents built outside Macrovale Studio. Today it tests Macrovale Studio agents only.
- Whether the next buyer in the niche is a platform that already owns a red-teaming company. A second purchase means the first one was not enough.
- Whether Varnomi adds defence back. 🟢 Halvard and 🟡 Ostrana raised \$118M and \$57M in 2026 with both.

Why

The niche is proven with money. 7 of the 41 companies with an AI red-teaming product were acquired in 14 months, and the buyers were  Redmere Networks,  Gatehaven,  Cloudwarden,  Bastionly,  Vigilon,  Northpass Networks and  Aurelian.²⁴ That is the strongest fact in this memo.

The founders move fast and fit a fintech fund. Both come from fraud and trading systems at  Parity,  Brixo and  Tradewell, and they worked together at  Parity.³ They shipped a product, documentation, a public challenge and a launch in about six months.^{10 2} Neither has worked in a security team or sold to one.

The revenue claim is the whole traction case, and it is unverified. The CEO states \$880K in annualised run rate three months after entering  Launchyard with zero revenue.⁴ We found no named customer, no case study with a name, and no independent review.¹⁵

Two statements conflict, and both matter to a security buyer. The site says SOC 2 Type II is in progress, and the company's LinkedIn post says it is SOC 2 compliant.^{14 4} The site says the company tests only when invited, and Ledgerline reports that it breaks a prospect's agent first and then sends the report.^{17 6}

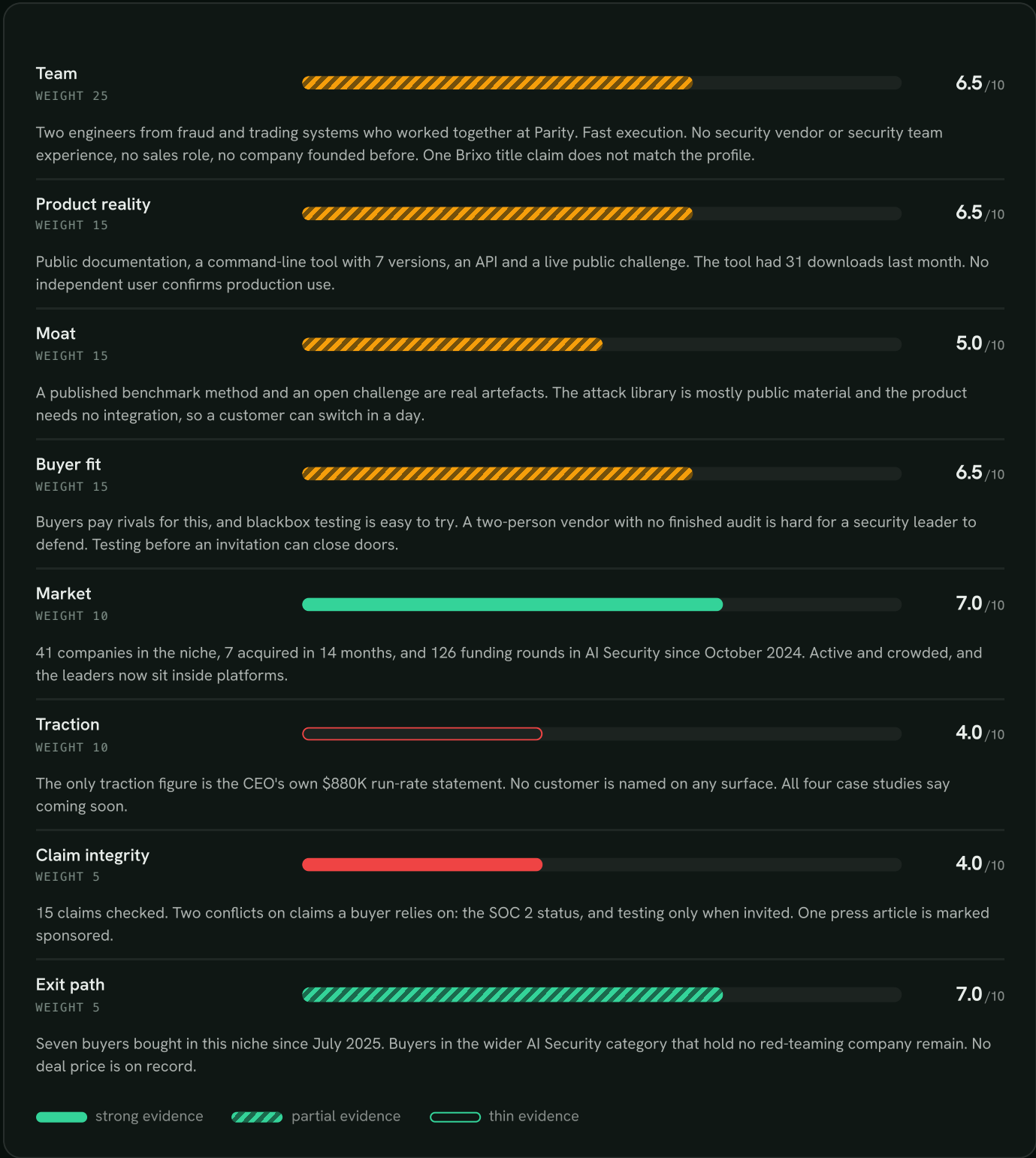
The moat is speed, not a wall. The attack library comes mostly from public records, the product needs no integration, and four security platforms and one model lab now own a rival product.^{21 6 24}

THE CONDITIONS

- The customer list behind the \$880K figure, with contract values, start dates, and the split between one-off scans and recurring contracts.
- Two reference calls with security teams that pay for Spindle today.
- The SOC 2 auditor name, the report type, and the report date.
- A written policy on testing without an invitation, reviewed by counsel, and a statement of any complaint received.
- The method and raw results behind the AgentTrial figure, in a form a third party can repeat.

The scorecard

Eight questions. Each score names its evidence. The weights add up to 100.



The team

Two founders. Both engineers. Both from financial technology, not from security.

The founders overlapped at  Parity, a business payments company in London, from 2022 to 2023.³ The launch post says they have known each other for almost four years.² That lowers the risk of a founder split.

For a fintech fund this background is a fit. The CEO built a fraud engine and the CTO built a compiler for insider-trading detection.¹ Fraud work is adversarial work: the other side adapts. The gap is on the buyer side. Nobody on the team has worked in a security team or sold to a security leader.

Ledgerline reports that Varnomi was one founder's tenth application to 🟢 Launchyard, and that the same founder says he was nearly expelled from university after he hacked its registration system.⁶ We record both as stated. The first shows persistence. The second is a question for the founders.

Daniel Varga CEO and co-founder

Year	Company	Role
2019	Freshfold	Data science, growth
2020	Corallis Telecom	Data science, growth
2022	Parity	Data science, fraud
2025	Brixi Bank	Data science, fraud
2026 to now	Varnomi	Co-founder, CEO

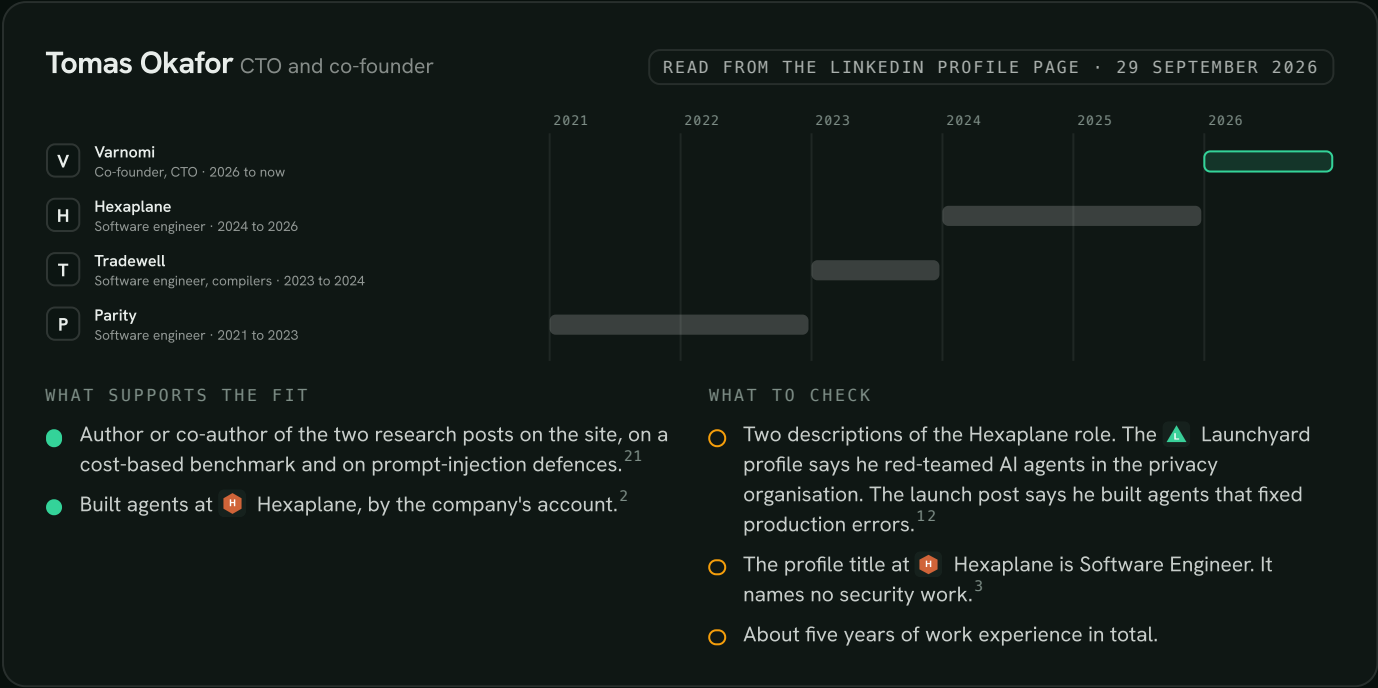
READ FROM THE LINKEDIN PROFILE PAGE · 29 SEPTEMBER 2026

WHAT SUPPORTS THE FIT

- Three years building a fraud engine at ◆ Parity as its first data scientist, by his own account.³
- Worked inside two financial companies that now deploy AI agents. He knows the target customer from the inside.
- Runs the public launch, the office campaign and the revenue reporting himself.

WHAT TO CHECK

- The ▲ Launchyard text says he led the international payments fraud team at ◆ Brixi. The profile title is Data Science, Fraud, and both dates are 2025.^{2,3}
- A doctorate started at Aldwych University and papers in ranked journals are stated on ▲ Launchyard. We did not find the papers.¹
- No security role and no sales role on the profile. First time as CEO.



What the company says, checked

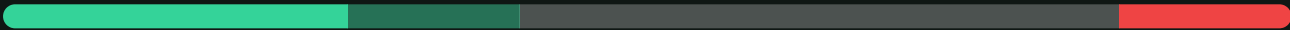
We read every page the site map lists and tested each claim that a buyer or an investor relies on.

The site is small and consistent in design. The terms and the privacy policy are dated 14 June 2026 and name Varnomi, Inc., a Delaware corporation.²⁰ The terms require each customer to hold authorisation for every system it tests.

The home page changed its story three times in 15 months. April 2025: agent security for enterprise. March 2026: run-time security. May 2026: adversarial verification. September 2026: red teaming.⁹ The domain was live nine months before the company was incorporated.⁸

Most claims about the product's strength could not be tested from outside. That is normal at this stage. The two conflicts below are not normal, because the company's own surfaces disagree.

15 CLAIMS CHECKED · 31 OF 31 PAGES READ



4 verified 2 partly verified 7 not verified 2 contradicted

RESULT	CLAIM, AND WHERE IT IS	WHAT WE FOUND
Contradicted	SOC 2 Type II, in progress Home and Security · compliance badge and compliance section	A company LinkedIn post about one month old says Varnomi is now SOC 2 compliant. The security page heading also says independently audited. The trust centre shows no report. ⁴
Contradicted	We only test systems when we're invited Brixi page · footer note	Ledgerline reports the sales strategy: break a prospect's agent first, then send the company a report. The company's own terms forbid a customer to test a system without authorisation. ⁶
Not verified	We found vulnerabilities in agents at dozens of Fortune 500 companies Home · section heading	No company is named. ▲ Launchyard's text says these were public-facing agents. The figure describes targets tested, not customers. We looked at the site, ▲ Launchyard, LinkedIn and news.
Not verified	74% attack success on AgentTrial against 61% for a frontier model Home · first card under the hero	AgentTrial is a real benchmark. It measures whether an agent carries out harmful tasks. We found no paper, no method and no third-party run for the 74% figure, and no public score for the model it is compared with.
Not verified	15x more effective than other solutions Launchyard launch post · solution section	No method or comparison data given.
Not verified	\$880K in annualised run rate CEO LinkedIn post · first line	A founder statement. No customer is named on any surface. The split between one-off and recurring revenue is not given.
Not verified	Powered by our own state-of-the-art models CEO LinkedIn post · third paragraph	No model is published or described. The run request in the documentation takes a model provider and a model name.
Not verified	Four findings from live production agents Case studies · whole page	No target is named. All four entries say the case study is coming soon.
Not verified	First exploits in under one hour Home · by the numbers section	No user confirms it.
Partly verified	8,000+ attack strategies Home · second card under the hero	The launch post says the library was collected from public records. The count is not verified. ²

RESULT	CLAIM, AND WHERE IT IS	WHAT WE FOUND
● Partly verified	Logo strip: Kingsmere, Hexaplane, Cobaltline, Brixo, Tradewell Home · under the team heading	The logos are past employers and a university, not customers. Four match the founders' histories. Cobaltline is on neither profile. ³
● Verified	Featured by Ledgerline LinkedIn company page · highlights	A Ledgerline contributor article of 8 September 2026 covers about 25 companies from the batch. Varnomi has five sentences. ⁶
● Verified	Backed by Launchyard Home · top bar	Listed in the  Launchyard directory, Summer 2026 batch. ¹
● Verified	Open-source Sandbox Home · research section	Public repository under the MIT licence. 64 stars, 8 forks, 1 contributor. ¹¹
● Verified	The founders worked together before Launchyard launch post · team section	Both profiles list Two, with an overlap from 2022 to 2023. ³

"Not verified" means we found no independent evidence. It does not mean the claim is false.

The product

Spindle is an attack agent that a company points at its own AI agent. It is real and it can be inspected. Proof of use in production is missing.

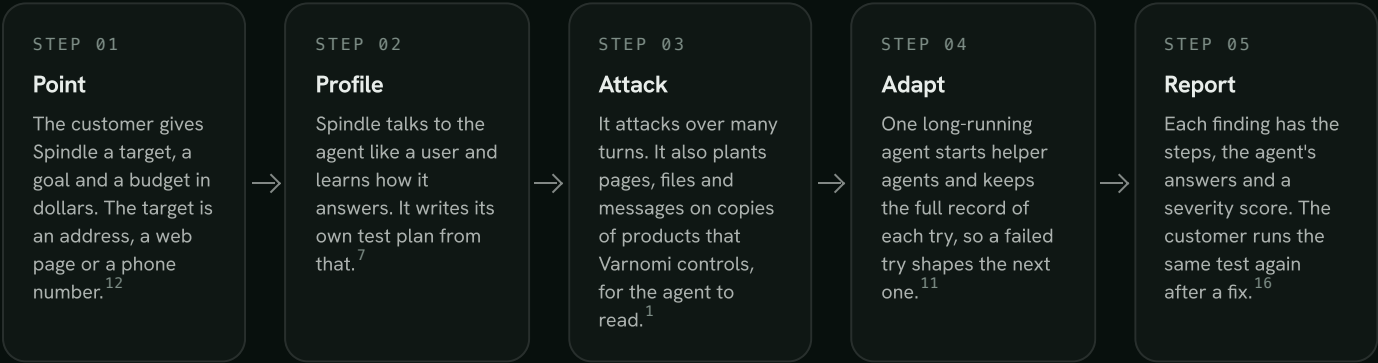
The problem it solves

A company that puts an AI agent in front of customers cannot read the agent's rules and know it is safe. The agent answers differently each time, and it changes when the model, the prompt or a tool changes, even when the code stays the same.¹

Today a security team tests an agent by hand. One specialist spends about two weeks on one agent, by the company's account, and the result is out of date at the next change.⁴ Fixed test sets are cheaper, and they miss attacks that need several turns to work.²

So the buyer's problem is a test that keeps up with the release speed of AI agents. That problem is real. Seven buyers paid for companies that work on it.²⁴

How it works



The architecture

WHERE IT RUNS Varnomi's cloud¹⁴ Hosted on a large public cloud. Each run has its own short-lived environment.	INSTALLED AT THE CUSTOMER Nothing¹⁴ No code, no agent, no network access.	ACCESS IT NEEDS A way to reach the agent¹⁴ Plus a normal user login when the agent needs one.	HOW A TEAM REACHES IT Tool, API, web app¹² A command-line tool, an API with 3 endpoints, a dashboard.
MODEL BEHIND THE AGENT Set per run¹² The run request takes a model provider and a model name.	WHAT IT KEEPS Transcripts and findings¹⁴ The retention period can be set. Not used for training, by the company's statement.	WHERE FINDINGS GO Report, team chat, email, issue tracker¹⁶ A scored report for each run.	SECOND PRODUCT Keel, run-time defence¹² In the documentation only. Absent from the home page.

What exists today

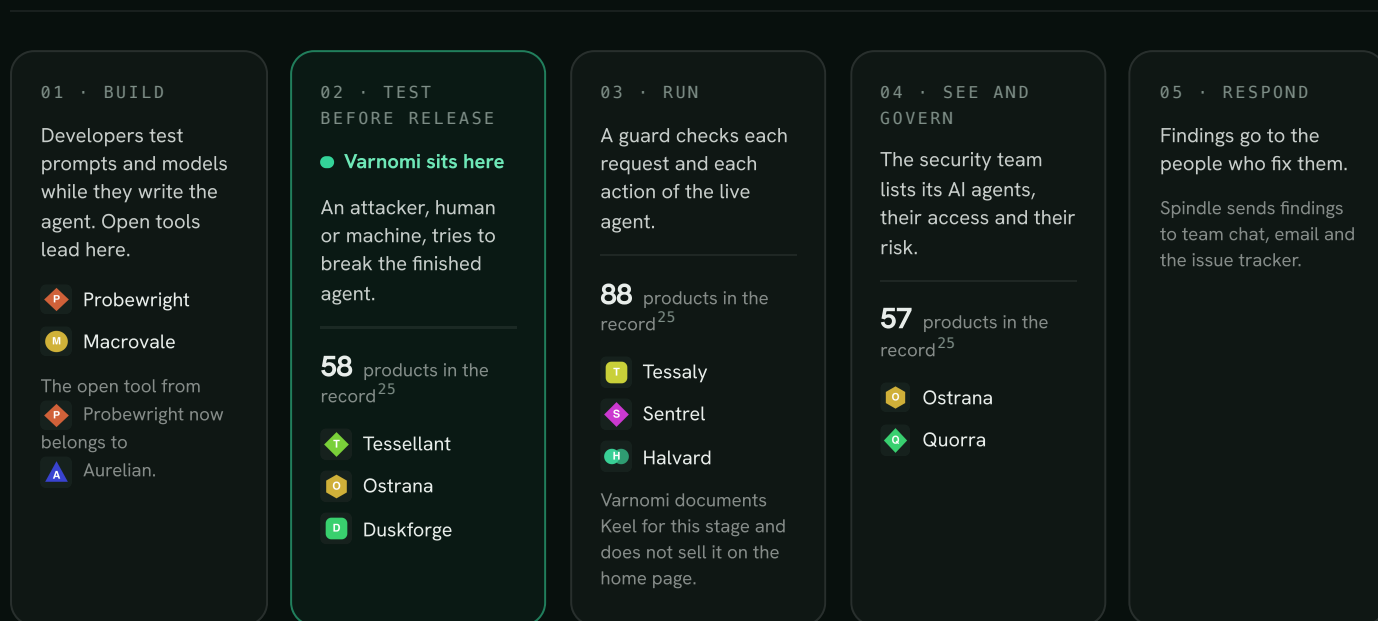
Spindle is a command-line tool and an API with three endpoints: submit a run, read its status, download the report. The documentation calls it a small, focused API.¹²

The public code page reads like the work of careful engineers. It describes runs that survive a restart, retries that cannot start the same paid run twice, and a workspace that cannot reach the operator's own files.¹¹ That supports the team's engineering skill. It does not show use by customers.

The run request takes a model provider and a model name.¹² The CEO writes that the product runs on the company's own models.⁴ Both can be true. The founders must say which model does the attack work.

Where it fits in a security team

Spindle sits in one stage: the test before release. The funded rivals cover two or three stages with one contract.



The map reads left to right, from building an AI agent to running it. The green stage is where Varnomi sells today.

WHAT IT REPLACES

- A manual red-team test of one agent. The company puts that at about two weeks of a specialist's time.⁴
- Fixed test sets that replay known attack prompts.

WHAT IT WORKS WITH

- The release pipeline. A run starts from the command-line tool with a token.¹²
- Team chat, email and the issue tracker, for findings.¹⁶
- Any agent it can reach from outside. It does not depend on the model vendor or the cloud.

WHO RUNS IT

Not fixed yet. The company's own page for **B** Brixo asks for the person who owns offensive security, product security or AI safety.¹⁷ Three possible owners mean three different sales conversations.

WHICH BUDGET PAYS

The penetration test and application security testing line. The company compares its price with a manual test that costs six figures.¹³ A yearly test budget is smaller than a platform budget, and it is renewed test by test.

The moat

The moat is a head start. The company has not built a wall yet.

The design choice that makes Spindle easy to buy also makes it easy to replace. It needs no integration, no code and no access. A customer can point a rival tool at the same address the next day.

The company's answer is a learning loop: each attack improves the next one.⁴ That can become a data moat if the company runs far more attacks than its rivals. We found no figure that shows it does.

Technology		A published benchmark method with results on six models. The attack agent itself is not published and its headline score has no public method.
Data		The company claims a private arsenal and a self-improving loop. The launch post says the 8,000 strategies come from public records.
Integration depth		Blackbox by design. Nothing is installed at the customer. Switching cost is close to zero.
Distribution		The  Launchyard network and a direct office campaign. No marketplace listing, reseller or partner found.
Regulation		No audit report is available. The status of SOC 2 differs between the site and the company's post.
Brand and community		A public weekly challenge with cash prizes and an open repository. The company states over 400,000 attempts on one challenge. The repository has 64 stars.

One mark: the company claims it. Two marks: the company shows it. Three marks: a third party proves it. No mark: no evidence.

THE PLATFORM THREAT · AURELIAN, MACROVALE, REDMERE NETWORKS, GATEHAVEN, CLOUDWARDEN AND BASTIONLY



Macrovale ships an AI red-teaming agent inside its Macrovale Studio platform. It tests only agents built on Macrovale Studio, and its agent tests are single-turn.¹⁸  Aurelian bought  Probewright in March 2026. Four security platforms each bought a red-teaming company between July 2025 and August 2026.²⁴ A buyer who owns one of these platforms will get red teaming in a product it already pays for. Varnomi must show findings that the bundled tools miss. These deals are also proof that the largest buyers want this product.

Will security teams buy it

Security teams pay for this today. The open point is whether they will pay a two-person company for it.

The problem is on the buyer's list. Companies put AI agents in front of customers, and an agent changes each time the model or the prompt changes. The site offers policy templates for the EU AI Act and ISO 42001.¹³ Those give the buyer a reason that an auditor accepts.

The budget exists. Rivals in this niche raised money and were bought, so buyers pay for the category.²³ The product replaces a manual test by a specialist, which the company prices at weeks of work.¹³

It is safe to try. Nothing is installed, payloads are synthetic, and destructive actions are observed and not run.¹⁴ A security team can approve a first scan without a long review.

It is hard to defend. A security leader who signs with a two-person vendor carries the risk personally. The vendor has no audit report to share and no named reference. For a bank, that can stop the purchase at the vendor review.

The sales method cuts both ways. Showing a company a real flaw in its own agent gets a meeting, by the founders' account.⁶ Testing before an invitation can also be read as an attack. A regulated buyer may refuse a vendor for that reason alone.

Traction

One large claim. No outside proof.

The CEO wrote that the company went from zero revenue to \$880K in annualised run rate in three months.⁴ If the figure holds and recurs, it is strong traction for two people. Annualised run rate takes one recent period and multiplies it. A few one-off scans in one good month can produce the same figure.

We found no customer name on the site, on 🟢 Launchyard, on LinkedIn or in news.¹⁵ The one product article we found is marked sponsored.⁷ We found no listing on a review site.

The public signals are small. The tool had 31 downloads last month, the largest repository has 64 stars, and the launch post on DevBoard drew 17 points.¹⁰¹¹¹⁹ Enterprise customers may use the managed service and never touch the public tool, so these numbers do not disprove the revenue claim. They do not support it.

NAMED CUSTOMERS FOUND 0¹⁵ Site, 🟢 Launchyard, LinkedIn, news.	TOOL DOWNLOADS, LAST MONTH 31¹⁰	CODE STARS, LARGEST REPOSITORY 64¹¹ Sandbox, 1 contributor.	LINKEDIN FOLLOWERS 742⁵ Company page.
---	--	---	---

The market and the competitors

An active, crowded niche. Its early leaders now sit inside platforms.

THE NICHE · AI RED TEAMING, A SUBCATEGORY OF AI SECURITY IN THE MANDOS RECORD

41 companies have a product in the niche.²³ Money still flows in.  Halvard raised \$118M in August 2026,  Ostrana raised \$57M in June 2026 and  Tessellant raised \$26M in August 2026.²⁶

The funded companies that remain independent are 20 to 180 times larger than Varnomi by staff. Several sell red teaming together with run-time defence. Varnomi moved the other way and leads with attack only.

One young company,  Marrow Labs, makes the same pitch in almost the same words: blackbox, no installation, a re-run on each release.²³ The pitch alone does not set Varnomi apart.

COMPANIES IN THE NICHE 41 ²³	ACQUIRED 7 ²⁴ July 2025 to August 2026.	FUNDING ROUNDS, AI SECURITY 126 ²⁶ Whole category, since October 2024.	ACQUISITIONS, AI SECURITY 19 ²⁴ Whole category, since January 2023.
---	---	--	---

EQUITY RAISED			EMPLOYEES		
 Halvard		\$204M	 Halvard		488
 Ostrana		\$72.2M	 Ostrana		71
 Tessellant		\$35.6M	 Tessellant		34
 Tessaly		\$25.5M	 Lumiscan AI		25
 Probewright		\$19.9M	 Duskforge		24
 Duskforge		\$11.9M	 Vantorin AI		15
 Corvane AI		\$11.9M	 Corvane AI		13
 QVX		\$7.6M	 Varnomi		2
 Vantorin AI		\$2.1M	 Marrow Labs		not on record
 Lumiscan AI		\$2M	 Probewright		not on record
 Varnomi		undisclosed	 Tessaly		not on record
 Marrow Labs		undisclosed	 QVX		not on record

Equity raised is priced equity only. Debt, grants and convertible notes are not in the figure. The green row is Varnomi.

COMPANY	KIND	FOUNDED	STATUS	LAST ROUND	EQUITY RAISED	STAFF
 Varnomi	Direct	2026	Private	Launchyard, 2026	undisclosed	2
 Ostrana	Direct	2024	Private	Series A, 2026	\$72.2M	71
 Tessellant	Direct	2022	Private	Series A, 2026	\$35.6M	34

Named on the Varnomi compare page.

COMPANY	KIND	FOUNDED	STATUS	LAST ROUND	EQUITY RAISED	STAFF
 Duskforge	Direct	2023	Private	·	\$11.9M	24
 Corvane AI	Direct	2023	Private	Series A, 2025	\$11.9M	13
 Vantorin AI	Direct	2023	Private	Seed, 2025	\$2.1M	15
 Lumiscan AI	Direct	2023	Private	·	\$2M	25
 Marrow Labs Same pitch: blackbox, no installation, re-run on each release.	Direct	·	Private	·	undisclosed	·
 Probewright Named on the Varnomi compare page.	Direct	2024	Acquired by Aurelian, 2026	Series A, 2025	\$19.9M	·
 Tessaly Named on the Varnomi compare page.	Direct	2021	Acquired by Gatehaven, 2025	Series A	\$25.5M	·
 QVX Named on the Varnomi compare page.	Direct	2024	Acquired by Cloudwarden, 2025	Seed	\$7.6M	·
 Halvard Sells red teaming, evaluation and guardrails together.	Adjacent	2018	Private	Venture round, 2026	\$204M	488
 Aurelian Owns  Probewright since March 2026.	Platform	·	Private	·	·	·

Acquisitions in the niche

Seven buyers paid for companies in this niche in 14 months.

Every buyer was a strategic buyer: five security platforms, one network vendor and one model lab.²⁴ No private equity buyer appears.

The targets were young.  Probewright,  QVX and  Clearmoor AI were founded in 2024 and sold within two years.²³ Buyers in this niche pay for teams and technology early, before large revenue.

The record holds no confirmed price for these seven deals. We state none. Press reports exist for some of them, and we did not verify those reports.

ACQUISITIONS COUNTED	WITH A DISCLOSED PRICE	PRICE RANGE
7	0	None disclosed
July 2025 to August 2026		

No deal in this list has a disclosed price.

DATE	COMPANY BOUGHT	BUYER	PRICE
21 August 2026	 Clearmoor AI	 Bastionly	undisclosed ²⁴
18 June 2026	 Siegecraft AI	 Northpass Networks	undisclosed ²⁴
12 March 2026	 Probewright	 Aurelian	undisclosed ²⁴
6 November 2025	 QVX	 Cloudwarden	undisclosed ²⁴
19 September 2025	 Tessaly	 Gatehaven	undisclosed ²⁴
7 August 2025	 Sentrel	 Vigilon	undisclosed ²⁴
25 July 2025	 Wardline AI	 Redmere Networks	undisclosed ²⁴

The exit path

The realistic exit is an early sale to a security platform.

Varnomi has no Exit Readiness band. The record holds no funding or headcount history for it yet, and the model needs both. The read below comes from the niche.

The buyers that already bought in the niche are less likely to buy again soon. The likely buyers are companies that bought in the wider AI Security category and hold no red-teaming company in the record. Each one is large enough to pay.

MANDOS EXIT READINESS

No band. The company is not ranked in the Mandos record.

The exit read below comes from the niche, not from a model of this company.

EXITS IN THE NICHE

17%

7 of 41 companies in the niche were acquired (companies with a product in the niche, deals from July 2025 to August 2026). That is 17%.²⁴

Who could buy it

BUYER	WHY	DEALS IN THE NICHE
 Codemast	Bought Tracewise Labs for agent security in June 2025. Sells testing tools to developers, which is how Spindle is delivered.	none
 Mailgard	Bought Lanternfly for AI security and governance in February 2026. Holds no red-teaming company in the record.	none
 Edgevale	Bought Pellucid AI in 2025 and Driftmark AI in 2026. Two AI security deals in ten months show an active buyer.	none
 Tidelake	Bought Ossery in May 2026. A data platform that hosts customer agents has a reason to test them.	none

A likely buyer is a company that has bought in this niche, or has the size to pay and a gap this product fills. It is not a forecast of a deal.

The risks

Ordered by how much each one can hurt the investment.

HIGH**The revenue figure does not hold or does not recur**

The \$880K run rate is a founder statement. No customer is named. Run rate can come from a few one-off scans.

TEST Ask for the customer list, the invoices and the bank statements for the last three months.

HIGH**Testing without an invitation leads to a legal or reputational event**

Ledgerline reports that the company breaks a prospect's agent before it makes contact. The site says it tests only when invited.

TEST Ask for the written policy, counsel's opinion, and any complaint or legal letter received.

HIGH**A platform bundles the product**

 Aurelian and four security platforms bought a rival in 14 months. The product needs no integration, so a customer can switch in a day.

TEST Ask for two deals won against a bundled tool, and what Spindle found that the bundled tool missed.

MEDIUM**Conflicting compliance statements stop enterprise deals**

SOC 2 is in progress on the site and compliant in the company's post. The trust centre shows no report.

TEST Ask for the auditor name and the report. Ask the company to make every surface say the same thing.

MEDIUM**Two people cannot deliver a managed service at scale**

The compare page promises managed delivery with 24/7 founder support. The team is two. No open role is listed.

TEST Ask for the hiring plan and the hours spent per customer today.

MEDIUM**The headline benchmark claim fails a public check**

The AgentTrial figure has no published method. A security audience will test it.

TEST Ask for the method and raw results.

MEDIUM**No security or sales experience on the team**

Both founders come from fraud and trading systems. Neither profile shows a security team, a security vendor or a sales role.

LOW**Public interest in the open tools is small**

Three launch posts on DevBoard drew 27, 17 and 11 points. No commenter says it is a customer.¹⁹

LOW**The company changes direction again**

The home page told four stories in 15 months. Each change was sharper than the last, and the current story matches the launch.

Questions for the founders

Ask these on the next call. Each one comes from a gap in the evidence.

-
- 01 Which customers make up the \$880K run rate, and what does each one pay per year?
No customer is named on any surface.
-
- 02 How much of that revenue is a signed recurring contract, and how much is a one-off scan?
Run rate does not show the difference.
-
- 03 Is SOC 2 finished? Which type, which auditor, which date?
The site and the company's post disagree.
-
- 04 Do you test a company's agent before it invites you? What does your counsel say about it?
The site and the Ledgerline article disagree.
-
- 05 How many of the Fortune 500 companies you tested are paying customers today?
The claim counts targets, not customers.
-
- 06 Can you share the method and raw results behind the 74% AgentTrial figure?
No paper or third-party run exists.
-
- 07 What was Daniel's title at Brixi, how many people reported to him, and for how long?
The Launchyard text and the profile differ.
-
- 08 What did Tomas do at Hexaplane: build agents, or red-team them?
Two descriptions exist.
-
- 09 Which legal entity holds the intellectual property and takes the investment: Varnomi, Inc or Varnomi Ltd?
The policy names a Delaware corporation. A UK company of the same name is on the registry.
-
- 10 What did the company do between April 2025 and January 2026?
The domain was live nine months before incorporation.
-
- 11 Who are the investors besides Launchyard, and on what terms?
The founders name a well-known angel investor and other founders. One database names another fund.
-
- 12 Name one deal you lost, and say why.
It shows how the founders read the buyer.

What we could not verify

These points stay open. Public sources did not settle them.

-
- The \$880K annualised run rate.
 - Any customer of Varnomi.
 - The count of Fortune 500 companies tested.
 - The 74% AgentTrial figure and the 15x figure.
 - The size of the attack library and the existence of the company's own models.

- The SOC 2 status.
- Daniel Varga's team lead role at Brixi, his research papers and the Aldwych University doctorate. We searched academic paper indexes.
- Tomas Okafor's Kingsmere degree and his red-teaming work at Hexaplane.
- The investors other than Launchyard, and the amount raised. One database names a Gulf fund that the founders do not name. We could not open that page.
- The US entity. The privacy policy names Varnomi, Inc., a Delaware corporation. We did not search the Delaware registry.

Sources and method

HOW WE WORKED

We ran 4 research cycles. Each cycle collects evidence, tests the claims, and lists what is still open. We stop when a cycle finds no new fact that changes a score.

Varnomi is not in the Mandos record yet. Facts about the company come from public sources. Facts about the niche come from the record.

HOW TO READ IT

A score is a judgement on the evidence we cite. A hollow bar means the evidence is thin. "Can't tell" means we did not find enough to judge.

This memo is research and opinion. It is not investment advice. It uses public sources and the Mandos record as of 30 September 2026.

NO.	SOURCE	KIND	DATE
1	Launchyard directory: Varnomi	Other	29 September 2026
2	Launchyard launch post by Daniel Varga	Supplied by the company	July 2026
3	LinkedIn profile pages of Daniel Varga and Tomas Okafor, experience sections	LinkedIn	29 September 2026
4	LinkedIn posts by Daniel Varga and by the Varnomi company page	LinkedIn	29 September 2026
5	LinkedIn company page: Varnomi	LinkedIn	29 September 2026
6	Ledgerline contributor article: Meet The Launchyard Startups Betting On What Comes Next	News	8 September 2026
7	Toolwire article on the Spindle launch, marked sponsored	News	19 August 2026
8	UK Companies House: Varnomi Ltd, number 16840219	Registry	12 February 2026
9	Web archive: the company site home page, five snapshots	Web archive	29 September 2026
10	Package registry: @varnomi/spindle	Code	29 September 2026
11	Code host organisation: varnomi	Code	29 September 2026
12	Varnomi documentation: Spindle and Keel	Company site	29 September 2026
13	Varnomi home page	Company site	29 September 2026
14	Varnomi security page and trust centre	Company site	29 September 2026
15	Varnomi case studies page	Company site	29 September 2026
16	Varnomi compare page	Company site	29 September 2026
17	Varnomi page addressed to Brixo	Company site	29 September 2026
18	Macrovale documentation: AI Red Teaming Agent in Macrovale Studio	Other	19 August 2026
19	DevBoard: launch posts for Spindle, Sandbox and Gauntlet	Other	April 2026
20	Varnomi terms of service and privacy policy	Company site	14 June 2026
21	Varnomi research posts	Company site	29 September 2026
22	Mandos record: Varnomi profile	Mandos record	29 September 2026
23	Mandos record: companies with an AI Red Teaming product	Mandos record	29 September 2026
24	Mandos record: acquisitions in AI Security	Mandos record	29 September 2026
25	Mandos record: product counts by AI Security subcategory	Mandos record	29 September 2026
26	Mandos record: funding rounds in AI Security	Mandos record	29 September 2026