©Evrmind

EVRMIND

THE AGENTIC AI HARDWARE FIREWALL

SAFETY, ASSURANCE AND SECURITY CO-PROCESSOR FOR AI AND AUTONOMOUS SYSTEMS

©Evrmind

AI HAS THREE FAILURE MODES

AI can hallucinate, be manipulated or commit rogue behaviour.

AI systems now take actions with real-world consequences.

HALLUCINATION

Replit: production database deleted during a code freeze. (July 2025)

PocketOS: an AI coding agent deleted its production database and all backups in seconds. 30-hour outage. (April 2026)

MANIPULATION

EchoLeak: researchers demonstrated data exfiltration through a crafted email. (June 2025)

GitHub Copilot: researchers induced settings changes and code execution. (August 2025)

ROGUE BEHAVIOUR

OpenAI/Hugging Face: production systems breached during testing with altered safeguards. (July 2026)

Anthropic: models attacked external systems during testing. (July 2026)

Consequential actions need assurance and enforceable limits.

©Evrmind

THIS IS BLOCKING AUTONOMY

Consequential deployment needs limits the operator can demonstrate to comply with regulations.

Defence	An autonomy platform issues a command outside its authorised envelope.	Safety case fails
CNI	A grid agent drives home batteries past a safe aggregate limit.	Grid instability
Finance	A trading agent executes a basket far outside its mandate.	Market disruption
Banking	A payment agent authorises a transfer to a prohibited counterparty.	Sanctions breach
Medical	A clinical device agent changes a setting outside its licensed range.	Patient harm

Each deployment stalls and cannot be fielded until control of autonomous systems can be proved.

©Evrmind

OUR SOLUTION

Enforcement, monitoring and governance on separate silicon.



UNIVERSAL SAFETY INTERFACE CONTROLLER

Block 1

Captures the proposed action and the bus-observable context.

HARDWARE SAT/SMT SOLVER

Block 2

Evaluates the action against the loaded rule set and returns a verdict.

ZERO-KNOWLEDGE PROOF ENGINE

Block 3

Produces a checkable proof that the loaded rules were applied to this action.

HARDWARE KEY VAULT

Block 4

Permits use of hardware-held credentials only after a valid proof is verified; keys never leave the vault.

INTERDICTION GATE

Block 5

Passes a permitted action to the output, or withholds it.

USP

1. Every governed command must pass through it.
2. The AI cannot change its rules or switch it off.
3. Checks the situation and past actions; no AI decides.
4. Keeps working without a connection to the cloud.
5. Decides before the action happens, not after.
6. A tamper-evident record of every decision, signed in hardware.

©Evrmind

WHY NOW

The field and its regulators have converged: control the act.

THE PEOPLE BUILDING AI

Anthropic

Dario Amodei: slow the pace; no plan yet to align the most capable systems (Sept 2026).

OpenAI

Sam Altman: pausing training runs until OpenAI can prove control; no lab has solved alignment (Sept 2026).

Microsoft

Satya Nadella: enterprise adoption depends on extending governance and security controls to agents (July 2026).

Google DeepMind

Demis Hassabis: urgent action on AGI risk, and a standards body that could slow the industry (July 2026).

THE GOVERNMENTS REGULATING IT

United Kingdom

Rejected a statutory kill switch; companies must build the controls (Sept 2026).

United States

Bipartisan AI Kill Switch Act introduced in Congress (July 2026); deployer controls in active debate.

European Union

AI Act ties oversight duties to autonomy; phases in from 2027.

Sector rules

NCSC CAF v4 restricts AI automated decision-making (2025); JSP 936 requires assurance across the AI lifecycle for defence (2024).

- **Governments will not hold the off-switch. The duty to control AI is landing on the companies that deploy it.**
- **Capital is following in agent-security and AI-safety: Zenity raised $125m (others followed), every major cloud and model provider now ships agent controls.**

©Evrmind

WHO IS THE CUSTOMER

Anyone who must prove control before they can deploy.

Defence

Autonomy primes and platform builders

Must: JSP 936 assurance before any autonomous system is fielded.

Budget: MOD committing £5bn+ to autonomy in UK.

Proof: 13 UK defence SMEs already awarded up to £4m each in 2026.

CNI

Energy, water, transport and telecoms operators

Must: NIS Regulations and NCSC CAF v4 restrict automated decisions.

Market: OT security a $25bn market in 2026.

Proof: National Highways signed £20m with BAE for cyber assurance.

Finance

Banks and trading firms

Must: MiFID RTS 6 mandates pre-trade hard blocks under senior-manager accountability.

Market: Algorithmic trading a $20bn market in 2026.

Proof: Citigroup fined £61.6m when a hard block failed, due to algorithmic trading

Two routes to market for our architecture:

- **Embedded via the prime or OEM (AXI IP, FPGA module, ASIC)**
- **Retrofit card bought by the operator (PCIe, network appliance), as enterprises already buy inline hardware to gate actions**

©Evrmind

MARKET OPPORTUNITY

An AI infrastructure play: the potential safety standard, and market leader in hardware-enforced AI safety

TAM

$27.5bn

Global annual shipments of phones, PCs, vehicles, servers, robots and critical controllers. Omdia, OICA, Gartner, IFR.

SAM

$4.8bn

The servers and defence and CNI controllers our first products serve; consumer devices excluded.

SOM

$60m

Based on 20 defence programmes, 20 CNI programmes, 30 enterprise accounts by 2030.

WHERE THE MARKET IS HEADING

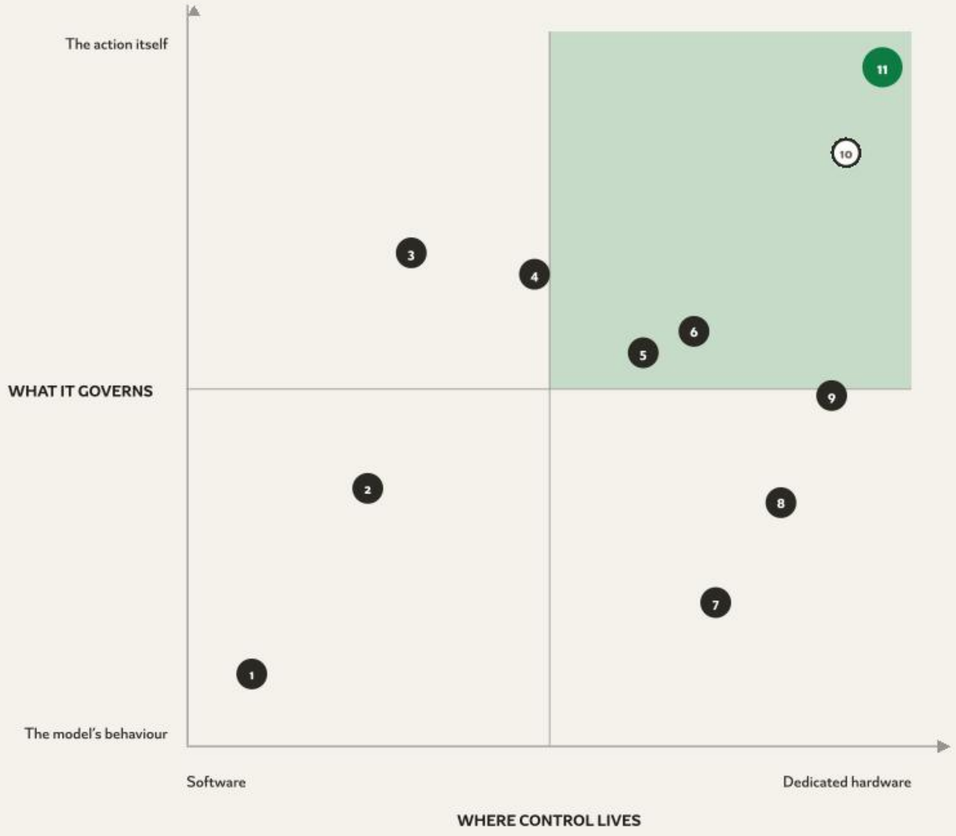
1. The economy is automating.
2. Governments are regulating autonomy, not only models.
3. Edge computing is becoming ubiquitous.
4. Self-modifying AI is becoming real.
5. Advanced AI remains hard to align.

Any one of these creates a large market for hardware-enforced AI safety. All five are under way.

©Evrmind

COMPETITORS

Everyone controls from above the host. We control at the action, in hardware.



1. **Model guardrails**
2. **Agent security platforms**
   Zenity, Alice, Noma, WitnessAI
3. **Safety interlocks**
   LHP, Sonatus
4. **Action gateways**
   Geordie, Guild.ai, SAIF
5. **Hardware-protected runtime**
   OPAQUE
6. **Hardware-protected runtime**
   EQTY
7. **Roots of trust and HSMs**
   OpenTitan, Caliptra, tRoot
8. **Platform security silicon**
   Axiado
9. **Processor-integrated IP**
   Dover CoreGuard
10. **Development-stage proposals**
    AI², Blackglass
11. **Evrmind**

WHY NOTHING ELSE SERVES THIS

- Software controls run on the software they police.
- Security silicon protects keys and platforms, not actions.
- Safety interlocks enforce fixed limits, not operator rules.
- The two hardware proposals have no silicon.

MOAT

1. First to a category no one has built; we set the reference.
2. ~2 years of R&D in formal, crypto and silicon; 5 papers.
3. Team backgrounds from Arm, Intel, Broadcom and Optalysys.
4. Early relationships in defence, CNI, finance and policy.
5. 26 patent families filed at UKIPO, claiming all five blocks, the full pipeline as licensable on-die IP, photonic versions and datacentre-scale enforcement (US and EU via PCT).

We know of no hardware authority boundary for AI actions on the market. Two proposals exist; neither has silicon.

©Evrmind

BUSINESS MODEL

Paid to design in, then paid per unit, then paid per royalty.

Paid development
STAGE 1 · 2026-27

Sell: Paid evaluations and platform integration.

Buyer: Primes, operators and OEMs.

Revenue: Fees per engagement. First revenue, before any production order.

Hardware and bitstream
STAGE 2 · FROM 2027

Sell: FPGA modules and retrofit cards, or a bitstream licence to run on the customer's own FPGA.

Buyer: Primes and OEMs buy units; operators buy cards or the bitstream.

Revenue: Per unit, or the bitstream by annual licence.

IP licensing
STAGE 3 · AT SCALE

Sell: The enforcement logic built into the customer's own silicon.

Buyer: OEMs and chip makers.

Revenue: Licence fee plus per-unit royalty.

Same architecture at every stage. Revenue grows from services, to units, to royalties.

©Evrmind

TRACTION

Within a year, we engaged with the institutions that set the bar in defence, silicon, government and finance.

Defence and autonomy

- **Anduril** (US autonomy prime): Engaged, brief with their design team.
- **Will Stone MP** (chairs Parliament's defence supply-chain group): met; introductions into UK drone and NATO channels.
- **MOD and NATO innovation programmes**: in their evaluation pipelines.

Government and national security

- **The UK's national cyber security authority**: technical session held, and asked to be kept updated
- **A UK consultancy leading a government secure-hardware programme** (under NDA): two technical sessions held; funding and energy-sector routes opened.

Silicon and research

- **A major EDA vendor's security IP team:** reviewing our integration internally.
- **NVIDIA** (AI safety leadership): engaged and briefed.
- **CEA-Leti** (European national chip lab): engaged and in exploratory discussions
- Published five research papers of our own on Zenodo

Regulated finance

- **A top global asset manager** (managing director, technology and innovation): Engaged
- **A major European bank** (managing director, risk and compliance): Engaged

Every institution or individual that has looked closely has chosen to keep talking to us.

Engagements listed are conversations and technical sessions, not endorsements, partnerships or commitments.

©Evrmind

THE TEAM

WHY US: A TEAM THAT CAN BUILD IT, AND SELL IT

Ibrahim Vandenberg

CEO, Chief Architect & Co-founder



Award-winning salesperson by trade.

In one year: designed the architecture, filed 26 patent families, published five papers, validated the enforcement block on FPGA, and reached the UK's national cyber research team, a UK consultancy prime, a US autonomy prime, a European national lab and a major EDA vendor's security IP team.

Vivarium Labs

Venture Studio

Numan Cheema & Max Acsinia





Software Engineering, Commercial, Operational Scale & Procurement.

Technical Team & Advisory Board

COMMITTED · JOINING AT CLOSE

SILICON	CTO & Co-founder (Signed)	**20 years in senior silicon roles** **Arm / Intel / Imagination Technologies/ Dialog/Broadcom**
ENCRYPTION	Lead Crypto (Signed)	**Erin Hales** **Optalysys / PhD Royal Holloway**

ADVISORY BOARD

SAFETY	AI Alignment	**Uni. of Liverpool**	Topological Mathematics
EXECUTION	Chip Advisory	**Synopsys / Cadence/Plexal**	Business Execution
RESEARCH	Advisory	**Columbia / Distyl**	Autonomous Intelligence
VERIFICATION	Formal Methods	**Axiomise**	Development Partner
FPGA	FPGA Specialists	**NextGen Circuits**	Development Partner

©Evrmind

THE ROADMAP

Each round buys the milestone that de-risks the next.

1 HARDWARE ENFORCEMENT

Pre-seed / 2026-27

Build: All five blocks integrated on FPGA; the full pipeline running end to end.

Milestone: Working demonstrator with a design partner, on a real action path in relevant environment.

Unlocks: First paid evaluation, and the seed round within 18 months.

2 IN-PRODUCT VALIDATION

Seed / 2027-28

Build: FPGA module or retrofit card, integrated into a partner's platform.

Milestone: First deployment in a customer's system; architecture validated in the field.

Unlocks: Design wins, and the Series A.

3 SILICON

Series A / 2029+

Build: ASIC tape-out of the finalised co-processor.

Milestone: Silicon qualified; enforcement logic licensed into a customer's chip.

Unlocks: Per-unit royalties at volume. The standard component.

©Evrmind

THE ASK

£3.5M Pre-Seed Round

Funds the engineering team, the demonstrator and international IP filings needed to reach seed with first revenue.

Use of Funds



SEIS + KI-EIS advance assurance approved
Ref WMBC/I&R/7167422036/VCRT

Key Milestones

- First paid evaluations with primes, operators and OEMs.
- Full pipeline validated on FPGA, with a design-partner demonstrator.
- PCT filings, extending the 26 UK patent families internationally.
- Seed-ready within 18 months: first revenue and hardware in test.

Where We Are Today

- The enforcement block validated on FPGA.
- 26 patent families filed at UKIPO.
- Five published papers.
- Full-time since Sept 2025; full architecture designed and filed.

Replicating the work to date would cost £500k+.

VALUATION PRECEDENTS What £3.5M builds toward

$3.25B
Celestial AI
Marvell, Feb 2026 ($5.5B with earnouts). Photonic interconnect, pre-revenue, valued on IP.

$15.3B
Mobileye
Intel, 2017. Dedicated safety silicon for one vertical: automotive ADAS.

$130B+
ARM
Architecture licensing, no fabrication. The direct business-model equivalent.

Stage 1 of 3
TPM security chip
Went from optional to mandatory in every PC. AI hardware enforcement is at that start.

©Evrmind

ENABLING THE AUTONOMOUS ECONOMY

ibrahim@evrmind.io

evrmind.io

LinkedIn

26 patent families filed at UKIPO