Peacemaker HQ-Lite

Network-first AI security for real networks

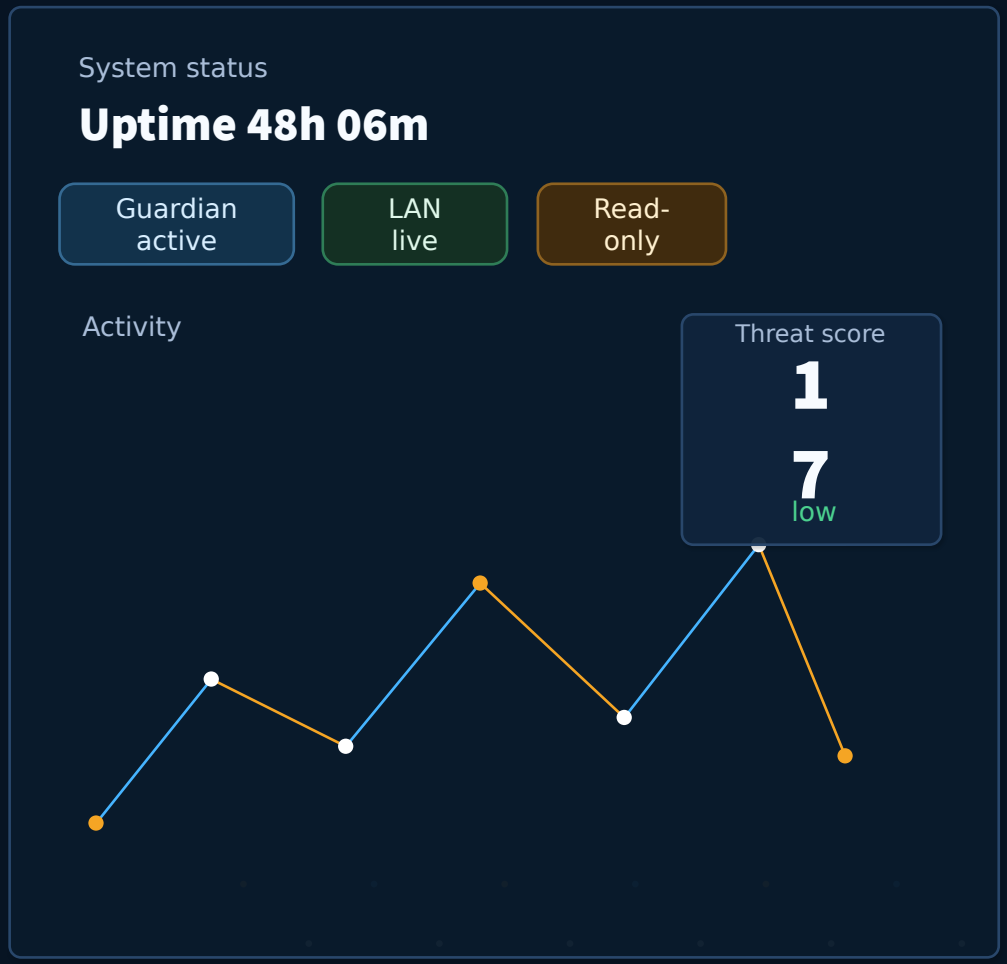
Bare-metal edge security appliance (WAN ↔ LAN) - observe • decide • enforce

Alpha v1 ISO shipped

WAN ↔ LAN

Operator-first

Inline deployment. Local decisioning. No mandatory cloud dependency for enforcement.

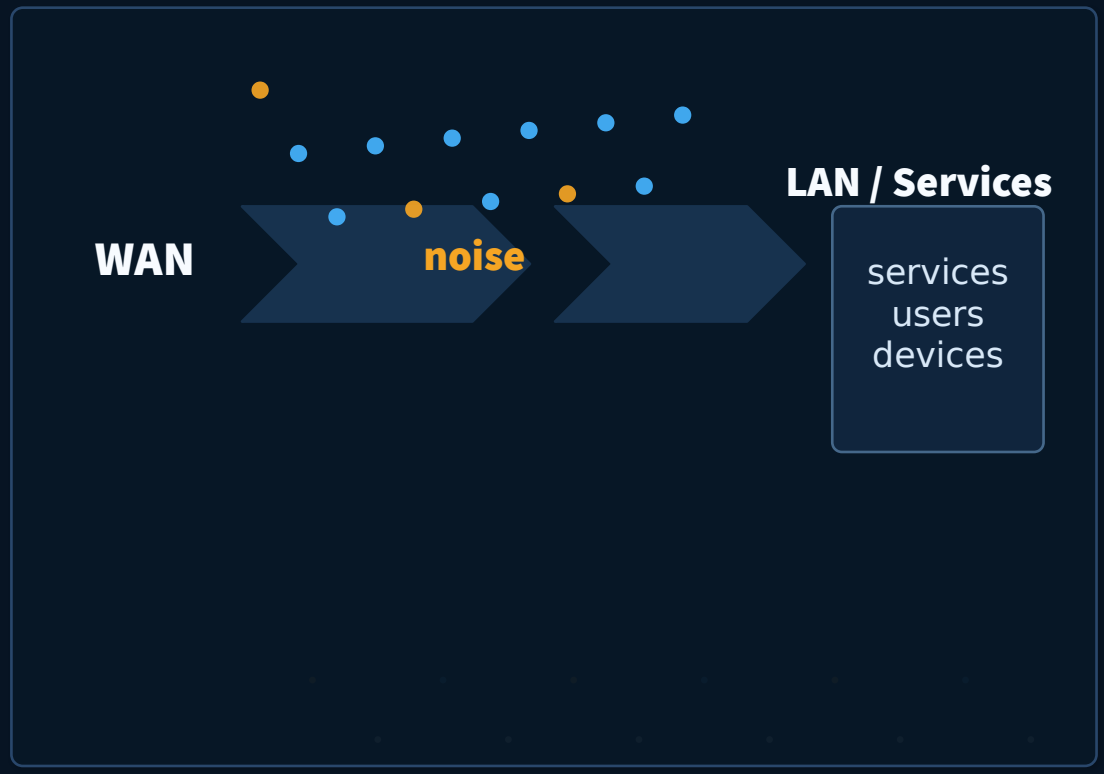


The edge is noisy - and most SME networks are blind.

Why this matters: attacks begin at the connection point, while most tools react too late.

- Cloud-first tooling = latency + dependencies
- Agents do not scale (cost, maintenance, fragility)
- Attacks start at the connection point (WAN)
- Firewalls do not understand intent or context

Result: limited visibility where the first decision should happen.

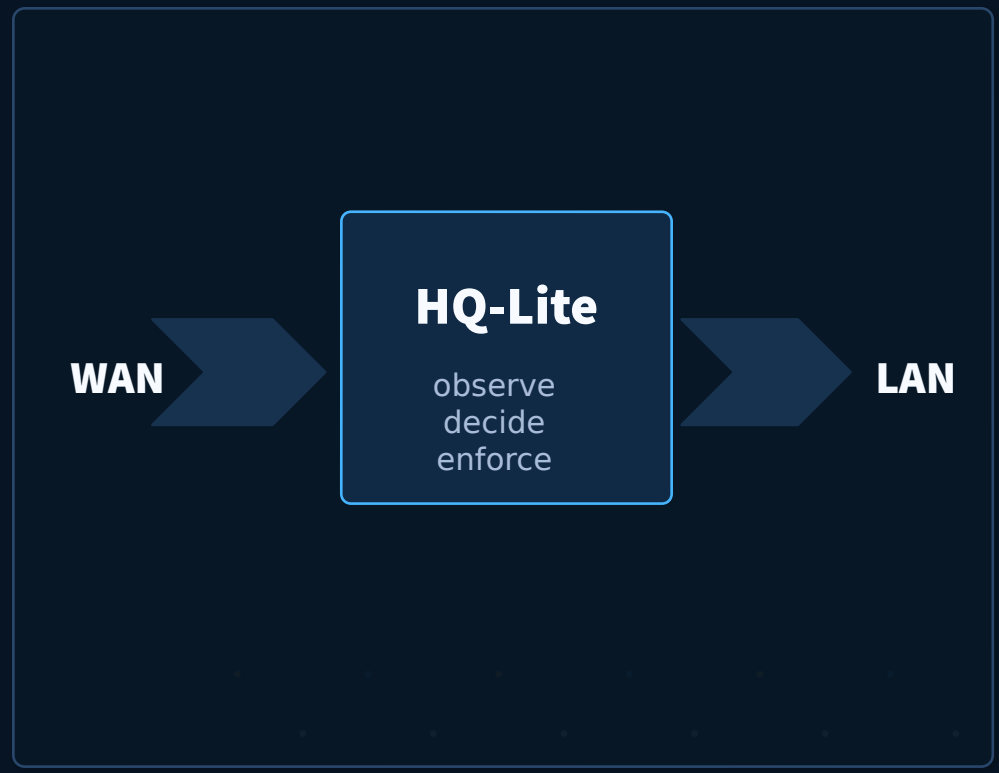


HQ-Lite is an inline edge node between WAN and LAN.

A straight answer: it sits at the point of connection and makes decisions locally.

It observes live traffic, learns the local baseline, scores risk, and enforces decisions at the point of connection - without endpoint agents and without cloud dependency for decision making.

- Inline edge node
- Local decisioning
- No endpoint agents



Layered model: reduce noise early, decide with context, enforce fast.

This is the architecture slide: XDP/eBPF -> Guardian -> Blackhole.

XDP/ eBPF

Edge pre-filter

first-pass filtering + edge counters on WAN

Guardian

Behavioural decisioning

observe + score + decide (patterns, memory, thresholds)

Blackhole

Enforcement

executes blocks via nftables (visible + auditable)

Adaptive Threshold: baseline-driven (no fixed one-size limits)

reduce noise early -> decide with context -> enforce fast

Not just detection. Real mitigation at the edge.

Why it differs from a smart router, firewall, or cloud-tethered IDS.

- On-prem & offline-capable (no cloud dependency)
- Network-first (no endpoint agents)
- Actionable: detection -> decision -> enforcement
- Runs on real hardware (low power, 24/7 capable)

Power

24h: 0.397 kWh / max 43.5W

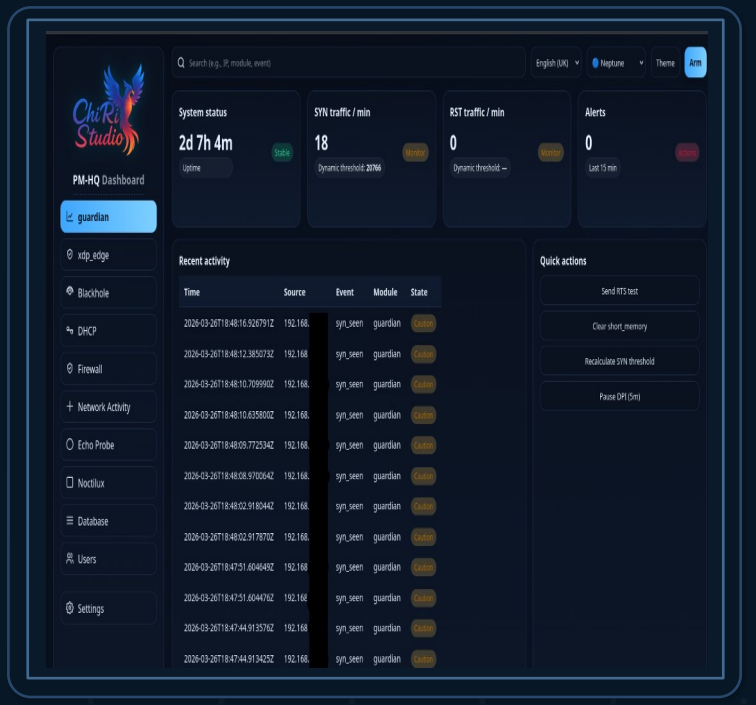
48h: 0.796 kWh / max 43.7W

Proof-lite: low-power SFF deployment aimed at 24/7 edge use.

Milestone: Alpha v1 ISO shipped (RTG install validation).

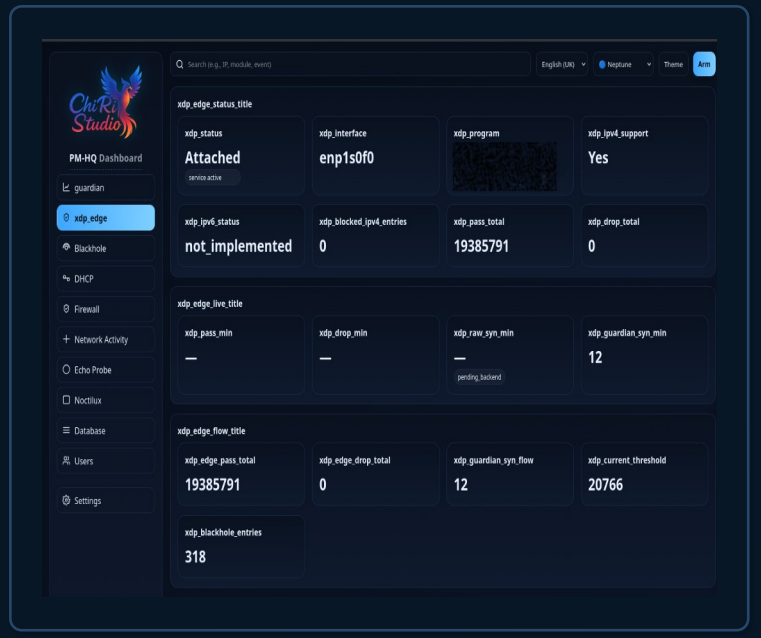
The message here is repeatable installation and factory-default bring-up, not polish theatre.

- Alpha v1 ISO built (16GB, internal install repeatability testing)
- RTG philosophy: install -> reboot -> system is live on factory defaults
- Current focus: stability, install pass rate, service correctness

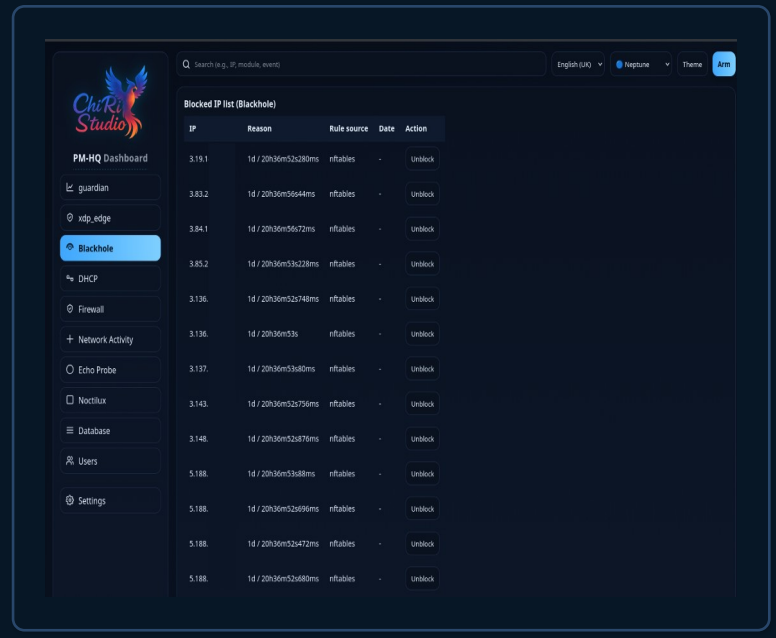


Operator-first dashboard (read-only in Alpha v1).

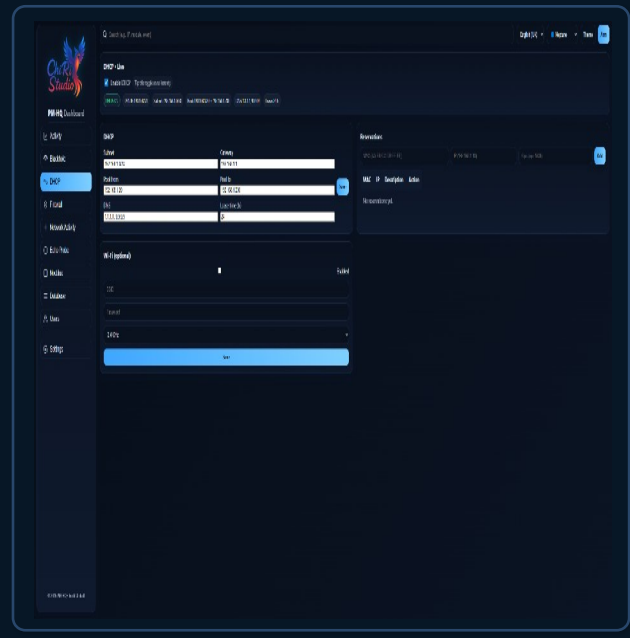
The operator should see what matters without dropping into the system.



Visibility: activity, traffic, blackhole list



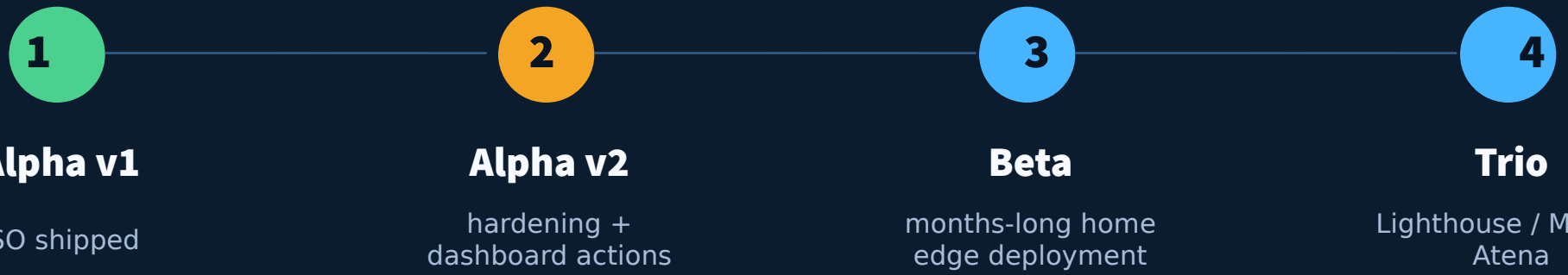
Armed mode and operational controls (next phases)



Export / reporting path for analysis

Next: Alpha v2 hardening -> Beta real-world deployment.

A staged roadmap without over-explaining internals.



Alpha v2: harden & arm, root/sudo lockdown, anti-tamper, users/roles, cleanup and predictable packaging

Beta / Trio: months-long home deployment, then Lighthouse / Matka / Atena for resilience, distribution, and governance

Built by practitioners.

UK-based, engineering-led, building on real hardware + real traffic.

P

Piotr

Co-founder & CTO

Security, networking, systems architecture

K

Kinga

Co-founder & CEO

Product vision, strategy, design & operations

ChiRi Studio

Hands-on build
real hardware
real traffic

We're looking for: pilots + early partners.

This deck exists to open practical conversations, not just to describe the product.

- Pilot validation (hosting / dedicated servers / VPS / SME edge networks)
- Investor conversations (UK/EU)
- Contact: info@chiristudio.com

Looking for aligned partners who value resilient, operator-led edge security.