HARP & Airlock HARP Gateway

Investor / Strategic Pitch (v0.1)

The Problem

AI coding agents are rapidly becoming autonomous.

They can: - Generate implementation plans - Modify source code - Apply diffs - Execute terminal commands - Commit and push code - Run migrations and deployment steps

Today, approvals are:

- UI-based
- Non-cryptographic
- Not bound to exact execution payloads
- Not out-of-band
- Not enterprise-governed

There is no standardized, cryptographically enforced human control layer for AI agents.

As autonomy increases, risk increases.

The Opportunity

AI agents will become a core development primitive.

Enterprises will demand:

- Human-in-the-loop control
- Cryptographic guarantees
- Auditability
- Zero-knowledge architecture
- Policy enforcement
- Governance across teams

There is currently no open standard for this.

We can define it.

Introducing HARP

Human Authorization & Review Protocol

HARP is an open, cryptographically verifiable protocol for human approval of AI agent actions.

HARP turns every agent action into a signed, reviewable artifact:

- Plan
- Task bundle
- Patch / diff
- Command
- Checkpoint (commit, push, deploy)

Approvals are:

- End-to-end encrypted
- Signed by a human-controlled device
- Bound to exact artifact hashes
- Replay-protected
- Scoped and time-limited

HARP becomes the human control layer for autonomous AI systems.

Introducing Airlock HARP Gateway

Airlock HARP Gateway is the commercial, zero-knowledge infrastructure implementing HARP.

It provides:

- Encrypted routing
- Device lifecycle management
- Push infrastructure
- Tenant isolation
- Enterprise policy enforcement
- Audit logging
- SLA-backed reliability

The Gateway sees only metadata and ciphertext.

It cannot decrypt artifacts. It cannot forge approvals.

HARP is the protocol. Airlock is the infrastructure.

Architecture Overview

Components:

1. Desktop Agent (IDE extension)
2. Mobile Approver (holds private signing keys)
3. Airlock HARP Gateway (blind relay)

Flow:

1. Agent action becomes a HARP artifact
2. Artifact is hashed and encrypted end-to-end
3. Mobile decrypts and signs approval
4. Desktop verifies signature and enforces execution
5. Gateway only routes encrypted payloads

This creates cryptographic binding between approval and execution.

First Implementation

Initial target:

Antigravity (VS Code-compatible extension)

- HARP integrated via extension
- MCP tool interface for artifact submission
- Desktop encryption and enforcement
- Mobile decryption and signing
- Gateway zero-knowledge routing

This becomes the reference implementation of HARP.

Why Open Standard?

Adoption.

Security protocols succeed when they are open.

Examples: - OAuth - TLS - SAML

HARP enables:

- IDE vendors
- AI agent platforms
- DevOps tooling
- Enterprise security systems

to integrate without vendor lock-in.

We define the control plane. The ecosystem builds on it.

Why Commercial?

Enterprises require:

- Device management
- Policy engines
- Compliance logging
- Tenant isolation
- SLA-backed service
- Abuse prevention
- Enterprise integrations

Airlock HARP Gateway provides this layer.

This mirrors: - OAuth → Auth0 - TLS → Cloudflare - SMTP → SendGrid

Open protocol. Commercial infrastructure.

Strategic Positioning

HARP:

The human authorization standard for autonomous AI systems.

Airlock HARP Gateway:

The secure, zero-knowledge approval network for AI agents.

We sit at the control plane of the AI-agent ecosystem.

Long-Term Vision

As AI agents evolve from coding assistants to autonomous operators:

- Infrastructure automation
- DevOps pipelines
- Cloud operations
- Data migrations
- Enterprise workflows

HARP becomes the default human authorization layer.

Airlock becomes the trusted governance network.

Human authority remains cryptographically enforced.

Summary

Problem: AI agents lack a cryptographic human control layer.

Solution: HARP (open standard) + Airlock HARP Gateway (commercial infrastructure).

Opportunity: Define the human control plane of the AI-agent era.