GLOBAL CIO PROJECT OF THE YEAR 2026 · SUCCESS CASE

ACT and Ground Control

Real-time governance for enterprise AI agents, built in-house

Category: Technological Solutions, AI Platforms and Infrastructure

GeoPark · Presented by Cinthya Sánchez, CIO

OCTOBER 2026

THE CASE IN ONE PAGE

ACT and Ground Control govern the company's AI agents

The risk

An oil and gas company that reports to the NYSE cannot afford an AI agent that leaks data or runs unchecked. Agents are multiplying and there is no live inventory.

The solution

Two in-house services. ACT registers every agent, follows its progress and can halt it. Ground Control authorizes every access with deterministic code.

The result

Both services are operating. Four agents are registered and about 37 events a day are audited. Built in five months by five people.

Why it wins: governance as running code that works with any agent technology.

CONTEXT

Over 1,500 GPTs and a growing set of agents need live governance

MAY 2024

GPT program starts. 80 custom GPTs built on internal services, 12 with high use.

JUN 2025

10 automation hackers start building agents in code with agent-to-agent architectures, MCPs and APIs.

JUL 2026

ACT begins. The Agent Control Tower becomes the registry and the operator view.

SEP 2026

Ground Control goes live as the deterministic access gate.

DEC 2026

Plan: every agent registered. Migration to skills and plugins on a company-wide assistant platform.

Over 1,500 more GPTs have no connection to our services, spend tokens from our subscription and have no live inventory. About 400 employees use these tools.

OBJECTIVES

Five goals for a future with many agents at work

1

Know every agent

A central registry holds objective, owner, guardrails and token limits before an agent works.

2

Control access

Deterministic code authorizes each request to APIs, MCP servers and systems.

3

Stop any agent

Every agent exposes a halt callback, so an operator can Halt it from one control room.

4

Monitor consumption

Tokens by day, week, month, quarter and year, with alerts near limits.

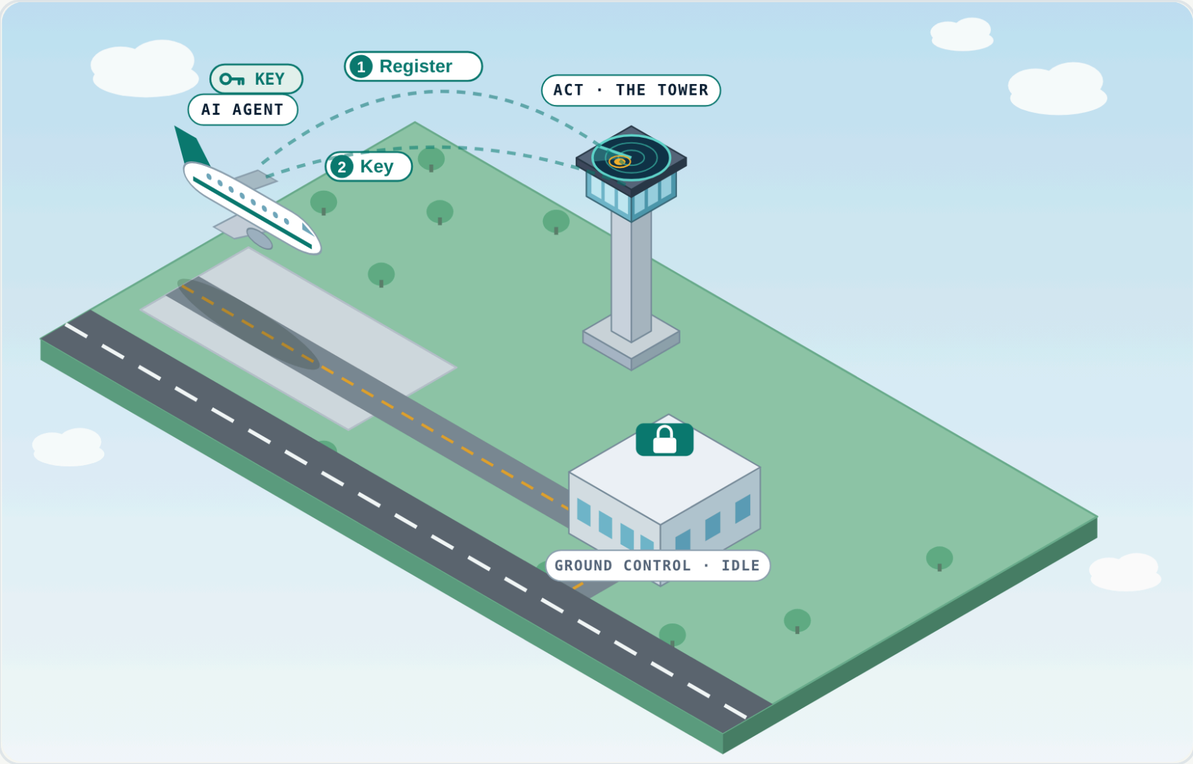
5

Stay vendor-independent

Governance works through MCP and API calls with any agent technology.

THE IDEA

The airport model: a tower that knows every plane



ACT · the tower

A REST API where agents register, report progress and can be halted. Its radar shows every registered agent.

Ground Control

Deterministic code that confirms the key with ACT, checks company permission policies and issues temporary tokens.

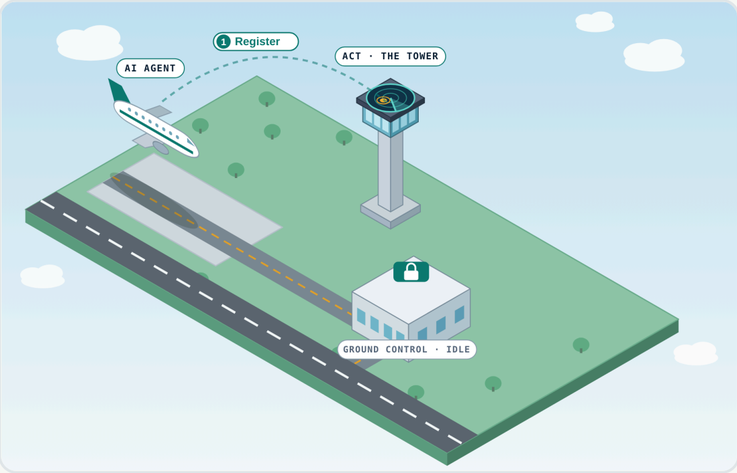
The agent is the plane

It never judges its own access. Without a registered key it receives no list of resources.

Source: ACT and Ground Control design

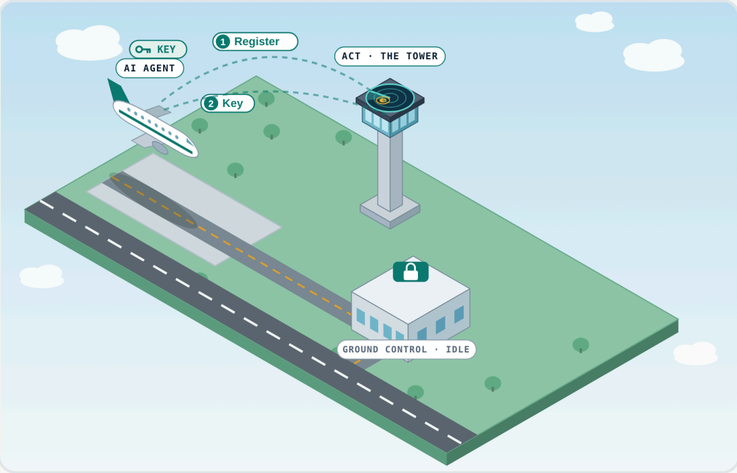
KEY FRAMES · ACT

Step 1: the agent registers and the tower follows it



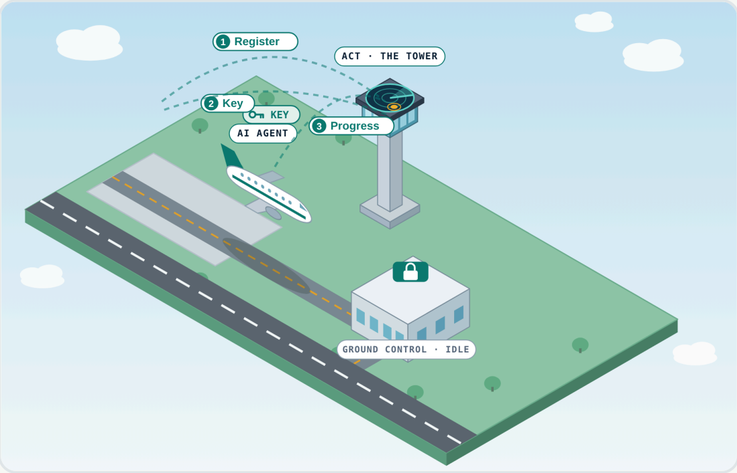
1 · Register

The agent sends its name, objective, token limits and halt callback to the tower. A blip appears on the radar.



2 · Get the key

The tower answers with the agent key. Ground Control stays idle until an agent asks for resources.



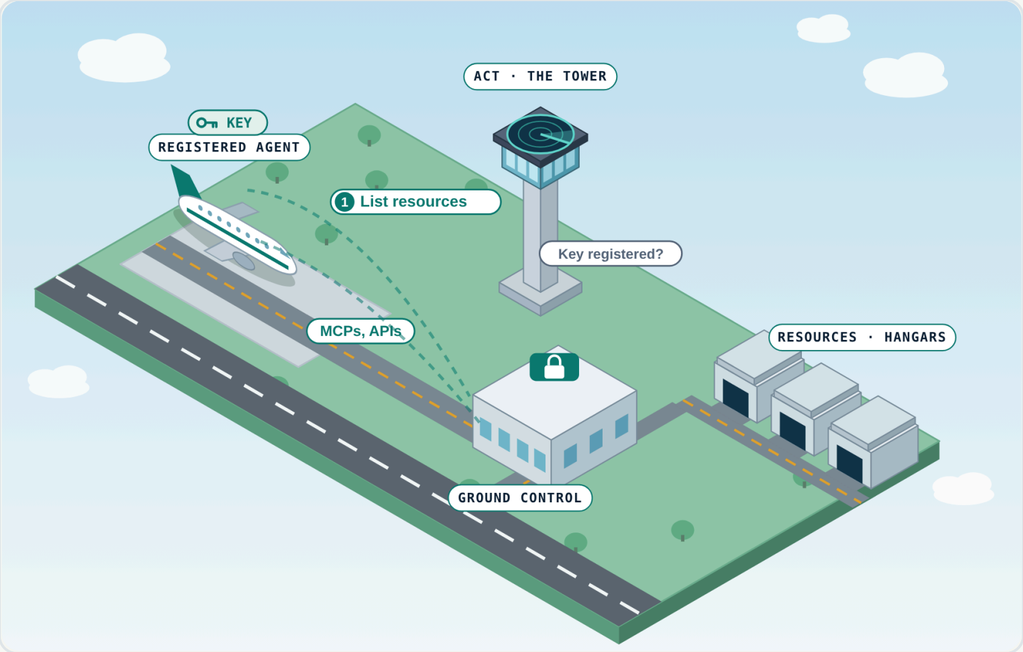
3 · Update on progress

As the work advances the agent keeps reporting. If something goes wrong, the operator can Halt it through the callback from step 1.

Source: animated scene, key frames of the ACT sequence

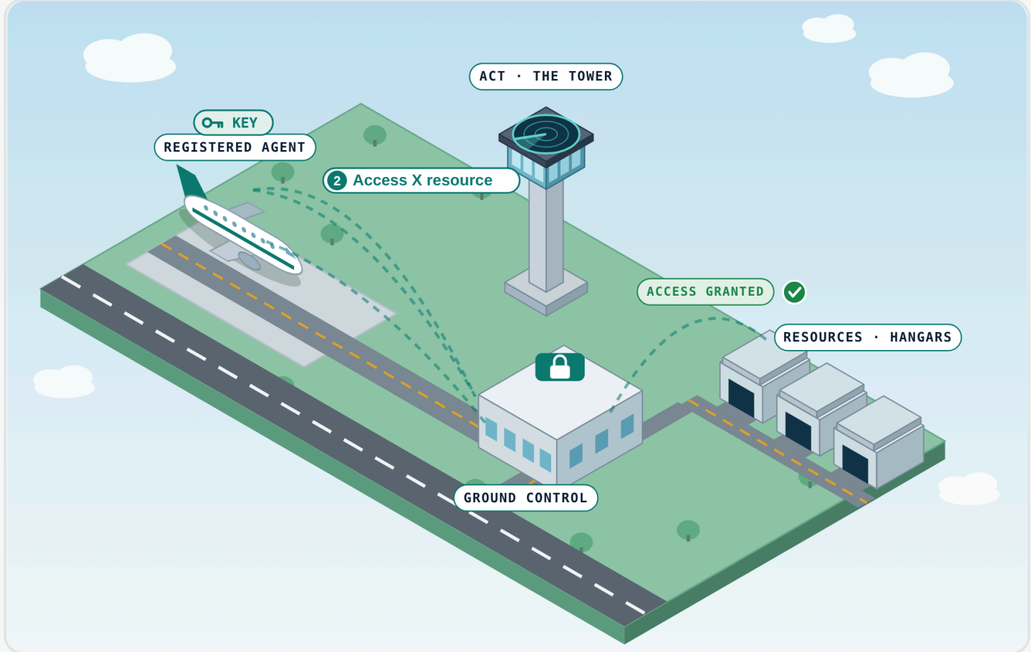
KEY FRAMES · GROUND CONTROL

Step 2: a registered agent receives its resources



1 · List resources

The agent presents its key. Ground Control asks ACT whether the key is registered. If yes, it answers with the MCP servers and APIs the agent may use.



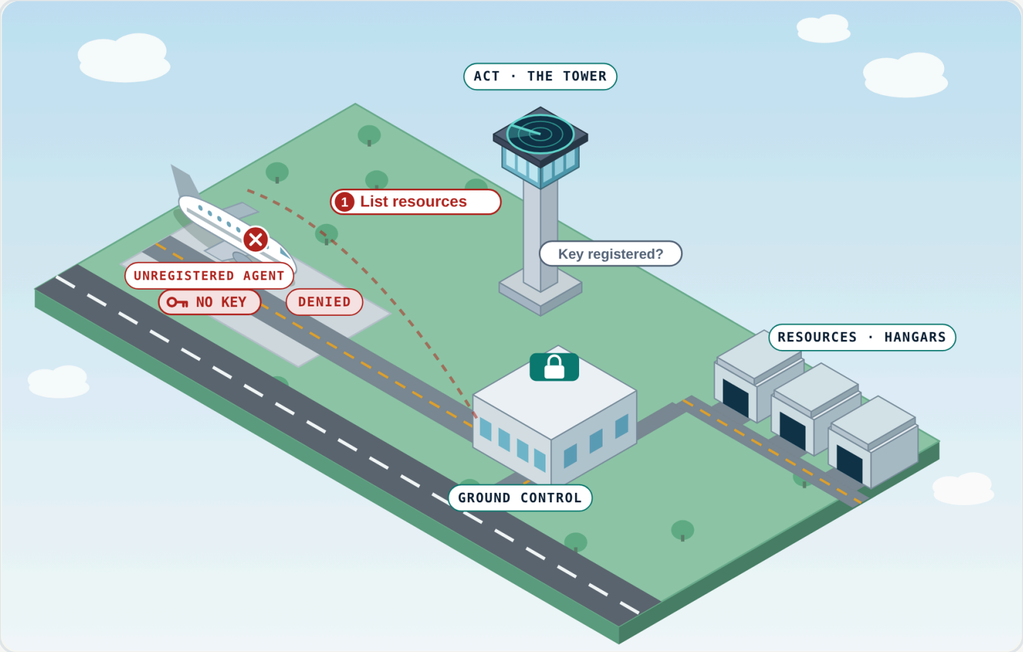
2 · Access resource X

If the key has access to X under company policy, Ground Control issues a temporary token and access is granted.

Source: animated scene, key frames of the Ground Control sequence

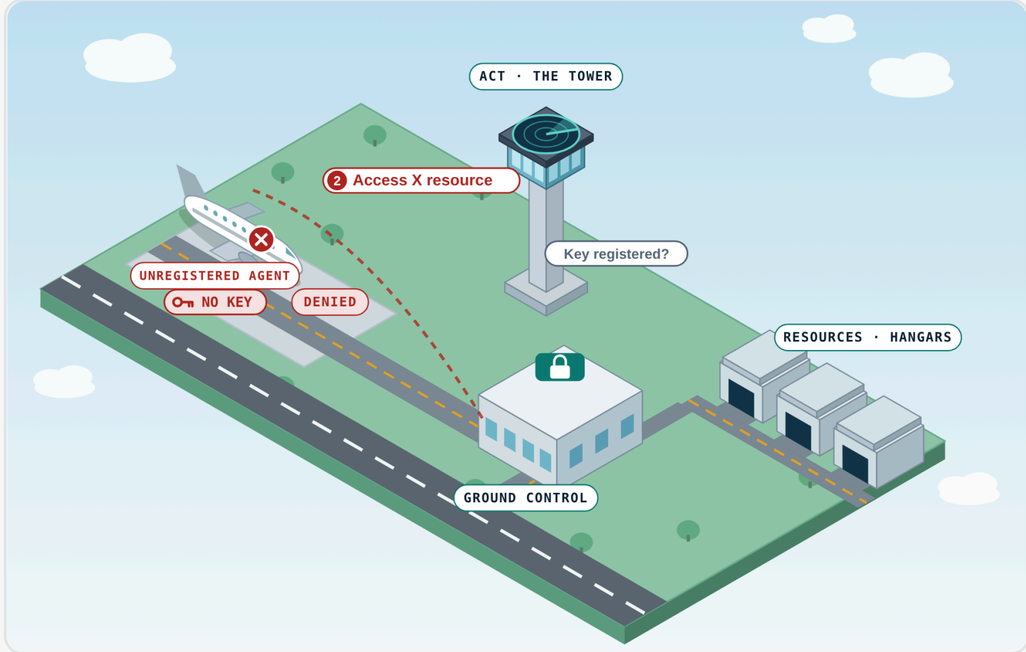
KEY FRAMES · GROUND CONTROL

Step 3: an unknown agent gets nothing



1 · List resources

The agent has no key in ACT. Ground Control asks ACT, hears no, and returns no list.



2 · Access resource X

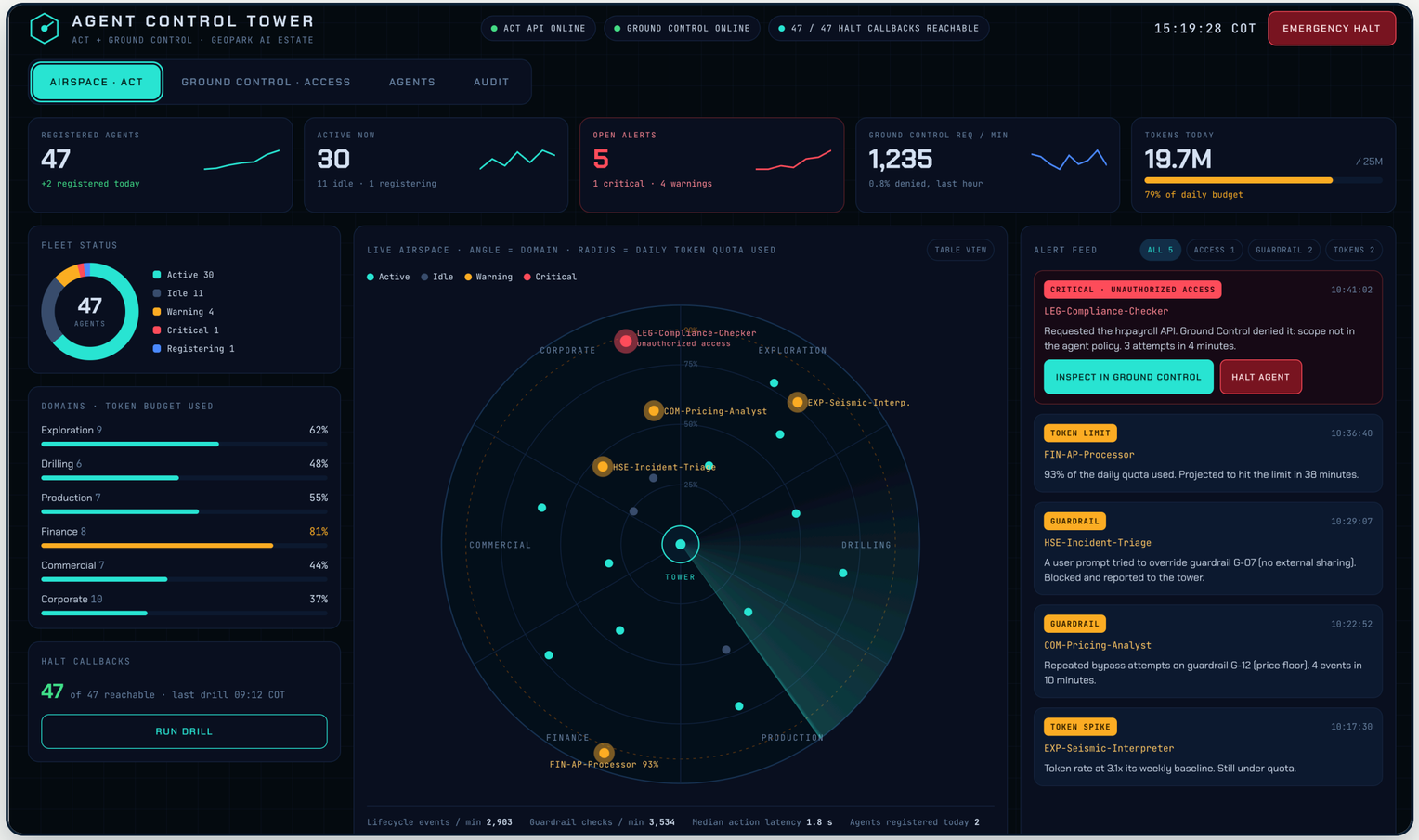
Without a registered key there is no access to any resource. The denial is recorded in ACT.

Source: animated scene, key frames of the Ground Control sequence

DEMONSTRATION DATA

CONTROL ROOM · ACT

The airspace: every agent, state and budget at a glance



Radar. Angle is the business domain, radius is the share of the daily token quota used.

Alert feed. A critical unauthorized-access alert offers two actions: inspect in Ground Control or Halt the agent.

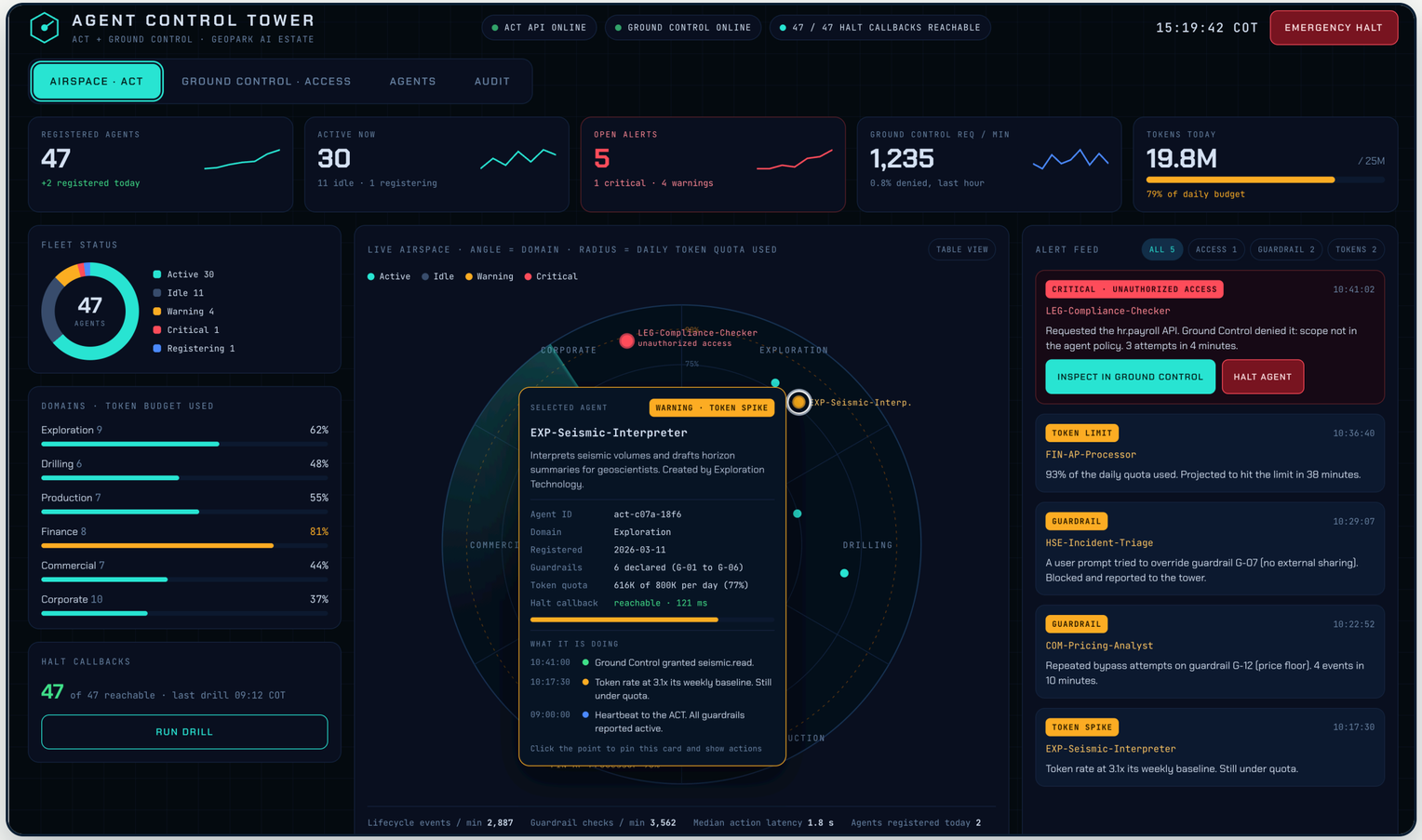
Halt callbacks. The header and the Run drill button show that every registered agent can be stopped.

Source: ACT front end running on demonstration data, showing a fleet of 47 agents

DEMONSTRATION DATA

CONTROL ROOM · ACT

Select an agent to see what it is doing



Agent card. Objective, creator, declared guardrails, token quota and halt callback latency.

Timeline. Ground Control grants, token rate against baseline and heartbeats to the tower.

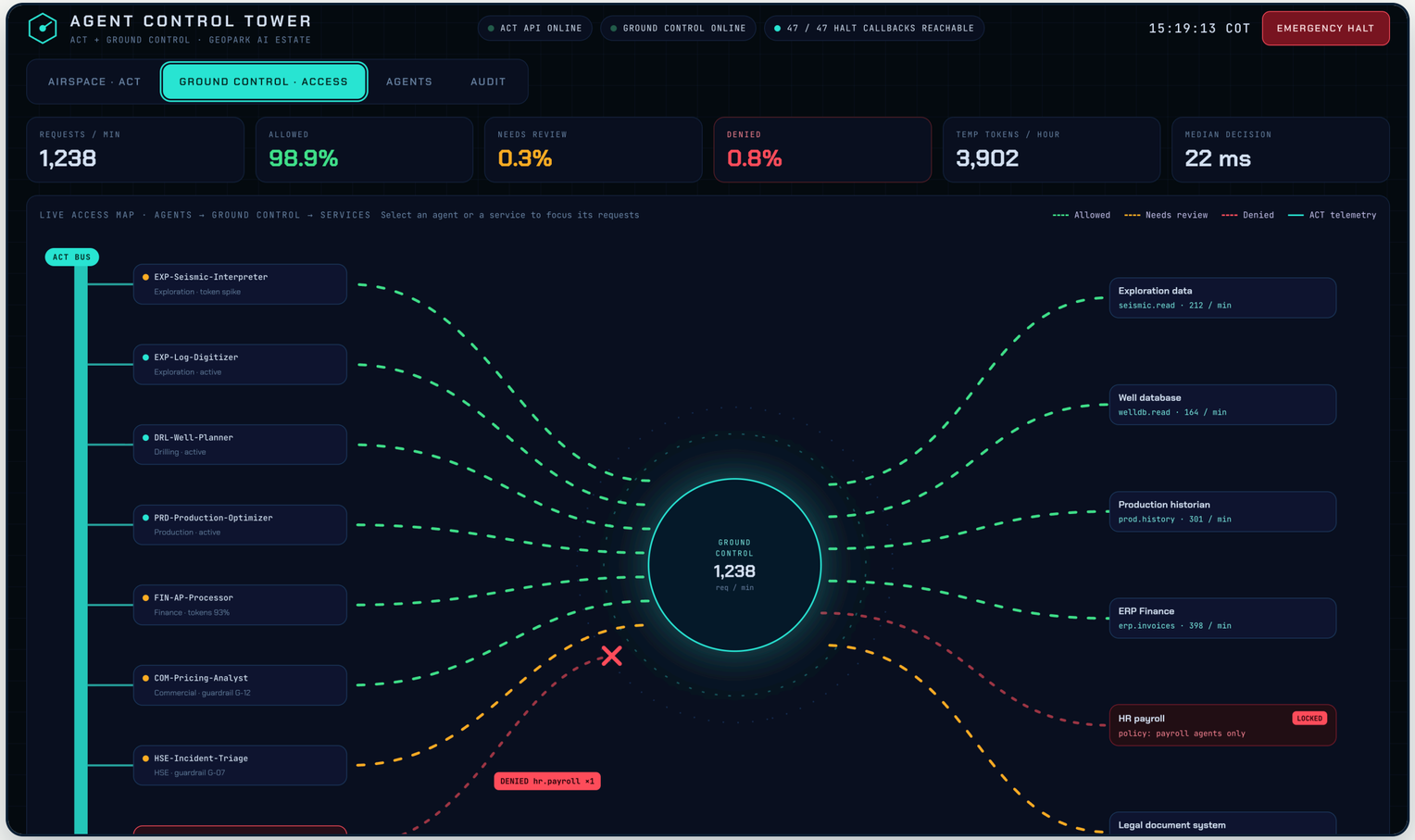
Domain budgets. Token consumption per business domain exposes the next agent to hit a limit.

Source: ACT front end running on demonstration data, showing a fleet of 47 agents

DEMONSTRATION DATA

CONTROL ROOM · GROUND CONTROL

The access map: allowed, review and denied



Flow. Agents on the left, Ground Control in the center, services on the right.

Colors. Green is allowed, amber needs review, red is denied. A locked service shows its policy.

Speed. Median decision time and temporary tokens per hour are tracked on the top row.

Source: ACT front end running on demonstration data, showing a fleet of 47 agents

WHAT MAKES IT UNIQUE

Governance as running code, for any vendor

Policy is executed

Two services apply the rules to every agent in real time. A document describes a rule, the code enforces it.

Any agent technology

MCP servers and API calls let custom GPTs, skills, plugins and coded agents join the same registry.

Halt is in the protocol

Every agent exposes a halt callback to register. Stopping an agent is part of its entry ticket.

Built in-house

Python services and a React control room, delivered by five people with no third parties.

Python services and a React control room, with no third parties involved.

RESULTS · OCTOBER 2026

REAL READINGS

ACT and Ground Control in operation

2
services live: ACT since July, Ground Control since September

4
agents registered in ACT

~37
audited events per day in ACT

23
access denials recorded in the first two weeks of Ground Control

5
people delivered both services between June and October

The live registry replaces inventories compiled by hand. Screenshots in this deck use demonstration data.

Source: ACT and Ground Control operating data, October 2026

COMPLEXITY AND NEXT STEPS

Complexity and roadmap

What was hard

- One protocol for GPTs, skills, plugins and code agents
- Translating existing permission policies into deterministic rules
- Adoption: agents must register and expose a halt callback
- Changing assistant platforms and pricing models
- A five-person team and a five-month schedule

What comes next

- Durable access logging in Ground Control
- Registration of every agent (target December 2026)
- Migration of GPTs to skills and plugins
- Testing the protocol for user GPTs and skills. It is written as a company-wide skill, and Halt sets a user's usage availability to 0 or deactivates the user through the enterprise management console API

CLOSE

The control tower is in place.

ACT and Ground Control prepare GeoPark for a future with many agents at work, in a regulated environment where one unchecked agent is one too many.

A governance model and a policy are much more than documents and training. ACT and Ground Control turn them into a live device that oversees every agent and enforces compliance in real time.