ZERO-TRUST DEPLOY GATE FOR AI CODING AGENTS ON AWS

AXIOM

AI agents hold proofs, not permissions.

Every AWS change an AI agent makes must be proved safe before a credential exists to make it.

BLOCK · touches a resource it never declared

ALLOW · 15-minute key for one change set

SWIPE →

Your AI agent has your AWS keys.

01 It can do anything those keys allow, whether it followed your instruction or a prompt injection hidden in an issue it read.

02 Reviewing every diff by hand doesn't scale. It throws away the speed the agent was brought in for.

03 An LLM reviewer is a probability, not a guarantee. It can be wrong, and it can be talked out of its own rules.

A guardrail you can argue with is not a guardrail.

02 / THE GATE

Four steps. Zero standing permissions.

01 DECLARE	The view-only agent submits its change and a declared scope: exactly which resources it will touch.
02 COMPUTE	AWS CloudFormation computes the change set, so AWS itself reports what will change.
03 DECIDE	Deterministic axioms and IAM Access Analyzer automated reasoning set the verdict. No model in the loop.
04 MINT	AWS STS issues a 15-minute credential for that one change set, tagged with its proof hash.

EVERYTHING ELSE → AccessDenied, enforced by IAM. Fails closed.

03 / THE DESIGN CHOICE

We removed the LLM from the security path.

LLM JUDGE	AXIOM
Probabilistic: the same change can get different verdicts	**Deterministic: same change, same verdict, every time**
Promptable: a template can argue back	**Immune: "ignore your rules" is just a string**
An opinion	**A proof: automated reasoning over IAM policy**
Hard to audit	**Every BLOCK traces to a named rule**

INTENT AS A CONTRACT

The agent declares its scope up front. Anything it touches outside that scope is blocked.

04 / VERIFIED ON LIVE AWS

Proved in production, not on slides.

12/12

live adversarial scenarios, every verdict as expected

15 min

credential lifetime, scoped to one change set

$0.00

fiat exposure, run on the AWS Free plan

<24 h

from zero to a live, verified deployment

DENIED The key that deployed a table could not delete it.

MATCH CloudTrail tied the proof hash to the exact key that executed the change.

05 / CREDITS

Built by an AI coding agent. Architected via Systemic Orchestration.

THE BUILDER · AI CODING AGENT (CLAUDE CODE)

Wrote the codebase, the infrastructure and the tests, and verified every claim against live AWS.

THE ORCHESTRATOR · SURYA PRASANTH R

Directed the build phase by phase, set the hard constraints (deterministic only, $0.00 fiat), made the product calls, and approved every production deploy.

ENTRY · AWS BUILDER CENTER · ZERO TO SHIPPED

builder.aws.com/project/3K7u8bnc2nRfkWZPa5NlKJkTkOd

#AISecurity #DevSecOps #ZeroTrust #AWS #AIAgents

Independent project. Not affiliated with or endorsed by AWS.