CEDAR AUTHORIZATION PRIMER

Cedar and the

Agentic Authorization Boundary

Where an agent's proposed action becomes a governed system decision

A neutral architecture primer with direct AWS Cedar implementation evidence and clearly bounded cross-framework comparisons.

FIRST-PARTY SOURCES / INDEPENDENT LUMINITY SYNTHESIS



Agentic Authorization Needs a Trusted Boundary

The model can propose an action. Identity, policy evaluation, enforcement, and evidence remain responsibilities of the trusted runtime.

AT A GLANCE

1	3	3	0
external decision for each material action	authority layers agent, delegation, user	conditions for an enforced block	provider adoption claims without direct evidence

Trusted Boundary 01

The runtime converts a model proposal into a request that can be authorized and enforced.

Evidence Boundary 02

Direct AWS use stays separate from compatible OpenAI and Anthropic control patterns.

IN THIS PRIMER

Key Points

01 Agent Actions Create an Authorization Boundary

The agent proposes an action. A trusted runtime establishes facts, obtains a decision, and enforces it before execution.

02 Shared Control Points Across Agent Frameworks

OpenAI and Anthropic document application-owned tool controls that align with the same boundary, without establishing Cedar adoption.

03 AWS AgentCore Uses Cedar at the Tool Boundary

AgentCore Gateway can intercept covered tool traffic and evaluate Cedar policies before allowing access to the target.

04 Multi-Agent Delegation Requires Layered Authority

A delegation chain needs separate checks for the invoking agent, each delegation hop, and the originating user's authority.

05 Enforcement Exists Only on the Covered Path

A Cedar decision becomes a blocking control only when the request uses the covered route, the engine is associated, and enforcement is active.

Cedar authorizes. The surrounding runtime establishes facts and enforces the result.

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

Cedar, AWS, OpenAI, and Anthropic first-party sources · verified Nov 14, 2026

Agent Actions Create an Authorization Boundary

The agent proposes an action. A trusted runtime establishes facts, obtains a decision, and enforces it before execution.

CONTROL EVIDENCE

- ✓ Agent proposal — UNTRUSTED PLAN
- ✓ Identity and context — TRUSTED SOURCE
- ✓ External decision — ALLOW OR DENY
- ✓ Runtime enforcement — BEFORE ACTION
- ! Prompt instruction — NOT AUTHORITY

Requested Action → Governed Execution

AUTHORIZATION PATH

Agent proposal | Trusted request | External decision

1. **Propose** — Tool and arguments
2. **Assemble** — Identity and context
3. **Authorize** — Policy decision
4. **Enforce** — Execute or block

FOUR INTERPRETATIONS

Proposal Is Evidence — MODEL

The model's output describes a requested action. It does not grant authority.

Facts Need Provenance — INPUT

Identity, session, resource, and request data come from trusted systems.

Decision Stays External — PDP

A policy engine evaluates the actual action outside the model's plan.

Execution Is Guarded — PEP

The runtime applies the result before the tool or system operation runs.

BOUNDARY TEST

Treat the model as untrusted | Authorize the actual request | Enforce before execution | Retain the disposition

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

AWS AgentCore Cedar rationale and Cedar authorization · verified Nov 14, 2026

Shared Control Points Across Agent Frameworks

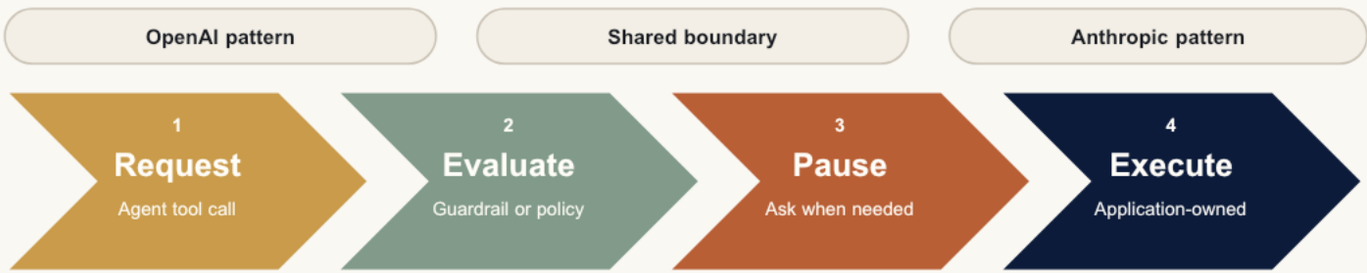
OpenAI and Anthropic document application-owned tool controls that align with the same boundary, without establishing Cedar adoption.

CONTROL EVIDENCE

✓ Tool call intercepted	APPLICATION
✓ Approval or policy check	BEFORE USE
✓ Custom tool execution	OWNED IN CODE
✓ Credentials isolated	RUNTIME
! Cedar endorsement	NOT ESTABLISHED

Requested Action → Governed Execution

AUTHORIZATION PATH



FOUR INTERPRETATIONS

OpenAI — PATTERN

Tool guardrails and approval interruptions sit around calls with side effects.

Anthropic — PATTERN

Managed policies evaluate allow, ask, or deny while custom tools remain application-owned.

Common Boundary — SHARED

A trusted harness controls credentials, execution, and side effects around model output.

Evidence Limit — LIMIT

Compatible architecture does not prove that either provider uses or endorses Cedar.

BOUNDARY TEST

- Separate model intent from execution
- Keep credentials outside the model
- Pause sensitive actions
- Avoid adoption claims

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

OpenAI guardrails and approvals and Anthropic permission policies · verified Nov 14, 2026

AWS AgentCore Uses Cedar at the Tool Boundary

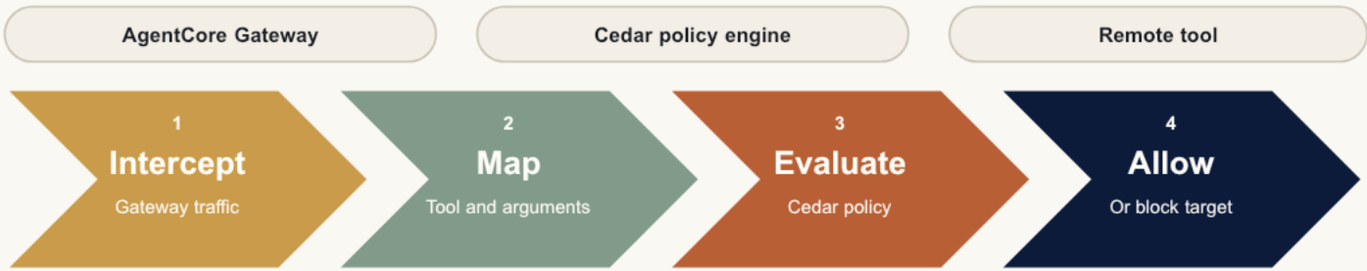
AgentCore Gateway can intercept covered tool traffic and evaluate Cedar policies before allowing access to the target.

CONTROL EVIDENCE

✓ Gateway in request path	COVERED TRAFFIC
✓ Policy engine associated	CONFIGURED
✓ Cedar request evaluated	PER INVOCATION
✓ Tool access controlled	RUNTIME
! Uncovered route	OUTSIDE BOUNDARY

Requested Action → Governed Execution

AUTHORIZATION PATH



FOUR INTERPRETATIONS

Direct Implementation — AWS

AWS documents Cedar as the policy layer for covered AgentCore Gateway traffic.

Default Boundary — POLICY

Associated policies selectively open a boundary that blocks covered traffic by default.

Authoring Analysis — ANALYSIS

Cedar Analysis supports checks for logical errors and policy conflicts.

Scope Limit — LIMIT

The example proves one implementation pattern, not universal agent governance.

BOUNDARY TEST | Attribute the design to AWS | Confirm Gateway coverage | Evaluate each invocation | Keep the claim narrow

Luminity Digital
INTELLIGENCE, ENGINEERED, DELIVERED.

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

AWS AgentCore Cedar rationale and Cedar security · verified Nov 14, 2026

Multi-Agent Delegation Requires Layered Authority

A delegation chain needs separate checks for the invoking agent, each delegation hop, and the originating user's authority.

CONTROL EVIDENCE

- ✓ Agent-to-tool authority — LAYER 1
- ✓ Agent-to-agent scope — LAYER 2
- ✓ Originating user context — LAYER 3
- ✓ Context integrity — VERIFIED
- ! Self-asserted trust — UNSAFE

Requested Action → Governed Execution

AUTHORIZATION PATH

Invoking agent | Delegation chain | Originating user

1. **Verify** — User and agent
2. **Constrain** — Hop and capability
3. **Evaluate** — All policy layers
4. **Record** — Decision evidence

FOUR INTERPRETATIONS

Agent to Tool — L1

Check the invoking agent's namespace, lifecycle, and tool authority.

Agent to Agent — L2

Bound delegation depth and requested capabilities at each hop.

Originating User — L3

Preserve the human's role and authentication context through the chain.

Authoritative Attributes — SOURCE

Production attributes need a trusted source, not an agent-controlled payload.

BOUNDARY TEST

Preserve the initiating user | Bound delegation depth | Validate agent attributes | Deny on any failed layer

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

AWS Cedar agentic authorization sample · verified Nov 14, 2026

Enforcement Exists Only on the Covered Path

A Cedar decision becomes a blocking control only when the request uses the covered route, the engine is associated, and enforcement is active.

CONTROL EVIDENCE

- ✓ Covered target — IN PATH
- ✓ Policy engine ID — AVAILABLE
- ✓ Enforcement mode — ENFORCE
- ✓ Decision disposition — OBSERVABLE
- ! LOG_ONLY mode — ALLOWS REQUEST

Requested Action → Governed Execution

AUTHORIZATION PATH

Covered route | Associated engine | ENFORCE mode

1. **Trace** — Actual topology
2. **Confirm** — Engine association
3. **Inspect** — Runtime mode
4. **Prove** — Blocked disposition

FOUR INTERPRETATIONS

Route Coverage — PATH

The policy remains inert for requests that bypass the covered Gateway target.

Engine Association — ENGINE

A deployed mode string cannot replace evidence that a policy engine exists and is attached.

Mode Matters — MODE

LOG_ONLY records a decision and still allows the request to continue.

Acceptance Evidence — PROOF

Retain topology, engine ID, mode, decision, and final execution disposition.

BOUNDARY TEST — Trace the real request path | Verify the engine association | Distinguish observe from block | Prove final disposition

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

AWS Builder Cedar enforcement article · verified Nov 14, 2026