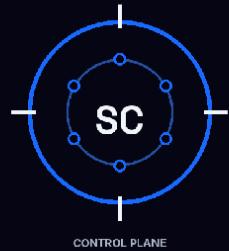


SESSION CUSTODY

EXPLAINER SERIES



PRINCIPLE EXPLAINER

Contain: Keeping Local Failure from Becoming Enterprise Exposure

Precise blast-radius control for changed authority, drift, and economic exposure.

GOVERN • CONTROL • ENFORCE



GOVERN THE SESSION, NOT THE REQUEST.

sessioncustody.ai

Publication Edition | Explainer T1 | April 30, 2026

EXPLAINER 11 | APRIL 30, 2026 | CONTAIN

Contain: Keeping Local Failure from Becoming Enterprise Exposure

Precise blast-radius control for changed authority, drift, and economic exposure.

The Purpose of Containment

Containment is the enterprise's ability to keep a local problem local. Autonomous work makes that harder because sessions can persist, retry, revise, and delegate. A small change in policy, approval, risk, or economic state can propagate if already-active work continues under authority that is no longer current.

The failure is often sequential. The session begins correctly, conditions change, and a chain of locally plausible actions continues. Containment prevents changed authority from becoming a later enterprise consequence.

Containment is complete only when affected active work - including descendants - cannot use stale authority for its next covered consequential action.

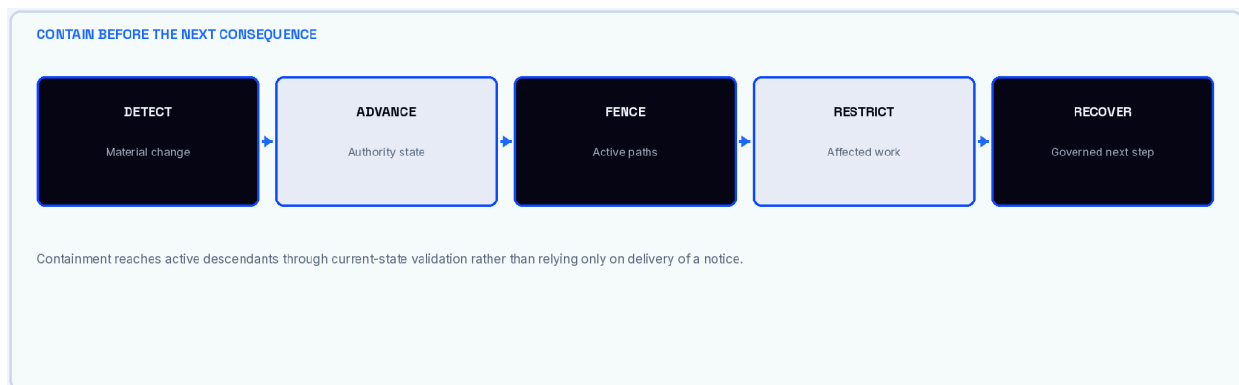


Figure 1. A material change advances authority state, fences affected paths, and authorizes a governed recovery response.

Why Notice Alone Is Insufficient

Publishing a revocation or policy-change message is necessary but not sufficient. Delivery can be delayed, a child can be disconnected, or a runtime can retain an older favorable instruction. The architecture therefore combines authoritative state advancement with action fencing at covered execution boundaries.

The action fence validates the presented policy and revocation binding against current authoritative state. If the binding is stale, superseded, expired, mismatched, or unverifiable, the earlier authorization is not reusable for that covered action.

Restrictive Handling Is Precise

Fail-restrictive operation does not require the same response for every uncertainty. The controlling policy defines behavior by action class, consequence, reversibility, and enforcement coverage. Expressly authorized diagnostics may continue under bounded conditions, while a payment, infrastructure change, credential issuance, or other high-consequence action may be held, escalated, denied, or quarantined.

Condition	Risk	Representative bounded response
Approval or exception expires	Earlier favorable authority may be reused outside its scope or duration.	Invalidate the stale binding; refresh, escalate, or deny the covered action.
Policy or risk state changes	Active sessions and descendants may continue under superseded assumptions.	Advance current authority state and require re-adjudication before covered consequence.
Parent is restricted	Child work may remain technically active after upstream authority narrows.	Fence affected descendants at their next covered consequential boundary.
Economic limit is reached	Retries, loops, and fan-out can turn local inefficiency into operating exposure.	Throttle, narrow, hold, escalate, or stop spend-bearing paths according to policy.
Enforcement state is unavailable	The control plane cannot establish preventive coverage for the action.	Apply the action-class-specific restrictive posture; do not expand authority through uncertainty.

Economic Containment

Cost can become authority-bearing when configured policy makes budget, burn rate, retry count, fan-out, or projected completion cost material to continuation. The objective is not merely to report spend. It is to prevent the affected session from continuing to consume resources after its economic authority has narrowed.

Recovery Is Also Governed

Containment is not the end of the lifecycle. Once the affected path is stable, the control plane can authorize a safe next step such as refresh, bounded resume, idempotent retry, compensation, human remediation, or continued quarantine. The orchestrator performs the recovery mechanics; the governing state defines which recovery is permitted, under what conditions, and with what evidence.

Contain gives autonomy a practical blast-radius boundary: changed authority reaches the affected work before its next covered consequence, and recovery proceeds under current authority.

OPERATING BOUNDARY

These explainers describe the Session Custody product and category at a conceptual and operational level. Coverage depends on supported sources, configured mappings, authenticated integrations, and declared enforcement paths. The architecture does not assume a universal policy language, permanent authorization, human approval for every action, or replacement of the systems that own native enterprise facts and outcomes.