

SESSION CUSTODY

EXPLAINER SERIES



SOLUTION EXPLAINER

Session Custody: The Enterprise Control Plane for Enterprise AI

How the Session Custody AGCP turns session governance into production-grade enterprise AI control.

GOVERN • CONTROL • ENFORCE



GOVERN THE SESSION, NOT THE REQUEST.

sessioncustody.ai

Session Custody: The Enterprise Control Plane for Enterprise AI

How the Session Custody AGCP turns session governance into production-grade enterprise AI control.

The Boundary Has Changed

Enterprise AI is no longer limited to producing answers for humans to review. The next operating shift is already underway: autonomous agents are beginning to perform work inside live enterprise environments. They retrieve records, call tools, update workflow systems, route approvals, prepare payment packets, provision infrastructure, delegate subtasks, spend compute, and continue operating across time.

That shift changes the control question. The enterprise no longer needs only to ask whether an AI-generated answer is accurate, useful, or safe to read. It must ask whether the next autonomous action should be permitted before it changes enterprise state.

Most organizations already have mature systems for identity, policy, approvals, observability, risk, compliance, audit, spend, and workflow management. Those systems remain necessary. But they were not designed to govern autonomous work as a continuous chain of action. They see credentials, requests, tickets, traces, policy records, and logs. They do not consistently see the full session: the objective, authority path, policy state, approval scope, delegated lineage, exception boundary, revocation state, economic posture, and evidence requirement at the moment the next side effect is proposed.

That is the enterprise control gap in autonomous work.

Why the Session Is the Governed Unit

Autonomous risk rarely appears as a single obviously invalid action. It usually emerges across time.

A procurement agent may begin with a valid vendor-onboarding objective, retrieve approved supplier data, route legal review, request finance approval, and prepare a purchase-order packet. Each action may appear reasonable in isolation. The session may become invalid only after the context changes: a temporary approval expires, a budget threshold is crossed, a vendor-risk status changes, or a delegated review continues under stale authority.

A request is a moment. A session is the full causal chain of autonomous work: objective, planning, tool use, retries, approvals, delegation, child sessions, side effects, containment, and termination. Risk and meaning accumulate across that chain. Governance must therefore attach to the session itself, not merely to individual requests or after-the-fact event records.

This is the core premise of the Agent Governance Control Plane, or AGCP: production autonomous work must be governed while it is executing, in context, before enterprise consequence occurs.

Session Custody AGCP

Session Custody is the patent-pending, vendor-neutral Agent Governance Control Plane for side-effecting autonomous enterprise workflows. It is built to govern autonomous work as supervised, attributable, policy-consistent, interruptible, economically bounded, and reconstructible sessions.

Session Custody does not replace the enterprise systems that already hold institutional authority. IAM remains authoritative for identity. GRC systems remain authoritative for policy records and control obligations. Workflow systems remain authoritative for approvals, tickets, and business process state. FinOps systems remain authoritative for spend signals. SIEM, incident, and audit systems remain authoritative for their respective review and response functions.

Session Custody sits above heterogeneous autonomous runtimes and below or alongside those systems of record. Its role is to bind their signals into session-level runtime authority. It computes whether the next autonomous side effect should be allowed, constrained, escalated, denied, throttled, restricted, quarantined, or terminated.

In simpler terms: Session Custody turns institutional policy into runtime control, and runtime behavior into evidence-of-record.

The Six Operating Principles

Govern

Every production agent requires identity, ownership, approved purpose, operating environment, sanctioning state, risk tier, and authority ceiling. Every session requires an objective, workflow context, policy context, approved tool and data scope, economic envelope, lineage root, and termination condition. Session Custody establishes that frame before autonomous work begins, preventing agent sprawl from becoming anonymous enterprise behavior.

Control

Autonomous work changes as it executes. Approvals expire. Budgets shift. Policy updates. Risk states move. Telemetry changes. Delegated work expands. Session Custody maintains a current session snapshot so each proposed action can be evaluated against live context rather than stale permission.

Enforce

Governance is not operational if it remains only in policy documents, approval notes, or retrospective logs. Session Custody performs pre-execution adjudication before side-effecting actions occur. It evaluates the proposed action against the session objective, effective policy, authority ceiling, exception state, delegated lineage, revocation state, and economic posture. Enforcement happens while there is still time to prevent consequence.

Delegate

Agents become useful when they can distribute work. They become dangerous when delegated work loses upstream constraint. Session Custody treats delegation and spawning as governed events. Child sessions inherit authority ceilings, policy context, budget boundaries, exception scope, lineage references, and revocation channels, so scale does not become a bypass path.

Contain

Authority can change after work has already begun. A parent session may be quarantined. A budget limit may be reached. A temporary exception may expire. A policy fingerprint may change. Session Custody uses revocation epochs, signed revocation artifacts, action fencing, economic circuit breakers, and restrictive defaults to prevent active downstream work from continuing under obsolete authority.

Reconstruct

Autonomous work must be explainable in operational terms. Session Custody preserves evidence-of-record: objective, agent identity, owner-of-record, policy lineage, effective-policy fingerprint, approval scope, exception state, delegated work, revocation status, economic state, decision rationale, side effects, and accountable parties. Reviewers should not have to stitch together prompts, traces, tickets, logs, and staff narratives to understand why an autonomous action was allowed.

The Architecture Boundary

The Session Custody AGCP is a control plane, not a monolithic runtime, model gateway, chatbot, observability console, sandbox, or generic compliance dashboard. It coordinates governance semantics across distributed execution environments.

Its core services include the governed-agent registry, session supervisor, policy compiler, pre-execution adjudicator, delegation and revocation services, bounded exception handling, economic controls, provenance ledger, replay engine, APIs, and control console.

Its runtime adapter layer projects local controls near each agent environment: public cloud, private cloud, SaaS workflow agents, sidecars, proxies, MCP gateways, sandboxes, model routers, and internal automation frameworks. Those runtime substrates enforce local mechanics. Session Custody retains the higher-layer governance semantics: policy lineage, approval meaning, authority inheritance, revocation state, economic boundaries, and evidence-of-record.

This boundary is essential. Enterprises will not standardize every agent, model, framework, cloud, workflow system, and runtime on a single vendor. They need one governance model that can operate across many execution surfaces while preserving institutional authority inside customer-controlled environments.

The Operating Outcome

Session Custody is designed for the moment when enterprise AI moves from pilot utility to production consequence.

For CIOs and CTOs, it creates controlled scale across autonomous workflows without forcing every team to rebuild governance logic. For CISOs and risk leaders, it provides pre-execution authority and containment before side effects occur. For CFOs, it ties compute and agentic work to bounded units of value rather than opaque consumption. For compliance and audit teams, it produces evidence that reconstructs decisions, not merely events. For workflow owners, it allows useful agents to move faster without falling back into manual gates.

The result is not slower autonomy. It is governed autonomy.

Agents can still reason, retrieve, act, delegate, adapt, and complete work across systems of consequence. But their work remains attributable, policy-consistent, interruptible, economically bounded, and reconstructible while it is happening.

That is what an Agent Governance Control Plane should accomplish. And that is the role Session Custody is built to serve: the enterprise control plane for autonomous AI in motion.

SESSION CUSTODY EXPLAINER SERIES

Govern the session, not the request

Attributable * Policy-consistent * Interruptible * Economically bounded * Reconstructible