STATE OF AI ARCHITECTURE

УПРАВЛЯЕМАЯ ОБВЯЗКА КАК ЗАВИСИМОСТЬ

Новый вектор vendor lock-in в эпоху AI-агентов

Q1 2026 / DEEP DIVE ANALYSIS

VENDOR: AWS

STATUS: PRODUCTION

Bedrock AgentCore (Управляемая память, хранилище инструментов).

VENDOR: GOOGLE

STATUS: PRODUCTION

Agent Builder (Глубокая интеграция с Vertex Search).

VENDOR: OPENAI

STATUS: PRODUCTION

Assistants API v2 (Треды, векторные хранилища, интеграция в Bedrock).

VENDOR: ANTHROPIC

STATUS: PRODUCTION

Anthropic Agents (Hosted-окружение поверх MCP).

Управляемая обвязка перестала быть привязанной к одному вендору модели. Это теперь **индустриальный стандарт**.

78%

ROI < 1 YR

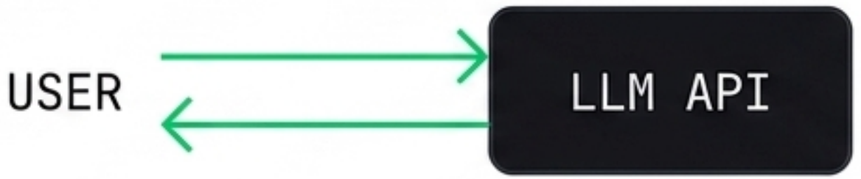
Демократизация: запуск AI-агента сократился с месяцев инженерных работ до часов.
(Данные: McKinsey State of AI 2025).

THE INVISIBLE DEBT

Иллюзия простоты

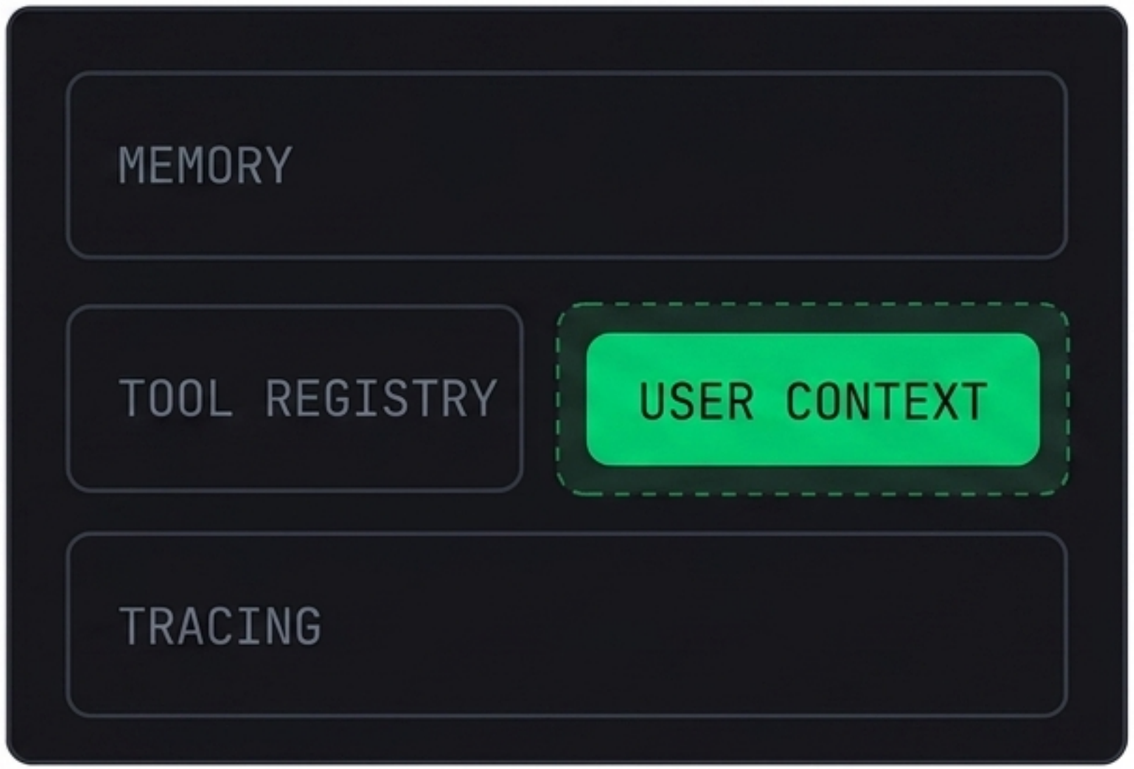
Внутри быстрого time-to-market спрятан новый вид зависимости. Этот lock-in сложнее, глубже и дороже для бизнеса, чем API-зависимость эпохи 2015 года.

STATELESS ROUTING (API 2015)



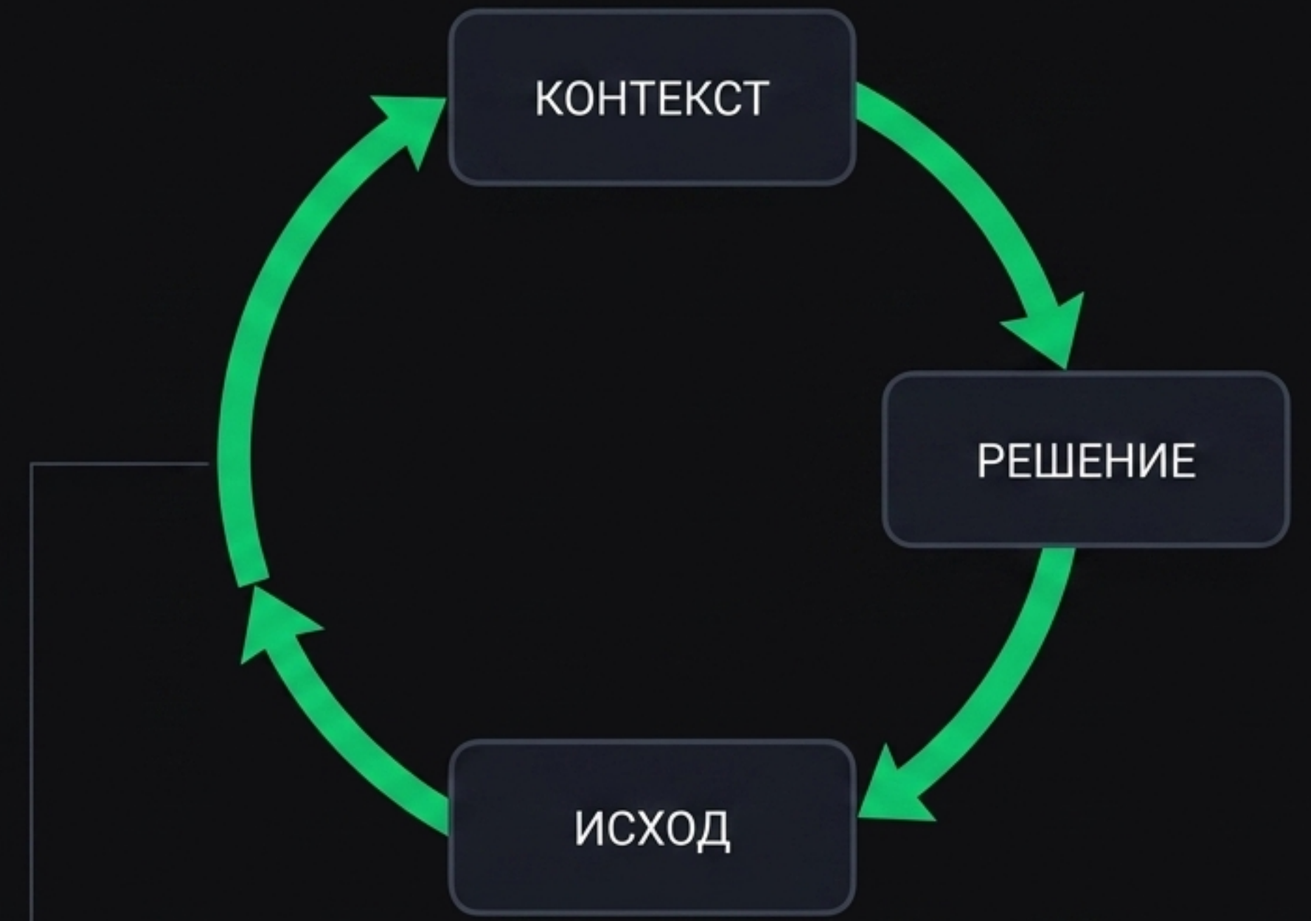
Логика, память и контекст живут на стороне клиента. Интеграция переписывается за недели.

STATEFUL ENVIRONMENT (HARNESS 2026)



Среда поглощает историю сессий, политики вызова инструментов и журнал решений. Контекст заперт внутри.

L1_VULNERABILITY: DATA GRAVITY

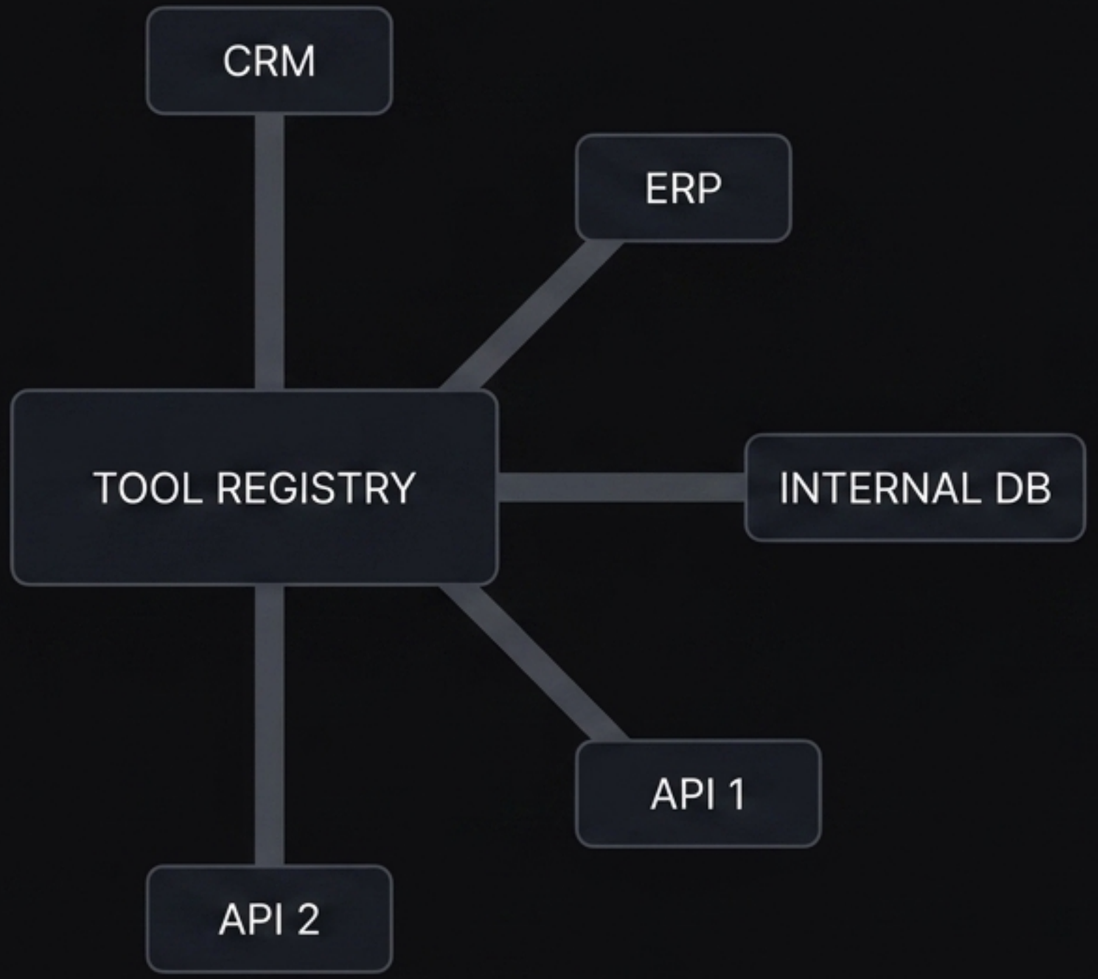


Память остаётся у провайдера.

Каждый диалог и след инструментального вызова оседает в управляемой памяти (Threads, Knowledge Bases).

Экспорт иллюзорен. Вы можете выгрузить файлы и JSON, но накопленная калибровка агента под специфику ваших процессов (этот цикл обратной связи) разрушается при миграции. Новый агент начнёт с нуля.

L2_VULNERABILITY: PROPRIETARY ROUTING



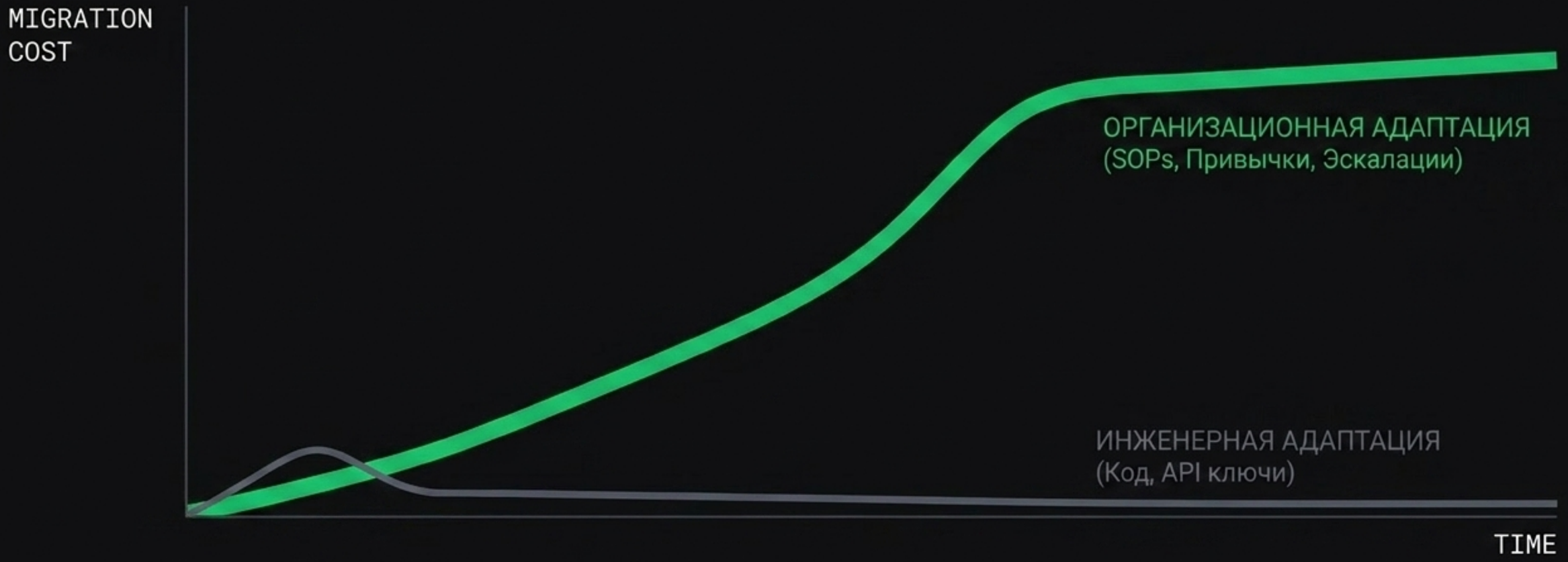
Маршрутизация решений.

Интеграция сотен внутренних инструментов пишется под конкретный contract провайдера.

CAVEAT: MCP

Anthropic Model Context Protocol формально снижает риск, но управляемая среда всё равно навязывает свой проприетарный слой абстракции для политик и управления. Открытость протокола не равна нейтральности платформы.

L3_VULNERABILITY: SOP INERTIA



Самый медленный и дорогой механизм. Люди адаптируются к поведению конкретного агента. Заново обучить организацию и пересобрать бизнес-процессы под нового агента занимает месяцы.

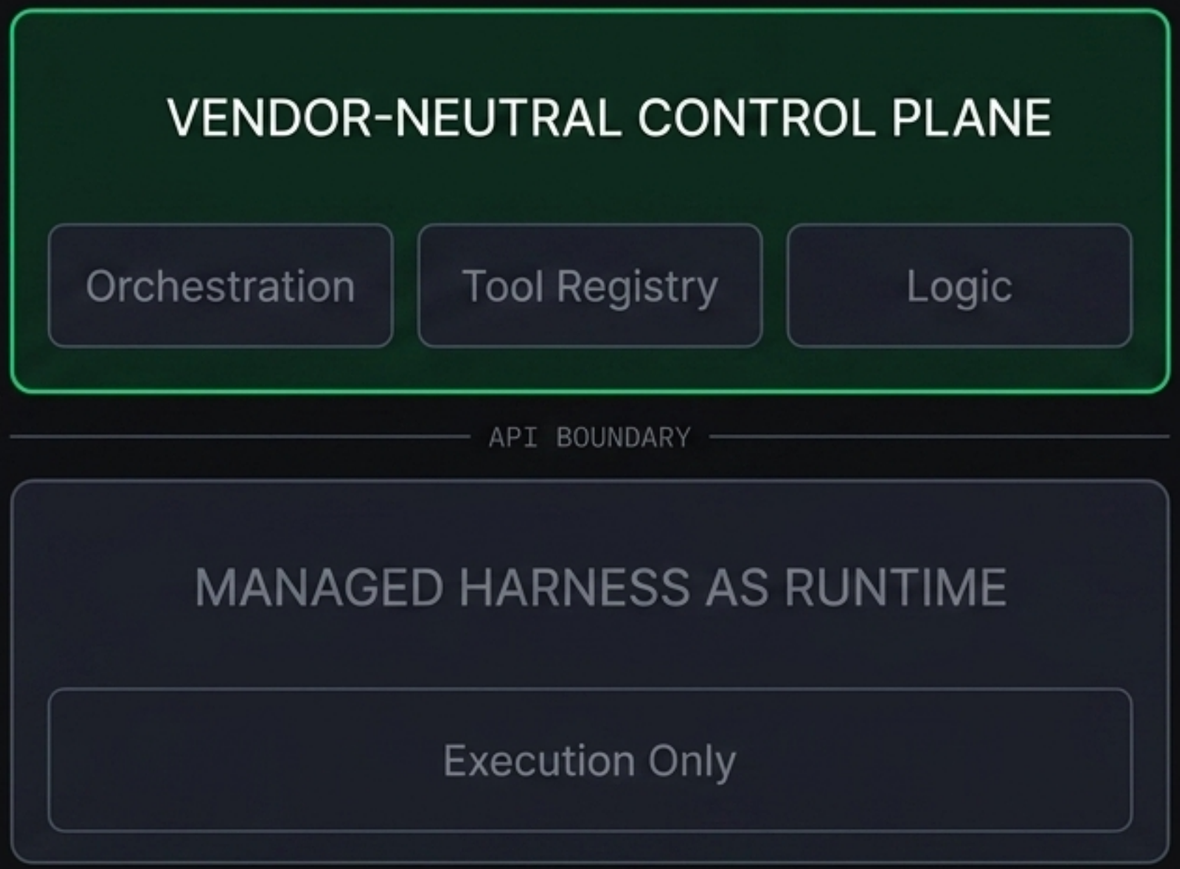
L4_DIAGNOSTIC: LOCK-IN DYNAMICS

ПАРАМЕТР	API LOCK-IN (2015)	MANAGED HARNESS (2026)
Что остаётся у поставщика	Маршрутизация запроса	Память, решения, SOP
Стоимость переключения	Недели инженерных работ	Месяцы организационной адаптации
Данные экспортируемы?	Да	Формально да, ценность теряется
Виден ли риск на старте?	Умеренно	Слабо — накапливается незаметно
Рычаг давления поставщика	Ценообразование	Ценообразование + операционная инерция

BUY = SAVE_INFRA + MODERATE_RISK

MANAGED_HARNESS = LAUNCH_SPEED + DEEP_OP_DEBT

«Просто запустить на managed harness» больше не является нейтральным выбором. Это разумный компромисс ради скорости, но требующий осознания накапливающейся операционной зависимости.



Архитектурная защита.

Защита строится не отказом от платформ, а выбором, где физически живёт control plane. (Примеры: LangGraph, Temporal, self-hosted MCP).

ROLE: ENGINEER

Держите control plane в своём коде и инфраструктуре. Используйте провайдера только как runtime-backend, а не как операционную платформу.

ROLE: EXECUTIVE

При оценке AI-проектов закладывайте стоимость переключения через 2-3 года в P&L уже сегодня. Незнание — это операционный риск.

ROLE: FOUNDER

Инвестируйте в нейтральную оркестрацию на старте. Это покупает возможность переключиться и даёт реальный рычаг в переговорах с вендорами позже.

RADAR: NEXT 12 MONTHS

РЕГУЛЯЦИЯ

Если AI Act начнёт требовать портируемости данных памяти агентов, провайдеры будут вынуждены конкурировать по openness.

АЛЬТЕРНАТИВЫ

Рост масштаба стартапов, предлагающих vendor-neutral agent orchestration как готовый продукт.

ЦЕНООБРАЗОВАНИЕ

Давление монетизации (платные вызовы памяти и registry) проявит финансовую зависимость быстрее, чем операционную.

- [x] Обвязка — это операционная платформа со скрытым состоянием, а не просто stateless API.
- [x] Ценность накопленных данных (калибровка) неотделима от контекста платформы провайдера.
- [x] Основная стоимость перехода — организационная (занимает месяцы, переписываются бизнес-процессы).
- [x] Архитектурное решение: Vendor-neutral control plane на вашей стороне, managed harness исключительно как runtime.

END OF BRIEF