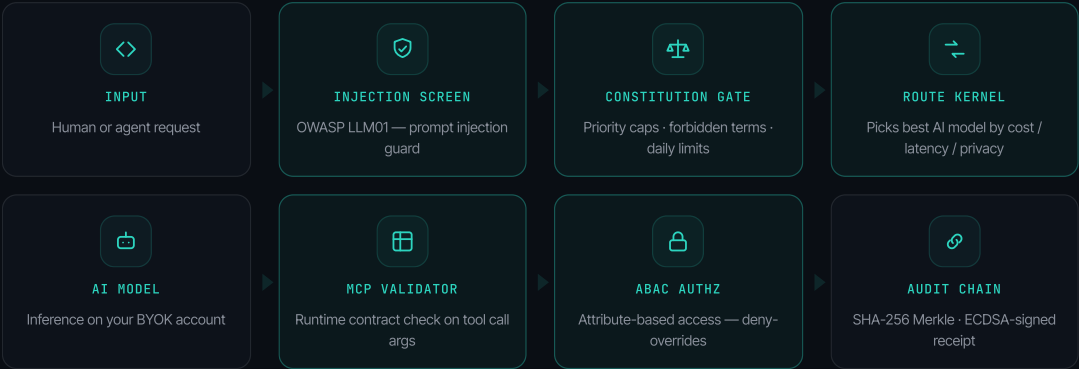


● BUSINESS BRIEF

The workspace where *agents do the work.*

EcoCloud is an **AI-native, agent-operable** task workspace. People (and their AI assistants) describe work in plain English; EcoCloud routes it, governs it, and executes it — with **scoped keys, a tamper-evident audit trail, and a human in the loop** for anything risky. Not a task board with AI sprinkled on top — an operating layer for humans and agents working together.

HOW AN AGENT ACTION FLOWS THROUGH ECOCLOUD



Every highlighted stage is a zero-dependency, isomorphic kernel — same logic runs in your browser and on the edge. All open-source, Apache-2.0.

WHAT IT DOES

AI Dispatch

Plain English → structured work

Type a sentence; EcoCloud extracts the task, owner, deadline and priority and routes it — instantly, on-device for the simple cases, with a model for the rest.

Agent-ready

Operable over MCP & REST

Any assistant or autonomous agent reads the discovery manifest and binds natively — scoped fdk_ keys, rate-limited and audited, 48+ governed signed tools.

Today Brief · new

The one screen that runs your day

Open work auto-triaged into Do now · Waiting on you · Blocked · Can slip, with a one-line plan and Team Capacity — who's overloaded, at a glance. All from your live tasks.

Routing Memory · new

Dispatch that learns your team

Every time you reassign a tagged task, EcoCloud remembers it — and auto-routes the next one to the right person. Deterministic, never overrides what you specify.

Outcome Receipts · new

"Done" you can prove

Completed governed work closes with an ES256-signed receipt — intent → action → verified result — checkable by anyone, offline, with no need to trust our database.

Governance

Constitution, ABAC & kill-switch

Per-agent rules, attribute-based micro-roles, confidence thresholds, an approval queue, and a one-switch pause over every autonomous action.

Route Kernel · new

Deterministic AI model routing

BYOK policy engine: hard-filters by health, capability and privacy level, then scores by cost and latency — returns ranked provider + signed attestation. Falls closed.

MCP Schema Validator · new

Runtime tool-call contracts

Protobuf-style field validation for every MCP tool/call argument: type, required, enum, bounds, format, nullable — per-field typed errors, signed attestation.

Company memory

A graph that proves itself

People, tasks, decisions and connected systems become a temporal knowledge graph — query what the team knew on any date, and who asserted it.

Workflows

Declarative DAG execution

Define multi-step work with dependencies, retries and human gates;

Reasoning

Execution diagnosis, not reporting

EcoCloud reasons over the work graph — surfacing the real delay drivers

Stripe billing · planned

Agent-initiated Pro upgrade

The flow is built — an agent calls start_checkout, the human pays on Stripe's hosted page, a signed webhook

the engine runs and records every transition for replay.

(blockers, stale work, throughput) with recommendations, from data.

writes the subscription row. Self-serve checkout activates once billing keys are configured ([tracked on /whats-live](#)).

THE FLAGSHIP KERNELS — OPEN SOURCE, ZERO DEPENDENCIES

These five are the flagship of a **40+ skill governance library** spanning six phases — authorize, measure, clear · settle · verify, identity & trust, lifecycle, audit & dispute. Run any of them live in your browser from the [Trust Layer](#).

K-01

Constitution
Gates the ACTION — priority caps, forbidden terms, objective tags, quiet hours, daily limits

isomorphic

K-02

Injection Screen
Guards the INPUT — NFKC+confusable+leet fold, split-payload check, OWASP LLM01 score ≥ 60 = BLOCK

v1.1

K-03

ABAC Authz
Gates RESOURCE ACCESS — attribute-based, deny-overrides, safe condition AST, fails closed

isomorphic

K-04

Route Kernel
Selects AI PROVIDER — BYOK policy, privacy-first hard filters, weighted scoring, 10/10 conformance

new

K-05

MCP Schema
Validates TOOL ARGS — JSON Schema subset, per-field errors, depth-8 + 50-item DoS caps, 12/12 conformance

new

Each kernel returns an ES256-signed attestation (kid: flowdesk-envelopes-2026) verifiable against the published JWKS — without trusting the database. Apache-2.0. Run them in your browser at [/route-kernel/](#) and [/mcp-schema/](#).

AGENT-DRIVEN BILLING — BUILT END-TO-END

AGENT
Calls start_checkout with the user's email — no payment data enters EcoCloud

→

STRIPE CHECKOUT
Human pays on Stripe's hosted page — card details never touch EcoCloud code

→

SIGNED WEBHOOK
HMAC-SHA256 verified via Web Crypto — checkout.session.completed fires

→

PRO UNLOCKED
Subscription row written by service-role — app reads status, gates change instantly

WHY **ECO CLOUD**

01 **Agent-operable, not just AI-powered**

Everyone ships a chat box. Very few ship memory, permissions, action execution and accountability — the things an agent needs to be a coworker, not a toy.

02 **Governance is the foundation, not a setting**

Scoped keys, a workspace constitution, approval gates and a kill-switch ship in the core — so you can let agents act without betting the company on it.

03 **A record you can prove**

A SHA-256 hash-chained, ECDSA-signed Merkle audit ledger makes every action tamper-evident. Your compliance story is "here's the cryptographic chain," not "trust our logs."

04 **Open-source governance kernels you can run yourself**

40+ skills

The governance logic — constitution, injection screen, authz, AI routing, MCP contract validation — ships as zero-dependency, Apache-2.0 code runnable in any browser or edge environment. Vendor lock-in on governance logic is a category-level risk. Ours is open.

05 **Your data, your model**

Bring your own model key so inference runs on your account; the Route Kernel picks the right provider by your own cost and privacy policy. Export or delete your data anytime.

06 **Commerce loop — designed**

roadmap

The billing path is built and HMAC-webhook-verified — start_checkout returns a Stripe URL, the human pays, a verified webhook upgrades the account. Self-serve checkout is planned: it goes live once Stripe keys are configured.

PLANS

SOLO

PRO

AI INCLUDED

ENTERPRISE

Free

- › Up to 5 projects
- › AI Dispatch
- › Agent API & MCP
- › All 40+ governance skills
- › Community support

\$12 / seat / mo

- › Everything, unlimited
- › Governance & approvals
- › AI model routing + MCP validation
- › Workflows & webhooks
- › Company memory & reasoning
- › 14-day trial · no card

Custom

- › SSO & SAML
- › SLA & priority support
- › Guided migration
- › Security review

Put your agents to work.

Minutes from sign-up to your first closed task. A 40+ skill governance library, signed outcome receipts, 48+ governed MCP tools.

Start free — no card →

© 2026 EcoCloud · AI-native, agent-operable, governed.

[Home](#) · [Trust](#) · [Due diligence](#) · [Download PDF](#) · agents@ecoclouddev.com