

PROBLEM

AI agents are moving into production, but there is still no safe way to let them spend money. API keys have no hard limits; one bad call can trigger unlimited spend.

SOLUTION

API keys are blank checks. A developer writes a rule in plain English (“Max \$100/day on OpenAI”). Sardis turns that into deterministic enforcement, provisions a payment identity, and blocks any payment that violates the rule. We don’t hold the money. We enforce the boundaries before settlement.

INTEGRATION (4 LINES)

```
from sardis import SardisClient
client = SardisClient(api_key="sk_...")
wallet = client.wallets.create(policy="Max $100/day")
tx = wallet.pay(to="openai.com", amount="25.00")
```

ARCHITECTURE

Control
Mandates, policy, rate limits

Execution
MPC wallets, stablecoins, cards

Proof
Merkle audit, policy evidence

Model suggests, policy decides. The same rules apply across cards and stablecoins, with tamper-evident audit logs.

Fail-closed
If policy, approval, or compliance signals are missing, execution stops.

Non-custodial
Turnkey handles signing. Sardis holds credentials and policy, not customer keys.

Rail-agnostic
The same mandate model can govern cards, stablecoins, and protocol payment flows.

WHAT TEAMS BUY FIRST

STEP 1

A developer adds Sardis to let an agent spend safely in sandbox or staging.

STEP 2

Production rollout pulls in approvals, audit exports, and finance/compliance stakeholders.

STEP 3

Revenue expands from developer tooling into controls, workflows, and enterprise assurance.

BUSINESS MODEL

Software pricing for mandates, approvals, and audit workflows, plus transaction fees when money moves. Free tier for developers, paid controls for production teams, and enterprise compliance add-ons.

ASK

Raising a \$3M seed to hire a forward deployed engineer, GTM lead, and protocol/security talent, then convert design-partner pull into the first paid production teams.

The near-term risk is GTM and trust, not whether the core product can be built.

WHY NOW

The timing signal is concrete: the standards and rails started arriving, but the control layer is still missing.

Apr 2025	Mastercard launched Agent Pay, validating agents as a real payment endpoint.
May 2025	Coinbase launched x402, making machine-readable stablecoin payments more practical.
Sep–Oct 2025	Google AP2 and Visa TAP pushed intent and identity forward, but neither solves deterministic spend control.

Sardis fits here: above the rail, before settlement, deciding whether an agent is allowed to spend at all.

TRACTION

15K+ installs, \$0 marketing

15 integrations

34 packages

15K+ organic installs with **\$0 marketing spend**. This is developer pull, not revenue. The next step is converting design partners into paid production users.

Activepieces LIVE

MCP Server

OpenClaw

AutoGPT

CrewAI

Vercel AI SDK

Composio

AutoGPT: package shipped and in discussion. Activepieces: live in marketplace.

Private-preview access on Stripe MPP.

PROOF OF BUILD

CORE	47+ API endpoints, 34 published packages, and a unified mandate model spanning SDKs and tool surfaces.
DISTRIBUTION	Activepieces is live in marketplace. The MCP server is published. Framework integrations create top-of-funnel developer reach.
BUYER PATH	Developers install first. Production deployment later pulls in approvals, finance controls, and audit requirements.

FOUNDER

Efe Baran Durmaz, 20. Solo technical founder. Top 0.04% nationally (1,405th / 3.5M), Bilkent full merit scholarship, Nokia AI automation engineer. The core product is built; the next job is pairing that technical speed with GTM and deployment credibility.

SHIPPING VELOCITY

47+ API endpoints

34 packages

15 integrations

Built solo. Every new payment rail or protocol increases the need for one control plane that can sit above all of them.

ECOSYSTEM ENGAGEMENT

Live:

Activepieces

MCP Server

Integrating:

Coinbase x402

Base

Tempo

OpenClaw

Access:

Stripe MPP early access

YEAR 1 PLAN

- M3:** design-partner pilots live, security/compliance workstreams active
 - M6:** first paid startup deployments in production
 - M12:** repeatable startup deployments, enterprise pilots underway
 - M18:** enterprise-ready controls and a credible Series A posture
- Wedge:** developers adopt free tooling first; production deployment pulls in compliance buyers later. Biggest near-term risk is GTM, not product depth.