

Know which agent is acting, and where.

Oathera gives every AI agent an identity bound to its host, approved by a named person, and checked every time it acts.

Every AI agent, sworn in.

THE PROBLEM

Your AI agents have no identity of their own.

- Your agents sign in with borrowed keys: a shared API key, a service account, someone's login.
- Registering an agent isn't verifying it. A directory entry is a name and a secret; copy the secret, copy the agent.
- You can't stop one agent without breaking a person's account.

HOW IT WORKS

Three steps, every agent

1

Enroll

The Oathera Identity MCP runs beside the agent, creates its key and records the host; a person approves it through your identity provider. Together that's your agent's DNA, recorded once.

2

Check every time

Each time the agent asks for a token, the Oathera identity service compares the host with the enrollment record and refuses a mismatch.

3

Prove every call

Your agent's fingerprint is on everything it does. The Gateway MCP verifies each signed operation; a copy on another machine leaves a different one.

WHY IT HOLDS

What makes the identity hard to steal

A copied agent is refused

The agent's key is created on its own host. The host is recorded at enrollment and compared again at every token.

A stolen token authorizes nothing

Tokens last five minutes at most. Every operation carries a proof signed with a key that never leaves the agent's memory.

A person answers for every agent

A named person approves each agent through the company's identity provider. The approval is part of the agent's enrollment record.

USE CASES

Where it matters

An agent with no identity

An agent calls your tools with no identity token. The Gateway MCP refuses the call before any service sees it and logs the refusal.

Identity, then service access

A person approves a new agent's identity. The Gateway MCP then checks every call to your tools against a proof signed on the agent's host.

Impersonation

Another agent presents this agent's token. It is refused, because it cannot prove it holds the agent's session key. A name alone is not a credential.

Cloning

AI agents can be cloned; identities cannot be. Copy an agent to another machine and the copy is caught at its next token. With enforce, it is refused.

WHO IT'S FOR

Built for the teams that run agents

FIRST USER

Platform and AI-enablement teams that run internal MCP servers.

BUYER

The security leader. Developers adopt; the security budget pays.

FITS BESIDE

Your identity provider, policy engine, egress controls and AI governance stay, each acting on an agent whose identity was proved.

PLANS

Plans

Free

Teams trying Oathera on their own agents

- 5 sponsor seats
- 100 active agents
- 1 gateway
- 30-day logs

Team

Platform teams running internal MCP servers

- SSO and SCIM
- SIEM export
- more gateways

Enterprise

Regulated and sovereign deployments

- Self-hosted control plane
- hardware key custody
- attestation
- SLA

Pricing confirmed at launch. Design partners start on dedicated tenants.

Become a design partner

About 10 teams start in early November 2026. You get a dedicated tenant, founder access and a say in what we build next. We ask you to run Oathera in front of one real tool and tell us what breaks.