Stop your AI agents when they go wrong. Prove what they did.

Excubitor watches every action your AI agents take, stops one that goes outside its job, holds irreversible actions for a person, and keeps a signed record your auditor can check without trusting us. It works across the agents, tools and models you already run.

WHAT IT DOES

STOP

- Refuses a tool call outside the agent's policy, and requests to destinations nobody approved
- Contains a runaway or racing run by rule, automatically
- Freezes any agent in one click; only an administrator releases it

HOLD

- Anything irreversible waits for a named person
- The approver sees the full chain of steps that led to the action
- Safe, reversible code fixes are kept only after your own tests pass

SIGN

- Every action is a hash-chained record; a rewrite or deletion shows
- A checkpoint of the ledger is signed every hour
- Prove one record offline with a public key, without the rest of the ledger (hosted)

DETECT

- Hidden instructions, secrets and personal data in what agents read and send
- Poisoned MCP tool descriptions and answers withheld before the agent reads them
- Every file an agent takes in, with what its bytes really are

UNDERSTAND

- Each agent compared with its own normal: new tools, new payees, new services
- Decision Replay: how any action came about, step by step
- A threat spreading from one agent to another, traced

GOVERN

- Model registry: approved model weights by fingerprint, attested by each model server
- Every agent has an owner, or is listed as unclaimed from its first call
- An AI register and governance report for auditors, recomputable from the ledger

WHERE IT RUNS

Hosted

We run it. Your application connects with a credential issued in the console. Records carry fingerprints, never your prompts, answers or keys. Data stored in the United States; a dedicated Enterprise deployment uses the region you choose.

Your cloud

Runs in your own cluster, on your storage, with your keys. Our servers never connect to it. Your people sign in through your identity provider and your own allow-list. Offline licence file.

Air-gapped

One signed offline bundle, checked before it is installed. Detection, containment, outbound checks and the model registry run inside your network, on your own model endpoint. Nothing calls out.

CHECK IT YOURSELF

Aurakore's own AI agents run on Excubitor. The latest signed checkpoint of our own ledger is public at **aurakore.ai/trust**, and anyone can check it.

No standing vendor access, ever.

SECURITY AND PRIVACY FACTS

Question	Answer
What the record holds	Fingerprints and findings: who acted, what was called, what was decided. Never the prompt, the answer, a file's contents or a key.
Model training	Your data is never used to train models.
Encryption	TLS in transit; encrypted at rest. Self-hosted, your storage and your keys.
Vendor access	None standing. Self-hosted and air-gapped, our servers never connect to your environment.
What you install	Every image and package is signed, with a software bill of materials and the public key to check it before it runs.
If Excubitor is unavailable	By default your agents keep running and the gap is recorded; you may choose to stop instead.
If a licence lapses	Recording never depends on the licence. There is no switch that blinds you.
Self-hosted console	Never opens without sign-in or a read token; every read and export is authenticated.
Leaving	Hosted: 30 days to export, then deletion from production within a further 30 days and from backups within 35 days after that.

WORKS WITH

MCP	Any MCP client and server, over HTTP or as a local process, with no change to either.
Your agents	One line per agent in any Python framework; a model proxy for applications you cannot change.
Identity	Okta, Microsoft Entra, any OpenID Connect provider or SAML 2.0; SCIM for joiners and leavers.
Security tools	Findings to your SIEM in the OCSF standard, as findings and fingerprints only.
AI-written code	A CI gate in your GitHub or GitLab pipeline that flags unsafe code, SQL injection included; we never hold your source.
Employees' AI use	Excubitor for Browsers: a managed extension for Chrome and Edge that checks pastes, sends and attachments on AI sites, on the device.

EDITIONS

Team
A handful of applications, one team.

Business
Several applications across teams, with a security owner.

Enterprise
Many applications, a formal security function, dedicated deployment options.

Priced per application, never per seat: reviewers, analysts and auditors cost nothing. Every edition includes containment, the signed ledger, the model registry and code review for your whole team. Any edition runs hosted, in your cloud or air-gapped.

Start with a proof of value on one of your own agents, against success criteria you write.

Want a demo?

sales@aurakore.com

aurakore.ai/security/excubitor

No standing vendor access, ever.