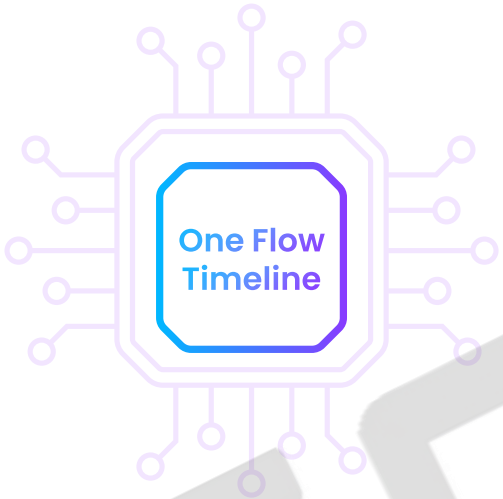
Trusted, Auditable AI Operations

Run where the data lives • Evidence for every run • Zero hardware changes

codebat.ai

CODEBAT



01 Encrypt & submit

02 Policy admission

03 Isolated run

04 Immutable Evidence

05 Offline verify

Executive Summary

Why it exists

Organizations want AI value without moving sensitive data or buying new hardware.

What you gain

Faster pilots, lower risk, and a defensible chain of custody.

What it does

Runs inside your environment and produces a tamper-evident evidence pack for each execution.

Codebat Technologies Inc.

Problem & Solution

Problem

The pain

Data shouldn’t leave.

Audits keep asking

“what exactly ran?”

Hardware changes stall timelines.

Solution

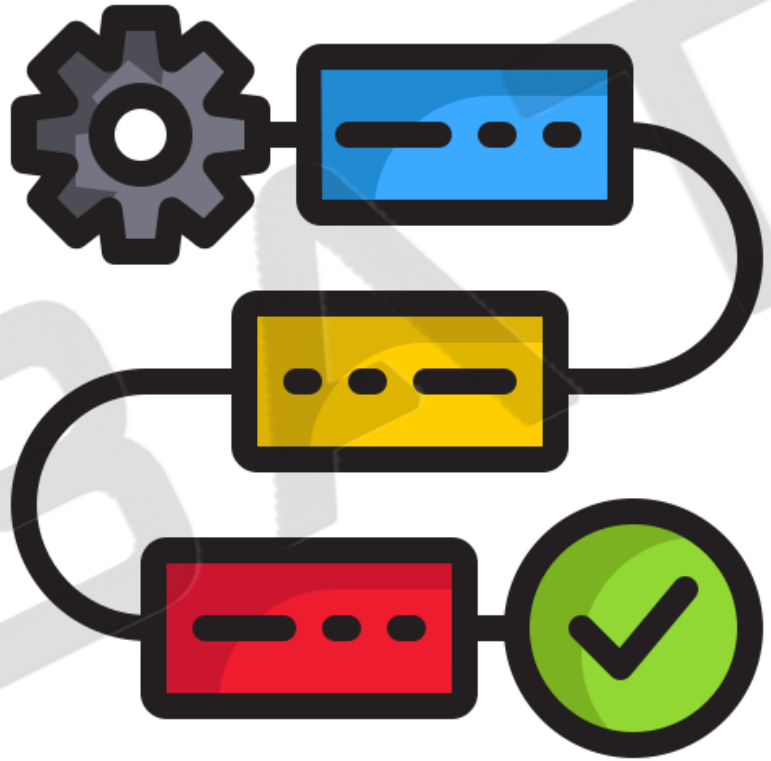
Our answer

In-place execution,

per-run evidence,

zero hardware changes—

so teams can move fast with proof.



Use Cases

Radiology — Lung Nodule Triage (ONNX)

Encrypted ONNX model runs inside the PACS/VNA network.

CT series → JSON report + mask overlay.

Every run writes an **evidence pack**(version, I/O hashes, signed timestamps, immutable link).

Clinical NLP — PHI De-Identification

Notes stay on the EMR subnet. Output is redacted text + diffs;

default no-egress,

evidence proves policy & monitoring.

Digital Pathology — WSI Tumor Detection

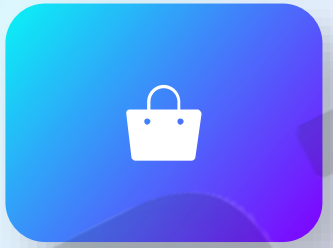
Gigapixel slides are tiled on GPU; no image leaves the lab. Heatmap + slide score returned, with per-run evidence.

Architecture at a Glance

How it’s wired

Secure Submit

Encrypted job, signed artifacts — data stays inside.

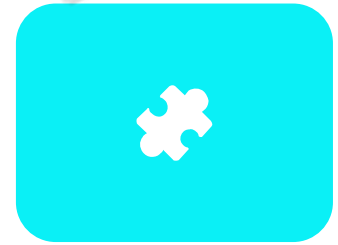


Policy & Scheduling

Verify → auto-place on your existing servers.

Isolated Execution

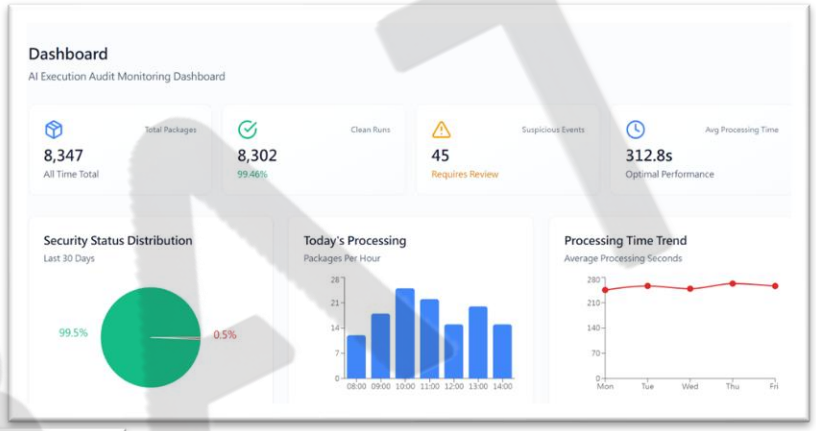
Read-only, memory-only, no egress. Keys just-in-time.

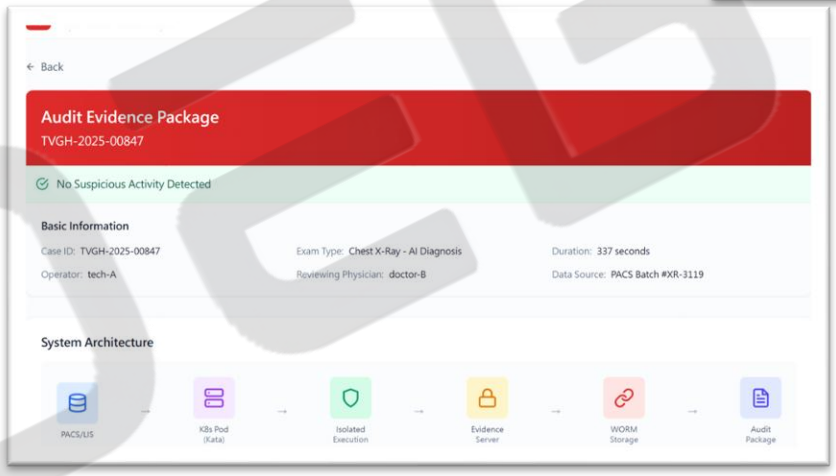


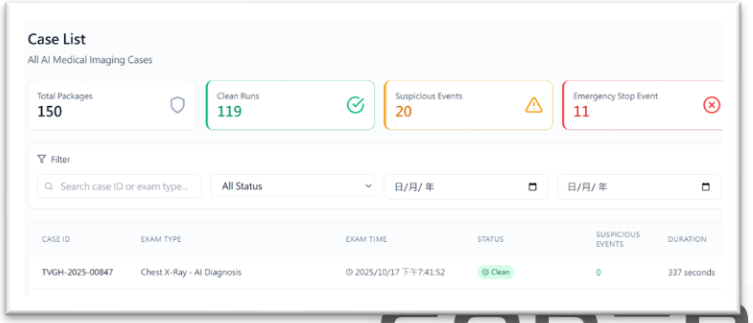
Evidence & Retention

Hash → Merkle → signed & time-stamped. Immutable, offline-verifiable.

Evidence Pack







Evidence for every run:

Who/when/where, exact version executed, input/output fingerprints, policy-admission ticket, host-monitor attestation, signed timestamps, immutable storage URI.

Performance & Operations

Starts in seconds

Starts in seconds for typical inference, tuned cold-start and scheduling.

No hardware changes

Works on existing servers and container stack.

Operational guardrails

Default no-egress, standardized runners, per-run evidence retention.

Compliance-Ready Technology

Built for reviewers:

Electronic audit trail with signatures and timestamps, stored immutably.

Auditors can verify integrity offline using public keys and timestamps.

Result: fewer cycles, clearer accountability.

compliance

21 CFR

compliance

HIPPA

The End

Thanks For Watching

LEARN MORE

CODEBAT

Appendix — One-Page Whitepaper

What It Is
A security-first platform that runs AI workloads inside your environment and produces a tamper-evident evidence pack for every run. It aligns security, compliance, and operations around a single, verifiable process.

Why It Matters
AI adoption stalls when data must move or when teams cannot prove what ran. We keep data in place, prove every execution, and avoid hardware changes—so pilots start faster and scale with confidence.

How It Works
Encrypted jobs arrive with declared versions and parameters. Policy admission validates provenance and configuration, then schedules to an isolated runner. The job executes with default no-egress and continuous host monitoring. We compute chained hashes and a Merkle root, sign a tree head, apply official timestamps, and preserve the record immutably. Auditors can validate integrity offline.

Security Highlights
Signed supply-chain artifacts prevent drift. Isolation reduces exposure during runtime. Keys are released only when policies and monitoring are provably active. Evidence is tamper-evident and independently verifiable.

Performance & Operations
Startup in seconds for typical inference, deployment on existing servers, and a predictable path from a single site to multiple sites—without proprietary appliances.