

FOR CCOS · GRC LEADS · INTERNAL AUDIT

Fast, Accurate Evidence — From Readiness to Report

Most AI compliance programs run on manual evidence collection: screenshots, spreadsheets, and quarterly fire drills. RuntimeAI generates evidence from real platform telemetry — every policy decision, every agent action, every audit-trail entry — verifiable operational data, not a self-assessed questionnaire.

80+ Regulatory Frameworks, Continuously Monitored

EU AI Act, NIST AI RMF, ISO/IEC 42001, SOC 2, FedRAMP, HIPAA, GDPR, PCI DSS, DORA, and more — no manual snapshot required.

THE PROBLEM

Manual Evidence Collection Doesn't Scale to AI



Screenshots, Not Evidence

Point-in-time snapshots and self-assessed questionnaires don't hold up when a regulator or auditor asks for the underlying operational proof.



Fragmented Workflows

Evidence for AI-specific controls scattered across folders, spreadsheets, and email threads — nobody owns the single source of truth.



No Real-Time Answer

"Show me your EU AI Act runtime logs" shouldn't take weeks to answer. Most compliance programs can't produce it in minutes.

WHAT RUNTIMEAI DOES

Evidence Generated From Live Telemetry

CAPABILITY	WHAT IT DOES
Automated evidence	Generated from real platform telemetry — every enforcement decision, every agent action — not self-assessed
EU AI Act logging	Automatic logging/documentation infrastructure required by Articles 9–14 for high-risk AI systems
Tamper-evident trail	Merkle-hash-chained audit records — retroactive tampering breaks the chain and triggers an alert, verifiable from a single root hash
Legal hold / e-discovery	Freeze any subset of records by agent, date range, or group; export encrypted e-discovery packages
Gap tracking	Every compliance gap gets a severity, an owner, and a recommended remediation — a prioritized queue, not a self-assessment spreadsheet

EU AI Act

NIST AI RMF

ISO/IEC 42001

SOC 2

FedRAMP

HIPAA

GDPR

PCI DSS

DORA

WHAT WE DON'T CLAIM

RuntimeAI does not hold third-party certifications on your behalf. We provide the **capability** to generate and preserve evidence — your organization's own certification and audit outcomes are yours to earn.

Signed evidence and attestations extend beyond RuntimeAI's core platform: **QuantoSign** provides AI-agent e-signature with cryptographic proof, and **Qutonomous PQ Comply** maps your cryptographic posture against CNSA 2.0 and FedRAMP PQC requirements — the same evidence discipline applied to your document and cryptography estate.

WHO THIS IS FOR

**CCO / GRC Leads**

One prioritized remediation queue, not a spreadsheet of controls to self-assess

**Internal Audit**

Direct access to source telemetry, not screenshots handed over on request

**Legal & Records**

Legal hold and e-discovery built in, not a separate manual process

**Regulatory Affairs**

EU AI Act Article 9–14 evidence produced in minutes, not weeks

WHY THIS MATTERS TO A COMPLIANCE LEADER

**Tamper-Evident by Design**

A Merkle hash chain means auditors can verify the integrity of the entire history from a single root hash — not trust your word for it.

**Quantum-Safe Retention**

Audit records carry post-quantum ML-DSA-87 timestamps — verifiable today, and still verifiable after quantum computing breaks classical signatures.

**A Marketplace, Not a Cold Start**

The Audit Marketplace (AAIC) connects you with pre-vetted audit firms for AI-specific audits — no separate "find an auditor" process.

See your framework coverage gap in one session

Request a demo — a real gap analysis against the frameworks that matter to you.

Roshan Shaik

Founder & CEO · RuntimeAI

roshan@runtimeai.io

www.runtimeai.io

calendly.com/roshan-runtimeai/30min