TECHNICAL OVERVIEW

Shadow Mode: The 50-Day Parallel Evaluation

How SENTR runs alongside your existing fraud stack — and what you receive at Day 50.

50 days	€0	8 days	<100ms
Parallel evaluation period	Cost to evaluate	API integration timeline*	Detection response time

* 8-day integration timeline subject to engineering sign-off before publication.

What shadow mode is — and what it is not

Shadow mode is a parallel risk evaluation. SENTR connects to your existing transaction and chargeback data via a read-only API and runs its Closed-Loop Risk Intelligence Engine against your live transaction stream — without making a single live decision.

Your existing fraud stack keeps running exactly as it is. Every live decision still goes through your current platform. SENTR observes, scores, and logs in parallel — building a complete picture of what it detects versus what your current system detects.

At the end of 50 days, you receive a full intelligence report showing the fraud detection delta: what SENTR found that your current platform missed, what it would have caught earlier, and what the commercial value of that delta is for your transaction volume.

EU AI Act: shadow mode starts your compliance clock

From August 2026, the EU AI Act requires payment operators using automated decision-making systems to maintain an explainable AI audit trail. SENTR generates a full explainability log for every fraud decision during shadow mode. You do not need to be live on SENTR before August. You need to be able to demonstrate you are building toward compliance. Shadow mode starts that clock.

How shadow mode works — step by step

1 Architecture Session — 20 minutes

You book a 20-minute Architecture Session with a SENTR engineer. We map your current fraud stack, understand your transaction volume and vertical, and confirm what shadow mode would surface for your specific setup. No commitment at this stage.

2 8-day API integration — nothing changes on your side

Our integration engineer connects SENTR to your existing transaction and chargeback data feed via a read-only API connection. Your fraud platform keeps running exactly as it is. No cutover. No data migration. No SLA risk. Your team provides API access and a technical contact. Typical timeline: 8 business days from kickoff to live.

3 50-day parallel operation — you watch, we find

SENTR's Closed-Loop Risk Intelligence Engine runs against your live transaction stream in shadow mode. It detects, scores, and logs every fraud event your current stack sees — and every event it misses. You have access to a live dashboard showing parallel detection in real time. No one touches your operations.

4 Day 50: you receive the full intelligence report

At the end of the shadow mode window, we deliver three things: (1) a full fraud intelligence report comparing SENTR detection vs your current platform output, (2) a compliance gap assessment against EU AI Act Article 13 transparency requirements, and (3) a board-ready ROI snapshot showing exactly what the detection delta is worth in recovered chargebacks and reduced analyst overhead. No invoice. No contract pressure. The data is yours either way.

5 You decide

After reviewing the Day 50 report, you decide whether to proceed with a full SENTR deployment. If the data shows a meaningful detection delta, the commercial case is already built. If it doesn't, you walk away having spent 50 days and nothing else.

What the Day 50 Intelligence Report contains

The report is structured in three sections:

- **Detection delta analysis:** Side-by-side comparison of SENTR detection vs your current platform across your full 50-day transaction volume. Broken down by fraud type, channel, and time-of-day pattern.
- **EU AI Act compliance gap assessment:** An audit of your current fraud stack's ability to satisfy Article 13 transparency requirements — explainability, documentation, and audit trail coverage. Gaps are itemised with remediation paths.
- **Board-ready ROI snapshot:** A single-page financial summary quantifying the detection delta in recovered chargebacks, reduced false positive analyst overhead, and projected VAMP threshold movement for your specific transaction volume. Uses your actual data, not industry benchmarks.

The security architecture during shadow mode

Shadow mode is a read-only integration by design. SENTR writes nothing to your production environment at any point during the evaluation.

- **Read-only API access:** SENTR connects via a read-only API connection. We cannot modify, write to, or interfere with any system in your production environment.
- **EU data centres:** All transaction data is processed within EU data centres. No data is transferred outside the EU. GDPR Article 44 compliant by architecture.
- **Immutable audit log:** Every SENTR decision during shadow mode is written to an immutable audit log at decision time. Exportable on demand for regulatory submissions.
- **Your stack stays fully in your control:** Your existing fraud platform continues to make every live decision. SENTR's shadow run has no operational impact.

What happens if shadow mode finds nothing

If SENTR's Closed-Loop Engine finds no meaningful detection delta versus your current platform, you receive the Day 50 report, keep all the data, and owe nothing. No invoice is issued. No contract was signed.

You also receive the EU AI Act compliance gap assessment — which has standalone value regardless of the detection delta. The audit trail documentation alone is worth the 50 days for most teams approaching the August 2026 enforcement window.

Who shadow mode is designed for

- **Payment service providers (PSPs):** Processing €500K+ per month with card scheme chargeback exposure and acquirer VAMP monitoring risk.
- **iGaming operators:** Running live betting with bonus abuse, first-party fraud, and MGA/UKGC audit documentation requirements.
- **Fintech and financial services:** Scaling transaction volumes with EU AI Act compliance obligations approaching August 2026.

Minimum qualification: €500,000+ monthly processed volume, 10,000+ daily transactions. (iGaming exception: any volume with live bet processing carries fraud exposure regardless of transaction count.)

Book your 20-minute Architecture Session

The Architecture Session is where we map your current risk setup and confirm exactly what shadow mode would surface for your transaction volume. 20 minutes. No pitch deck. No commitment.

Book at sentr.io/proof

Questions before you book? hello@sentr.io — we reply same day.

SENTR · Closed-Loop Risk Intelligence · sentr.io · EU AI Act compliant · GDPR compliant · All data processed within EU