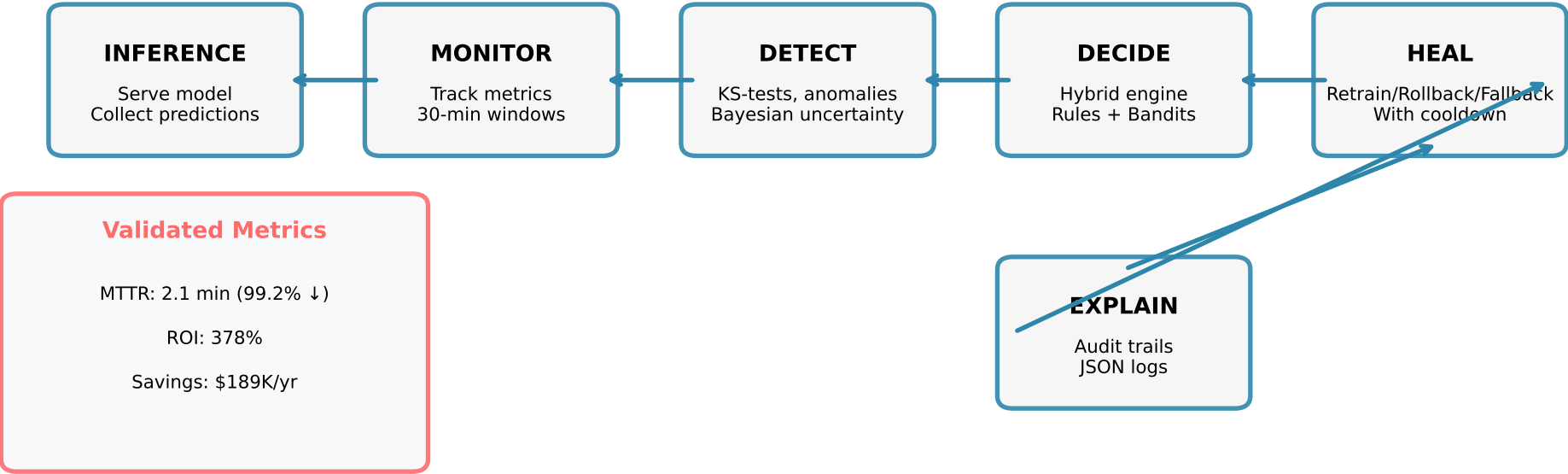# Self-Healing ML Pipelines: 6-Layer Control Loop

*Hybrid Architecture: Rules (Safety) + Bandits (Optimization)*

**Safety Mechanisms**

✓ Confidence Gating (80% min)

✓ Deterministic Fallback

✓ 30-min Cooldown

✓ Human Veto

✓ Audit Compliance

**INFERENCE**
Serve model
Collect predictions

**MONITOR**
Track metrics
30-min windows

**DETECT**
KS-tests, anomalies
Bayesian uncertainty

**DECIDE**
Hybrid engine
Rules + Bandits

**HEAL**
Retrain/Rollback/Fallback
With cooldown

**EXPLAIN**
Audit trails
JSON logs

**Validated Metrics**

MTTR: 2.1 min (99.2% ↓)

ROI: 378%

Savings: $189K/yr

**Key Innovation:**
Hybrid Control = Safety + Optimization
• Rules guarantee safe fallback
• Bandits optimize for cost/performance
• Confidence gating prevents overreach