AI AGENT SECURITY FOR FINANCIAL SERVICES

Your AI Agents Are Executing Transactions. Nobody's Watching What They Do Next.

AI agents in banking, insurance, and wealth management authenticate with valid credentials, clear MFA — and then act. Trade executions, payment approvals, customer data queries. The identity layer said yes. Runtime said nothing.

Identity Fraud at Scale

A valid OAuth token used by a service account that just queried 400 customer accounts it has never touched. Valid credential. Wrong behavior. No alert.

45B+ NHIs vs human identities by 2027

Activity Fraud in the Transaction Layer

An AI agent approved $2.4M in transactions in 11 minutes. Daily baseline: $80K. No SoD gate. No behavioral baseline. No kill switch.

9 sec compromise-to-impact (PocketOS 2026)

Harvest Now, Decrypt Later

Every RSA/ECDSA-encrypted customer record collected today is on a compromise timer. Financial data with 10-year retention requirements is already exposed to quantum adversaries.

FIPS 203/204/205 — migrate now, not 2030

SCENARIO	GAP	RUNTIMEAI RESPONSE
AI Payment Agent — Anomalous PO Approvals	Behavioral baseline exceeded 30×; no SoD enforcement	Agent Finance Rails + Activity Fraud Shield
OAuth Token Theft — Cross-Tenant Queries	Valid credential; 700 enterprise tenants accessed (Salesforce/Drift pattern)	Identity Fraud Shield + KYA fingerprint baseline
PCI Cardholder Data in LLM Context Window	Tokens leak via prompt history, agent memory, model outputs	PII Shield + PQ TokenVault FPE at egress

RUNTIMEAI FOR FINANCIAL SERVICES

Runtime Enforcement — Across Every AI Agent Action

DISCOVER
Know Your Agent
KYA
Every AI agent registered, fingerprinted, org-mapped. Shadow AI foreclosed at DNS before TCP.

GOVERN
Identity Fabric
JIT Entitlements
Ephemeral credentials, JIT access, SoD enforcement, conditional access, proxy tokens that never expose real secrets to agents.

ENFORCE
Fraud Shield
Identity + Activity Fraud
Identity Fraud + Activity Fraud detected inline. Behavioral baseline per agent. Risk score 0–100. Kill Switch <50ms.

TRANSACT
Finance Rails
Agent Commerce
Agent-initiated payments and procurement within approved guardrails. Human approval gates for high-value transactions. Full audit trail.

PROTECT
PQ Data Security
PQData Platform
PCI cardholder data tokenized with FPE before any model sees it. QuantumVault ML-KEM-1024 encryption. HNDL-proof today.

AEP — AGENTIC ENABLEMENT PLATFORM

- **Know Your Agent (KYA)** — cryptographic agent identity, org hierarchy
- **Agent Fraud Shield** — Identity Fraud + Activity Fraud, real-time 0–100 risk score
- **Agent Finance Rails** — payment/procurement within policy limits
- **JIT Entitlements** — no standing privileges, task-scoped access
- **Audit Black Box** — tamper-proof, cryptographically chained audit trail
- **PII Shield** — redacts at egress before any model sees plaintext
- **Agent Memory Vault** — encrypted, tenant-isolated agent context

PQDATA — POST-QUANTUM SECURITY

- **QuantumVault** — ML-KEM-1024 key encryption, HNDL-proof secrets
- **PQ TokenVault** — format-preserving tokenization (FPE) for PCI cardholder data
- **PQ Transit Shield** — post-quantum mTLS for all inter-service traffic
- **PQ Sign** — ML-DSA-87 audit log signing — verifiable in 2045
- **PQ CryptoGuard** — crypto posture scanning, CBOM generation
- **PQ Comply** — automated PQC compliance reporting

PCI DSS v4 · SOC 2 Mappings · DORA · FINRA · SEC Rule 17a-4 · NIST AI RMF · ISO 42001 · FIPS 203/204/205

RuntimeAI does not pursue third-party certifications. It provides its own compliance documentation to support customer assessments — CISA SSDF self-attestation, SOC 2 Trust-Service-Criteria control mappings (documentation, not a certificate), an independent-style security review, a threat model, architecture documentation, and a current SBOM. For regulated data, on-prem / air-gapped / sovereign deployment is recommended so the customer's own controls and compliance boundary govern the data.

DIFFERENTIATION

Policy Without Intercept Is a Slide Deck. We Intercept.

CAPABILITY	CASB/SASE	NHI/PAM	DLP	SIEM	RUNTIMEAI
Agent identity model (NHI-native)	✗	~	✗	✗	✓
Inline fraud scoring before transaction	✗	✗	✗	✗	✓
Separation of Duties for AI agents	✗	✗	✗	✗	✓
Behavioral baseline per agent (LSTM)	✗	✗	✗	~	✓
Kill Switch <50ms — agent fleet	✗	✗	✗	✗	✓
Post-quantum cryptography (FIPS 203/204/205)	✗	✗	✗	✗	✓
PCI FPE tokenization before LLM sees data	✗	✗	~	✗	✓

WHY FINANCIAL SERVICES TEAMS CHOOSE RUNTIMEAI

One Platform Across the Entire AI Agent Stack

Discovery → Identity → Runtime Enforcement → Compliance. Replaces 4–6 fragmented point products. One policy engine, one audit trail, one compliance dashboard.

Compliance-Ready on Day 3, Not Month 3

SOC 2, PCI DSS v4, DORA, FINRA evidence auto-generated at every agent action. Audit artefacts are produced by the platform, not assembled from logs.

Enforcement at Machine Speed

<50ms kill switch. <5ms policy evaluation. Fraud scoring inline before the transaction completes. Not a dashboard — an enforcement layer.

Start a 30-Day Pilot

RuntimeAI deploys as a control plane overlay. Day 1 deployment. Compliance-ready by Day 3.

Roshan Shaik

CEO & Co-founder · RuntimeAI

roshan@runtimeai.io

www.runtimeai.io

calendly.com/roshan-runtimeai/30min