2198 Four Winds Blvd., Kissimmee, FL 34746
https://zerotrusted.ai
contact@zerotrusted.ai
407-507-9350

ZeroTrusted.ai for Banking

Securing AI, Data, and Digital Trust in Financial Services

1. Executive Summary

Financial institutions are rapidly adopting Artificial Intelligence (AI) across fraud detection, AML/KYC, customer engagement, risk modeling, algorithmic trading, and internal automation. However, integrating AI brings new systemic risks such as model manipulation, data poisoning, prompt injection, regulatory exposure, privacy breaches, supply chain vulnerabilities, and reduced auditability.

2. The Banking AI Risk Problem

Banks face five critical AI risk domains:

- Model manipulation
- Sensitive uploads to AI
- Data poisoning
- Data drift
- Prompt injection
- Regulatory exposure
- Privacy violations and supply chain vulnerabilities

3. ZeroTrusted.ai Banking Architecture

- **1. AI Firewall™**: Detects prompt injection and adversarial attacks
- **2. AI Gateway™**: Centralized AI API / MCP inspection
- **3. AI HealthCheck™**: Tests models for bias, hallucination, and drift
- **4. AI SOAR™ – AI Command Center**: AI-specific incident response workflows
- **5. AI Visibility & Observability**: Token usage monitoring / Violation Discovery

4. Banking Use Cases

- AI Model / Agent Testing and Mitigation
- Shadow and Embedded AI Discovery
- Fraud & AML Protection: Secure fraud detection pipelines and monitor AI-generated compliance outputs

5. Business Outcomes

- Reduced AI regulatory exposure
- Improved compliance monitoring
- Enhanced digital trust and privacy
- Stronger risk mitigation strategies