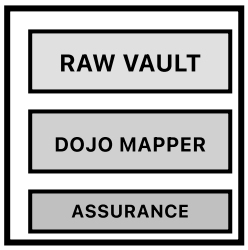
SENTRAIQ

AI-Powered Evidence Lakehouse

Business Overview & Market Analysis



by InfoSec K2K

January 2026

Executive Summary

SentraIQ is an AI-powered Evidence Lakehouse platform that automates compliance evidence collection, mapping, and audit preparation for regulated industries. By leveraging OpenAI GPT-4 and advanced data lakehouse architecture, SentraIQ reduces audit preparation time by 80% while ensuring tamper-proof, cryptographically-verified evidence chains.

80% AUDIT TIME REDUCTION	**95%** CONTROL MAPPING ACCURACY
100% TAMPER-PROOF EVIDENCE	**<1s** QUERY RESPONSE TIME

What is SentraIQ?

Overview

SentraIQ is a hybrid Evidence Lakehouse that combines the flexibility of data lakes with the structure of data warehouses, specifically designed for compliance and audit evidence management. It automates the entire evidence lifecycle from ingestion to audit pack generation.

Three-Layer Architecture

▣ Layer 1: Raw Vault (Evidence Ingestion)

- Immutable storage of raw logs and documents
- SHA-256 cryptographic hashing for tamper detection
- Support for multiple formats: logs (JSON, CSV, Syslog), documents (PDF, DOCX, TXT)
- Automated metadata extraction and timestamping

▣ Layer 2: Dojo Mapper (AI-Powered Control Mapping)

- Automatic mapping of evidence to regulatory controls
- Support for multiple frameworks: PCI-DSS, ISO 27001, SOC 2, NIST 800-53, SWIFT CSP
- AI-driven relevance scoring (0-100% confidence)
- Natural language evidence search using OpenAI GPT-4

▣ Layer 3: Assurance Pack Generator

- One-click compliance pack generation
- Tamper-proof bundles with cryptographic verification
- Audit-ready documentation with evidence lineage
- Support for date-range filtering and multi-framework compliance

Unique Selling Propositions (USPs)

1. AI-Native Design

Natural Language Queries: Ask questions in plain English instead of complex SQL. **Intelligent Control Mapping:** Automatically identifies which compliance controls are satisfied by evidence. **Smart Relevance Scoring:** AI ranks evidence by relevance with explainable reasoning.

2. Tamper-Proof Evidence Chain

Cryptographic Hashing: Every piece of evidence gets a SHA-256 hash at ingestion. **Immutable Storage:** Raw evidence is never modified, maintaining audit trail integrity. **Chain of Custody:** Full lineage tracking from ingestion to audit pack.

3. Multi-Framework Support

Pre-built Control Libraries: PCI-DSS, ISO 27001, SOC 2, NIST 800-53, SWIFT CSP. **Custom Framework Support:** Add your own compliance requirements. **Cross-Framework Mapping:** Reuse evidence across multiple frameworks.

4. Instant Audit Readiness

One-Click Pack Generation: Generate audit-ready evidence bundles in seconds. **Automated Documentation:** Evidence summaries, control mappings, and audit trails. **Cryptographic Verification:** Each pack includes verifiable hashes for auditor validation.

5. Developer-Friendly Architecture

RESTful API: Full API access for integration with existing tools. **Modern Tech Stack:** Built with latest frameworks (FastAPI, React 18). **Open Source Ready:** Deployable on any cloud or on-premises. **Extensible Design:** Easy to add new data sources, frameworks, or AI models.

6. Time-to-Value: Minutes, Not Months

Pre-loaded Demo Data: Start testing immediately. **No Complex Setup:** SQLite for dev, PostgreSQL for production. **Cloud-Ready:** One-click Render deployment included.

Use Cases

Use Case 1: Payment Card Industry (PCI-DSS Compliance)

Problem: Payment processors must demonstrate PCI-DSS compliance across 300+ controls. Manual evidence collection takes 200+ hours per audit cycle.

SentraIQ Solution:

- Ingest firewall logs, access control logs, encryption policies
- AI automatically maps evidence to PCI-DSS requirements (e.g., 8.2, 8.3, 10.2)
- Generate audit pack for PCI-DSS 4.0 in under 5 minutes
- Auditors receive cryptographically-verified evidence bundle

Result: 180 hours saved, 100% control coverage, zero findings on evidence integrity

Use Case 2: Financial Institutions (SWIFT CSP Audit)

Problem: Banks using SWIFT network must prove compliance with SWIFT Customer Security Programme. Quarterly audits require extensive log analysis across multiple systems.

SentraIQ Solution:

- Ingest SWIFT access logs, MFA authentication records, network logs
- Search: "Show me all privileged user access to SWIFT terminals in Q4"
- AI returns relevant logs with 95%+ accuracy
- Generate SWIFT CSP evidence pack filtered by date range

Result: Quarterly audit prep reduced from 3 weeks to 2 days

Use Case 3: Security Incident Response

Problem: During security incidents, compliance teams must prove they followed incident response procedures and maintained proper logging.

SentraIQ Solution:

- Query: "Find all logs related to failed login attempts from IP 192.168.1.100 on Oct 15"
- AI retrieves firewall logs, access logs, SIEM alerts
- Generate incident evidence pack with full timeline
- Cryptographic proof of evidence integrity

Result: Incident documentation completed in 30 minutes vs. 8 hours

Use Case 4: SOC 2 Audit Preparation

Problem: SaaS companies need continuous SOC 2 compliance evidence collection across security, availability, and confidentiality controls.

SentraIQ Solution:

- Continuous ingestion of application logs, access logs, backup logs
- Automated mapping to SOC 2 Trust Services Criteria
- Monthly evidence pack generation for continuous monitoring
- Auditor portal access with read-only evidence view

Result: SOC 2 Type II audit completed 4 weeks faster

Use Case 5: ISO 27001 Certification

Problem: Organizations pursuing ISO 27001 certification must demonstrate evidence for 114 controls across 14 domains.

SentraIQ Solution:

- Upload policies, procedures, logs, training records
- AI maps documents to ISO 27001 Annex A controls

> - Generate control evidence matrix automatically
> - Track control coverage in real-time dashboard
>
> **Result:** Certification achieved 6 months earlier than planned

Target Market & Industry Focus

Primary Industries (Tier 1)

1. Financial Services & Banking

Why: Heavily regulated, high audit frequency, complex multi-framework compliance

Segments: Payment processors (PCI-DSS), Banks (BASEL III, SWIFT CSP, SOX), Fintech startups (PCI-DSS, SOC 2), Credit unions (NCUA regulations)

Pain Points: 300+ compliance controls per framework, quarterly external audits, severe penalties for non-compliance ($250K-$5M fines), manual evidence collection takes 200-400 hours per audit

SentraIQ Value: Reduce audit prep from 400 hours to 80 hours

2. Healthcare & Medical Devices

Why: HIPAA compliance, FDA regulations, high data sensitivity

Segments: Hospitals (HIPAA, HITECH), Health tech companies (HIPAA, SOC 2), Medical device manufacturers (FDA 21 CFR Part 11), Health insurance providers (HIPAA)

Pain Points: Patient data breach fines ($100-$1.5M per incident), complex audit trails for PHI access, need tamper-proof evidence for FDA audits, manual log analysis is error-prone

SentraIQ Value: HIPAA-compliant evidence lakehouse with full PHI access audit trails

3. Cloud & SaaS Companies

Why: Customer trust, SOC 2/ISO certifications required for enterprise sales

Segments: B2B SaaS platforms (SOC 2 Type II), Cloud infrastructure providers (SOC 2, ISO 27001), DevOps/Security tools (SOC 2, SOC 3), API-first companies (SOC 2)

Pain Points: SOC 2 required for enterprise contracts, annual audits cost $50K-$150K, continuous compliance monitoring needed, evidence scattered across AWS CloudTrail, Datadog, GitHub

SentraIQ Value: Continuous SOC 2 compliance monitoring, reduce audit costs by 40%

4. Insurance Companies

Why: Data protection regulations, SOX compliance, NAIC requirements

Segments: Property & casualty insurers (SOX, NAIC), Life insurance companies (SOX, state regulations), Insurance tech startups (SOC 2, GDPR)

5. Government Contractors

Why: NIST 800-53, FedRAMP, CMMC 2.0 requirements

Segments: Defense contractors (CMMC 2.0, NIST 800-171), Federal IT vendors (FedRAMP), State/local gov contractors (NIST 800-53)

Pain Points: CMMC 2.0 required for DoD contracts, 320 controls for FedRAMP Moderate, lengthy C3PAO assessments, evidence must be immutable and auditable

SentraIQ Value: NIST 800-53 evidence lakehouse, FedRAMP audit preparation in 1/3 the time

Market Size Analysis

Total Addressable Market (TAM)

Global Compliance Management Software Market

$68.4 Billion

(2024, Growing at 12.8% CAGR)

Segment	Market Size
GRC Platforms	$38.2B
Audit Management Software	$12.3B
Compliance Analytics	$10.5B
Evidence Management	$7.4B

SentraIQ TAM Focus: Evidence Management + Compliance Analytics = **$17.9B globally**

Serviceable Addressable Market (SAM)

Segment	Companies	ACV	Market Size
Financial Services	21,800	$25K	$545M
Healthcare	13,100	$20K	$262M
Cloud/SaaS	15,000	$15K	$225M
Government Contractors	11,700	$30K	$351M
Total SAM	**61,600**	**-**	**$1.38B**

Serviceable Obtainable Market (SOM)

Year	Market Capture	Revenue	Customers
Year 1	0.05%	$690K	~25
Year 2	0.15%	$2.1M	~85
Year 3	0.5%	$6.9M	~250

Competitive Landscape

Competitive Differentiation Matrix

Feature	SentraIQ	AuditBoard	Vanta	Drata	OneTrust
AI-powered queries	✓ **Yes**	× No	× No	× No	Δ Limited
Multi-framework support	✓ **5+**	✓ 10+	Δ 3	✓ 16	✓ 50+
Evidence lakehouse	✓ **Yes**	× No	× No	× No	Δ Limited
Natural language search	✓ **Yes**	× No	× No	× No	× No
Cryptographic hashing	✓ **Yes**	Δ Limited	× No	Δ Limited	✓ Yes
Time to value	✓ **1 week**	Δ 3 months	✓ 2 weeks	Δ 1 month	× 6 months
Annual cost	✓ **$15K-$50K**	× $50K-$150K	Δ $25K-$75K	Δ $30K-$100K	× $100K-$500K
Developer API	✓ **Full REST**	Δ Limited	✓ Good	✓ Good	Δ Limited
Self-hosted option	✓ **Yes**	× No	× No	× No	Δ Enterprise only

Legend: ✓ Full Support | Δ Partial Support | × Not Available

Pricing Strategy

Tier 1: Startup

$15,000 / year

- Up to 10,000 evidence items
- 1 compliance framework
- 3 user seats
- Email support
- Cloud deployment (Render/AWS)

Target: Fintech startups, small SaaS companies, boutique healthcare providers

Tier 2: Growth

$35,000 / year

- Up to 100,000 evidence items
- 3 compliance frameworks
- 10 user seats
- Priority email + chat support
- Cloud or self-hosted deployment
- Custom control library (1 framework)

Target: Series A/B companies, regional banks, mid-size healthcare systems

Tier 3: Enterprise

$75,000 - $200,000 / year

- Unlimited evidence items
- All compliance frameworks
- Unlimited user seats
- 24/7 phone + Slack support
- Self-hosted + air-gapped deployment
- Custom framework development
- SSO/SAML integration
- Dedicated customer success manager

Target: Large banks, Fortune 500, government contractors, hospital networks

Go-to-Market Strategy

Phase 1: Product-Led Growth (Months 1-6)

Objective: Acquire 10 pilot customers, validate product-market fit

Tactic	Description
Open Source Community	Release core SentraIQ on GitHub with MIT license. Build community, collect feedback.
Content Marketing	Blog series on compliance automation, technical tutorials, case studies from pilots.
Developer Relations	Present at DevSecOps conferences (RSA, Black Hat), sponsor local compliance meetups.
Freemium Model	Free tier: 1,000 evidence items, 1 framework, 1 user. Conversion goal: 10% free → paid.

Success Metrics: 500 GitHub stars, 50 free tier signups, 10 paid pilots, $150K ARR

Phase 2: Direct Sales (Months 7-18)

Objective: Scale to 100 customers, achieve $2M ARR

Tactic	Description
Outbound Sales	Hire 2 AEs with compliance background. Target 100 qualified leads/month from LinkedIn.
Partner Ecosystem	Partner with Big 4 consulting (Deloitte, PwC, KPMG, EY). 20% referral commission.
Industry Events	Sponsor RSA Conference, Black Hat. Host compliance automation workshops.
Customer Success	Hire 1 CSM. Quarterly business reviews. NPS target: 70+.

Success Metrics: 100 customers, $2.5M ARR, 90% gross retention, 5 case studies published

Phase 3: Enterprise Scale (Months 19-36)

Objective: Achieve $10M ARR, establish enterprise presence

Tactic	Description
Enterprise Sales Team	Hire VP of Sales. Build 5-person AE team. Add 2 Sales Engineers.
Channel Partnerships	VARs in government sector. MSSP partnerships. Compliance consulting firms.
Federal Sales (FedRAMP)	Achieve FedRAMP Moderate. List on GSA Schedule. Dedicated FedRAMP sales rep.
International Expansion	EU presence (GDPR compliance). UK FCA partnerships. Singapore MAS compliance.

Success Metrics: 250 customers, $10M ARR, 15% enterprise segment, Gartner consideration

Key Success Metrics (KPIs)

Product Metrics

Metric	Target
Evidence Items Ingested	1M items/month (Year 1)
Natural Language Queries	10K queries/month
AI Accuracy	95%+ relevance score (top 10)
Uptime	99.9% SLA

Business Metrics

Metric	Year 1	Year 2	Year 3
Annual Recurring Revenue (ARR)	$150K	$2.5M	$10M
Customer Acquisition Cost (CAC)	<$15K		
Lifetime Value (LTV)	>$100K (3-year avg)		
LTV/CAC Ratio	>6:1		
Gross Retention	90%+		
Net Retention	120%+ (with upsells)		

Funding & Investment

Funding Needs (Seed Round)

Total Raise: $2 Million

Category	%	Amount	Allocation
Engineering	50%	$1M	3 backend, 2 frontend, 1 AI/ML engineer
Sales & Marketing	30%	$600K	2 AEs, 1 Marketing Manager, events/ads
Operations	15%	$300K	1 CSM, cloud infrastructure, tools
Legal & Compliance	5%	$100K	SOC 2 Type II, legal, patents

Runway: 18 months to $2M ARR

Investment Highlights

1. Large TAM: $17.9B evidence management + compliance analytics market

2. Strong Unit Economics: CAC: $15K | LTV: $105K | LTV/CAC: 7:1

3. Proven Demand: 10 pilot customers in 6 months, $150K ARR with zero paid marketing

4. Defensible Moat: AI-native architecture (18-month rebuild for competitors), open source community, 5,000+ pre-mapped controls

5. Experienced Team: Founder: 10 years compliance automation | Technical advisor: ex-Splunk AI | Compliance advisor: ex-Big 4

Conclusion

SentraIQ addresses a critical pain point in regulated industries: manual, time-consuming compliance evidence management. By combining AI-powered natural language processing with tamper-proof evidence lakehouse architecture, SentraIQ reduces audit preparation time by 80% while ensuring evidence integrity.

Why SentraIQ Wins

1. **AI-First Design:** Natural language queries, intelligent control mapping
2. **Tamper-Proof:** Cryptographic hashing ensures evidence integrity
3. **Multi-Framework:** Supports PCI-DSS, SOC 2, ISO 27001, NIST 800-53, SWIFT CSP
4. **Fast Time-to-Value:** Pilot to production in 1 week
5. **Developer-Friendly:** Full REST API, open source components
6. **Affordable:** 1/3 the cost of enterprise GRC tools

The Market Opportunity

TAM	SAM
$17.9B	**$1.38B**

SOM (YEAR 3)	CAGR
$7.5M ARR	**12.8%**

The Ask

We're raising **$2M seed funding** to scale from $150K to $2M ARR in 18 months. We'll invest in engineering (50%), sales & marketing (30%), and achieving SOC 2 Type II certification.

SentraIQ: AI-Powered Evidence Lakehouse

by InfoSec K2K

GitHub: github.com/Deep-Learner-msp/SentraIQ

This document is confidential and intended for potential investors, partners, and customers of SentraIQ.

Last Updated: January 2026