FINCH SECURITY

Security & Architecture Whitepaper

Technical overview of Finch's data handling, deployment architecture, and compliance infrastructure for security and procurement review.

DOCUMENT	Security & Architecture Whitepaper v1.0
CLASSIFICATION	Confidential — For Evaluation Purposes
DATE	February 2026
CONTACT	security@finch.io

ARCHITECTURE & DATA FLOW

Where Your Data Lives

Finch is designed around a single principle: **your data never leaves your infrastructure**. Unlike SaaS compliance tools that require data upload to vendor servers, Finch deploys directly into your environment. The model comes to your data, not the other way around.

Core Architecture Principles

Zero Data Egress

In Private VPC and Air-Gapped modes, no customer data, PII, transaction records, or compliance documents are transmitted outside your network boundary. All AI inference runs locally within your infrastructure.

No Third-Party API Calls

Finch does not call OpenAI, Anthropic, Google, or any external LLM API. The model weights are deployed on-premise. No data is sent to any third-party service for processing.

Encryption at Rest & In Transit

All data stored by Finch is encrypted using AES-256 at rest. All internal service communication uses TLS 1.3. Encryption keys are managed within your infrastructure — Finch never holds or has access to your encryption keys.

Tenant Isolation

Each Finch deployment is a single-tenant instance. There is no shared infrastructure, no shared database, and no multi-tenant data commingling between customers.

Data Flow by Deployment Mode

	PUBLIC CLOUD	PRIVATE VPC	AIR-GAPPED
Model location	Finch-managed cloud	Your AWS/Azure VPC	Your physical hardware
Data egress	Yes — evaluation only	None	None
Internet required	Yes	For updates only	No
External API calls	None	None	None

Encryption keys	Finch-managed	Customer-managed	Customer-managed
Recommended for	POC / testing only	Production use	Gov / high-security

Important: Public Cloud mode is intended for workflow evaluation and testing only. Finch recommends Private VPC as the minimum deployment mode for any environment processing real customer data or compliance documents.

COMPLIANCE & AUDIT

Audit-Ready by Default

Finch generates immutable, timestamped audit trails for every decision automatically. These records are designed to satisfy examination requirements from federal and state regulators without manual preparation.

What Gets Logged

- Every compliance decision (approval, rejection, escalation) with timestamp and officer ID
- AI recommendations and the specific policy sections they referenced
- Officer overrides — what the AI recommended vs. what the officer decided, and why
- Document ingestion events — what was added to the Living Vault and when
- Rule changes — who modified Decision Engine rules, what changed, and effective date
- Access logs — who accessed the system, what they viewed, from where

Regulatory Framework Compatibility

FRAMEWORK	AUTHORITY	HOW FINCH ADDRESSES IT
BSA / AML	FinCEN	SAR workflow support, CTR tracking, transaction monitoring, CDD automation
KYC / CIP	USA PATRIOT Act	Identity verification workflows, PEP screening, risk-based due diligence
SOC 2 Type II	AICPA	Immutable decision logs, access controls, automated audit trail generation
OFAC	Treasury	SDN list screening, near-match escalation, documented screening records
State MTL	State regulators	Jurisdiction-specific rule ingestion, multi-state compliance support
GLBA	FTC / OCC	On-premise data residency, financial data safeguards, customer privacy

Data Retention & Deletion

Audit logs are retained for the duration configured by the customer, with a recommended minimum of 5 years to satisfy BSA recordkeeping requirements. Customers have full control over data retention policies and can configure automated deletion schedules.

Upon contract termination, all customer data, model weights, and audit logs are permanently deleted from Finch systems within 30 days. A certificate of destruction is provided upon request.

Certification Status

CERTIFICATION	STATUS	EXPECTED
SOC 2 Type I	In progress	Q3 2026
SOC 2 Type II	Planned	Q1 2027
Pen test (third-party)	Scheduled	Q2 2026

NEXT STEPS

For a detailed security review, architecture walkthrough, or to schedule a penetration test of your deployment environment, contact:

security@finch.io | demo@finch.io

We're happy to participate in your vendor security assessment process and complete any security questionnaires your procurement team requires.