VOUCHCORE

Autonomous Trust Defense Platform

Technical Architecture Overview

Ref: VC-ENG-2026-02 · Confidential · March 2026

EXECUTIVE SUMMARY

The Threat Has Evolved. The Defense Must Too.

Business Email Compromise, AI-generated voice fraud, and vendor impersonation attacks now represent the primary financial threat vector facing Community Financial Institutions and SLTT organizations. Legacy email security tools were built to filter spam. They were not built to evaluate intent.

VouchCore is an Autonomous Trust Defense Platform purpose-built for CFIs and the full SLTT landscape — State, Local, Tribal, and Territorial organizations. Our Conviction Engine evaluates behavioral context, communication anomalies, and transactional intent in real time, with a Human-in-the-Loop architecture that ensures expert validation before any high-impact decision executes.

THE THREAT LANDSCAPE

Intent as the Attack Vector

Modern fraud does not arrive as malware. It arrives as a perfectly composed email from your CFO's legitimate account, a vendor call from a spoofed but authenticated number, or a wire instruction that passes every technical filter — because technically, it is clean. The compromise is not in the packet. It is in the intent behind it.

Threat Vector	Legacy Defense	VouchCore Response
BEC from compromised accounts	Blind — passes DMARC	Behavioral intent classification
AI-generated voice fraud	No detection capability	Caller-ID weaponization signals
Vendor impersonation	Display name filters only	Deep relationship context analysis
Wire fraud instructions	Rule-based triggers	Transactional intent scoring

---

CORE ARCHITECTURE

The Conviction Engine

The Conviction Engine is VouchCore's primary intelligence layer, powered by Gemini via Vertex AI. It operates across three integrated capability domains:

Capability	Implementation	Outcome
Vertex AI Intent Analysis	Gemini extended context window evaluates communication vectors	BEC, impersonation, and caller-ID weaponization classified pre-delivery
BigQuery ML Peer Defense	Predictive clustering across community threat telemetry	Patient Zero detection broadcast across all enrolled nodes
HITL Analyst Interface	Human-in-the-Loop validation before all high-impact decisions	Expert authority retained over context and consequence

---

CORE DIFFERENTIATOR

Sovereign Stewardship — Architecture as a Promise

VouchCore provides every enrolled CFI and SLTT organization with a physically isolated, GCP-native VPC perimeter. Whether the tenant is a Tribal nation, county government, municipal utility, or community credit union — their data is categorically isolated. Not co-mingled. Not mined. Not used to train external models. Ever.

· Threat telemetry strictly localized within tenant GCP boundary

· Vertex AI inference executes within the secure perimeter only

· No civic or financial metadata exposed to public internet egress

· No tenant data used for unauthorized third-party model training

· Cross-tenant data access is a hard architectural blocker — by design

· Built by an active CFI practitioner and U.S. Marine veteran

---

12-MONTH ROADMAP

Three Phases. One Mission.

`Phase 01 · The Construct · Months 1–4`

Deployment of the Conviction Engine as the primary communications and identity verification layer for enrolled CFI and SLTT beta partners. Real-time DMARC enrichment, BEC signal classification, caller-ID weaponization detection, and HITL analyst interface — all within a Sovereign Stewardship perimeter per enrolled tenant.

Outcome: Beta partners achieve measurable reduction in BEC exposure within 60 days.

`Phase 02 · Sovereign Enclaves · Months 5–8`

Dedicated GCP tenant architecture per enrolled institution, designed to satisfy CJIS, GLBA, and Tribal data sovereignty mandates. BigQuery ML predictive clustering activated across the peer network. Patient Zero detection broadcast across all enrolled nodes. SOC 2 readiness infrastructure in place.

Outcome: VouchCore becomes the compliance-grade trust defense layer for institutions under the most stringent regulatory environments.

`Phase 03 · Pre-Fraud Syndicate · Months 9–12`

Activation of the federated intelligence mesh across all enrolled Sovereign Enclaves. Each node contributes anonymized threat telemetry. The Conviction Engine aggregates mathematical threat weights — never raw data — into a continuously evolving, network-wide threat model. Every new enrolled institution strengthens the collective defense of all others.

Outcome: A permanent competitive moat and collective defense capability no siloed vendor can replicate.

INFRASTRUCTURE

Why Google Cloud

VouchCore is GCP-native by design, not by convenience. Google Cloud's Vertex AI, BigQuery ML, and VPC Service Controls provide the exact combination of frontier intelligence, compliance-grade isolation, and public sector trust infrastructure that CFI and SLTT deployments require.

GCP Service	VouchCore Usage
Vertex AI	Conviction Engine inference — Gemini model family
BigQuery ML	Peer defense clustering and Patient Zero detection
Cloud Functions	vouchcore-outreach — daily 09:00 UTC pipeline
VPC Service Controls	Sovereign Stewardship perimeter enforcement
Cloud Logging	Production verification and audit trail
Cloud Scheduler	Automated outreach and enrichment cadence

VouchCore is currently operating in stealth, selecting founding beta partners from the CFI and SLTT ecosystem. Institutions that can no longer afford to wait for enterprise vendors to notice they exist — we built this for you.

daniel@vouchcore.com · vouchcore.com · Veteran Owned & Operated · Pacific Northwest, USA