Security Claim Verification Report

FedShredder

Claims mapped to repository file paths; snippets extracted via pattern match.

Contractual controls are Operator commitments. Implemented controls reflect current open-source codebase.

no-training [contractual] ✓

Pilot Data is not used to train foundation models.

Evidence:

- `marketing/public/security/developer/sources/pilot-data-addendum.md`

 # Pilot Data Addendum FedShredder LLC This Pilot Data Addendum ("PDA") suppleme

 # Pilot Data Addendum FedShredder LLC This Pilot Data Addendum ("PDA") suppleme

 # Pilot Data Addendum FedShredder LLC This Pilot Data Addendum ("PDA") supplemen

gemini-subprocessor [implemented] ✓

Gemini API is the named LLM subprocessor for extraction.

Evidence:

- `marketing/public/security/developer/subprocessor-register.json`
- `backend/services/ai_service.py`

{ "registerVersion": "1.1.0", "lastUpdated": "2026-05-29"

{ "registerVersion": "1.1.0", "lastUpdated": "2026-05-29"

{ "registerVersion": "1.1.0", "lastUpdated": "2026-05-29", "operator": "FedShredder",

t__(self): api_key = os.getenv("GEMINI_API_KEY") or os.getenv("API_KEY") if not api_key:

("Gemini API key is missing. Please set GEMINI_API_KEY in your environment variables.") genai.con

"Check PDF text extraction (OCR) and GEMINI_API_KEY.") elif gap_count > 0:

cors-localhost [implemented] ✓

Backend CORS is restricted to localhost dev origins.

Evidence:

- `backend/main.py`

add_middleware(CORSMiddleware, allow_origins=["http://localhost:3000", "http://127.0.0.1:3000"], allow_cred

orm from fastapi.middleware.cors import CORSMiddleware from fastapi.responses import JSONResponse, Response from p

CORS middleware app.add_middleware(CORSMiddleware, allow_origins=["http://localhost:3000", "http://127.0.

chroma-telemetry-off [implemented] ✓

ChromaDB anonymized telemetry is disabled.

Evidence:

- `backend/services/vector_store.py`

=db_path, settings=Settings(anonymized_telemetry=False)) # Get or create collectio

html-sanitize [implemented] ✓

AI HTML output strips script tags.

Evidence:

- `backend/services/ai_service.py`

t__(self): api_key = os.getenv("GEMINI_API_KEY") or os.getenv("API_KEY") if not api_key:

("Gemini API key is missing. Please set GEMINI_API_KEY in your environment variables.") genai.con

"Check PDF text extraction (OCR) and GEMINI_API_KEY.") elif gap_count > 0:

scanned-pdf-block [implemented] ✓

Scanned/low-text PDFs return blocking OCR-required error.

Evidence:

- `backend/processors/ingestion.py`

blocking_error = (f"OCR Required - Scanned Document Detected " f"({best.char

alueError("This PDF is password-protected. Please provide an unlocked version.")

Error("This PDF is password-protected. Please provide an unlocked version.")

no-auth [not_implemented] ✓

Multi-tenant authentication is not implemented in the app.

Evidence:

- `backend/main.py`

add_middleware(CORSMiddleware, allow_origins=["http://localhost:3000", "http://127.0.0.1:3000"], allow_cred

orm from fastapi.middleware.cors import CORSMiddleware from fastapi.responses import JSONResponse, Response from p

CORS middleware app.add_middleware(CORSMiddleware, allow_origins=["http://localhost:3000", "http://127.0.

localstorage-persistence [implemented] ✓

Frontend persists projects in browser localStorage without server encryption.

Evidence:

- `frontend/services/storageService.ts`

ects.push(stored); } localStorage.setItem(STORAGE_KEY, JSON.stringify(projects));

roject for backward compatibility localStorage.setItem(CURRENT_PROJECT_KEY, JSON.stringify(stored)); }

d current project const current = localStorage.getItem(CURRENT_PROJECT_KEY); if (current) {

no-soc2-claim [disclosed] ✓

SOC 2 is roadmap only — not claimed as certified.

Evidence:

- `marketing/lib/security-pack.ts`

*/** CISO-ready security packet — proactive pilot scope and verifiable artifacts. */ export const SECURITY_PACK = {*

*ve pilot scope and verifiable artifacts. */ export const SECURITY_PACK = { title: "Security & dat*

*pilot scope and verifiable artifacts. */ export const SECURITY_PACK = { title: "Security & dat*

Controls matrix rows: 20