TVCRpro — Security Posture Brief

For information security reviewers

DOCUMENT	TVCR-SEC-001-A
VERSION	1.0
BUILD	Site v31.1 · Worker 1.0.0-phase3.14
DATE	May 5, 2026
CLASSIFICATION	Public
OPERATOR	Atomic Armstrong (sole proprietor, Ontario, Canada)
PATENT	USPTO Application 64/045,951 · Confirmation #7707 · Filed April 21, 2026
COMPANION	Sister brief for non-technical decision-makers: TVCR-SEC-001-B

1. Scope

This brief covers the TVCRpro public website (tvcrpro.com), the analyzer interaction surface (/analyzer), and the supporting Cloudflare Worker (api.tvcrpro.com). It does not cover any service that has not yet shipped.

2. What TVCRpro is

A measurement framework for AI-generated work. The operator pastes a prompt and a response; the system returns an eleven-dimension rubric score, a single composite ratio, and a coaching anchor. The composite combines the eleven dimensions under a patent-pending weighting and token-normalization layer that is not exposed to the operator's browser and not transmitted to the inference vendor.

3. Data flow

3.1 Visitor browsing static pages

Browser to Cloudflare CDN to Cloudflare Pages-hosted static assets. No origin server. No application database. No cookies set by tvcrpro.com. Cloudflare logs request metadata at the edge under its standard terms.

3.2 Visitor using /analyzer

1. Operator pastes prompt and response (and optional context) into form fields in their browser.
2. On submit, the browser POSTs JSON to https://api.tvcrpro.com/score.
3. The Cloudflare Worker validates payload size limits (prompt 16 KB, response 24 KB, context 400 chars), enforces CORS allow-list (tvcrpro.com, www.tvcrpro.com), and constructs a single Anthropic Messages API call.
4. Anthropic returns dimension scores 0–1 plus a coaching sentence. The worker applies the patent-pending weights and token-normalization, computes the composite, and returns JSON to the browser.
5. The browser renders the result in-page. Nothing is persisted in the browser beyond the in-tab session.

3.3 What is logged

- **Cloudflare:** standard edge access logs (IP, URI, status, timestamp, country) under Cloudflare's data-processing terms. Prompt and response bodies are not extracted into application logs.
- **Worker:** errors are logged to Cloudflare Workers logs without prompt or response payload. Token counts and request id are recorded for diagnostics.
- **Anthropic:** the operator-pasted prompt and response are processed by Anthropic to generate the rubric output, under Anthropic's commercial terms. Anthropic does not use API inputs or outputs to train models.[1]
- **TVCRpro origin:** none — there is no TVCRpro origin server beyond the Cloudflare Worker. There is no application database. There is no analytics pixel.

4. Architectural separation

The framework is deliberately split:

Component	Where it lives	What is exposed
Eleven-dimension rubric definitions	/methodology (public)	Full text, public
Rubric scoring (per-dimension 0–1)	Anthropic API call	Operator's pasted text travels to Anthropic; no TVCRpro weights, no normalization constants, no thresholds
Composite weighting, token-normalization curve, bucket thresholds	Cloudflare Worker	Server-side only. Inlined at build time; never in source repo, never in browser bundle, never transmitted to the inference vendor
Anthropic API key	Cloudflare Worker secret	Encrypted at rest; not visible to the worker editor UI after creation; rotatable

Verification:

- Browser DevTools Network tab on /analyzer: only outbound request to `api.tvcrpro.com/score`.
- Browser DevTools Sources tab: search for any of `0.45`, `0.55`, `elasticity`, `reference_token`, `composite_weights` — zero matches.
- Worker bundle (`worker.js`, served from Cloudflare): grep for `sk-ant` returns nothing.

5. Sub-processors

Five sub-processors with role and trust-center URL.

Function	Provider	Jurisdiction	Trust center
Static site hosting · DNS · WAF · Worker runtime · CDN	Cloudflare, Inc.	U.S. (with Canada and EU PoPs)	cloudflare.com/trust-hub
Email (operator inbox)	Proton AG	Switzerland	proton.me/legal

Function	Provider	Jurisdiction	Trust center
Productivity suite, document workflow	Microsoft 365 (Canada tenant)	Canada	microsoft.com/trust-center
Document tooling (PDF render, signing)	Adobe Inc.	U.S.	adobe.com/trust
Inference for the eleven-dimension rubric	Anthropic, PBC	U.S.	trust.anthropic.com

The current page count of sub-processors on /security and in the site footer are kept in sync. Any change requires both pages to be updated, the document registry to be incremented, and a new build deployed.

6. Network and platform controls

6.1 Edge controls (Cloudflare)

- WAF rate limit on `POST api.tvcrpro.com/score`: 3 requests / 10 seconds per source IP, with a 1-minute block on breach. Tuned to deter abuse while permitting good-faith pilots.
- TLS 1.2+ enforced; HSTS with preload (managed by Cloudflare).
- Custom CSP via Cloudflare Transform Rule: `default-src 'self'; script-src 'self' 'unsafe-inline' https://www.google.com https://www.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; img-src 'self' data:; frame-src https://www.google.com; connect-src 'self' https://api.tvcrpro.com`. The CSP is intentionally restrictive on `connect-src` so that the analyzer can reach only the named worker subdomain.
- Additional response headers: `X-Content-Type-Options: nosniff`, `X-Frame-Options: DENY`, `Referrer-Policy: same-origin`.

6.2 Worker controls (Cloudflare Worker)

- CORS allow-list restricted to `https://tvcrpro.com` and `https://www.tvcrpro.com`.
- Method allow-list: `OPTIONS`, `POST /score`, `GET /healthz`. All other methods and paths return 404 / 405. (The exact 404-for-root behavior is intentional and used as a worker-alive signal during deploy verification.)
- Body validation: prompt at most 16 KB, response at most 24 KB, context at most 400 characters. Oversized bodies are rejected before reaching Anthropic.
- Anthropic API key supplied as a Cloudflare Worker secret; rotatable from the Cloudflare dashboard.
- Anthropic monthly spend cap enforced at the Anthropic console: USD 25 / month.

6.3 Build controls

- Site source: Astro static-site generator. Output is plain HTML/CSS/JS uploaded to Cloudflare Pages by the operator. No CI/CD pipeline; no build server.

- Worker source: TypeScript bundled to a single `worker.js` via esbuild. Trade-secret weights are inlined at build time from a local secrets file (never committed). Bundles are inspected (grep) for secret patterns before upload.
- Every site deploy carries a build identifier in the page footer (e.g., `v31.1`) and a machine-readable /build.json at the site root for reviewer reference.

7. Operator obligations

Operators using /analyzer should not paste content that contains regulated personal data (PHI, PCI, regulated PII), trade secrets they are not authorized to share with Anthropic, or material covered by export-control restrictions. The form is a thin gateway to Anthropic; controls there are Anthropic's, not TVCRpro's.

8. What this brief is not

- **Not a SOC 2 report.** No SOC 2 Type I or Type II audit has been performed. No third-party audit firm has been engaged. The operator is a sole proprietor; there is no audit committee.
- **Not a penetration test report.** No external penetration testing has been performed against tvcrpro.com or api.tvcrpro.com.
- **Not a formal vendor risk assessment.** Sub-processor selection was made by the operator; no third-party VRM service has reviewed the chain.
- **Not a privacy program certification.** No GDPR Article 27 representative is appointed; no CCPA service-provider attestation is published; no DPA template is provided. Pilot engagements include a one-page DPA on request.
- **Not a continuity plan.** No documented incident response runbook beyond operator-direct notification through pilot@tvcrpro.com.

The current trust artifacts are: (1) the patent filing, (2) the architectural separation between the public rubric and the protected weighting, (3) the public sub-processor disclosure, and (4) direct access to the operator. Pilots are scoped accordingly. These gaps are intentional disclosures, not omissions.

9. Independent verification

A reviewer can independently confirm every claim in this brief without contacting the operator.

Claim	Independent verification path
Patent filing exists	patentcenter.uspto.gov — search Application 64/045,951
Site is on Cloudflare	`dig tvcrpro.com NS` or `curl -I https://tvcrpro.com` (header `server: cloudflare`)
Worker exists at api.tvcrpro.com	`curl https://api.tvcrpro.com/healthz` returns `{"ok":true,"worker":"1.0.0-phase3.14","prompt":"1.0.0"}`
Build identifier matches this brief	`curl https://tvcrpro.com/build.json` returns `{"version":"v31","build":"1",...}`

Claim	Independent verification path
Sub-processor count and identities	tvcrpro.com/security#sub-processors
CSP enforces connect-src allowlist	`curl -I https://tvcrpro.com/analyzer` and read the `content-security-policy` header
Worker bundle has no embedded API key	View Source on the analyzer page; the page only references `https://api.tvcrpro.com/score`. The worker bundle is not served to the public; its absence of secrets is asserted by the operator and can be confirmed during pilot scope on request.

10. Contact

- **Operator (direct):** Atomic Armstrong — atomicarmstrong@proton.me
- **Pilot inquiries:** pilot@tvcrpro.com
- **Security disclosures:** security@tvcrpro.com (NDA-friendly; please include a reproducer)

---

[1] https://www.anthropic.com/legal/commercial-terms

This brief is updated whenever the build identifier changes. The current build identifier is visible in the footer of every page on tvcrpro.com and at https://tvcrpro.com/build.json.

Next planned brief revision: when SOC 2 Type I scoping commences, when penetration testing is performed, or when the sub-processor list changes — whichever comes first.