Sentinel Security Whitepaper

Sentinel Edge Networks LTD · Registered in England & Wales 17150600 · Version 1.0 · 16 July 2026 · canonical copy at sntlhq.com/security-whitepaper

Sentinel is a real-time fraud detection API (sntlhq.com). This document states our security posture plainly for procurement and security review: the controls in place today, how data is handled, and — deliberately — what we do not yet have. It is written to be checked, not to impress: every claim here is verifiable on the linked public pages, and we do not list controls we don't have.

1. Certifications & audits — the honest version

Sentinel is **pre-audit for SOC 2 Type II** and holds no SOC 2, ISO 27001, HIPAA, or PCI DSS attestation today. No third-party penetration test has been commissioned yet. We say this here rather than imply otherwise with badge walls; this section will be updated as each milestone lands, with the change dated on our changelog. A responsible-disclosure program is active (/responsible-disclosure, RFC 9116 `security.txt` published).

2. Technical controls in place today

CONTROL	IMPLEMENTATION
Authentication	Email + bcrypt-hashed password, Google OAuth (RS256, JWKS verified), TOTP 2FA, reviewable active-session list with per-device revocation, account lockout on repeated failures.
API key management	Keys generated with `crypto.randomBytes` (prefix `sk_live_`); rotation and instant revocation via dashboard; key rotation and password change require re-authentication.
Password breach check	Have I Been Pwned k-anonymity (5-character SHA-1 prefix only) on signup and password reset — the password itself never leaves our infrastructure.
Transport security	TLS 1.2+; HSTS preload; CORP same-origin; CSP with allowlists and live violation reporting; X-Content-Type-Options nosniff; X-Frame-Options DENY; Permissions-Policy locks camera/mic/geolocation/payment.
Rate limiting	Per-API-key and per-source-IP caps on evaluation endpoints; exponential backoff on authentication endpoints.
Session invalidation	Password change/reset or admin suspension immediately invalidates all sessions (token-epoch bump).
Encryption at rest	Managed encryption at rest on the primary database (Turso / libSQL).
Uptime transparency	Self-hosted status page with persisted 90-day probe history and real measured uptime at /status — no vanity numbers.

3. Data handling & retention

DATA	POLICY
Lookup IPs	Raw IPs retained 7 days, then reduced to a one-way hash.
Signup emails (API signal)	Checked transiently against disposable-domain feeds; never stored or logged.
Device linking	Per-customer only, stored as one-way hashes; never linked across customers.
Account deletion	GDPR Art. 17 self-service deletion with password re-auth; immediate deletion plus encrypted-backup roll-off within 60 days.
Analytics & advertising	None. Fonts self-hosted; no third-party analytics or ad providers anywhere on the product or site.

4. Sub-processors

Cloudflare (CDN/edge), Railway (hosting), Turso (database), Resend (transactional email), Google (Sign-In only), Have I Been Pwned (k-anonymity check), plus network- and device-intelligence providers named to customers under DPA. The live list with a dated change log is public at /sub-processors; new data-processing sub-processors get 30 days' advance notice with right to object.

5. Compliance framework

UK GDPR / EU GDPR aligned (processor role for evaluation traffic; DPA with SCCs available for every customer — request via sales@sntlhq.com). CCPA honored. Security questionnaires (SIG-Lite, CAIQ, bespoke) completed within 5 business days of request. MSA available where click-through Terms can't be accepted.

This document is a plain-language summary, not a contract; contractual commitments live in the Terms, DPA, and (for enterprise) MSA/SLA. Verify anything here against the live pages: /trust, /privacy, /status, /sub-processors. Questions: support@sntlhq.com.