Covren Security & Compliance Brief

Last updated: March 2026 | For RFP and compliance review

Data Encryption

In transit: TLS (HTTPS) on all connections. HSTS enforced. Cookies marked Secure and SameSite=Lax.

At rest: AES-256-GCM with per-tenant key derivation (HKDF-SHA256). Passwords hashed with bcrypt. No plaintext credentials stored.

Tenant Isolation

Every database query is scoped to the requesting tenant. No implicit shared context. Access controls enforced on every request, not just at the boundary.

Authentication & Access Control

Email/password with bcrypt hashing. Optional SSO via OIDC and SAML 2.0. Server-side sessions with HTTP-only, Secure cookies. Account lockout after repeated failed logins.

Four RBAC roles (Editor, Member, Admin, Super Admin) control access to draft approval, content export, and tenant administration.

AI Data Handling

- Covren ingests change metadata (commit messages, PR descriptions, diff summaries) — **not full source code**
- Secrets, PII, raw code, and API keys are stripped before LLM processing
- All AI-generated content requires **human review and approval** before delivery. Nothing is auto-published
- AI provider (Anthropic) does not train on API customer data. Data retained 30 days for safety monitoring only

API & Application Security

Control	Implementation
Rate Limiting	Redis-backed sliding-window. Per-tenant (120/min), per-IP (30/min), per-endpoint buckets.
Input Validation	Typed schemas on all endpoints. 20 MB body size limit.
Security Headers	X-Content-Type-Options, X-Frame-Options: DENY, HSTS, Referrer-Policy, CSP.
Webhook Verification	HMAC-SHA256 with constant-time comparison. Payload redaction (secrets, tokens, keys stripped).
Error Handling	Structured responses with support ID. No stack traces or internal paths exposed.

Audit Trail & Compliance

Append-only audit logs for all significant actions (approvals, rejections, assignments, content queries). Immutable rows with timestamp and actor ID. Configurable data retention (90, 180, 365, or 730 days). Full tenant data export (GDPR Article 20) and right-to-erasure with 14-day grace period.

Incident Response

72-hour breach notification per GDPR Article 33. Notifications include: nature and scope, data categories affected, remediation measures, and a point of contact. Sent to account owner and order form contacts.

Infrastructure & Billing

- PostgreSQL with TLS, connection pooling, and statement timeouts
- Secrets loaded from environment variables with 300s TTL refresh (rotation without restarts)
- Health endpoints (/health/live, /health/ready) for orchestration
- Payments via Stripe — no card data stored. Webhook signature verification on all events
- 7 alert rules monitor LLM errors, latency, request errors, queue backlog, pool exhaustion, budget limits, and worker health

Sub-processors

Provider	Purpose	Data	Location
Anthropic	AI classification & drafts	Redacted change summaries	US
Stripe	Billing & payments	Email, subscription data	US
SendGrid	Transactional email	Email addresses	US
Railway	Hosting, DB, cache	All data (encrypted)	US

Verification & Trust Signals

- CSA STAR Level 1 self-assessment • OWASP ASVS Level 1 self-assessment • Mozilla Observatory scan
- SSL Labs TLS report • security.txt (RFC 9116) • Automated dependency scanning (pip-audit in CI)
