

Trusted with your revenue pipeline data.

A snapshot of the technical & operational controls protecting the accounts, signals and integrations that flow through Indicato.

0

CRITICAL OR HIGH FINDINGS

SECURITY PILLARS

A

Identity & Access
Multi-tenant JWT auth with TOTP MFA, brute-force lockout and per-tenant role scoping.

B

Data Protection
TLS in transit, encryption at rest, tenant-scoped queries, no secrets in logs or client storage.

C

Application Hardening
Pydantic-validated inputs, rate limiting, server-side price validation and CSRF-safe cookies.

D

Observability
Immutable audit log, session tracking, integration sync logs and a real-time ops status page.

VERIFIED CONTROLS

DOMAIN	CONTROL IN PLACE TODAY
✓ Authentication	Tenant slug + email + password + optional TOTP MFA. bcrypt with adaptive cost. 5-attempt lockout with 15-minute cool-down.
✓ Session & Tokens	JWTs signed with pinned algorithm, delivered via HttpOnly, Secure, SameSite cookies. Tokens never touch localStorage.
✓ Tenant Isolation	Every write is scoped to the authenticated tenant. 139 tenant-filtered query sites verified.
✓ Payments	Stripe amounts are read server-side from an immutable pricing catalogue. Client-provided prices are ignored.
✓ Password Reset	Cryptographically random 256-bit tokens, single-use, 1-hour TTL. Endpoint returns constant response to prevent user enumeration.
✓ Rate Limiting	SlowAPI limits applied to authentication, password reset, marketing intake and pixel ingestion endpoints.
✓ Audit Trail	Immutable append-only audit log across 100+ call sites: logins, user changes, tenant edits, integration grants, checkout events.

APPLICATION BOUNDARIES

- No **raw HTML injection** in the client — React 19 auto-escapes; no dangerouslySetInnerHTML.
- No **eval / exec** anywhere in the backend or frontend codebase.
- No **tokens or API keys** stored in browser storage — cookies only, HttpOnly.
- No **shell interpolation** with user input — subprocess calls use argv arrays.

COMPLIANCE POSTURE

- CCPA / CPRA**: User opt-out endpoint operational; PII fields are catalogued and access-logged.
- SOC 2 Type II**: Evidence collection underway — this document is part of the Access Control & Cryptography narratives.
- GDPR**: Data residency configurable per tenant; no third-country transfer of enrichment data without explicit consent.
- Vendor security**: Stripe, ElevenLabs, DeepSeek and Zoho are all SOC 2 attested upstream.

SECURITY ROADMAP

NOW

Zero critical or high findings from the July 2026 internal review.

Q3 2026

Enterprise password policy, transactional reset email delivery, security-headers middleware.

Q4 2026

External penetration test, SOC 2 Type II attestation, Snyk continuous supply-chain scanning.