

Requiems API — Security & Architecture Packet

For enterprise security reviews and procurement teams

1. Core Security Model — Stateless Architecture

Requiems API is engineered as a zero-trust, stateless processing engine. Every API request is processed entirely in volatile server memory (RAM). The moment your HTTP response is delivered, the payload is permanently purged. We have no mechanism to recover submitted data because it was never written to disk, a database, or any persistent medium.

- In-memory execution — payloads never touch disk or any persistent layer
- Zero data retention — no database of user API inputs or outputs exists
- No request/response cache or logging of payload content
- Anonymized telemetry only — HTTP status codes and timestamps, never payload content

2. Transparency — The Counter API Exception

Our Counter API endpoint (`/v1/technology/counter/{namespace}`) is the only endpoint that persists data beyond a single request. It stores a named integer count value (e.g., namespace "page-views" maps to an integer). No request payload, no user content, and no identifying data is stored — only the counter value itself. This endpoint is rarely used and can be avoided entirely if zero-persistence is required by your organization.

3. Network Perimeter — Cloudflare

All inbound traffic is routed through Cloudflare before reaching our origin servers.

- Enterprise-grade DDoS mitigation at the edge
- Web Application Firewall (WAF) filtering on all requests
- TLS 1.3 enforced — no downgrade to older protocol versions
- Rate limiting and abuse prevention at the network layer
- IP reputation filtering

4. Physical Infrastructure — Hetzner (EU)

Our custom datasets and processing code are hosted on servers in European Union data centers operated by Hetzner Online GmbH, an ISO/IEC 27001-certified provider.

- All data centers located in the European Union

- ISO/IEC 27001 certified facilities (physical security, environmental controls)
- Strict physical access controls and 24/7 CCTV monitoring
- Redundant power systems and network connectivity
- Hetzner's ISO 27001 certificate available upon request

5. API Authentication & Access Control

- High-entropy API keys issued per account — cryptographically random, not guessable
- Instant key revocation available via user dashboard
- TLS 1.3 required on every API request — keys transmitted only over encrypted channels
- Rate limiting enforced by the Go API per API key
- Cloudflare Origin Pulls and Caddy mTLS prevent direct-origin bypasses

6. Compliance Scope Alignment

Because Requiems API maintains a 100% stateless architecture for user payloads, a traditional SOC 2 data-retention audit does not apply to our operational footprint. We satisfy the core Security and Confidentiality principles of SOC 2 by design — never retaining data at rest. Physical infrastructure compliance is inherited via Hetzner's ISO 27001 certification. Network compliance is inherited via Cloudflare's enterprise security controls.

- GDPR: No user input stored or profiled. EU-only infrastructure. Data minimization is structural.
- CCPA: No sale or sharing of personal data. No user input database exists to share.
- SOC 2 Security/Confidentiality: Satisfied by never retaining data at rest.
- Physical Compliance: Inherited from Hetzner ISO 27001 certification.

7. Incident Response

In the event of a security incident, we commit to notifying affected clients within 72 hours of discovery. Contact: eliaz@bobadilla.tech