Security & Compliance Brief

Prepared for security, compliance, and procurement review · www.fastyoke.io/enterprise

Executive summary

FastYoke treats regulated workloads as a **design constraint**, not a retrofit. Every tenant operates on its **own database file** — isolation is mechanical at the operating-system layer, not a shared-row filter. State transitions are enforced through a **finite state machine** with sandboxed guard evaluation, recorded in an **append-only event log**, and exposed through **role-gated APIs**.

This brief complements the Security executive summary with deployment substrates, AI retrieval posture, and compliance tooling that security and compliance officers evaluate during enterprise procurement. It does not replace the full technical Trust Center or the printable PII security summary.

Deployment substrates — where your data lives

Compliance posture varies by substrate. The same application code runs across all options; operators choose where tenant databases, audit logs, and retrieval indexes reside.

SUBSTRATE	COMPLIANCE RELEVANCE
Managed Runtime	Fully managed cloud with TLS everywhere, infra encryption at rest, Litestream backups, and optional **Enterprise+ region pinning** for residency obligations.
On-Prem / air-gap	Single-binary deployment inside your network. **No outbound traffic required** — tenant databases, FSM rules, WASM scripting, and audit logs stay on your hardware. Ideal for HIPAA private cloud, OT/IT boundaries, and data-localisation mandates.
Substrate ✦ (mobile fleet)	Native Android/iOS apps distributed privately via MDM or token-gated install links — **no public App Store footprint**. OTA bundles are Ed25519-signed; compatible with On-Prem so PHI and operational data never leave your network.
FastYoke DB	Distributed SQL substrate for HA, geo, and DR at Enterprise+ scale — per-tenant isolation preserved at the datastore layer.

Full deployment detail: On-Prem overview · Substrate overview · Runtime overview

Five-control security posture

CONTROL	SUMMARY
1. Tenant isolation	Dedicated SQLite file per tenant (or FastYoke DB at scale). Cross-tenant access is mechanically impossible — the application never holds two tenants' files open simultaneously.
2. Encryption	TLS in transit; infra encryption at rest; optional **PII/SPI field-level encryption** (AES-256-GCM per-tenant keys) for tagged fields — opaque to platform admins without the authorized read path.
3. Access control	72-permission RBAC catalog; scoped Personal Access Tokens with hard refusals outside granted scopes; WorkOS AuthKit SSO; Strategic Partner consent grants.
4. Auditability	Append-only event log (no UPDATE/DELETE); sealed ed25519 PDF exports; immutable posted journal entries; role-change audit with export.
5. Operational security	`security@fastyoke.io` with 24-hour acknowledgement SLA; Dependabot + gitleaks + cargo deny on every PR; documented incident response; continuous Litestream backup.

Full PII scope, shared-responsibility model, and subprocessor detail: Security executive summary · Subprocessor list

Yoker — retrieval-augmented generation (RAG)

WHY COMPLIANCE TEAMS CARE ABOUT YOKER

Yoker is FastYoke's docked AI assistant. It answers natural-language questions grounded in **tenant-scoped entity records** and **text attachments** (PDF, Word, plain text). Retrieval runs **on your VM** — embeddings use ONNX locally; vector search runs in Rust against tenant-scoped `rag_chunks`. Tenant data is **not sent to external providers for search**.

RAG PROPERTY	POSTURE
On-VM embeddings	Record chunks embedded with ONNX on the FastYoke VM; no external embedding API.
Tenant-scoped corpus	Retrieval indexes only the requesting tenant's records and attachments — cross-tenant queries are impossible by construction.
Cited sources	Every answer includes `used_sources` chips so auditors can verify which records grounded the reply.
Ephemeral sessions	Chat history is not persisted server-side; each turn is forgotten after the answer.

RAG PROPERTY	POSTURE
Entitlement gating	Yoker requires Enterprise / Fleet (included) or the paid `yoker` add-on on Pro+ — endpoints fail closed with `403` when not entitled.
LLM synthesis	Optional external LLM for answer synthesis only; PII scrubbing applies on AI write paths; retrieval itself stays local.
Graceful degrade	When RAG assets are unavailable, the assistant answers without retrieval rather than exposing cross-tenant data.

Pair Yoker with **Compliance Yoke** (below) to run framework-readiness sweeps, then ask tenant-scoped questions about collected evidence. Detail: Yoker overview · Yoker docs

Compliance Yoke — continuous audit readiness

The **Compliance Yoke** marketplace app maps platform evidence to framework controls (SOC 2, HIPAA, GDPR, and others):

- **Evidence connectors** — automated collectors for GitHub, cloud posture, and platform attestations.
- **Framework readiness scoring** — connector results plus operator attestations roll into per-framework readiness views.
- **Auditor Room** — deterministic sampling packages evidence for external auditors; **OSCAL export** and ZIP download for review packets.
- **Trust Center** — publishable posture page for customers and procurement; optional tenant-scoped AI Q&A gated by admin toggle.

Compliance Yoke is Enterprise-tier. Detail: Compliance Yoke docs

Attestations & frameworks

ATTESTATION	STATUS
VPAT 2.5 (accessibility)	Current — download PDF, regenerated on every release.
SOC 2 Type II	Roadmap — controls operating; bridge letter available on request.
HIPAA posture	Available — BAA on Enterprise / ISV+ with HIPAA add-on.
GDPR readiness	Current — DPA, data-subject rights, EU region pinning.
PCI DSS	Not in scope — cardholder data routes through Stripe (PCI DSS Level 1).

Identity, access & shared responsibility

- **72-permission RBAC** — every API and UI surface gates on explicit permissions.
- **Personal Access Tokens** — scoped `fy_pat_` tokens; hard refusals outside granted scopes.
- **Strategic Partner consent** — implementation partners reach a tenant only while a per-tenant grant is active.

Some controls are customer-operated: field `is_pii` / `is_spi` tagging, SSO + 2FA on operator accounts, BAA execution before PHI processing, and subprocessor list review. See the shared-responsibility table on the Security page.

Artifacts & next steps

- **This brief (PDF)** — deployment substrates, RAG posture, Compliance Yoke summary.
- **PII security summary (PDF)** — full five-control model, PII scope, subprocessors.
- **Security questionnaires:** security@fastyoke.io
- **Procurement & sales:** Contact sales · sales@fastyoke.io
- **Technical Trust Center:** www.fastyoke.io/docs/security/trust-center