S I X T A

Security Architecture Pack

Data flow, permissions model, network posture, and audit approach

---

For internal vendor security evaluation

Full technical reference: sixta.ai/sixta-docs.html

March 2026

01

Data Flow Summary

No PII collection by design. SIXTA reads only performance metadata, query fingerprints, schema structure, and configuration values. PII is excluded by the way SIXTA queries databases — not filtered after collection. No row-level data is accessed or transmitted.

Data Category	Contents	Destination	Leaves Network?
Database telemetry	Query metrics, execution plans, lock/session data, replication status, schema metadata	Processed locally within customer infrastructure	No
LLM reasoning context	Performance metadata, query fingerprints, table names, configuration values	Configured LLM endpoint (Anthropic API, internal, or local)	Configurable*
Findings & recommendations	Root-cause analysis, remediation recommendations, alerts, status updates	Slack, Teams, API, or custom integrations	Configurable
Observability enrichment	Metrics, logs, APM traces, incidents, SLO data from existing platforms	Ingested from CloudWatch / Datadog / Percona PMM	No (pulled in)

** Air-gapped deployment available: SIXTA can run entirely within your network with a local LLM (e.g. Ollama, vLLM). In this configuration, zero data leaves your infrastructure.*

What SIXTA does not do: No SIXTA telemetry is sent back to SIXTA the company. No usage data, metrics, or diagnostics are collected. PostHog analytics on the marketing site uses memory-only persistence (no cookies).

02

Permissions Model

SIXTA uses two distinct access levels. Read-only covers all diagnostics. Autonomous permissions are optional, separately credentialed, and individually grantable.

PostgreSQL (minimum read-only)

Privilege	Purpose	Mode
pg_monitor role	Session stats, replication stats, all pg_stat_* views	Read-only
SELECT on pg_stat_statements	Query risk analysis and performance baselining	Read-only
Standard catalog access	pg_class, pg_locks, pg_settings (via pg_monitor)	Read-only
pg_table_size(), pg_total_relation_size(), pg_indexes_size()	Capacity and growth tracking. Available to all roles by default.	Read-only
ALTER SYSTEM (PG 15+) or superuser (PG 14-)	Parameter tuning — separately credentialed. In PG 15+, superuser can grant ALTER SYSTEM on individual parameters. In PG 14 and below, superuser is required.	Autonomous (opt-in)
Table ownership (target tables)	CREATE INDEX CONCURRENTLY	Autonomous (opt-in)
pg_signal_backend	Terminate runaway queries	Autonomous (opt-in)

MySQL (minimum read-only)

Privilege	Purpose	Mode
SELECT on performance_schema, sys	Wait events, statement history, thread activity	Read-only
PROCESS	Active connections, SHOW ENGINE INNODB STATUS, EXPLAIN FOR CONNECTION	Read-only
REPLICATION SLAVE	Topology detection via SHOW REPLICAS	Read-only
SYSTEM_VARIABLES_ADMIN	Runtime parameter tuning via SET GLOBAL	Autonomous (opt-in)
INDEX on target schema(s)	CREATE/DROP INDEX	Autonomous (opt-in)

Privilege	Purpose	Mode
CONNECTION_ADMIN	KILL runaway queries	Autonomous (opt-in)

Observability platforms

Platform	Credentials	Access Level
AWS	IAM Role (recommended), IAM User access keys, or AWS CLI profile	Read-only: Performance Insights, CloudWatch, CloudWatch Logs, RDS Describe* APIs
Datadog	API Key + scoped Application Key	Read-only: metrics, events, monitors, logs, APM, incidents, SLOs
Percona PMM	Grafana Service Account Token (Viewer)	Read-only: metrics, QAN, inventory, alerts

03

Network Posture

SIXTA deploys inside your infrastructure (VPC, on-prem, or air-gapped). It connects outbound to the configured LLM endpoint and, if using Slack/Teams, to api.sixta.ai for websocket coordination only.

Connection	Direction	Protocol	Data	Required?
Database instances	SIXTA -> DB	PostgreSQL / MySQL (TLS required)	Performance metadata only — no row data	Yes
LLM endpoint	SIXTA -> LLM	HTTPS	Query fingerprints, metadata, config values	Yes (can be local)
api.sixta.ai relay	SIXTA <-> relay	WSS (443)	Slack/Teams websocket coordination only	Only for Slack/Teams
Observability platforms	SIXTA -> API	HTTPS	Metric queries, event correlation	Optional
Output integrations	SIXTA -> target	HTTPS / webhook	Findings & recommendations	Configurable

api.sixta.ai: This relay handles Slack/Teams websocket coordination only. No customer data flows through it. Not needed for API-only access, custom integrations, or air-gapped deployments.

Air-gapped mode: SIXTA can run fully air-gapped with a locally-deployed model (Ollama, vLLM, etc.) and custom output integrations. In this configuration, zero outbound connections are required.

04

Autonomous Actions & Guardrails

Autonomous actions are off by default. Each action type is independently enabled and requires its own database credential. All actions are logged in the audit trail before execution.

Action	Scope	Guardrails	Status
Parameter tuning	ALTER SYSTEM SET (PG) / SET GLOBAL (MySQL) / ModifyDBParameterGroup (RDS)	Dry-run by default; previous values recorded for automatic rollback	**Live**
Index creation	CREATE INDEX CONCURRENTLY	Query risk analyzer produces exact DDL with risk classification	**Planned**
Query termination	Terminate runaway queries exceeding defined thresholds	Duration + resource threshold; query can be re-executed by application	**Planned**
Vacuum / Analyze	VACUUM / ANALYZE based on vacuum advisor	Maintenance operation; always safe to run	**Planned**

05

Audit Logging

Every SIXTA action — diagnostic, autonomous, and communication — produces a structured audit record. Records are stored locally and optionally forwarded to your SIEM or log aggregator.

General action log (every tool invocation, 90-day default retention):

Field	Type	Description
id	ULID	Time-sortable unique identifier
timestamp	UTC ISO 8601	When the action occurred
tool	string	e.g. vacuum_advisor, tune_apply, query_risk_analyzer
instance_id	string	Logical instance name (e.g. prod-pg)
action_kind	string	result (auto-stored tool output)

Field	Type	Description
severity	enum	info | warn | critical
params	JSON	Original invocation parameters
data	JSON	Full tool output (complete assessment/result)
summary	string	One-line human-readable description
db_engine	enum	postgresql | mysql
expires_at	timestamp	Retention expiry (90 days default)

Parameter change operations additionally log: dry_run flag, score_before, workload type, per-parameter detail (knob, previous_value, new_value, applied, error), and rolled_back status.

06

Deployment Options

Option	LLM Access	Network	Best For
Standard SaaS	Anthropic API	Outbound HTTPS to api.anthropic.com	Fastest deployment; most teams
Private LLM	Customer-hosted (Ollama, vLLM, etc.)	LLM stays in-network; SIXTA outbound optional	Regulated environments; data sovereignty
Fully air-gapped	Local model + custom integrations	Zero outbound connections	Highest security; no external dependencies

Setup Timeline

Day 1: Deploy SIXTA, grant read-only credentials, connect observability. **Week 1:** SIXTA observes, baselines, and produces first diagnostic reports. **Week 2+:** Optionally enable autonomous actions after reviewing recommendations.

Full technical reference with grant SQL, network diagrams, and audit schema:

sixta.ai/sixta-docs.html

Questions? ewen@sixta.ai