ZeroOne DOTS.ai — Security Brief (1-Pager)

Posture: Responsible AI — Outcome-first — Data Safeguard First

Security posture (at a glance)

- Least privilege and separation of duties — access is scoped, reviewed, and time-bound.
- Encryption — AES at rest; TLS 1.2+ in transit (TLS 1.3 on the roadmap).
- Privacy and minimization — collect and process only what's needed; prefer tokenization or redaction.
- AppSec — build and test against OWASP-style controls; shift-left security in CI.
- Auditability — comprehensive audit trails, access logs, and break-glass procedures.
- Compliance alignment — SOC 2 Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Data handling

- PII strategy — default to minimization; pseudonymize where feasible; manage secrets via KMS or Secret Manager; rotate keys regu
- Storage and transit — AES at rest; TLS 1.2+ in transit with a migration track to 1.3.
- Residency and isolation — per-customer isolation; BYO-VPC option when required.

Identity and access

- RBAC and short-lived credentials — enforce least privilege; automatic expiry; periodic reviews.
- SSO and MFA — strong authentication for admin and data-path roles.

Reliability and operations

- SLOs and error budgets — alert on multi-window burn-rate policies tied to user impact.
- Change safety — canary or blue-green deployments with automatic rollback on SLO breach.
- Incident response — runbooks, post-incident reviews, and captured learnings.

Development lifecycle

- Secure defaults — templates enforce security checks; CI pipelines block on security tests.
- Secrets management — no secrets in code; centralized KMS or Secret Manager; audit and rotation.

What this means for you

- Lower risk via least-privilege design and strong cryptography.
- Faster, safer change via SLO-aware alerting and canary releases.
- Easier audits with SOC 2-aligned controls and OWASP-style coverage.