ENTERPRISE DEPLOYMENT

Trinity Guard® Enterprise Deployment Overview

Dedicated Infrastructure Model for Regulated & Large-Scale Operations

Trinity Guard® combines mobile-first patrol execution with a dedicated backend deployment architecture designed for regulated and large-scale operational environments.

The Enterprise Deployment Model supports on-premise, private cloud, and governed cloud infrastructure while maintaining operational continuity for field teams.

Under this model, patrol workflows remain unchanged for guards and supervisors. Infrastructure, data governance, and lifecycle control operate entirely within a customer-controlled environment.

Strategic Benefits of Dedicated Deployment

Data Sovereignty

- All operational data is processed and stored inside customer-controlled infrastructure.
- No shared database layer.
- No multi-tenant backend exposure within the Enterprise deployment model.
- Data residency, retention, and access governance remain internal.

Financial Structuring Flexibility

- Supports a Long-Term Operational Rights structure aligned with institutional procurement.
- CAPEX-compatible structuring for enterprise budgeting frameworks.
- Predictable lifecycle ownership for long-term operational continuity.

Governance & Compliance Alignment

- Designed to support alignment with GDPR and ISO 27001 readiness expectations.
- Accommodates sector-specific compliance integration requirements.
- Supports logging, SIEM integration, audit retention, and internal monitoring.

Technical Deployment Architecture

Deployment Options

- **On-Premise:** Customer-operated data centers and controlled network zones; internal segmentation; local oversight.
- **Private Cloud:** Dedicated tenant environments in AWS, Azure, or Google Cloud; customer-controlled identity integration (SSO/policies).
- **Governed Cloud:** Government-operated or strictly regulated zones; restricted access and controlled connectivity paths.

Reference Architecture (Conceptual):
Mobile Application → Secure API Routing → Dedicated Backend Environment → Customer-Controlled Infrastructure

Operational principle:
Field teams use the official App Store / Google Play applications. Enterprise deployment changes only the backend environment and governance controls — not day-to-day patrol execution.

Operational Continuity & User Experience

- Official Apple App Store and Google Play applications remain unchanged.
- Secure backend routing adapts to enterprise governance requirements without altering field workflows.
- No change to day-to-day patrol operations for field teams.
- Enterprise-grade infrastructure control is achieved without adoption friction.

Engagement Framework

Engagement Process

- Infrastructure alignment discussion
- Technical scoping
- Commercial structuring
- Deployment planning

Required Inputs

- Target environment (on-premise / private cloud / governed cloud)
- Estimated user, site, and device scale
- Identity integration requirements (SSO, roles, policy enforcement)
- Logging and monitoring stack (SIEM) and audit retention needs
- Data residency and compliance constraints

Risk Mitigation & Separation Model

- Single-tenant isolation aligned to enterprise governance requirements.
- No cross-client data exposure and no shared persistence layer.
- Independent lifecycle management for upgrades, maintenance, and oversight.
- Clear contractual boundaries supporting internal operational rights (no resale, redistribution, or sublicensing unless explicitly agreed).

Dedicated Enterprise Deployment

Trinity Guard® — regulated & large-scale operations