



TELAGENTO

ENTERPRISE AI ENGAGEMENT

Deployment & Data Boundary Options

Choose where the platform runs and what Telagento controls

Ready for your enterprise requirements.

Telagento gives enterprises a secure standard platform and configurable rails for customer-specific hosting, data handling, access, privacy, retention, integrations, and evidence.

For architecture, security, privacy, and procurement review

Capabilities and customer-specific options. Availability depends on the agreed architecture, providers, contracts, configuration, and implementation scope.

The deployment boundary is part of the product decision

Telagento starts with a managed standard environment. When an engagement needs a different location, provider set, network boundary, or responsibility model, the architecture can be tailored and documented before production use.

Standard managed environment Shared platform operations with organization-scoped application records, standard service providers, controlled access, deployment checks, and documented support boundaries.	Dedicated customer deployment A customer-specific platform environment with an agreed cloud or hosting boundary, provider set, data location, networking, credentials, operating model, and evidence package.
Approved partner-hosted option A scoped partner environment can be evaluated where a customer needs a specific hosting relationship. Services, locations, evidence, and shared responsibilities are confirmed for that deployment.	Customer-connected architecture Keep selected systems and sensitive records in customer or provider environments while Telagento exchanges only the identifiers and workflow data required for the use case.

Decide what enters the Telagento boundary

Provider systems retain their own data and evidence under their contracts. Telagento owns the configuration, data flows, records, logs, queues, exports, backups, and forwarding paths inside the agreed Telagento boundary.

Data area	Preferred boundary	Customer decision
Conversation content	Save only what the use case and agreed retention require	Channels, recording, transcription, retention, export, deletion, and analytics
Payment details	Provider-hosted collection; Telagento receives opaque references	Payment provider, workflow, receipts, and permitted metadata
Customer system records	Retrieve or update only through scoped integration permissions	Systems, objects, fields, actions, and credential ownership
Operational evidence	Store bounded audit and deployment records without unnecessary subject identifiers	Evidence recipients, review cadence, retention, and approvals
Backups	Encrypted backup stream with separately controlled recovery identity	Schedule, location, retention, recovery owners, and restore testing

Turn the architecture decision into an operating agreement

Data-flow map	Document sources, destinations, fields, storage, logs, analytics, transfers, exports, backups, and deletion paths.
Responsibility matrix	Assign customer, Telagento, hosting, and service-provider responsibilities without inheriting another party's assurances.
Control profile	Set access, secrets, retention, privacy workflow, monitoring, incident contacts, change control, and evidence requirements.

Launch evidence Record tests, approvals, configuration checks, smoke results, known exceptions, and the production boundary.

The result is a deployment that matches the opportunity, with responsibilities and evidence defined before launch.