

# FROM ARCHITECTURE REVIEW TO A SCALABLE, SECURE SAAS FOUNDATION

Theradocx is building a highly sensitive SaaS platform for psychotherapists, enabling secure audio recording of therapy sessions and AI-powered generation of reports.

The platform operates under strict regulatory requirements (GDPR, ISO 27001, AI Act) and ambitious growth targets of 1,000+ users.

## CHALLENGE

The team faced key questions:

- How can we further improve our architecture for healthcare-grade requirements?
- Can the platform scale cost-efficiently to thousands of therapists?
- Can we identify optimization opportunities in the current cloud infrastructure, cryptography, and operations?
- How prepared is the organisation for incidents, outages, and audits?

## APPROACH

Posedio conducted a structured software architecture review based on a deep-dive workshop with the Theradocx engineering team. The engagement focused on:

- Azure Cloud & infrastructure architecture
- Multi-tenant security model
- Cryptographic design and key management
- Scalability of databases and AI workloads
- CI/CD, observability, and operational excellence

Theradocx commissioned an independent review as part of their continuous security and compliance strategy, to validate their setup and receive concrete, actionable recommendations.

The review followed Posedio's Structured Software Architecture Review Guide, adapted to the maturity and scale of Theradocx. The review incorporated technical expertise from Azure and Terraform specialists and was further augmented by an independent peer review conducted by a senior software architect.

## SOLUTION

Posedio validated that Theradocx already had a strong architectural foundation and was following numerous industry best practices. Building on this, the review delivered clear improvement paths across four critical dimensions:

### 1 SECURITY & COMPLIANCE

In the area of security and compliance, the review validated the use of tenant-isolated encryption based on Azure Key Vault. It defined a clear roadmap for implementing a zero-trust architecture, improving network security, and a Web Application Firewall (WAF).

In addition, recommendations were provided for key rotation, session-based encryption keys, and enhanced identity management. The engagement also outlined concrete steps toward ISO 27001 readiness and the implementation of GDPR-aligned controls.

## 2 SCALABILITY & COST EFFICIENCY

To enhance scalability and cost efficiency, Posedio recommended consolidating databases into a unified, scalable data model. At the same time, strategies were developed to reduce cloud costs while preserving strict tenant isolation. The review further provided guidance on optimising AI workloads and improving transparency around infrastructure and processing costs.

## 3 RELIABILITY & OPERATIONS

To strengthen reliability and operations, the review introduced the systematic use of SLOs, SLIs, and structured SLA tracking. It also recommended establishing an incident management process as well as disaster recovery and backup strategies. Posedio also recommended implementing observability enhancements that utilize metrics, logs, and traces to ensure operational visibility without exposing sensitive information.

## 4 ENGINEERING ENABLEMENT

In the area of engineering enablement, the review focused on hardening CI/CD pipelines through immutable artefacts and automated rollback mechanisms. It established best practices for Infrastructure as Code using Terraform pipelines and defined a clear strategy for automated onboarding and environment provisioning to support future organisational growth.

# RESULTS

### SCALABILITY

Architecture validated for growth to 1,000+ tenants.

### RISK MITIGATION

Reduced operational and cost risks

### AUDIT-READINESS

Improved readiness for audits, incidents, and certifications

### DATA SECURITY

Clear security roadmap for sensitive healthcare data.

### ENGINEERING SUPPORT

Engineering team empowered with concrete, prioritised actions

Posedio confirmed that Theradocx is well-positioned to scale, with targeted improvements that significantly reduce risk while keeping development velocity high.

## Why It Matters

For healthcare and AI-driven SaaS platforms, trust, security, and scalability are non-negotiable.

This engagement helped Theradocx turn a solid technical foundation into a future-proof platform, ready for growth, regulation, and safe operations.

