

VON DER ARCHITEKTUR-ÜBERPRÜFUNG ZU EINER SKALIERBAREN, SICHEREN SAAS-BASIS

Theradocx entwickelt eine hochsensible SaaS-Plattform für Psychotherapeut:innen, die eine sichere Audioaufzeichnung von Therapiesitzungen sowie die KI-gestützte Erstellung von Berichten ermöglicht.

Die Plattform stand vor strengen regulatorischen Anforderungen (DSGVO, ISO 27001, AI Act) und ambitionierten Wachstumszielen von über 1.000 Nutzer:innen.

HERAUSFORDERUNG

Das Team stand vor zentralen Fragen:

- Wie können wir unsere Architektur für die Anforderungen im Gesundheitswesen weiter verbessern?
- Kann die Plattform kosteneffizient auf Tausende von Therapeut:innen skaliert werden?
- Können wir Optimierungspotenziale in der aktuellen Cloud-Infrastruktur, Kryptografie und dem Betrieb identifizieren?
- Wie gut ist der Service auf Incidents, Ausfälle und Audits vorbereitet?

ANSATZ

Posedio führte ein strukturiertes Software-Architektur-Review durch, basierend auf einem Deep-Dive-Workshop mit dem Engineering-Team von Theradocx.

Der Fokus lag auf:

- Azure-Cloud- und Infrastruktur-Architektur
- Multi-Tenant-Sicherheitsmodell
- Kryptografisches Design und Schlüsselmanagement
- Skalierbarkeit von Datenbanken und KI-Workloads
- CI/CD, Observability und Operational Excellence

Theradocx beauftragte eine unabhängige Überprüfung im Rahmen ihrer kontinuierlichen Sicherheits- und Compliance-Strategie, um das Setup zu validieren und konkrete, umsetzbare Empfehlungen zu erhalten.

Das Review folgte dem strukturierten Architecture Review Guide von Posedio, angepasst an die Anforderungen und Größe von Theradocx. Es wurde durch technische Expertise von Azure- und Terraform-Spezialist:innen und einem unabhängigen Peer-Review durch eine:n Senior Software Architekt:in unterstützt.

LÖSUNG

Posedio stellte fest, dass Theradocx bereits über eine starke architektonische Basis verfügt und zahlreiche Best Practices der Branche umsetzt. Darauf aufbauend lieferte das Review klare Verbesserungsvorschläge in vier kritischen Bereichen:

1 SICHERHEIT & COMPLIANCE

Der Einsatz von per-Tenant Verschlüsselung auf Basis von Azure Key Vault wurde validiert. Zudem wurde eine klare Roadmap für die Umsetzung einer Zero-Trust-Architektur, die Verbesserung der Netzwerksicherheit sowie den Einsatz einer Web Application Firewall (WAF) definiert.

Darüber hinaus wurden Empfehlungen zu Schlüsselrotation, sitzungsbasierten Verschlüsselung und verbessertem Identity-Management gegeben. Die Analyse skizzierte außerdem konkrete Schritte zur ISO-27001-Readiness sowie zur Implementierung DSGVO-konformer Kontrollen.

2 SKALIERBARKEIT & KOSTEN

Im Hinblick auf Skalierbarkeit und Kosteneffizienz empfahl Posedio die Konsolidierung von derzeit getrennten Datenbanken in ein einheitliches, skalierbares Datenbankmodell. Parallel dazu wurden Strategien entwickelt, um Cloud-Kosten zu senken und gleichzeitig eine strikte Tenant-Trennung zu gewährleisten. Zusätzlich lieferte das Review Leitlinien zur Optimierung von KI-Workloads sowie zur besseren Transparenz von Infrastrukturkosten.

3 RELIABILITY & BETRIEB

Zur Stärkung der Zuverlässigkeit und dem Betrieb wurde der systematische Einsatz von SLOs, SLIs und strukturiertem SLA-Tracking vorgestellt. Das Review enthielt Empfehlungen zum Aufbau eines Incident-Management-Prozesses sowie zu Disaster-Recovery- und Backup-Strategien. Zudem wurden Verbesserungen im Bereich Observability vorgeschlagen, die durch eine optimierte Nutzung von Metriken, Logs und Traces operative Einblicke ermöglichen, ohne sensible Informationen offenzulegen.

4 ENGINEERING ENABLEMENT

Im Bereich Engineering Enablement stand die Optimierung von CI/CD-Pipelines durch immutable Artefacts und automatisierte Rollback-Mechanismen im Fokus. Zudem wurden Best Practices für Infrastructure as Code mit Terraform-Pipelines überprüft und eine klare Strategie für automatisiertes Onboarding und Environment-Provisionierung definiert, um zukünftiges organisatorisches Wachstum zu gewährleisten.

ERGEBNISSE

RISIKOMINIMIERUNG

Reduzierte Risiken bei Betrieb und Kosten.

AUDIT-READINESS

Bessere Vorbereitung für Audits, Incidents und Zertifizierungen.

SKALIERBARKEIT

Die Architektur gewährleistet ein Wachstum auf über 1.000 Therapeut:innen.

DATENSICHERHEIT

Eine klare Sicherheits-Roadmap für sensible Gesundheitsdaten.

ENGINEERING SUPPORT

Unterstützung des Engineering-Teams durch konkrete, priorisierte Maßnahmen

Posedio bestätigte, dass Theradocx eine solide Grundlage für Skalierung besitzt. Die gezielten Verbesserungsvorschläge des Reviews reduzieren die Risiken signifikant und ermöglichen gleichzeitig eine hohe Entwicklungsgeschwindigkeit.

Warum das wichtig ist

Für Gesundheitswesen- und KI-getriebene SaaS-Plattformen sind Vertrauen, Sicherheit und Skalierbarkeit nicht verhandelbar. Diese Zusammenarbeit half Theradocx dabei, eine solide technische Basis in eine zukunftssichere Plattform zu verwandeln – bereit für Wachstum, Regulierung und einen sicheren Betrieb.

WEITERE
INFOS

