RISHABH SOFTWARE

Case Study

Security and Production Hardening for an AI-Built Analytics Platform

Application security hardening that turned a working AI-built app into a secure, production-ready spend intelligence platform



PROJECT OVERVIEW

A fast-growing B2B SaaS provider in the Middle East built a cloud-based spend intelligence platform using AI prompting and semi-technical teams. However, vibe coded app security had fallen behind. Controls, architecture discipline and operational ownership had not developed at the same pace as the app. Rishabh Software stepped in to strengthen AI application security while retaining working components and avoiding a costly rebuild.

Capability	Industry	Country
Application Engineering	B2B SaaS	Middle East

KEY FEATURES

The application already worked, with managed authentication, a modular backend and automated functional tests in place. Engineers focused on AI-generated code security, data protection, reliability and release validation gaps.

Hardened Database and Administrative Access

As part of application security hardening, the team strengthened database access controls, authentication and credential handling to reduce the risk of unauthorized access to customer data and administrative functions.

Assessed Asynchronous Processing and Recovery

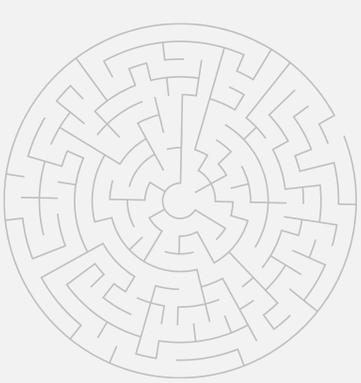
The team assessed how background jobs behave under failure, helping identify recovery considerations beyond normal operating conditions.

Strengthened Customer Isolation

The team added validation at customer boundaries to reduce reliance on application-level filters alone and strengthen separation between customer data.

Remediated Application Controls

Engineers fixed AI code security weaknesses, including unsafe rendering, exposed assets and other application-level flaws, to reduce unintended exposure of sensitive information.



CHALLENGES

- Customer isolation relied heavily on application-level filters, creating a risk of cross-customer data exposure if a filter failed or was bypassed.
- Database access and administrative controls had gaps that increased the risk of unauthorized access to customer data.
- Unsafe rendering, exposed assets and session gaps created potential paths for unintended exposure of sensitive information.
- External AI calls lacked consistent data-minimization controls, creating a risk that unnecessary customer information could be shared with external services.
- Analytical context supplied by the browser could introduce untrusted inputs into AI-assisted analysis.

SOLUTION

The targeted assessment confirmed that the existing architecture was sound. We retained the modular design, API, and background-worker split, and built the missing AI application security, validation, and release controls.

Trust-Boundary Enforcement

Engineers moved access checks and analytical logic into trusted server-side components, reducing dependence on information supplied by the browser for authorization and analytical decisions.

Preserved Architectural Boundaries

The existing API and background-worker separation was retained, keeping user-facing requests distinct from asynchronous processing and supporting clear separation of responsibilities.

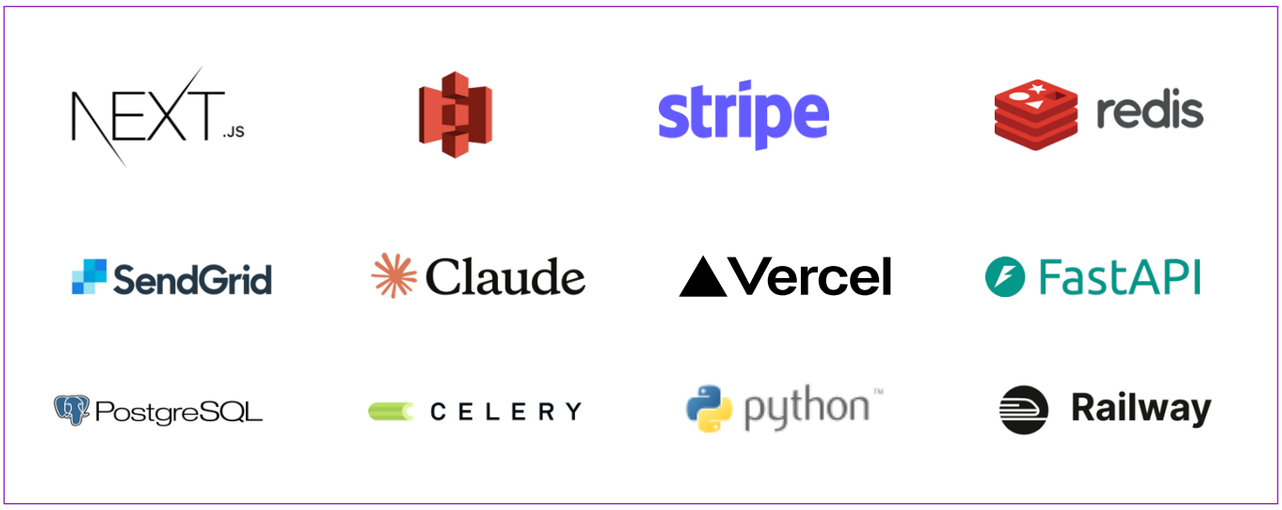
Governed Data and AI Flows

The team introduced data-minimization controls for external AI calls and made provider data-retention practices and processing geography explicit considerations for business decisions.

Improved Release Accountability

The team added security checks and broader workflow validation alongside the existing functional test suite. This gave the client clearer evidence for release decisions and a prioritized list of follow-up engineering work.

TECHNOLOGIES & TOOLS



Outcomes

426+
automated tests reviewed as part of production readiness

18
API modules reviewed

47
frontend improvement areas identified

ABOUT RISHABH SOFTWARE

As a Digital Engineering and Enterprise Transformation leader, we empower businesses to scale, innovate, and thrive in today's digital-first world through technology rooted in trust and transparency. We leverage emerging capabilities such as Cloud, Data Engineering & Analytics, AI, Automation and Application Engineering to drive digital transformation and unlock new opportunities. We have successfully served across 25+ countries, and we work towards customer delight as "WE CARE."

sales@rishabhsoft.com

+1-877-747-4224

Copyright © Rishabh Software Private Limited and its subsidiaries. All rights reserved.

RISHABH SOFTWARE