Fairvalue Insuretech (InsureCRM)

Production-Grade Monitoring & Security Observability Baseline for a Life-Insurance Renewal Platform

Client Overview

Customer: Fairvalue Insuretech Private Limited (InsureCRM)

Industry: Insurtech – Life Insurance Renewal & Policyholder Retention

Location / Region: India (AWS ap-south-1, Mumbai)

InsureCRM, an India-based insurtech focused on life insurance renewals and retention, operates a brownfield-refactored CRM platform on Amazon ECS (EC2) with RDS, ElastiCache, OpenSearch, and DocumentDB. Preparing for a production launch and 3–5x seasonal traffic growth, the company engaged Inadev to implement production-grade monitoring and security observability.

Engagement Overview

Engagement Type

Cloud Operations – Monitoring & Security Observability Implementation

Scope

CloudWatch/SNS monitoring baseline and security observability across a two-account (Non-Production/Production) AWS environment, with groundwork for a planned Q1 2026 Grafana rollout.

Technology Stack

Key Business Challenge

Ahead of a production launch expected to bring 3–5x renewal-season traffic spikes, InsureCRM needed a production-grade observability and security baseline across a multi-tier architecture spanning compute, caching, search, and document data stores

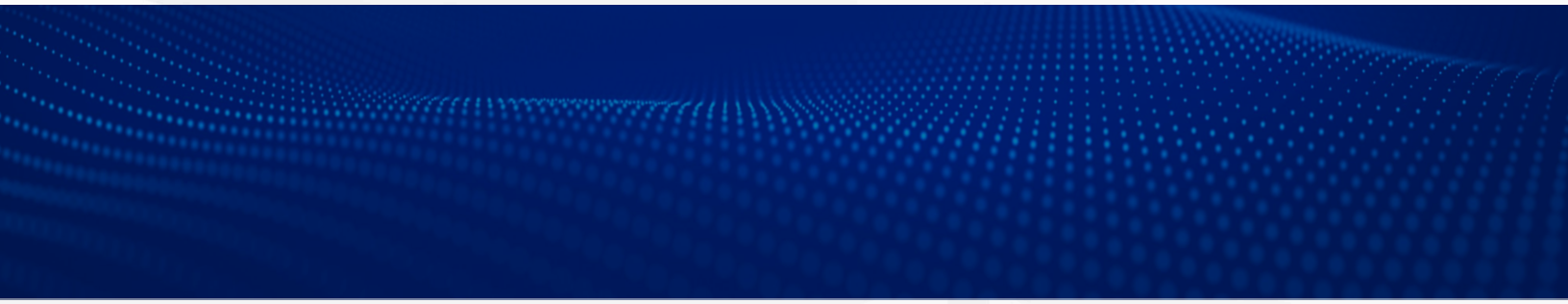
- **No consolidated alerting** across the ECS, RDS, ElastiCache, OpenSearch, and DocumentDB tiers, risking blind spots during traffic spikes.
- **Security observability** (threat detection, configuration compliance, vulnerability scanning) was not yet established ahead of go-live.
- **Renewal-season traffic was expected to spike 3–5x above baseline**, requiring alarm thresholds calibrated for seasonal load rather than steady-state averages.
- **Monitoring configuration needed to be reproducible and consistent** across the Non-Production and Production accounts.

Engagement Objectives

- **Establish a production-grade CloudWatch/SNS** observability baseline across all compute and data tiers.
- **Implement security observability** (Config, Inspector) to maintain a high compliance score.
- **Ensure alarm coverage supports detection** ahead of 3–5x renewal-season traffic spikes.
- **Lay Terraform-managed groundwork** for a planned Q1 2026 Grafana rollout.

Proposed Solution

Inadev implemented a CloudWatch- and SNS-centered observability baseline across InsureCRM's full application and data stack, paired with a security observability layer and Terraform-managed infrastructure as code, while preparing the environment for a planned move to Grafana in Q1 2026.



Core Monitoring Baseline

- 14 CloudWatch alarms configured across ECS, RDS, ElastiCache, OpenSearch, and DocumentDB, with SNS-based notification routing to the operations team.

Security Observability

- AWS Config configured with 3 compliance rules; Amazon Inspector enabled for ECS vulnerability scanning;

Data Protection & Access Observability

- KMS key usage and Secrets Manager access patterns monitored for audit and anomaly detection.

Infrastructure as Code & Future Readiness

- All monitoring and alerting configuration managed as Terraform in the Client's GitHub Enterprise repository, with Non-Production/Production parity, and a documented readiness plan for a Q1 2026 Grafana rollout.

Architecture Overview

InsureCRM's platform runs on **Amazon ECS (EC2 launch type)** behind an Application Load Balancer with AWS WAF and Shield for edge protection, in the ap-south-1 (Mumbai) region.

The data layer spans RDS, ElastiCache, OpenSearch, and DocumentDB, with DocumentDB configured for primary/secondary failover. 14 CloudWatch alarms span the compute and data tiers, routed through SNS to the operations team. Security observability is provided by AWS Config, and Amazon Inspector, layered across a two-account model (Non-Production, Production) with no shared VPCs.

All monitoring configuration is managed as Terraform IaC in the Client's GitHub Enterprise repository, with a documented target architecture for adding Grafana on top of this CloudWatch baseline in Q1 2026.

Security, Governance & Compliance

- **AWS Config for continuous resource configuration** monitoring and compliance enforcement.
- **Amazon Inspector performing ongoing vulnerability scanning** of ECS workloads.
- **KMS and Secrets Manager access patterns monitored** for audit and anomaly detection.
- **Two-account model** (Non-Production/Production) with no shared VPCs, enforced consistently via Terraform IaC.

Results & Key Performance Indicators

The engagement was measured against the following key performance indicators:

KPI	Baseline	Target	Actual
Platform Uptime	Not yet in production	**99.9%+** (Multi-AZ availability target)	**99.94%** (as of January 2026)
Priority-1 (P1) Incidents	N/A – pre-launch	Minimize critical incidents	Zero P1 incidents recorded

Business Impact

Reliability

99.94% uptime achieved as of January 2026, with zero P1 incidents recorded since go-live.

Scalability headroom

Alarm coverage and capacity validated for **3–5x** renewal-season traffic spikes without incident.

Operational efficiency

40–50% reduction in infrastructure management effort reported following the observability and IaC rollout.

Compliance posture

96% AWS Config compliance score maintained across the two-account environment.

Lessons Learned & Continuous Improvement

- **Calibrating alarm thresholds for 3–5x seasonal traffic spikes** — rather than steady-state averages — was essential to avoid both alert fatigue and missed incidents during renewal season.
- **Establishing the CloudWatch/SNS baseline and Terraform IaC discipline** first made the subsequent transition to a planned Grafana rollout (Q1 2026) far lower-risk.
- **Maintaining strict Non-Production/Production parity via Terraform** prevented configuration drift that could otherwise have masked issues before go-live.
- **Layering security observability** (Config, Inspector) before go-live rather than after allowed compliance issues to be resolved without production impact.