

Cutting operational noise ~30% by unifying observability on Elastic Cloud

Cathay moved off self-managed monitoring to Elastic Cloud and unified observability and security-relevant telemetry on one Elasticsearch data layer across 300+ applications and 100+ stations, cutting operational IT noise about 30% and giving infrastructure and security teams one shared view.

~30%

Reduction in operational IT noise

98%

Of applications moved off legacy infrastructure

300+

Mission-critical apps on one platform

100+

Stations worldwide on one data layer

The challenge

- ✗ Split teams on separate tools and mismatched formats; every incident opened with 'infra or security?'
- ✗ Self-managed on-prem meant constant patching, server lifecycle, and hardware maintenance
- ✗ Static logging could not keep pace with dynamic, containerized cloud workloads
- ✗ Monitored CPU and memory symptoms, not the booking or payment they were breaking

The solution

- ✓ One Elastic Cloud deployment on a single Elasticsearch data layer, one schema, one query language
- ✓ Observability and security-relevant telemetry ingested together across 300+ apps and 100+ stations
- ✓ Logs from many systems normalized to one consistent format on the way in
- ✓ Booking, payment, and inventory monitored as end-to-end business transactions

How it works

1. Ingest & normalize

All telemetry to one format on the way in

2. Unify the layer

One schema, one query language for every team

3. Watch the transaction

Booking, payment, inventory end to end

4. Read & decide

Context pre-assembled; analyst judges, escalates

Before

- 5–6 major incidents a day, MTTR 4+ hours, in firefighting mode
- Time lost reconciling data formats and debating ownership before investigating
- Watching infrastructure symptoms, surfaced after the problem hit

After

- One platform, one query language; the ownership debate is gone
- Booking, payment, and inventory watched as business transactions
- ~30% less operational noise; teams shifting to prevention

“By moving to Elastic Cloud we **cut about 30% of the operational noise** — the patching and hardware work that was never our real job. I would rather be told something is going wrong early than find out after the whole estate is affected, and now the team can act earlier and stay proactive.”

— Rajeev Nair, General Manager IT Infrastructure & Security, Cathay

Why it matters beyond one estate

The lesson travels past aviation: unify the data on one layer, let the platform assemble context, and free the team for the work that takes judgment. Cathay's roadmap collapses the line between observability and action, stays model-agnostic to avoid AI lock-in, and moves from signal to recommended action, with predictive capability spreading into customer-facing functions like dynamic fare rules.

[See how Elastic Observability monitors the business, not just the boxes or start a free trial →](#)