

CASE STUDY · NETWORK & STORAGE · AUSTRALIA AND THAILAND

30–40 TB a Day of Log Management for a Network and Storage Provider

A provider of network and storage services to enterprise customers in Australia and Thailand runs Secure60 as its log management platform, in continuous production, at 30–40 TB of ingest a day.

Network & telecommunications

Australia

Thailand

Log Management

SIEM

INGEST

30–40 TB/day

DEPLOYMENT

Sovereign SaaS, Australia and Thailand regions

IN SCOPE

Log Management, SIEM

OPERATING MODEL

Customer-operated, Secure60 experts on call

CURRENT SITUATION

High-volume telemetry across two jurisdictions

The provider's network estate produces a sustained 30–40 TB of logs a day across Australian and Thai operations. The incumbent tooling was priced per gigabyte ingested, so retention was being shortened to contain cost, and the Thai and Australian environments were monitored separately because moving data between the two raised residency questions under Thailand's PDPA.

The operations team needed one platform that could take the full volume, hold it long enough for investigation and customer reporting, and keep each country's data in that country.

WHAT SECURE60 DELIVERED

One platform across two sovereign regions

Secure60 was deployed as sovereign SaaS in both regions: the Australian estate lands in the Australian region and the Thai estate on Rackcorp infrastructure in Thailand. Both sit under one tenant, so the provider's team works in one console with one context across both countries while each country's data remains in that country.

Ingest runs through Secure60 collectors at the provider's edge, with parsing into the common information model so network, storage and access telemetry can be correlated. Every log stays active and searchable for the full retention window, so an investigation never waits on a restore from cold storage, and purpose-built compression keeps multi-month retention affordable at this volume. Detection content from the managed rule library runs on the same data.

COMPONENTS IN OPERATION

01 Continuous ingest at 30–40 TB/day

Collectors at the network edge in both countries, with parsing into the common information model on arrival.

02 Sovereign regions in Australia and Thailand

Each country's data resides in-country; one tenant and one console across both.

03 Full-window retention

Multi-month retention sized for investigation windows and customer reporting obligations, with every log active and searchable across the whole window.

04 Managed detection content

The Secure60 rule library runs on the ingested data, tuned with Secure60 experts.

BUSINESS IMPACT

Before and after

AREA	BEFORE SECURE60	AFTER SECURE60
Ingest volume	Capped by per-GB pricing; sources dropped to control cost	Full estate ingested, 30–40 TB/day sustained
Retention	Shortened to fit the budget	Multi-month retention, all of it searchable
Data residency	Two separate stacks, one per country	One tenant, data resident in each country
Investigation	Searches split across two tools, minutes at volume	Seconds, from one console, across both countries
Detection	Rules maintained in-house on partial data	Managed rule library on the full data set

OUTCOMES

Results

■ Cost per terabyte

Platform pricing rather than per-gigabyte metering removed the incentive to drop sources. The full estate is ingested at a lower cost per terabyte than the incumbent, with retention extended rather than cut.

■ Residency answered

Australian data resides in Australia and Thai data in Thailand under one platform, which is the documented answer to the PDPA residency question.

■ Operational cadence

Ingest and retention run on schedule without daily intervention from the operations team.

■ Reference for scale

The deployment is the reference point Secure60 uses for per-site ingest behaviour and retention at volume when scoping larger estates.

Scoping a High-Volume Estate

An architecture review covers ingest rate, retention and region placement for your environment.

Talk to us

www.secure60.io/contact/

Start for free

30 days, every feature switched on. No credit card.
portal.secure60.io

ONE PLATFORM, ONE CONTEXT

Log Management, SIEM, Vulnerability Management, Governance, AI Security and Digital Risk Protection on one platform and one context, with the experts and digital workers to run the parts you choose.

Log Management

SIEM

Vulnerability Management

Governance

AI Security

Digital Risk Protection