

CASE STUDY · PROFESSIONAL SERVICES · INDONESIA

AI-Supported Analytics for a Global Accounting Network's Indonesian Member Firm

The Indonesian member firm of one of the five largest accounting networks in the world uses Secure60 for a project that combines its security telemetry with analytic and AI-supported processing, on infrastructure in Indonesia.

Professional services

Indonesia

Log Management

AI Security

Governance

ORGANISATION

Member firm, top-five global accounting network

DEPLOYMENT

Sovereign SaaS, Indonesia region

IN SCOPE

Log Management, AI Security, Governance

WORKLOAD

Analytic and AI-supported processing on platform data

CURRENT SITUATION

An AI project that needed governed data

The firm was standing up a project that applies analytic and AI-supported processing to operational and security data. Two constraints shaped it: as a member of a global network the firm inherits group security policy, and as an Indonesian entity it operates under PP 71/2019, BSSN technical standards and the UU PDP with its 72-hour breach notification.

The data feeding the project had to stay in Indonesia, every access to it had to be recorded, and the AI components had to be governed in a way the firm could evidence to both the group and a regulator.

WHAT SECURE60 DELIVERED

The AI workload on the platform that already holds the data

The workload runs against the Secure60 platform in the Indonesia region, on the data the platform already holds, so no export to a separate analytics environment is required. Log Management holds the source data; the AI Security capability records prompts, responses, tool calls and model access in the same context, so the AI components are audited alongside everything else on the platform.

Governance maps the resulting evidence to the controls the group policy and the Indonesian instruments require, so the firm has one trail covering the data, the processing and the people who touched it. Secure60 experts worked with the firm's team on scoping and on the control mapping.

COMPONENTS IN OPERATION

01 Sovereign SaaS in Indonesia

The platform and the data it holds reside on Rackcorp infrastructure in-country.

02 AI activity in the audit trail

Model access, prompts, responses and tool calls are recorded in the same context as the security telemetry.

03 Control mapping

Evidence mapped to group policy and to the Indonesian requirements, maintained as the project evolves.

04 Expert scoping and review

Secure60 experts engaged for scoping, control mapping and periodic review.

BUSINESS IMPACT

Before and after

AREA	BEFORE SECURE60	AFTER SECURE60
Data location	Analytics would have required export to a separate environment	Processing runs where the data already resides, in Indonesia
AI governance	No record of model access or prompt activity	AI activity audited in the same trail as security events
Evidence for group and regulator	Assembled per request	Mapped to controls and maintained continuously
Platform scope	Log management only	Log management plus analytic and AI-supported workload

OUTCOMES

Results

One trail

Data, processing and access are recorded in one place, which is what a BSSN readiness check or a group audit examines.

AI adopted with a governance record

The AI components of the project carry an audit trail from day one rather than being retrofitted.

Residency held

The data and the processing remained in Indonesia for the duration of the project.

Platform beyond logs

The platform carries the firm's analytic and AI-supported workload alongside its security telemetry, on the same governed data, with scope extended as the project grows.

Governing an AI Workload on Operational Data

An environment review covers where the data resides, what the AI components touch, and what the group and the regulator will ask to see.

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