

CASE STUDY · PAYMENTS · AUSTRALIA

Regulated Payments Operations on One Platform in Australia

An Australian payment-gateway provider, regulated as a financial-services business and subject to card-scheme obligations, operates Secure60 in production across its transaction, network and corporate environments.

Payments & financial services

Australia

Log Management

SIEM

Vulnerability Management

Governance

ORGANISATION

Payment gateway, regulated financial services

DEPLOYMENT

Sovereign SaaS, Australia region

IN SCOPE

Log Management, SIEM, Vulnerability Management, Governance

OPERATING MODEL

Customer-operated, Secure60 experts on call

CURRENT SITUATION

Evidence assembled by hand from four tools

The provider ran separate tools for log collection, detection, vulnerability scanning and compliance tracking, each holding part of the evidence. When the regulator, a card scheme or an acquiring bank asked for evidence that a control operated, the answer was assembled by hand from all four, and the same requests recurred each audit cycle.

Transaction and cardholder-environment logs had to stay in Australia, and retention had to satisfy both the regulator's expectations and the card-scheme audit window.

WHAT SECURE60 DELIVERED

One context across logs, detection, vulnerabilities and controls

Secure60 replaced the four tools with one platform in the Australian region. Log Management holds the transaction, network and corporate telemetry; SIEM runs the managed rule library over it; Vulnerability Management tracks exposure across the same asset set; Governance maps the evidence from all three to the controls the regulator and the card schemes examine.

Because the capabilities share one context, a detection references the vulnerability state of the host it fired on, and the control evidence draws on the same records the analysts use. The provider's team operates the platform, with Secure60 experts engaged for tuning and audit preparation.

COMPONENTS IN OPERATION

01 Consolidated platform in Australia

Log Management, SIEM, Vulnerability Management and Governance on one tenant in the Australian region.

02 Retention to the audit window

Retention sized to the longer of the regulator's expectation and the card-scheme window, with every record active and searchable across it.

03 Managed detection content

The Secure60 rule library, tuned to the payments environment with Secure60 experts.

04 Continuous control evidence

Governance maps evidence to controls as it is produced, ready for the annual cycle.

BUSINESS IMPACT

Before and after

AREA	BEFORE SECURE60	AFTER SECURE60
Tooling	Four products with separate consoles and renewals	One platform and one console
Evidence for regulator and schemes	Assembled by hand each cycle	Mapped to controls continuously
Investigation	Logs in one tool, vulnerability state in another	One context: detection, host state and evidence together
Retention	Constrained by per-GB pricing	Sized to the audit window, all of it searchable
Data residency	Mixed, tool-dependent	Australian region throughout

OUTCOMES

Results

Audit preparation

Evidence is available when a request arrives, so preparation for each cycle is a review of existing records measured in days rather than a project measured in weeks.

Tooling spend

Four renewals became one, with licence and infrastructure spend reduced accordingly and a single contract to manage.

Faster investigation

Analysts see the host's vulnerability state next to the detection rather than switching tools.

Reference available

The customer is available as a reference on shortlisting, under NDA.

Regulated Payments on One Platform

A readiness call covers the regulator and scheme obligations in scope, retention, and which tools the platform replaces.

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