CASE STUDY · PAYMENTS · CENTRAL ASIA

In-Country Security Operations for a Payment Gateway in Central Asia

A payment gateway in Central Asia, connecting merchants to card schemes and domestic transfer rails, runs its security operations on Secure60 with the platform and its data on Rackcorp infrastructure inside the country.

Payments & financial services | Kyrgyzstan | Log Management | SIEM | Governance

ORGANISATION **Payment gateway, merchant acquiring and transfers**	DEPLOYMENT **Sovereign SaaS, in-country (2 datacentres)**
IN SCOPE **Log Management, SIEM, Governance**	OPERATING MODEL **Secure60-operated, digital workers on triage**

CURRENT SITUATION

Scheme obligations and a new cybersecurity law

The gateway handles card and account-transfer traffic for merchants, which brings card-scheme security obligations, and holds personal data registered under the Law on Personal Information (No. 58 of 2008). The Law on Cybersecurity (No. 121 of 2024) then brought critical information infrastructure under state coordination.

The scheme obligations and the two laws all require security operations to be running and evidenced, and the data was expected to stay in the country. The company's IT team was small and had no security operations function of its own.

WHAT SECURE60 DELIVERED

In-country platform operated by Secure60

Secure60 was deployed on Rackcorp infrastructure in-country, where Secure60 has two datacentres, so the platform and every log it holds stay within the jurisdiction. Log Management takes the gateway, network and corporate telemetry; SIEM runs the managed rule library over it, with payments-specific tuning; Governance maps the evidence to the scheme requirements and to both laws.

Secure60 runs the operation. Digital workers triage alerts around the clock and Secure60 experts handle escalation, investigation and the periodic evidence reviews, so the gateway's IT team keeps its focus on the payments platform.

COMPONENTS IN OPERATION

01 Sovereign in-country deployment

Platform and data on Rackcorp infrastructure in the country, across two datacentres.

02 Payments telemetry in one context

Gateway, network and corporate logs collected and parsed into the common information model.

03 24/7 triage and escalation

Digital workers on first-line triage, Secure60 experts on escalation and investigation.

04 Evidence against schemes and both laws

Governance maintains the control evidence the schemes and the State Agency for Personal Data Protection can examine.

BUSINESS IMPACT

Before and after

AREA	BEFORE SECURE60	AFTER SECURE60
Security operations	None dedicated; IT team on best effort	24/7 triage by digital workers, experts on escalation
Data location	Unresolved for any hosted option	In-country, two datacentres
Scheme and regulatory evidence	Prepared per request	Maintained continuously against schemes and both laws
Detection	No correlation across gateway, network and corporate logs	Managed rule library over one context
Time to triage	Next business day	Minutes, 24/7

OUTCOMES

Results

Coverage without hiring

A security operations function running from day one, without the gateway recruiting analysts.

Residency settled

The platform's location answers the residency question for the schemes and the regulator.

Obligations evidenced

Evidence for the scheme assessment and both laws is maintained rather than assembled.

IT team back on the product

Alert handling left the IT team's queue. First-line triage runs around the clock, and the team is called only when an escalation warrants it.

Secure60

Payments Security Operations in Central Asia

A readiness call covers the scheme obligations, both laws, the in-country footprint and how the operation is staffed.

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

ISO 27001:2022 certified
Independently audited · 16 sovereign SaaS regions

www.secure60.io
© 2026 Secure60