40° South Guard

Guard alongside Portkey

Different problems, different products

Version 1.1, May 2026

Why this comes up

Both products sit between an application and an AI model. They solve different problems.

Portkey is an AI gateway built for engineering reliability. It routes requests across more than 1,600 models, handles fallbacks, and gives teams observability over latency and spend.[1]

40° South Guard is compliance middleware built for Australian regulated industries. Every call generates a cryptographically signed attestation mapped to specific obligations under APRA CPS 234,[2] Privacy Act APP 8,[3] and the December 2026 ADM transparency reforms.[4]

Side by side

Capability	40° South Guard	Portkey
Primary purpose	Australian regulatory evidence per AI call.	LLM gateway: routing, fallbacks, cost control.
Australian PII	Native TFN, Medicare, ABN and BSB detection with checksum validation.	Available via integrated providers such as Microsoft Presidio and Guardrails AI.[5]
Regulatory mapping	CPS 234, Privacy Act APP 8 and ADM transparency mapped per call.	Generic guardrail violations. Not mapped to Australian regulations.
Per-call attestation	Cryptographically signed attestation (Cloud KMS ECDSA P-256) with regulatory mapping in the payload.	Tamper-evident audit logs across the platform. No per-call signed regulatory attestation.
Data residency	`australia-southeast1` (Sydney) by default. AU-sovereign by design.	Global SaaS control plane. Australian residency requires the Enterprise tier (private cloud or VPC). [6]
Multi-model routing	Single upstream per call. Routing is the customer's choice.	Routing across 1,600+ models with fallbacks and load balancing.

Could you run them together?

In principle, yes. Portkey upstream for routing economics, Guard for regulatory evidence. In practice, most regulated Australian businesses pick one proxy.

Pick Portkey if the problem is AI cost or model availability.

Pick Guard if the problem is proving to APRA, the OAIC, or your board that every AI call meets its compliance obligations.

Contact

hello@40south.au
40south.au

Sources

1. Portkey, "Enterprise-grade AI Gateway." portkey.ai/features/ai-gateway
2. APRA, "Prudential Standard CPS 234 Information Security" (July 2019), paragraph 15 covers third-party assessments. www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
3. OAIC, "Chapter 8: APP 8 Cross-border disclosure of personal information." www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information
4. Privacy and Other Legislation Amendment Act 2024 (Cth), Schedule 1, Part 15. ADM transparency obligations commence 10 December 2026. www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd016
5. Portkey Docs, "Use Portkey Guardrails for PII Protection." portkey.ai/docs/guides/use-cases/guardrail-pii-use-case
6. Portkey, "Enterprise-grade security and compliance." portkey.ai/features/security-compliance