# 40° South Guard

## Guard alongside Vanta

### Different problems, different products

Version 1.0 | May 2026

## Why this comes up

Vanta is a compliance automation platform that continuously monitors cloud infrastructure, code repositories, and HR systems to collect evidence for frameworks like SOC 2, ISO 27001, HIPAA, and PCI DSS. Many Australian businesses use it to prepare for security audits.

The question we hear is: "We already have Vanta managing our compliance posture. Why would we need Guard on top of that?"

The short answer: Vanta automates the collection of IT security evidence for periodic audits. Guard generates per-call compliance evidence for every AI inference your business makes, in real time, mapped to Australian obligations. They are complementary, not competing, but they address fundamentally different evidence problems.

## Side by side

| Capability | 40 South Guard | Vanta |
|---|---|---|
| Primary purpose | Per-call compliance evidence and attestation for all AI providers | Compliance automation for IT security frameworks (SOC 2, ISO 27001, HIPAA, PCI DSS) |
| Architecture | Inline API proxy. One API change, every AI provider covered. | Agent-based monitoring of cloud accounts, code repos, HR systems, and SaaS tools |
| Australian PII | Purpose-built detection with checksum validation for TFN, Medicare, ABN, and ACN | No AI-call PII detection. Monitors data handling policies across IT systems. |
| Regulatory mapping | Every call mapped to CPS 234, the AI Safety Standard, and the Privacy Act | SOC 2, ISO 27001, HIPAA, PCI DSS. No per-call mapping to APRA CPS 234, Privacy Act APP 8, or the December 2026 ADM transparency obligations. |

| | | |
|---|---|---|
| Per-call attestation | Cryptographically signed attestation per API call with tamper-evident 7-year audit trail | Aggregated evidence for periodic audits. No per-call signed attestation for AI calls. |
| AI-specific controls | Prompt injection detection, model inventory, shadow AI blocking, policy enforcement | AI vendor risk tracking if connected to cloud providers. No inference-time scanning or controls. |
| Data residency | Australian-hosted infrastructure. Data never leaves AU jurisdiction. | US-hosted SaaS. Australian data residency not guaranteed by default. |

## Could you run them together?

Yes, and there is a natural integration point. Vanta tracks your overall compliance posture across IT controls. Guard generates the AI-specific evidence that feeds into that posture.

A practical deployment would use Vanta to manage your SOC 2 or ISO 27001 programme, and Guard as the AI compliance layer that produces signed attestations, PII findings, and regulatory mappings that your Vanta programme can reference as evidence of AI governance controls.

Vanta answers: "Are our IT controls documented and auditable?" Guard answers: "Can we prove to APRA that every AI call met its compliance obligations at the time it was made?"

## Suggested next step

We can run a 30-minute proof of value showing Guard generating per-call compliance evidence that maps directly to CPS 234, the Privacy Act, and the AI Safety Standard. You will see how Guard's evidence vault complements the broader compliance picture Vanta already provides.

---

## Contact

hello@40south.au

40south.au



---

## Sources

1. APRA Prudential Standard CPS 234 Information Security, July 2019. www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
2. Vanta, "Vanta product overview." www.vanta.com
3. Australian Government, "Voluntary AI Safety Standard," August 2024. www.industry.gov.au/publications/voluntary-ai-safety-standard

4. 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
5. 40 South Guard technical documentation. 40south.au