40° South Guard

Guard alongside Microsoft Purview

Different problems, different products

Version 1.0 | May 2026

Why this comes up

Microsoft Purview is a natural part of the conversation for any organisation running M365 and Copilot. It handles data loss prevention, information protection, and compliance within the Microsoft ecosystem.

The question we hear is: "We already have Purview. Why would we need Guard as well?"

The short answer: Purview protects the Microsoft perimeter. Guard protects every AI call your organisation makes, regardless of provider. CPS 234 requires controls across all information assets, not only Microsoft information assets.

Side by side

Capability	40 South Guard	Microsoft Purview
Primary purpose	Per-call compliance evidence and attestation for all AI providers	Data loss prevention and compliance for the Microsoft ecosystem (M365, Copilot)
Architecture	Inline API proxy. One API change, every provider covered.	Embedded in Microsoft services. Covers M365, Copilot, and Azure OpenAI only.
Australian PII	Purpose-built detection with checksum validation for TFN, Medicare, ABN, and ACN	Australian PII detection available but limited to Microsoft-hosted services
Regulatory mapping	Every call mapped to CPS 234, the AI Safety Standard, and the Privacy Act	Compliance frameworks available but no per-call regulatory mapping to AU standards
Per-call attestation	Cryptographically signed attestation per API call with tamper-evident audit trail	Audit logs within Microsoft Compliance Centre. No per-call signed attestation.

AI-specific controls	Prompt injection detection, model inventory, shadow AI blocking across all providers	Copilot-specific controls. No visibility into non-Microsoft AI usage.
Data residency	Australian-hosted infrastructure. Data never leaves AU jurisdiction.	Depends on M365 tenant and Azure region configuration

Could you run them together?

Yes, and in most enterprise environments you would. Purview is the right tool for protecting sensitive data within your Microsoft ecosystem. Guard is the right tool for proving to a regulator that every AI call, across every provider, has active compliance controls.

They solve different problems. Purview answers: "Is our Microsoft data protected?" Guard answers: "Can we demonstrate to APRA that our AI governance controls are active on every call?"

Running both gives you Microsoft ecosystem DLP through Purview and provider-agnostic AI compliance evidence through Guard.

Suggested next step

We can run a 30-minute proof of value showing Guard alongside your existing Purview deployment. You will see per-call attestation, Australian PII detection, and regulatory mapping working across a non-Microsoft AI provider, demonstrating the coverage gap Guard fills.

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. Microsoft, "Microsoft Purview documentation." learn.microsoft.com/en-us/purview/
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