

Songlines Control® Architecture Brief

Published by: Cetus AI Pty Ltd | cetusai.com.au | hello@cetusai.com.au

Date: July 2026

Version: 2.1

Availability: Microsoft Azure Marketplace | MACC Eligible | Audit-Ready

Executive Summary

Songlines Control® is an enterprise-grade AI control plane designed specifically for Australian enterprise and government organisations. It sits between applications and AI models, providing a single pane of glass for real-time cost attribution, intelligent model routing, immutable audit trails, and sovereign-first governance.

By operating at the proxy layer rather than the application layer, Songlines Control® ensures that enterprise policies are enforced at the point of execution — before a single token reaches an AI model.

Songlines Control® is available for purchase directly on the Microsoft Azure Marketplace, making it the first Australian-built, sovereign-first AI governance product available through Microsoft's commercial channel. Enterprise customers with a Microsoft Azure Consumption Commitment (MACC) can apply their pre-committed Azure spend directly to Songlines subscriptions — reducing procurement friction and accelerating time to deployment.

Product Architecture Note: The Three Modes of Songlines Control®

To provide clarity on how the capabilities described in this brief are implemented, it is important to understand the deployment architecture of Songlines Control®. The platform operates as a single unified control plane with three distinct operating modes, reflecting an organisation's AI maturity journey:

Operating Mode	Primary Focus	Key Capabilities
Observe Mode	Visibility & Telemetry	Shadow AI Detection, Model Inventory, Usage Reporting, Cost Attribution
Enforce Mode	Inline Governance & Routing	Inline PII Redaction, Policy Enforcement, Immutable Audit Trail
Orchestrate Mode	Agentic Workflow Management	State Externalisation, Context Window Management, Intelligent Routing

The Architectural Gap in Enterprise AI

As AI scales across the enterprise, a critical infrastructure gap has emerged. Applications and autonomous agents are connecting directly to large language models (LLMs) via APIs, bypassing traditional governance and observability controls. This direct-connection model creates three significant risks:

Financial Risk: Token consumption scales unpredictably without real-time visibility or budget controls. AI spend behaves like a meter running 24 hours a day — and without a control layer, no one is watching.

Compliance Risk: Sensitive data including Personally Identifiable Information (PII) is transmitted to external models without automated redaction or auditability, creating exposure under the Privacy Act 1988, APRA CPS 234, and the APS AI Policy.

Operational Risk: Autonomous agents operate outside defined boundaries, creating "shadow AI" ecosystems that are invisible to security teams, compliance officers, and boards.

Songlines Control® addresses this gap by introducing a dedicated control layer that intercepts, evaluates, and governs every AI interaction — before it reaches any model.

Core Architecture

The Songlines Control® architecture is built on a high-performance proxy engine that intercepts API calls to AI models. It evaluates these calls against enterprise policies in real time — with 0ms added latency for budget alerts — and routes them accordingly.

1. Request Interception

Every AI request from enterprise applications, autonomous agents (including LangChain, AutoGen, and CrewAI workflows), or individual users is routed through the Songlines control layer instead of connecting directly to the model provider. No changes are required to calling application code.

2. Policy Evaluation

Enterprise policies are evaluated instantly at the point of execution. This includes checking real-time budget thresholds and spend caps; scanning prompts for sensitive data (PII) and applying automated redaction across 20+ entity types; verifying user and application access permissions against role-based access controls (RBAC); and evaluating data residency requirements to determine whether a request may leave Australian infrastructure.

3. Intelligent Routing

Tokens are optimised and the request is routed to the most appropriate model based on cost, latency, policy, or data residency requirements. Simple tasks are automatically routed to cheaper, faster models without requiring code changes in the calling application. Sensitive data is routed exclusively to approved sovereign or on-premise models, enforced at the proxy layer.

4. Governed Response

The response from the AI model is returned through the control layer, ensuring full observability and compliance logging end-to-end. Every prompt, model selection, and response is cryptographically signed and logged to an immutable audit trail.

Key Technical Capabilities

Capability	Category	Description
Real-Time MTD Spend Tracking	Economic Control	AI spend tracked in real time across all models, workflows, and users — with built-in model pricing tables and zero manual tagging.
Cost Attribution	Economic Control	Spend attributed by model, workflow, and individual user, with CSV export for finance reconciliation.
Intelligent Model Routing	Economic Control	Simple tasks are automatically routed to cheaper models (e.g., GPT-3.5) while complex tasks use frontier models (e.g., GPT-4o), reducing token spend.
PII Redaction	Data Sovereignty	Automated detection and redaction of 20+ PII entity types before prompts leave the enterprise boundary.
Sovereignty Enforcement	Data Sovereignty	Technical controls ensure regulated data only transits approved Australian infrastructure (e.g., Azure Australia East).
Immutable Audit Trail	Governance	Every AI interaction is cryptographically signed and logged, creating a tamper-proof record for regulatory review.
Shadow AI Detection	Governance	Unauthorised model usage is detected, flagged, and blocked at the network layer.

The Regulatory Imperative

Australian regulators are clear: AI governance must lead deployment, not lag it. The Songlines Control® architecture provides the exact capabilities required to meet the expectations of Australia's primary regulatory bodies.

ASIC REP 798 (Beware the Gap): In October 2024, ASIC warned that the pace of AI adoption was outrunning governance frameworks, specifically highlighting the lack of AI inventories, fragmented model registers, and the failure to assess risk through a consumer lens. Songlines Control® provides the centralised inventory and immutable audit trails that ASIC demands.

APRA AI Letter (April 2026): APRA called for a "step-change in AI-related risk management and governance" for all regulated entities, warning that "where entities fail to adequately identify, manage or control AI risks... we will take stronger supervisory action and, where appropriate, pursue enforcement."

ASIC Open Letter (May 2026): ASIC issued an open letter to all AFS licensees requiring board-level AI risk discussions to be documented. Songlines Control® is the purpose-built response to this regulatory trajectory — providing the governance infrastructure that regulators are now actively looking for.

Security Hardening (July 2026)

In July 2026, Songlines Control® underwent a comprehensive security review and hardening exercise. The following controls were implemented to strengthen the platform's security posture across all deployment models:

Control	Description
SSRF Prevention	Removed arbitrary upstream URL routing. Only 5 allowlisted AI providers (OpenAI, Anthropic, Azure OpenAI, Google Vertex AI, AWS Bedrock) are accepted as valid upstream targets.
Endpoint Authentication	All scheduled and internal endpoints now require valid session authentication. No unauthenticated internal routes remain.
Org Enumeration Prevention	Public-facing portal URLs use randomised organisation slugs instead of sequential numeric IDs, preventing enumeration attacks.
Session Duration	Default session lifetime reduced from 12 months to 30 days with mandatory re-authentication. Cookies are signed with HMAC-SHA256, scoped to the application domain, and set with HttpOnly, Secure, and SameSite=Lax attributes.
Header Allowlist	Gateway proxy forwards only 5 explicitly approved headers (content-type, authorization, accept, user-agent, x-request-id) to upstream providers. All other headers — including cookies, internal routing metadata, and custom headers — are stripped at the gateway layer.
Tenant Isolation	API keys and data queries enforce dual-scope filtering (userId + orgId) at the database layer, preventing cross-tenant data leakage even in multi-organisation deployments.

These controls were verified through internal penetration testing and code review. No critical vulnerabilities were identified. The hardening applies to all deployment models (SaaS, Private Cloud, and On-Premise).

Deployment Models

Songlines Control® is designed for deployment flexibility to meet varying security and sovereignty requirements:

Deployment	Description	Best For
Azure Marketplace SaaS	Fully managed, deployed via Microsoft Azure Marketplace. MACC-eligible. 30-day free trial available.	Enterprises seeking rapid deployment with minimal procurement friction
SaaS (Direct)	Fully managed multi-tenant environment. Operational within 10 minutes.	Organisations requiring rapid deployment without Azure Marketplace procurement
Private Cloud	Dedicated instance within the organisation's own cloud environment (Azure, AWS GovCloud, or equivalent).	Organisations with existing cloud commitments and data residency requirements
On-Premise / Air-Gapped	Fully sovereign deployment for highly classified environments, ensuring 100% Australian data residency by architecture.	Government agencies, defence, and critical infrastructure operators

Integration Ecosystem

Songlines Control® integrates seamlessly with existing enterprise AI stacks without requiring changes to calling application code:

AI Models: OpenAI GPT-4o, Anthropic Claude, Google Gemini, Azure OpenAI, AWS Bedrock, and local or sovereign models.

AI Frameworks: LangChain, AutoGen, CrewAI, and any framework that communicates via standard OpenAI-compatible API endpoints.

Microsoft Ecosystem: Azure OpenAI Service, Azure AI Foundry, Microsoft Entra ID (for identity and access management), and Microsoft Azure Marketplace (for procurement and MACC consumption).

Enterprise Systems: CRMs, vector databases, SIEM platforms, and custom internal APIs via webhook and log export.

Pricing and Plans

Songlines Control® is available on the Microsoft Azure Marketplace with a 30-day free trial. Two plans are available:

Product	Description	Price (AUD)
Songlines Control®	Visibility, cost attribution, policy enforcement (Observe + Enforce Modes), and immutable audit trail	\$9,995/month
Songlines Control® — Orchestrate Mode	Everything in Control, plus intelligent model routing across all providers to reduce token spend	\$19,995/month

Organisations can start with Control and upgrade to Orchestrate Mode as their AI governance maturity grows — with no changes required to their existing application code.

Conclusion

Songlines Control® transforms AI from an unpredictable, ungoverned capability into a managed, observable, and secure enterprise asset. By enforcing policy at the point of execution, it provides the confidence required to scale AI deployments across the organisation — and the audit trail required to demonstrate that confidence to regulators, boards, and customers.

As the first Australian-built AI governance platform available on the Microsoft Azure Marketplace, Songlines Control® combines the commercial accessibility of a global distribution channel with the sovereign-first architecture that Australian enterprise and government organisations require.

© 2026 Cetus AI Pty Ltd. All rights reserved. Songlines Control® is a registered trademark of Cetus AI Pty Ltd. All pricing in AUD and exclusive of GST. Pricing current as at July 2026 and subject to change. Contact hello@cetusai.com.au for enterprise and government pricing.
Version 2.1 — July 2026 | Cetus AI | cetusai.com.au