

Enterprise AI Systems Architecture – Portfolio Summary

Howard Pincham | AI Systems Architect

Purpose

This portfolio artifact summarizes how I design enterprise-grade AI systems that are secure, governable, operable, and financially sustainable. The focus is not on AI novelty, but on applying proven enterprise architecture principles to AI-enabled solutions.

Design Principles

AI is treated as a first-class enterprise capability, subject to the same rigor as other critical systems: centralized access control, enterprise identity, explicit network boundaries, operational observability, and predictable cost management.

Reference Architecture (Build 1)

Users access AI capabilities through a controlled ingress and centralized application/API layer. The application authenticates users via Microsoft Entra ID and accesses Azure OpenAI using managed identities. Supporting planes include identity and access management, network segmentation, observability, and cost guardrails.

Key Architectural Decisions

- AI access is mediated through a centralized API layer.
- Microsoft Entra ID is used for user and service authentication.
- Network ingress is controlled via standard enterprise patterns.
- Observability is centralized with privacy-aware logging.
- Cost guardrails enforce predictable AI spend.

What This Architecture Enables

Secure and auditable AI adoption, predictable cost behavior, scalable onboarding of new use cases, and alignment with enterprise governance and risk models.

Artifacts Available

- Architecture diagram (Build 1)
- Architecture Decision Records (ADR-001 through ADR-005)
- Implementation notes and operational lessons learned