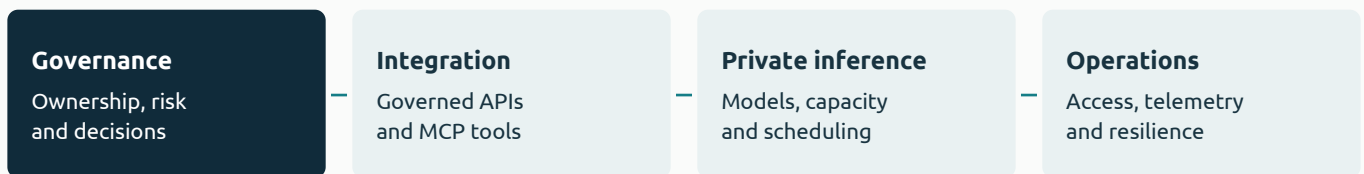


INDEPENDENT ARCHITECTURE CONCEPT

Secure AI and enterprise integration

Connecting AI to real business systems while retaining control of access, operational behaviour and service quality.

LOGICAL ARCHITECTURE



INTEGRATION AND AUTHORITY

Separate business capabilities from vendor-specific interfaces. Governed APIs and Model Context Protocol (MCP) expose approved tools and information. Identity, role-based access and scoped permissions apply to each operation.

PRIVATE INFERENCE AND CAPACITY

Hosting, information boundaries, GPU capacity, model selection and concurrency are architectural choices. Workload scheduling and admission control must complement application and network capacity planning.

SERVICE QUALITY AND VISIBILITY

Assess QoS/DSCP policy across the complete service path. Connect application behaviour with Kubernetes telemetry, Linux networking and eBPF-based visibility to identify contention, enforcement gaps and integration failures.

GOVERNANCE AND EVALUATION

Define ownership, change controls and recovery responsibilities. Measure latency, availability, recovery and access-control criteria using realistic workloads and failure scenarios. Distinguish read access from consequential actions.

Design principle

Control the whole service, then validate it. Packet marking alone does not guarantee delivery; AI output variability still requires constraints and validation.

Brett Moore combines nearly 30 years of enterprise integration, infrastructure, security and transformation experience with architecture governance and practical platform depth.

Independent reference design for discussion, prototyping and evaluation. It does not disclose a client implementation or claim validated production performance, safety, availability or commercial outcomes.