Component	Purpose	Security consideration
LLM core	Reasoning and language understanding	Token limits, prompt injection defense
Memory store	Short-term and long-term context retention	Data residency, encryption at rest
Planning module	Task decomposition and sequencing	Execution scope limits
Action APIs	Tool invocation and external system calls	Least-privilege access, rate limiting
Governance layer	Audit trails, approval workflows, compliance checks	Immutable logging, role-based controls