

Architecture & scope

Purpose

Connect internal memory and business tools through MCP. Choose approved external inference or local models according to your security requirements.

Available platform capabilities

Trust review, key policies, search traces and replay, conflict review, memory import/export and MCP onboarding.

Customer-specific scope

The following are proposed implementation scenarios, using example data. Access controls, connector availability and acceptance criteria are agreed per project.

Reference flow

Customer systems > source permissions and tool limits > memory/MCP hub > transmission policy > approved external model or local inference > referenced response.

Data boundary

Approved text and tool results can leave the customer environment when external inference is selected. Provider training exclusion and retention are separate contractual questions.

Extensions

Organization SSO/RBAC, document ACL synchronization, connector implementation, data-specific masking and comprehensive tool-call auditing require separate implementation and acceptance criteria.

Implementation candidates

Data MCP / PostgreSQL / MySQL

Read-only natural language analysis, with table and column allowlists, user permissions, query timeouts and result limits.

Code MCP / GitLab / GitHub

Repository navigation, change summaries and related incidents. Evaluate accuracy, review time and rework on the same tasks.

Operations MCP / EKS / CloudWatch

Investigate logs and metrics with diagnostic read access. Production changes use a separate approval process.

Knowledge MCP / documents / files

Draft answers within source permissions, with references and freshness checks. People review the original before use.

How to validate

Use the same tasks before and after implementation. Check permissions, references, accuracy, freshness, task completion and human review. Scenarios on the website use example data and do not call live systems.

Pilot, cost & operations

01 / Scope & pilot

Start with selected sources and a shared baseline. A four-week pilot is a planning target, subject to access and security readiness.

02 / Harden & extend

Validate permissions, source ACLs, customer-specific masking and operational procedures. Organizational SSO and RBAC are separate extensions.

03 / Expand & maintain

Expand only accepted sources and departments. Operate freshness, review, conflict and deletion policies, and continue measuring task quality.

Cost model

3-year TCO = initial implementation + 36 x monthly operations + change, training and exit costs

Assessment conditions

The proposal records workload assumptions, pricing date, currency, tax and support scope. No fixed savings or performance outcome is guaranteed.

Inquiry privacy

Consultation collects company, contact name and reply email; phone and message are optional. Retention is 180 days from receipt. Do not submit secrets, customer records or internal document originals.

Next step

Discuss selected sources, permission boundaries, workload and acceptance criteria at <https://anchormind.net/solutions/>.