What MCP Is

Model Context Protocol is a standard way for AI applications to connect with tools, data, and services. It matters because agents are moving from answering questions to using tools.

What Buyers Should Ask

1. What can the agent read?
2. What can the agent write?
3. What can the agent buy or trigger?
4. What data is exposed?
5. Who approves sensitive actions?
6. How are tool calls logged?
7. How are tool calls billed?
8. How can a tool be disabled quickly?

Red Flags

- No tool owner.
- No audit log.
- No approval gate.
- No tenant isolation.
- No clear permission model.
- No rollback path.
- Public exposure of private data.
- Vague "AI agent" pitch without operational controls.

What DID Sells

DID sells practical MCP readiness and hosting:

- Readable business data.
- Controlled MCP tools.
- Private hosting.
- Safety review.
- Approval gates.
- Usage metering.
- Support and monthly upkeep.

First Step

Start with an Agent Readiness Audit unless the buyer already has a documented tool inventory and auth model.