PRODUCT DATASHEET

Krista MCP Server

One governed entry point for every AI client. Vetted tools, role-based access, and a complete audit trail.

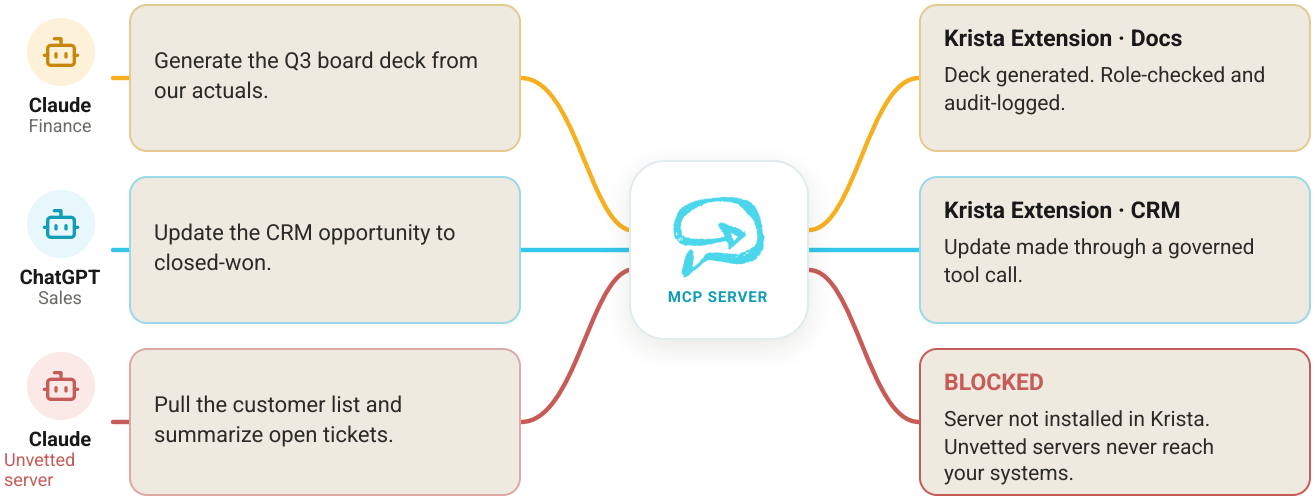
The Problem

AI clients like Claude and ChatGPT now act on real business systems. They query CRM records, send email, trigger workflows, and write files. The protocol arrived faster than the controls. The result is Shadow MCP: employees install MCP servers on personal machines, connect public AI clients to enterprise systems, and IT never knows it happened. No vetting. No role mapping. No record of what ran.

This is not theoretical. When enterprises open corporate access to AI clients, Security Operations Center, MCP, and DLP-related events are immediately exploding. Ungoverned MCP tools invoked enterprise systems with no controls in place. The risk grows with every new AI client. Without a governed MCP server and role-based policy, three questions stay unanswerable:

1. **Which MCP servers are running in your environment?**
2. **Who has access to which tools, and is that enforced?**
3. **Were any of those tools reviewed before they connected to your systems?**

Without a governed MCP server, every AI client is a blind spot:



Krista routes every tool call through role-based access and logs every invocation. Unvetted servers are blocked before they connect to any enterprise system.

Role-approved → Krista Extension · Governed tool call · Blocked: unvetted server

The Solution

IT deploys the Krista MCP Server once. Every AI client that needs tools connects to Krista. Every tool invocation runs through role-based access control. Every action is logged. If a model invokes tools in a runaway loop, rate limiting stops it before it reaches back-end systems.

On the tool side, Krista brings more than a standard MCP server. Any Krista extension registers as an MCP tool with no separate integration layer. Krista conversations expose multi-step orchestrated workflows as a single governed tool call. Any third-party MCP server IT approves installs inside Krista, under the same governance umbrella.

The Krista MCP Server makes Krista's enterprise capabilities available to any Gen AI model. Full governance, role-based access, and an audit trail included.

Why It Matters

Anthropic, OpenAI, Google, and Microsoft all support MCP. AI clients built on these models connect to CRM systems, financial platforms, payroll systems, and BI tools right now. Thousands of MCP servers are available. Most have no governance layer, no rate limiting, and no audit trail.

No executive is pulling AI access off everyone's desktop. The gap between capability and control is the problem the Krista MCP Server closes. Without a governed MCP server, Shadow MCP operates outside IT's view. With the Krista MCP Server, IT knows exactly which tools are active, which roles have access, and which capabilities passed review.

BEFORE

- × MCP servers installed on personal machines, invisible to IT
- × No role-based access. Any tool, any user
- × No audit trail when something goes wrong
- × SOC events with no explanation

AFTER

- ✓ One governed MCP server, deployed by IT
- ✓ Tools scoped to user role. Policy set once, applied everywhere
- ✓ Every invocation logged with user, tool, and timestamp
- ✓ Rate limiting stops runaway model behavior before it causes damage

Key Capabilities

Extensions as MCP tools

Register any Krista extension as an MCP tool. Claude, ChatGPT, and other MCP-compatible clients discover and invoke it directly. Tools with no role assigned stay inactive and invisible to every AI client.

IT-managed deployment

IT deploys the Krista MCP Server once. No per-machine configuration. No JSON editing on employee laptops. Approved tools are available across the workforce automatically from that point forward.

Role-based tool access

Each user's AI client sees only the tools their Krista role permits. A tool with no role assigned is inactive. Krista's existing permission model controls access. No separate MCP-specific configuration layer is required.

Third-party MCP server governance

IT installs any approved third-party MCP server inside Krista. AWS, Zoho, or any vetted server. Once installed, its tools fall under the same role-based access, rate limiting, and audit trail as every native Krista extension.

Rate limiting

Krista monitors tool invocation rate from every connected AI client. If a model invokes tools at abnormal speed, a send-email loop for example, Krista throttles it and stops it entirely. Back-end systems stay protected without manual intervention.

Conversations as tools

Register a Krista conversation as a single MCP tool. The AI client makes one call. Krista runs the full multi-step orchestration. This solves a documented MCP limitation: models get lost trying to complete complex tasks through five sequential low-level calls.

Audit trail and usage analytics

Every tool invocation is recorded: user, tool, action, and timestamp. Administrators review the log by user or by session. This is a current-release capability, not roadmap. When a ChatGPT session triggers an entity search, then a second entity search, then a send-mail, every step logs under the user who initiated it.

Who this is for

CISOs and security leaders

- Cannot ban MCP. Need a governed path instead
- Need Shadow MCP off personal machines and into a controlled server
- Require a full audit trail across every AI client tool invocation

IT and operations

- Want one place to approve tools, assign roles, and review logs
- Need to install vetted third-party MCP servers without losing governance
- Set policy once in Krista. It applies automatically across the workforce

AI client users

- Connect Claude or ChatGPT to Krista. Every approved tool is available immediately
- No manual server hunting. No per-machine configuration
- Request access to a new third-party server. Once IT approves it, it appears automatically

Enterprise architects

- Expose complex multi-step workflows as a single governed tool call
- Scale AI-driven automation without giving up auditability
- Every invocation logged. Compliance evidence is built in for regulated industries

Krista

NEXT STEP

Talk to Krista about deploying the MCP Server in your environment.

krista.ai