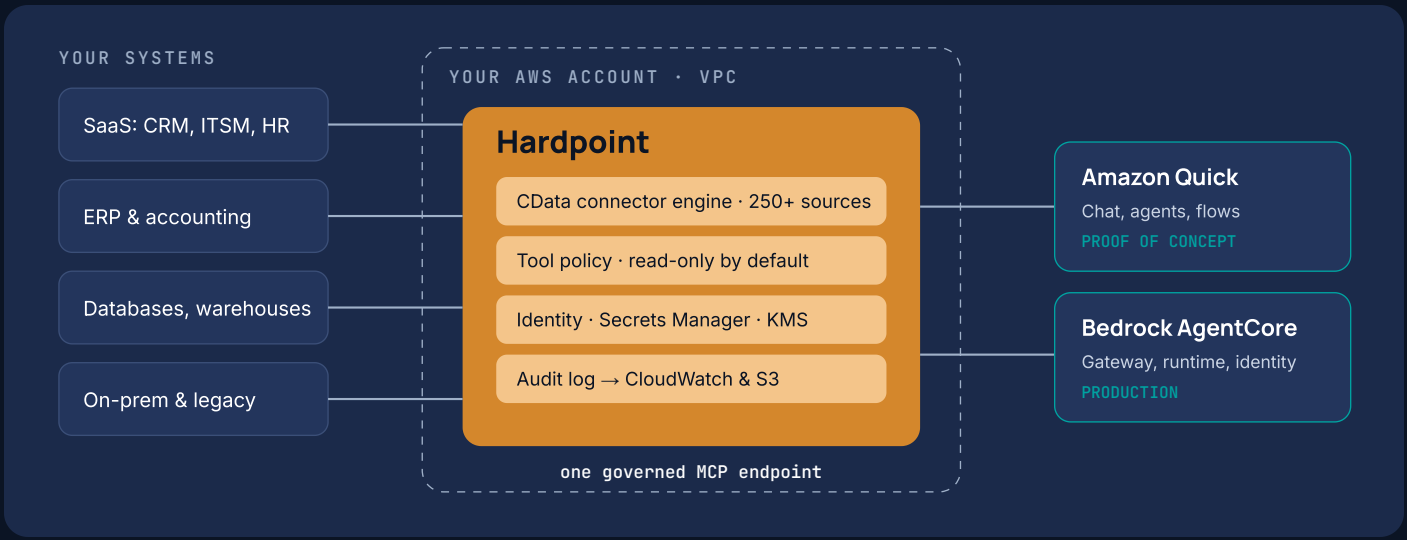
ARCHITECTURE

One governed MCP endpoint, in your AWS account.

Hardpoint sits between your systems of record and the AWS AI services that call them. It runs CData's connector engine behind a single Model Context Protocol endpoint, and applies tool policy, identity scoping, secret handling and audit logging on every call.



COMPONENTS

COMPONENT	WHAT IT DOES
Connector engine	CData connectors to 250+ SaaS, database, warehouse and legacy sources, exposed through one consistent SQL-style interface.
MCP endpoint	Publishes the approved tools to Amazon Quick (MCP connector) and to Amazon Bedrock AgentCore Gateway (MCP target).
Tool policy	Per-connector allow-list of tools. Read-only by default, with write access granted one tool at a time.
Identity scoping	Maps the calling user to source-system permissions, so results reflect what that user is entitled to see.
Secrets & keys	Source credentials in AWS Secrets Manager, encrypted with customer-managed AWS KMS keys.
Audit log	One record per call (caller, tool, source, timing, outcome) written to Amazon CloudWatch Logs and Amazon S3 in your account.

WHAT HAPPENS ON A CALL

1. **An agent asks.** A user's question in Amazon Quick, or an AgentCore agent step, selects a Hardpoint tool.
2. **Policy checks the tool.** Hardpoint confirms the tool is allowed for that connector and that caller.
3. **Identity is applied.** The request runs with the caller's entitlements, not a shared super-user.
4. **The source answers.** The CData connector queries the system of record live, using credentials from Secrets Manager.
5. **The call is logged.** Caller, tool, source and outcome are written to CloudWatch and S3.
6. **The agent responds.** Only the result set returns to the AWS AI service that asked.

SECURITY CONTROLS

What “hardened” means, control by control.

CONTROL	IMPLEMENTATION	EVIDENCE YOU KEEP
Network isolation	Runs in your VPC. No public endpoint required. Amazon Quick connects over VPC connectivity for MCP.	VPC, security group and endpoint configuration
Least privilege	Tool allow-list per connector, read-only by default, and scoped source-system service accounts.	Tool policy export
User-level access	The caller’s identity is carried through to source permissions.	Per-call identity in the audit log
Secret handling	Credentials live only in Secrets Manager with KMS encryption. They are never placed in prompts or config files.	Secrets Manager and KMS key policies
Audit	Every agent-to-data call is recorded, reads and writes alike.	CloudWatch Logs and S3 objects
Change control	Infrastructure is defined in CloudFormation, and connector and policy changes are versioned.	Stack history and change sets

WHERE IT PLUGS IN

- **Amazon Quick.** Registered as an MCP connector. Admins can enable or disable individual tools, and new tools sync as connectors change.
- **Amazon Bedrock AgentCore.** Registered as an MCP target behind AgentCore Gateway, alongside AgentCore Identity and Runtime.
- **Other MCP clients.** Any MCP-capable client you approve can use the same endpoint and the same policy.

BEFORE DEPLOYMENT

- **An AWS account** with a VPC, plus permission to deploy a CloudFormation stack.
- **Service accounts** in each source system, scoped to what agents should see.
- **Network path** to any on-premises sources, such as VPN or AWS Direct Connect.
- **A tool list:** which actions agents may take, per system.

WHO DOES WHAT

RESPONSIBILITY	YOU	EFS NETWORKS	CDATA	AWS
Connector library and updates			•	
Packaging, hardening, deployment		•		
Tool policy and access decisions	•	advises		
Source-system service accounts	•	assists		
Hardpoint support and upgrades		•	escalation	
Amazon Quick, AgentCore, underlying AWS services				•

Status. Hardpoint is in early access, and the AWS Marketplace listing is in preparation. This document describes the reference design. Each early-access deployment is scoped with the customer, including connectivity to on-premises sources and the exact tool set.