

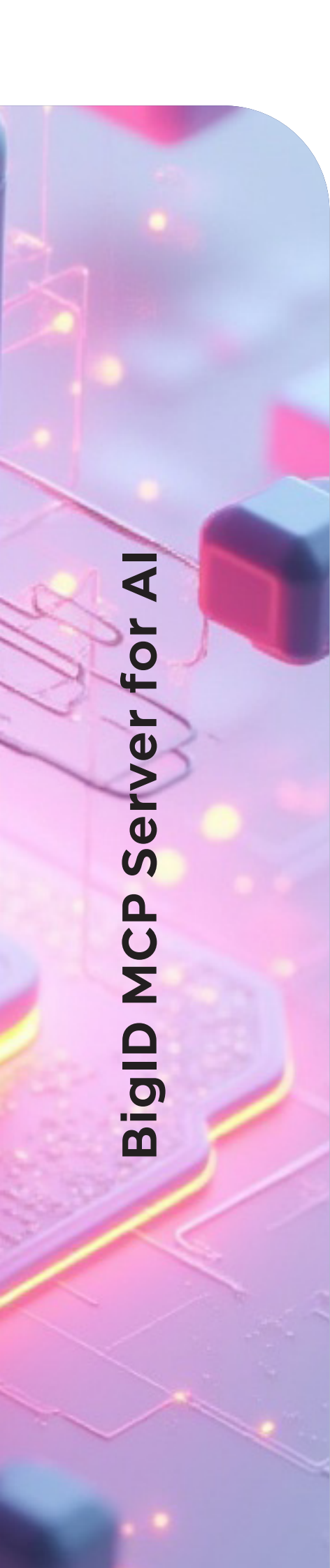


BigID MCP Server for AI

**Connect AI agents to
trusted enterprise data —
securely and intelligently.**

Unlock contextual insights,
governed access, and
actionable intelligence to
power safe, data-aware AI.



An abstract digital background featuring glowing yellow and orange lines, a blue cube, and a keyboard, suggesting a high-tech or AI theme.

BigID MCP Server for AI

BigID MCP Server for AI

BigID's MCP Server bridges enterprise data and AI, giving organizations a secure, governed, and AI-native way to deliver enterprise data context — not raw data — into AI workflows. It enables AI agents to securely access metadata, insights, and governance context across the broadest set of data sources: structured, unstructured, on-prem, cloud, business applications, and AI frameworks.

Built on BigID's discovery and classification foundation, the MCP Server provides a secure, standardized bridge that connects AI agents to enterprise metadata through token-based authentication and role-based access control (RBAC). The result: governed access, continuous visibility, and explainable AI grounded in trusted enterprise data context.

- **Connect securely:** Bridge AI agents and enterprise metadata through governed, token-based authentication.
- **Empower intelligence:** Deliver classification, sensitivity, lineage, and risk insights to AI applications.
- **Drive action:** Let AI agents query, summarize, and visualize data context securely.
- **Maintain control:** Extend governance, privacy, and compliance guardrails into AI workflows.

When AI Lacks Context

AI agents are only as effective as the context they can access — yet most enterprise data context is scattered across silos, systems, and security layers. Traditional AI tools operate without visibility into where data resides, how it's classified, or what risks it carries. The result: limited insights, unmanaged exposure, and unexplainable AI decisions.

A Secure Bridge Between AI and Enterprise Metadata

BigID's MCP Server gives organizations the missing link between enterprise metadata and AI innovation. By securely connecting AI agents to BigID's data intelligence, enterprises can provide AI with the context it needs to interpret and act on data responsibly — without ever exposing sensitive information.

Unlike uncontrolled integrations or manual pipelines, BigID provides continuous governance, granular authorization, and deep metadata context for every AI interaction.

Outcomes

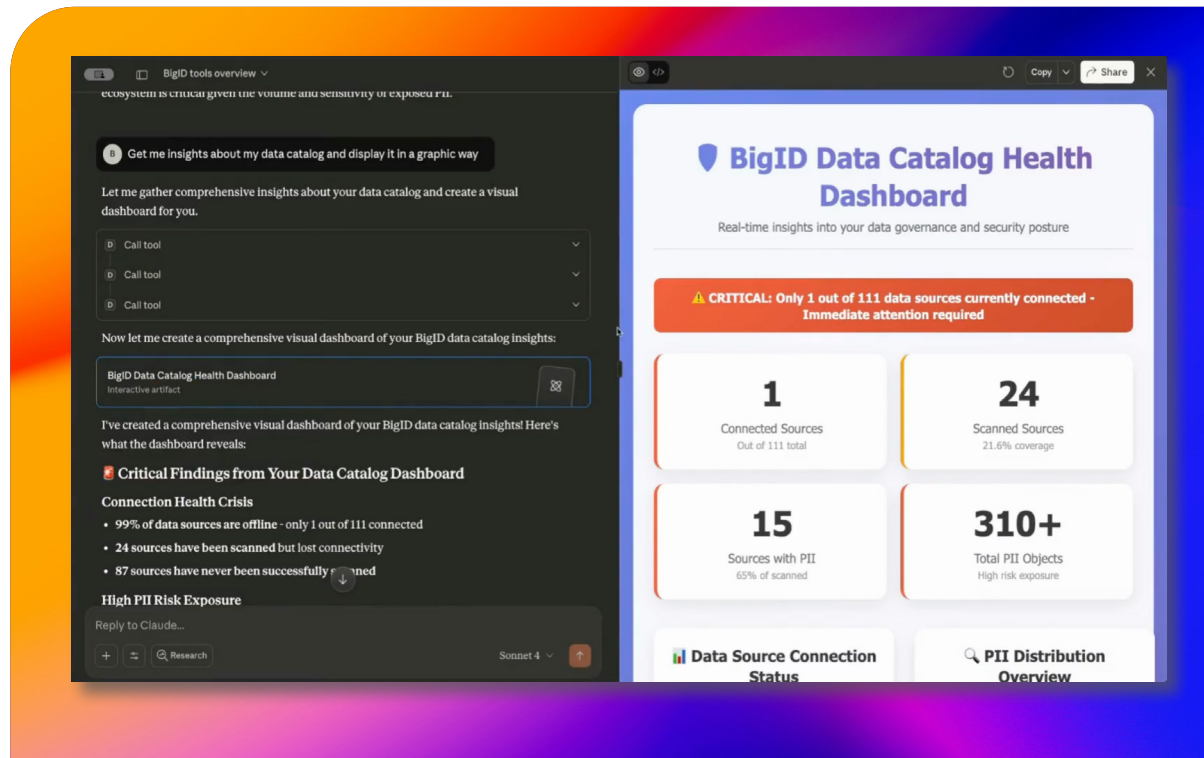
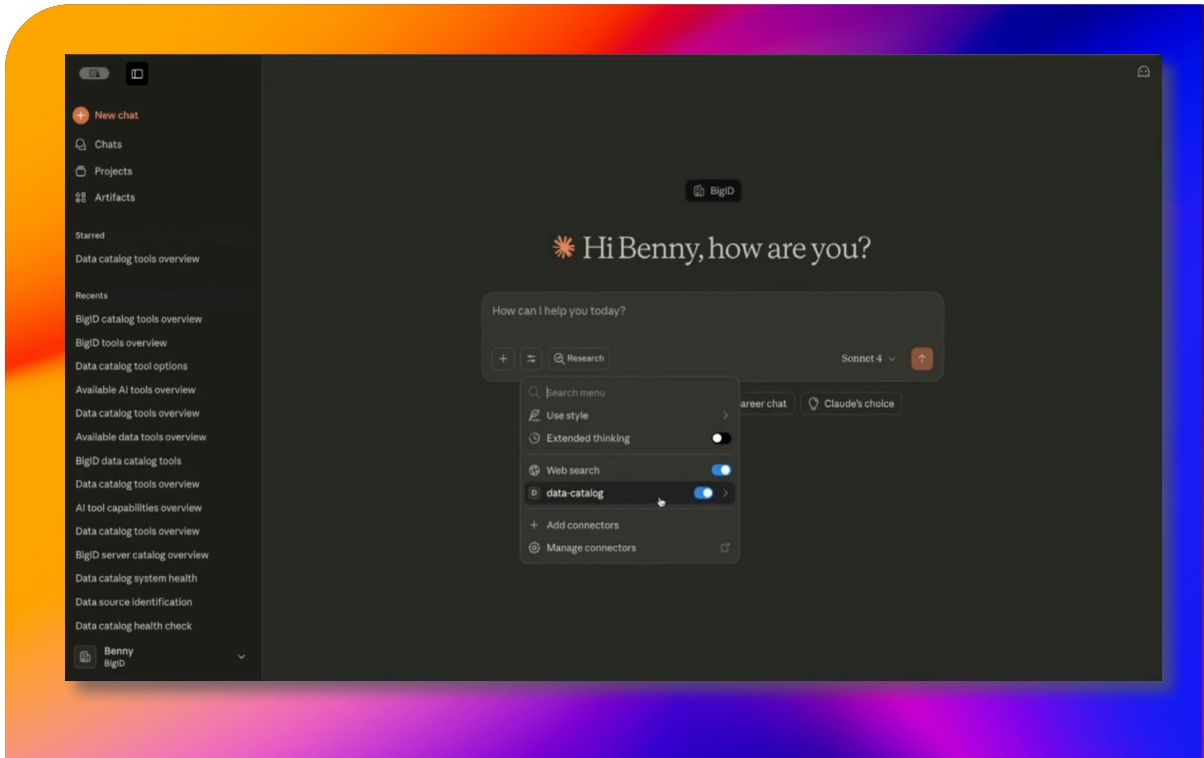


Secure AI Access – Governed, token-based authentication keeps enterprise metadata protected while AI agents query securely.

Contextual Intelligence – Enrich AI outputs with classification, sensitivity, and risk metadata for more explainable and accurate results.

Actionable Insights – Enable AI to summarize and visualize metadata instantly, turning context into decision-ready intelligence.

Continuous Governance – Extend access controls, auditability, and compliance enforcement into every AI-driven workflow.



Capabilities that Power BigID MCP Server for Data Catalog

AI-Native Metadata Connectivity

Connect AI agents and copilots directly to BigID's data catalog across structured, unstructured, and hybrid environments. The MCP Server exposes BigID's metadata APIs through a secure protocol that allows AI tools to query data context instantly — enabling continuous visibility into data sources, classifications, and relationships across the enterprise.

Governed Access Controls

Built with token-based authentication and RBAC authorization, the MCP Server ensures every AI interaction is secure and auditable. Access is scoped by policy, preventing agents from viewing unauthorized or sensitive metadata. Organizations maintain precise control over which datasets, APIs, and insights each AI tool can access.

Contextual Data Intelligence

Expose BigID's deep metadata — classification, sensitivity, lineage, and risk — to AI agents for more informed, explainable reasoning. Instead of raw data, agents receive governed intelligence that lets them understand relationships, interpret risk, and act with context.

Dynamic Insights & Visualization

Empower AI agents to go beyond static analysis — generating governed summaries, interactive dashboards, and visual overviews of enterprise data context. By leveraging BigID's APIs, agents can visualize data distribution, sensitivity trends, and risk hotspots — transforming metadata into actionable intelligence.

Continuous Governance & Auditability

Every AI-driven action through the MCP Server is logged and governed. Security, privacy, and compliance teams gain continuous oversight and traceability, ensuring all AI access aligns with enterprise data policies. Organizations get full visibility into who accessed what, when, and how — across all AI workflows.

AI-Ready Integration Framework

The MCP Server sets the foundation for future AI integrations — supporting any compliant AI agent or copilot, not just Claude. It provides a standardized, secure way to connect BigID's data intelligence with evolving AI ecosystems, enabling enterprises to scale safely as AI adoption grows.

About BigID

BigID helps organizations connect the dots across data & AI: for security, privacy, compliance, and AI data management. BigID enables customers to find, understand, manage, protect, and take action on high risk & high value data, wherever it lives.

Customers use BigID to reduce their AI & data risk, automate security and privacy controls, achieve compliance, and understand their data throughout their entire data landscape: from the cloud, on-prem, and everywhere in between.

Connect the Dots Across Data & AI

Security • Compliance • Privacy • AI Data Management

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.



Tools like BigID are the future.

Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.



Ryan O'Leary

Future of Trust: Battling Data Discovery Confusion