Model Context Protocol (MCP)

The foundation for secure, explainable, and governed AI across your enterprise.

Overview

AI safety and compliance require context — about where data comes from, how it's classified, and who can access it. Bedrock's Model Context Protocol (MCP) is an architecture that continuously feeds AI pipelines with metadata from the Bedrock Metadata Lake. MCP ensures models understand not just the data, but the risk, ownership, lineage, and policy constraints behind it. It creates a governed interface between data security and GenAI, enabling responsible AI at scale.

Why Model Context Protocol Matters

- **AI Governance:** Enforce policy boundaries and data residency restrictions for GenAI pipelines
- **Risk Control:** Prevent sensitive data from being ingested or exposed in AI-generated output
- **Auditability:** Maintain explainable lineage from prompt to output, including which data was used
- **Scalability:** Standardize secure model interactions across AI tools, LLMs, and internal agents

Bedrock Security MCP vs. Uncontrolled GenAI Architectures

CAPABILITY	BEDROCK SECURITY MCP	UNCONTROLLED GENAI PIPELINES
Data Context	Enriches models with classification, lineage, access, & sensitivity metadata	None — models ingest context indiscriminately
Prompt Guardrails	Dynamic filters based on user, policy, & data context	No per-user enforcement or policy control
Output Traceability	Maps responses to underlying data inputs	Opaque generation with no audit path
Integration Model	Standardized protocol across apps, agents, & orchestration layers	Custom, unscalable integrations
Governance Support	Supports Responsible AI initiatives & compliance audits	No lineage, metadata, or risk controls

About Bedrock Security: Bedrock Security, the ubiquitous data security and management company, accelerates enterprises' ability to harness data as a strategic asset while minimizing risk. Its industry-first metadata lake technology and AI-driven automation enable continuous visibility into data location, sensitivity, access and usage across distributed environments. Bedrock's platform continuously catalogs data, enabling security, governance and data teams to proactively identify risks, enforce policies and optimize data usage — without disrupting operations or driving up costs. Trusted by leading financial institutions, healthcare providers and Fortune 1000 companies, Bedrock Security empowers organizations to improve data security posture management (DSPM), confidently deliver Responsible AI initiatives, and manage the exponential data growth. Learn more at **https://bedrock.security.**

Learn More

REQUEST A DEMO