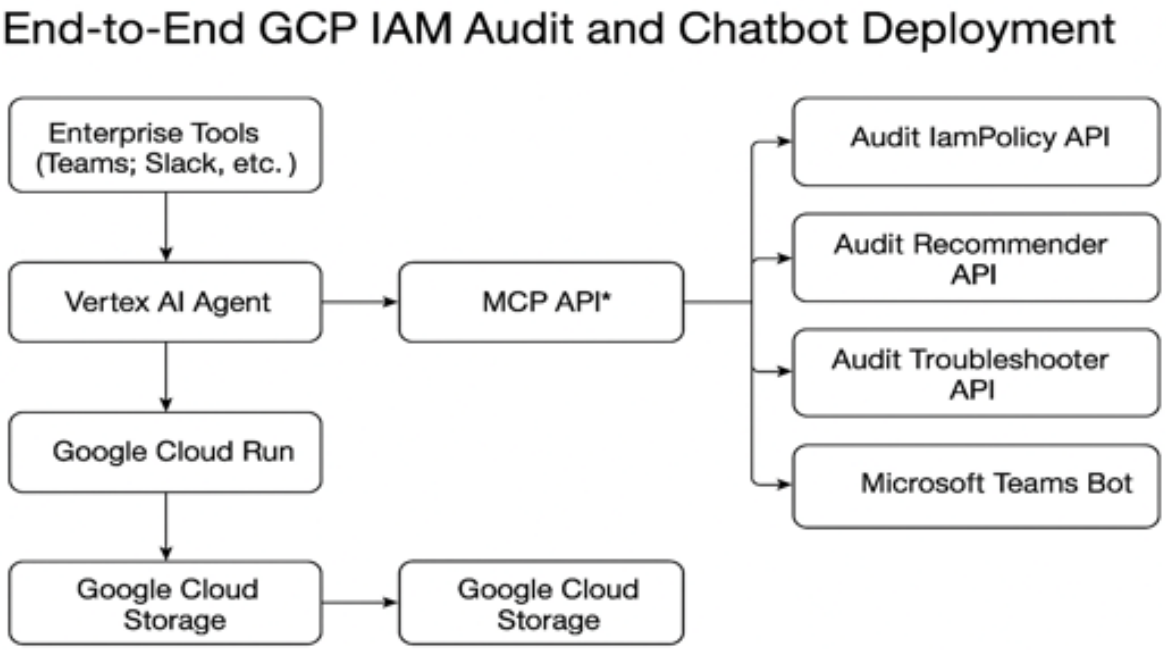
GCP IAM Audit Chatbot - Demo & Architecture



This architecture shows the complete GCP IAM Chatbot deployment pipeline.

Users interact via Microsoft Teams, Slack, or Web UI. Their queries are processed by a GenAI agent built with Vertex AI. The agent forwards IAM-related queries to a backend MCP Python service deployed on Cloud Run. This service uses IAM Recommender, Policy Analyzer, and the Policy Troubleshooter APIs.

The audit pipeline runs automatically or manually to detect risky IAM permissions, unused roles, and policy drift. Logs are sent to GCS, and alerts are routed to Splunk and Microsoft Teams.

Rego policies enforced through Terraform ensure that deny policies, naming rules, and service account key protections are in place. CI/CD pipelines run OPA tests, behavior tests, and allow approvals for prod deployments.

This architecture brings together audit, security enforcement, alerting, and conversational AI in one integrated GCP-native solution.