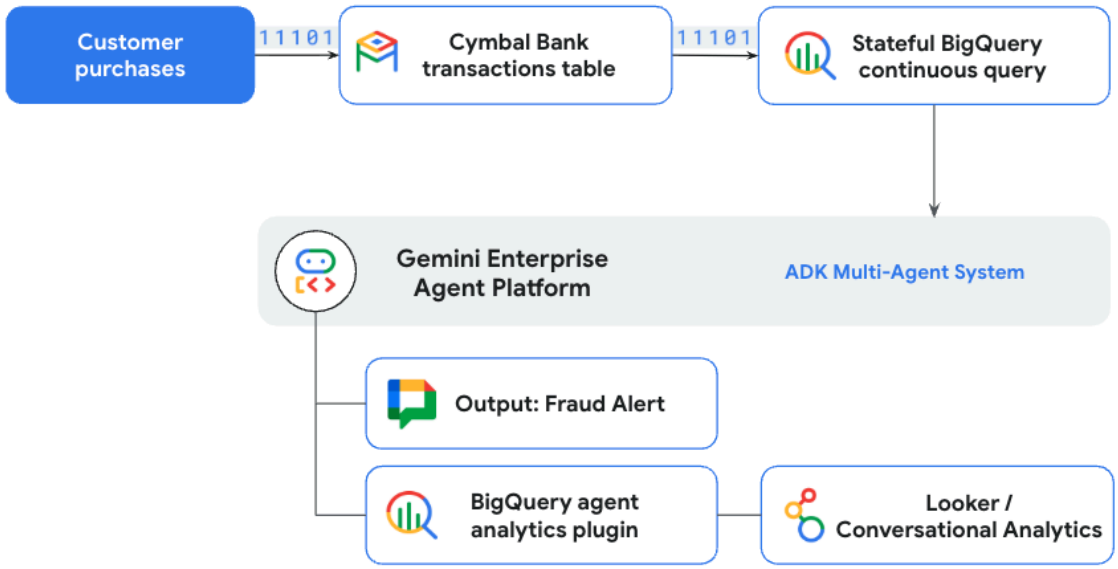
The Agentic Data Cloud Demo: Near Real-Time Fraud Prevention

Overview

Google Cloud's Agentic Data Cloud evolves enterprise data from a static repository into a dynamic System of Action. As a practical demonstration, Cymbal Bank leverages a unified, AI-native stack to identify and remediate fraudulent transactions using only SQL and natural language, bridging the gap between operational data and autonomous reasoning. This AI-powered system, built on Google's Agent Developer Kit (ADK), orchestrates four specialized autonomous agents to investigate suspicious transactions in near real-time. By analyzing transaction history, merchant reputation, and receipt images in parallel and sequence, these agents automatically distinguish real fraud from false positives, significantly reducing analyst workload.

The Investigation Pipeline: From Data to Action



The journey from a customer purchase to a resolved threat is a seamless loop of ingestion, analysis, and automated reasoning:

1. **Transactional Ingestion**: Purchases are written to an AlloyDB database and replicated in real-time to BigQuery via Datastream.
2. **High-Speed Filtering:** A BigQuery continuous query acts as the 'high-speed first filter.' Leveraging new stateful stream processing capabilities, it performs complex windowed aggregations with 2-minute tumbling windows to calculate high level fraud risk signals.
3. **Autonomous Investigation**: Potential threats trigger a multi-agent system built with the Agent Developer Kit (ADK) running on the Gemini Enterprise Agent Platform.
4. **Intelligent Response**: Confirmed fraud results in a rich, AI-generated alert sent to the fraud investigation team via Google Chat for immediate action.

The Multi-Agent Investigation Team

Four specialized AI agents work in concert to perform deep investigations, reducing manual workload by automatically distinguishing real fraud from false positives:

Agent	Responsibility & Key Actions
Investigation Agent	**Behavioral Analysis**: Analyzes the customer's previous 7-day transaction history for complex patterns like "impossible travel" or velocity signals that a simple rule would miss.
Google Search Agent	**Merchant Verification**: Vets merchant reputation using the Google Search API to identify external risk factors, such as known scams (e.g., "Coin Doubler Solutions") or recent data breaches.
Multimodal Agent	**Visual Audit**: Performs OCR on purchase receipts to find red flags like mismatched business names, infeasible fee amounts, or fictional contact information.
Decision Agent	**Orchestration & Verdict**: Synthesizes findings from all agents to make a final Level 2 analyst decision (False Positive vs. Escalation Needed).

These agents are developed as 'hybrid agents,' meaning they interleave deterministic code (like SQL tools) with generative reasoning. This provides the precise control needed to meet enterprise-level quality and safety standards in financial services.

Technical Stack

- **Infrastructure:** Real-time transactional data is written to AlloyDB for PostgreSQL and replicated in real-time to BigQuery via Datastream. BigQuery continuous queries act as the "high-speed first filter," leveraging stateful tumbling windows to perform complex risk analysis as transactions arrive.
- **Agentic Development Framework:** The Agent Developer Kit (ADK) is used to build "hybrid agents" that interleave deterministic code, such as SQL lookups, with generative reasoning to meet enterprise-level safety standards.
- **AI Platform:** The Gemini Enterprise Agent Platform (hosted on Gemini Enterprise Agent Platform) provides the enterprise-grade hosting and operations required for the multi-agent system.
- **Engagement & Observability:** Google Chat delivers real-time notifications populated with rich, AI-generated investigative summaries for human remediation. Simultaneously, Looker and Conversational Analytics enable stakeholders to query performance metrics and token costs in plain natural language.

Architecture Benefits

✓ **Responsive**: Collapses the time between detection and resolution by stopping fraud in its tracks in near real-time, shifting the enterprise from reactive batch monitoring to proactive, agent-scale execution.

✓ **High-Performance and Intelligent**: Accelerates deep investigations through parallel execution, allowing the system to simultaneously perform historical BigQuery lookups and Google Search merchant reputation checks.

✓ **Integrated & Multimodal**: Automates the audit of unstructured data using Gemini to identify receipt anomalies—such as mismatched merchant names, infeasible fee amounts, or fictional contact info—that traditional rules-based systems often miss.

✓ **Precision-Driven**: Leverages stateful stream processing and 2-minute tumbling windows to analyze behavioral velocity, minimizing false positives by grounding AI reasoning in historical context and live data.

✓ **Enterprise-Grade**: Built on the Gemini Enterprise Agent Platform to deliver a scalable environment with unified observability, logging, and zero-trust security controls, including temporary signed URLs for artifact protection.

✓ **Fully Auditable**: Captures a 100% transparent audit trail of every reasoning step and tool call via the ADK Agent Analytics plugin, providing the grounded data necessary for compliance and continuous retraining

✓ **Cost Efficient**: The system leverages BigQuery as a low-cost, high-speed filter to trigger agents only when a risk threshold is met. This avoids overwhelming LLM context windows with raw data and massively reduces token consumption

---