Google Cloud

Webinar | AMER & EMEA

Community TechTalks

August 13, 2025

Secure Agent MCP Tool Governance using Apigee

https://goo.gle/Recordings

Apigee

Housekeeping Notes

- 🎥 This session is being recorded so you can revisit it on demand later.
- 🔇 Please remain muted during the presentation
- 💬 Feel free to share questions anytime through the chat.
- 🎤 We'll open the floor for discussion and live questions at the end of the session.
- 👍 Use reactions and emojis to engage throughout the presentation.
- 🤝 Please help us keep the space respectful and welcoming for everyone.

Speaker



Tarun Abraham

Customer Engineer, Apigee



Secure Agent MCP Tool Governance using Apigee

Agenda

01 Agent Tool Governance MCP Blindspot

02 Framework for Safe Tool Use

03 Apigee Security Capabilities

04 Scaling Secure Agent Tool Ecosystems

The Single Endpoint Blindspot

How traditional API architectures fail to secure Agentic tool transactions.



The API Gateway Illusion

Traditional gateways see the single POST /mcp connection, but completely miss the invisible tool context inside.



The MCP Black Box

Because all traffic funnels through one multiplexed endpoint, legacy security cannot see which specific AI tool is being called.



Flying Blind on GenAI

If you can't see the tool, you can't govern it. You lose all ability to control individual tool usage and manage risk.

The Cost of the Status Quo



Invisible Data Exfiltration

Without payload visibility, malicious agent actions and data exfiltration blend perfectly into normal traffic.



Broken Access Controls

You cannot rate-limit, audit, or policy-enforce individual AI tools when they are all masked behind a single gateway endpoint.



Need for Deep Inspection

Basic routing isn't enough. Safely scaling Agent interactions requires real-time payload inspection to parse specific tool requests.

The Dual-Privilege Framework

Safe AI requires **dual-privilege control**: You must independently govern what the AI agent can execute, and what the human user is authorized to request.

LEVEL 1

Agent Control

Restricts the agent's absolute capabilities (The Can).

Example: *A public Storefront Agent is strictly blocked from accessing internal operations databases.*

LEVEL 2

User Control

Enforces human access rights and authorization (The Should).

Example: *A standard store clerk cannot use an internal agent to execute an executive-level inventory override.*

Eliminate the Blindspot with ParsePayload

PRIMARY OUTCOME

Expose the Black Box

Apigee transforms the generic **POST /mcp** connection into readable data, restoring the visibility that traditional gateways lack.

Inspect in Real-Time

Use the ParsePayload policy to extract the specific tool name and context hidden within the agent's request.

Enforce Proactive Security

Immediately block unauthorized tools or apply granular routing rules before the request ever reaches your backend.

Unified Governance with Apigee API Products

PRIMARY OUTCOME

Group Tools with Payload Operations

Bundle specific agent tools within **API Products** to transform them from a single endpoint into uniquely governable assets.

Authorize Agents (Level 1)

Explicitly define which tools an AI agent can access. Apply strict rate limits and quotas to these groups to prevent agent abuse.

Govern Human Users (Level 2)

Attach custom attributes (like OAuth scopes) to individual tools, verifying the human user is authorized to execute the specific action.

Scaling Secure AI Ecosystems

Enterprise-grade visibility, dual-privilege governance, and standardized security for agentic workflows.

VISIBILITY

No More Blind Spots

Regain complete visibility into MCP traffic, turning a black box into actionable, parsable data.

GOVERNANCE

Dual-Privilege Control

Safely enforce what your AI agents are capable of and what your human users are authorized to do.

SCALE

Future-Proof Scale

Standardize your AI Agent tool governance across the enterprise using Apigee's proven API management layer.



Demo

Q&A

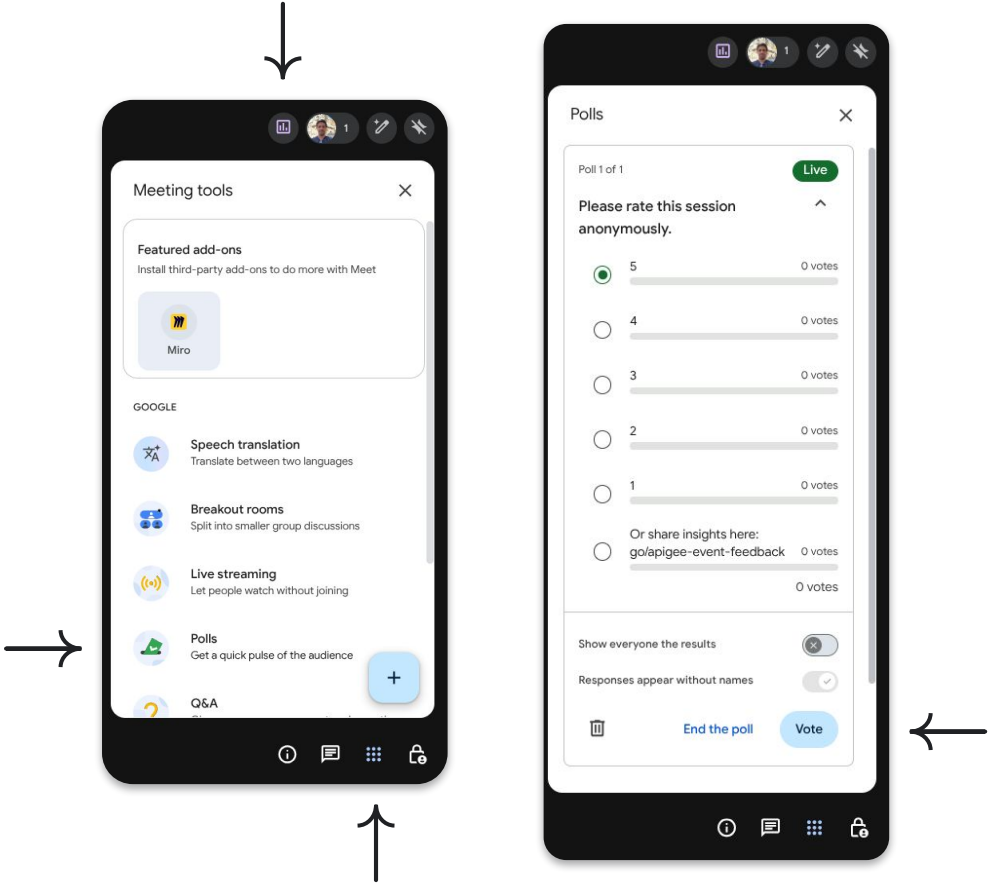


Please share your feedback!

Help us make our sessions even better!

Please provide your **anonymous feedback** by rating this session.





Catch up!

New Community Content

- Troubleshooting API Proxy Performance Issues in Apigee Hybrid

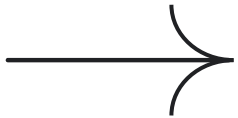
Upcoming Events

- **Sept 1st** | Apigee AI Horizon London
- **Sept 10** | Apigee Community TechTalk en français avec Christophe Lalevée
- **Oct 13** | Apigee AI Horizon Paris

Google Cloud

Community





Thank You

Apigee