

Community

TechTalks



May 7, 2026

Productizing AI: Transforming APIs into Governed Agentic Tools



<https://goo.gle/Recordings>

Agenda



Intro



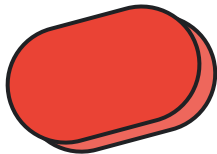
Productizing AI



Demo



Discussion / Q&A



Speaker



**Christophe
Lalevée**

BAP Solution Specialist



Productizing AI:
Transforming APIs into
Governed Agentic Tools

AI agents plan, reason, and execute tasks for users

Four key components



Model(s)

Used to reason over goals, determine the plan and generate a response.



Tools

Fetch data, perform actions or transactions by calling other APIs or services.



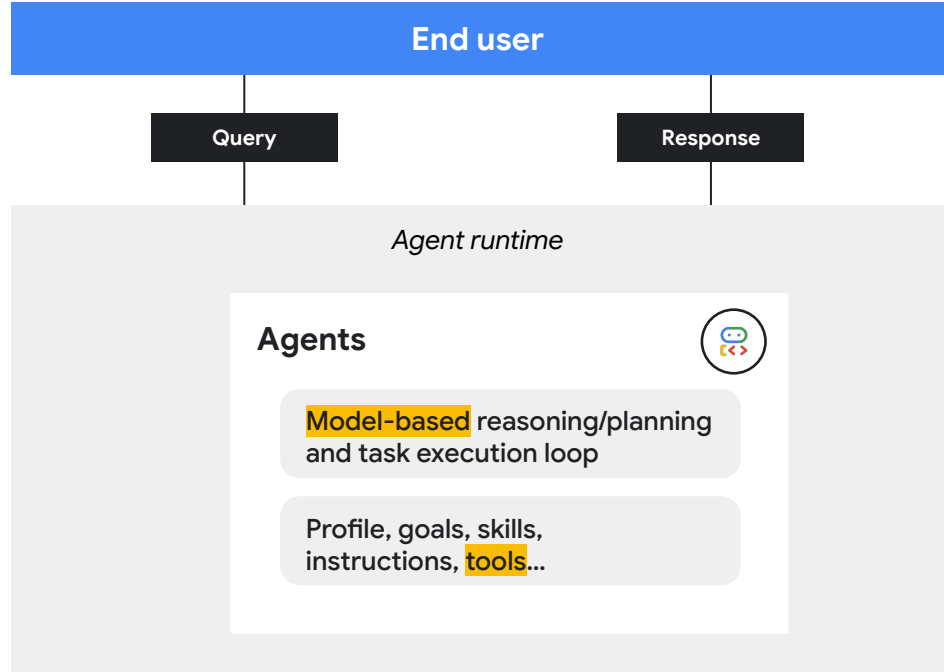
Orchestration

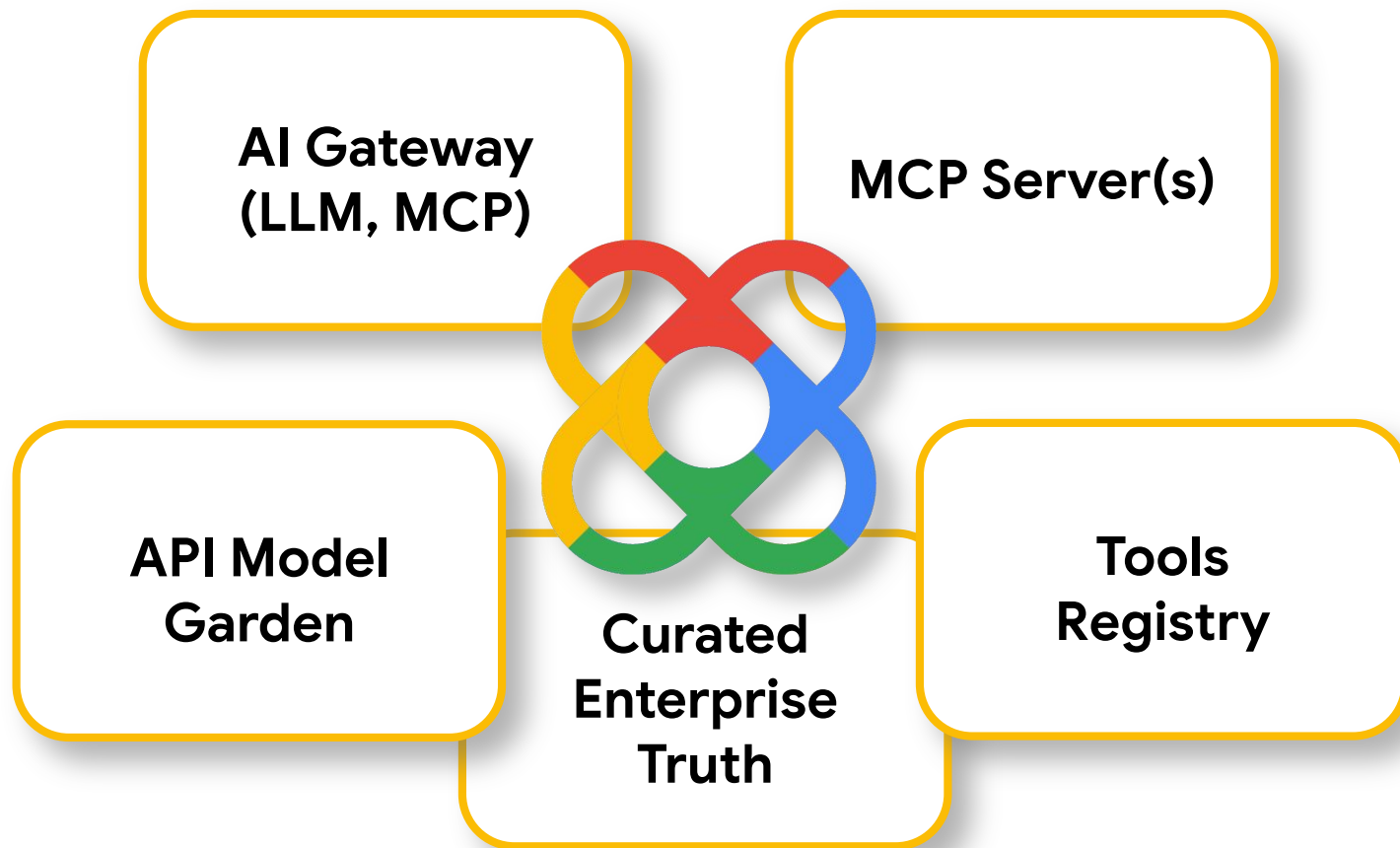
Maintain memory and state (including the approach used to plan), tools, data provided/fetched, etc.



Runtime

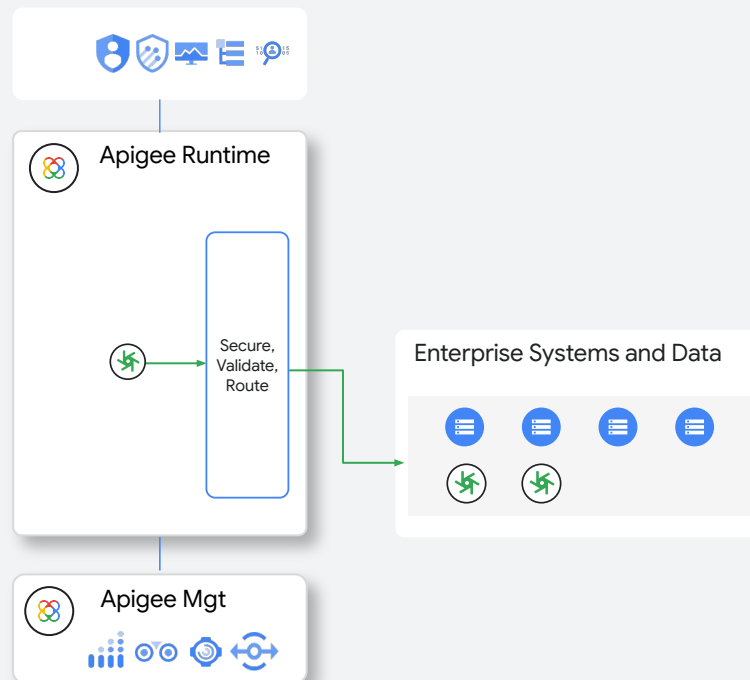
Execute the system when invoked.



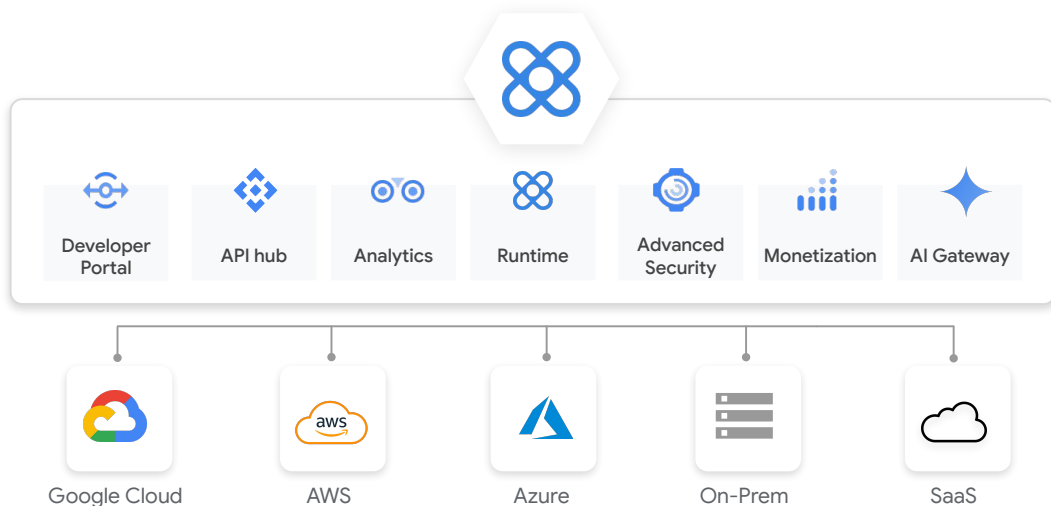


Apigee API management

Apigee API management platform



Apigee API management



Primary use-cases

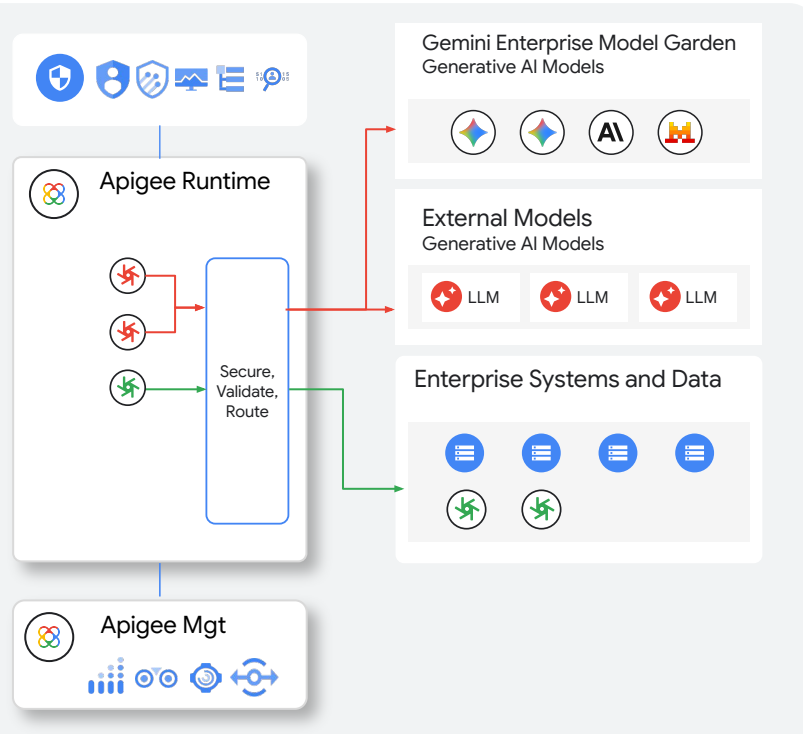
- Productize APIs for AI, monetization and modernization
- API platform for standardization, visibility, analytics
- Deploy, run, secure APIs at scale



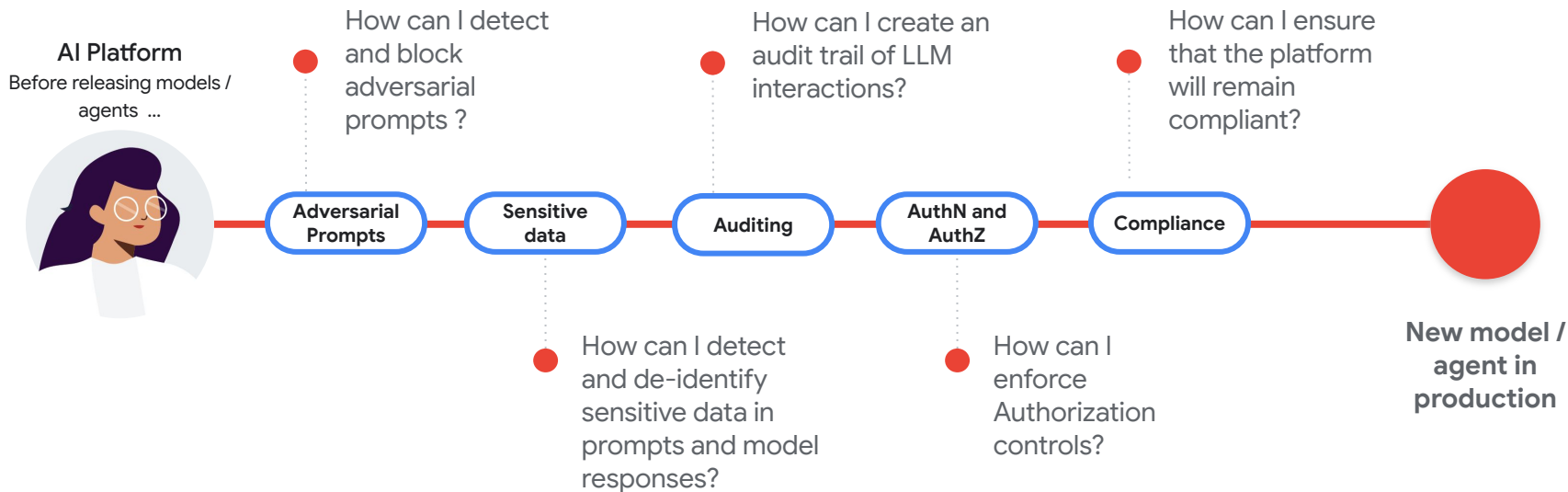
Google is recognized as a **Leader** for the tenth consecutive time and positioned **highest in Ability to Execute** this year among all vendors evaluated.

Google scores the **highest in the AI Enablement Use Case** in the 2025 Gartner® Critical Capabilities for API Management

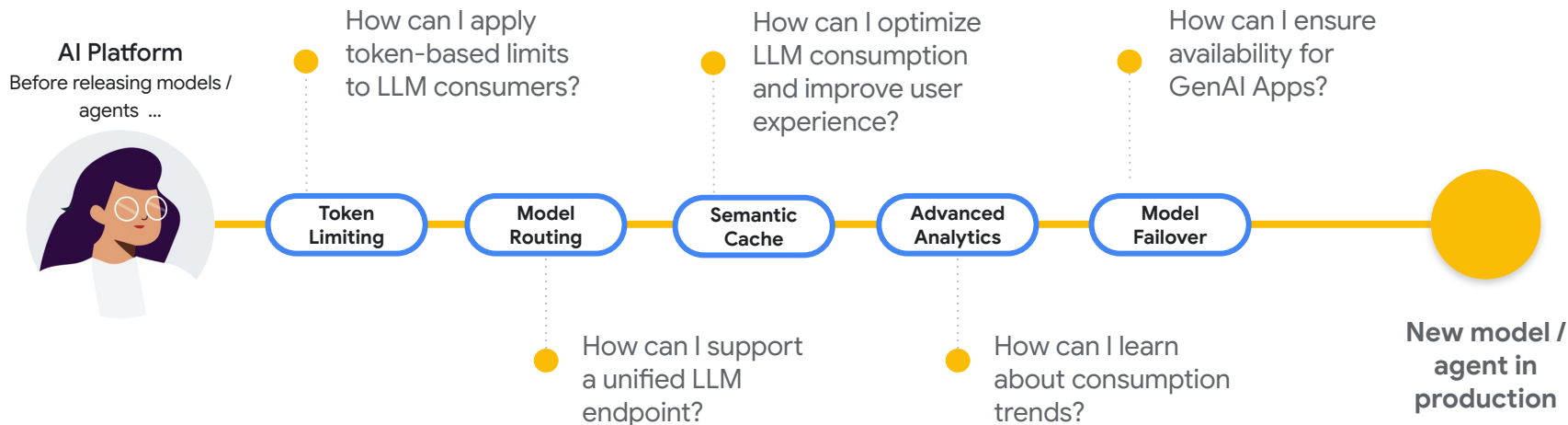
Apigee LLM Gateway



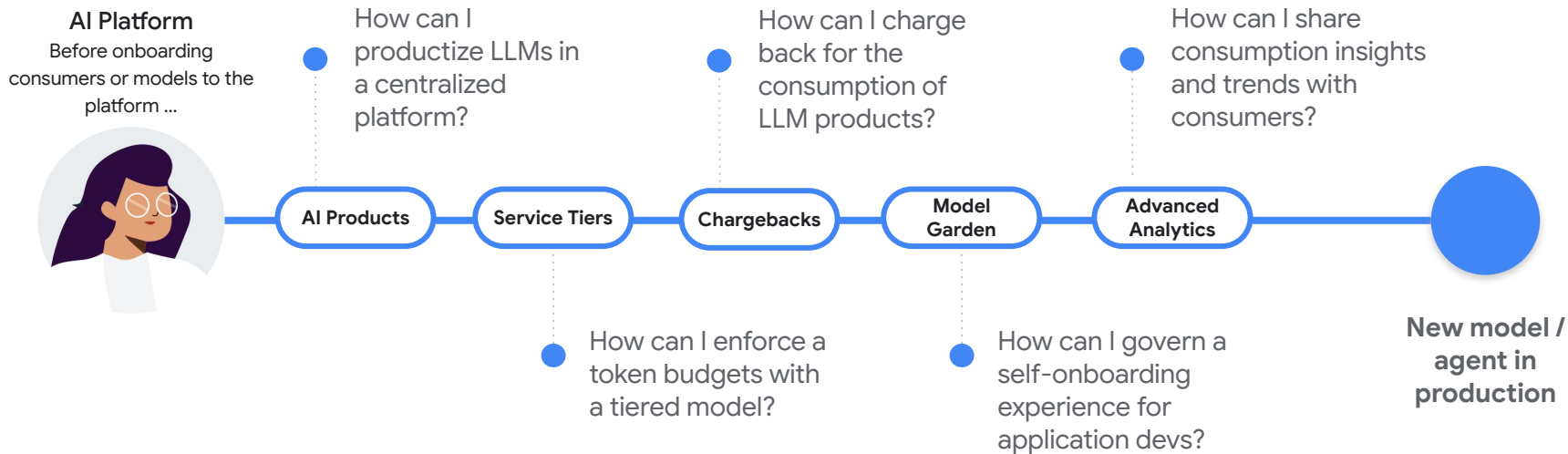
Apigee AI Gateway: the **security** lens



Apigee AI Gateway: LLM **consumption** challenges



Apigee AI Gateway: AI Productization challenges



Native AI Gateway controls & services with Apigee



Model Safety



AuthN / AuthZ



Advanced Security



Semantic Caching



Model Routing and Failover



Advanced Analytics



Monetization



AI Marketplace



Streaming Support (SSE)



Token Limits



JSON-RPC (MCP, A2A, AP2)



Model Armor

Unified safety and security for LLM prompts and responses. Mitigate risks such as sensitive data leakage, prompt injections, and offensive content



Apigee API Management

Apply policy-based configuration for AuthN, AuthZ and logging. Govern onboarding and democratize access.



Advanced API Security

Detect misconfigured endpoints and remain compliant. Detect and block traditional application attacks.



Semantic Caching

Improve performance and optimize costs by storing and reusing the meaning of data, allowing for more intelligent and flexible retrieval even when prompts vary slightly



Model Routing and Failover

Centralized management of traffic for multiple LLM providers, simplifying failover, logging, and security functions while maintaining availability



Advanced Analytics

Gain insights into LLM endpoint performance, quota usage, and failover events. Adjust capacity allocations based on actual traffic patterns and usage



AI Products and Chargebacks

Define token-based service tiers, fine-grained model access and chargeback models



Custom Model Garden

Democratize access to LLM / AI products by publishing to a model garden with a self-onboarding experience

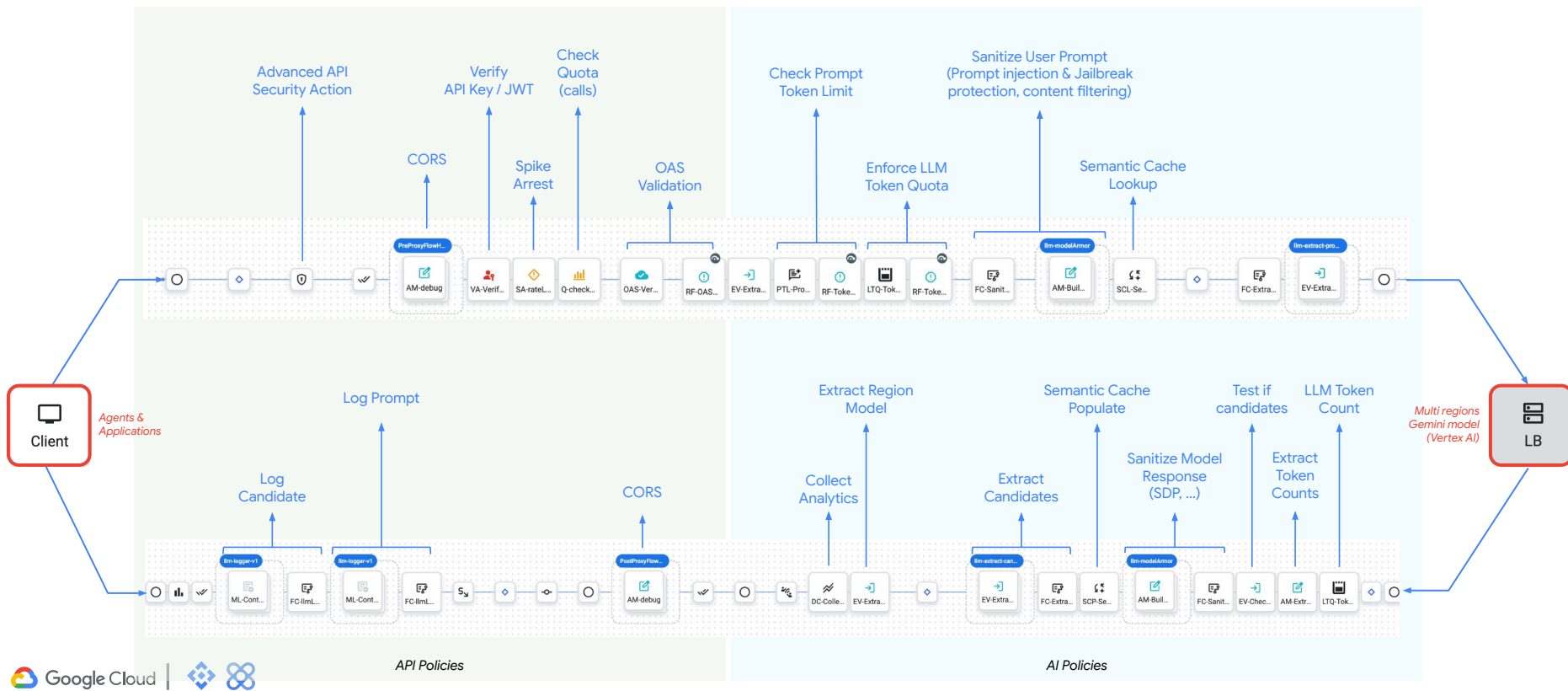


Advanced Visualizations

Share consumption insights with consumers so that they can manage token budgets and monitor historical model performance

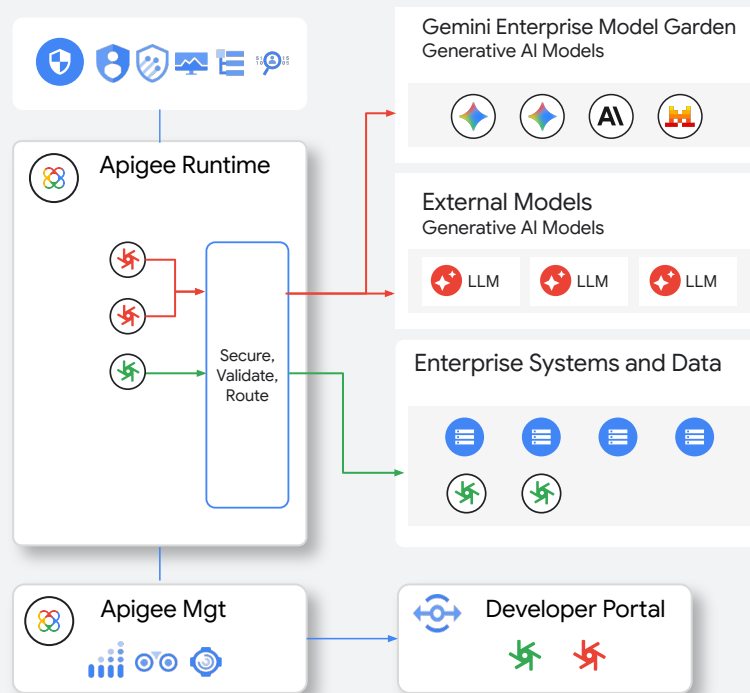
LLM Gateway by Apigee: proxy sample (debug view)

(* All steps / policies are optional and can be configured according to your specific use case)



API Model Garden

Apigee Developer Portal: API Model Garden



Apigee Developer Portal: API Model Garden Sample

The screenshot displays the Apigee Developer Portal's API Model Garden. The top navigation bar includes links for Home, APIs, Analytics, Quick Start, Gen AI Solar, and a user profile (lalevee@google.com). The main section is titled "APIs" and features a search bar and a filter sidebar. The sidebar allows filtering by title & description and by category, with "LLMs (Large Language Models)" selected. The main content area shows "4 results match category: LLMs (Large Language Models)".

Filter by title & description

Filter by category

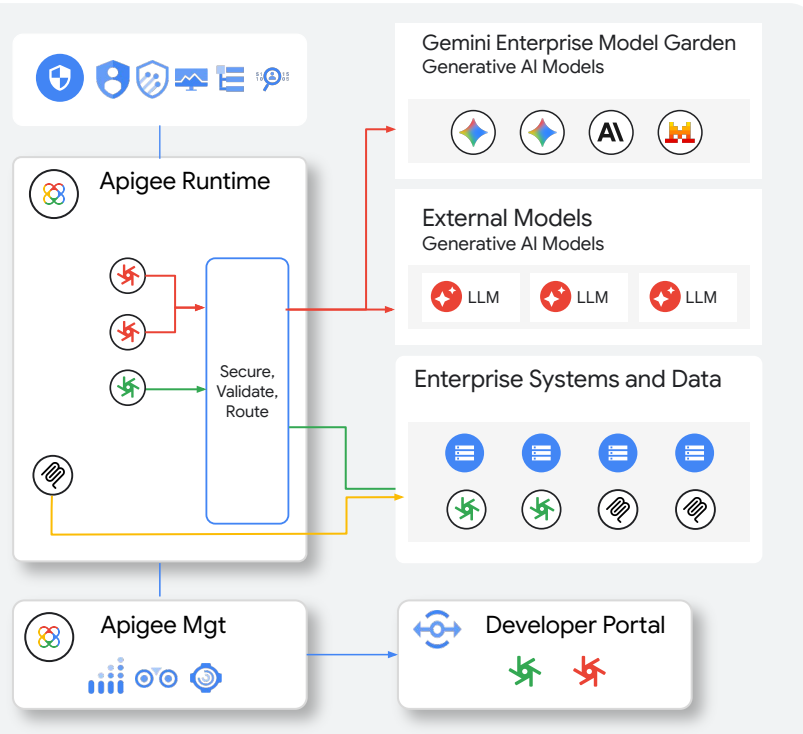
- ☐ None
- ☐ Energy
- ☐ Financial Services Industry
- ☐ Food and Agriculture
- ☐ GCP Service
- ☐ IT
- ☒ LLMs (Large Language Models)
- ☐ New
- ☐ Retail
- ☐ Transport
- ☐ Uncategorized

4 results match category: LLMs (Large Language Models)

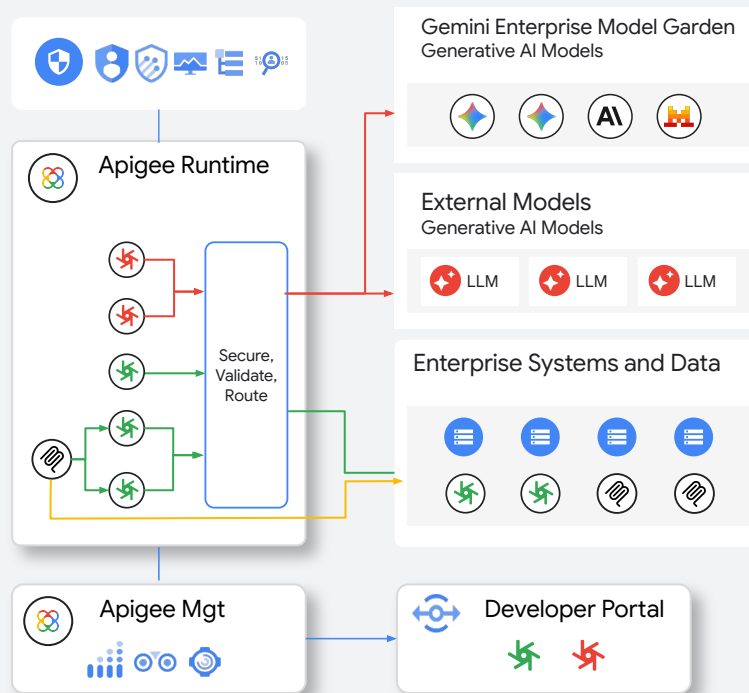
- Anthropic Claude Opus 4-5**
Generate content from a text input, with the Claude Opus 4-5 API
Vertex AI
LLMs (Large Language Models)
- Apigee Global Model Router**
The Global Multi-Region Model Gateway is a resilient API interface that leverages Apigee's load balancing and failover to intelligently route traffic across geographically distributed model endpoints, ensuring Traffic Distribution and High Availability through automated failover.
New LLMs (Large Language Models)
- Apigee Nexus Model 1.0 routed**
Generate content from a text input ("chat/completions") with the Gemini or Mistral or Hugging Face API
LLMs (Large Language Models)
- Google Gemini 2.5 Flash**
Generate content from a text input, with the Gemini-2.5-flash API
Vertex AI
LLMs (Large Language Models)

Apigee MCP

MCP proxy on Apigee

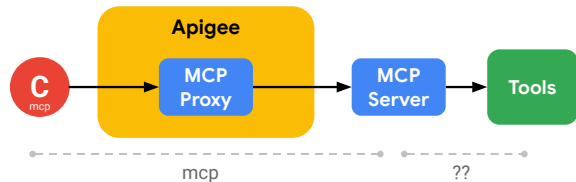


MCP proxy + server (“wrapper”) on Apigee



Apigee: Unified Governance for Any MCP Architecture

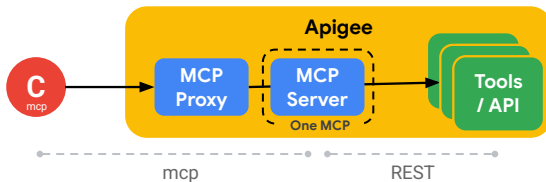
1



Proxy 3rd party MCP server

- Apigee can proxy JSON-RPC requests
- Any MCP server is supported

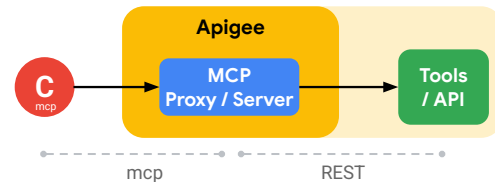
2



Apigee's Native MCP Server

- Hosted in Google dedicated MCP infrastructure
- GCP supported transcoding
- Forwards MCP tool calls to API Proxies as Tool
- Only on Apigee X
- Supports multiple OpenAPI Specs

3



MCP Server as Apigee Proxy (custom)

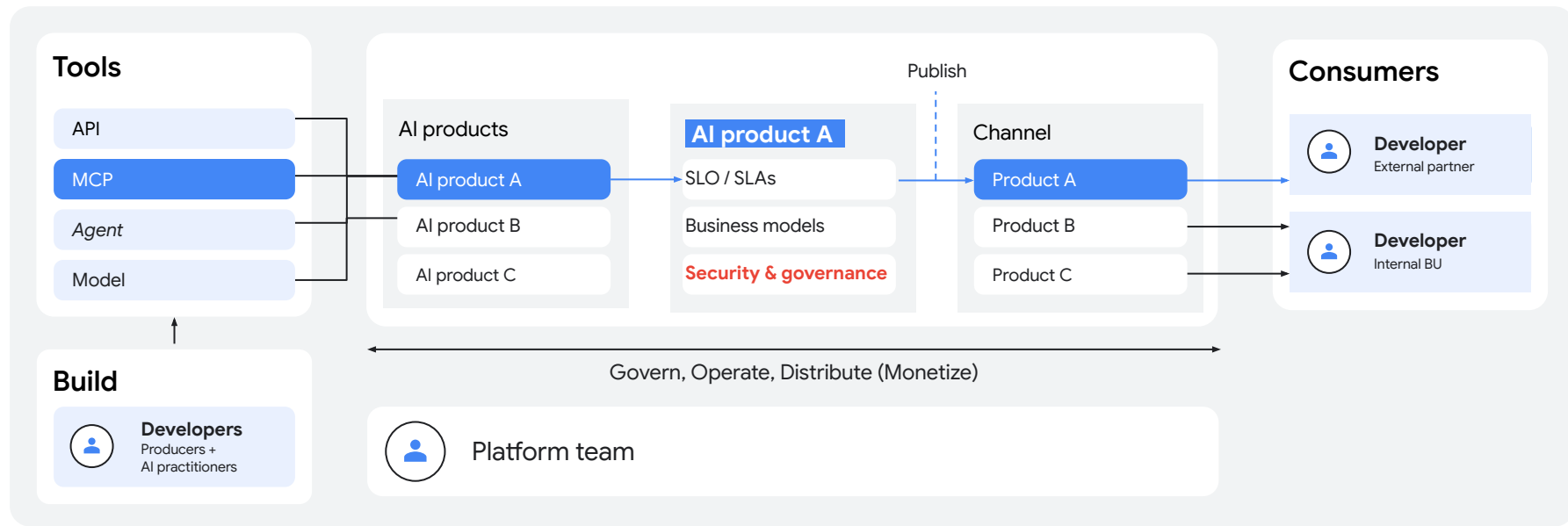
- Uses Apigee policies to expose MCP endpoints
- Apigee custom transcoding logic (opened)
- Can also run on Apigee Hybrid
- Integrated with [apigee go-gen](#)
- Specific for one OpenAPI Spec

UC 1

UC 2

“AI” Products: Govern tool distribution

(“productize your MCP server”)



“AI” Products: Govern tool distribution

(“productize your MCP server”)

The image displays two screenshots of the Google Cloud Apigee console, illustrating the configuration of AI products.

Left Screenshot (Product: cl-model-gemini-v3):

- Product details:**
 - Name: cl-model-gemini-v3
 - Display name: cl-model-gemini-v3
 - Description: N/A
 - Space: N/A
 - Environments: default-dev
 - Access: public
 - Request approval: Automatic
 - API quota: N/A
 - LLM token quota: N/A
 - Allowed OAuth scopes: N/A
- Operations:** Specify operations allowed on an API proxy, including resource paths, HTTP methods, and quotas.

Proxy	Path	Method(s)	Api quota
cl-LLM-Gemini-3	/	POST	100 requests every
- LLM Operations:** Specify operations allowed on an API proxy, including model, resource paths, and token quotas.

Proxy	Path	Model	Method(s)
cl-LLM-Gemini-3	/	gemini-2.5-flash	POST
- GraphQL Operations:** Specify operation types with optional operation name to apply quota upon.

Proxy	Operation Name	Operation Type(s)	Quota
No rows to display			

Right Screenshot (Product: axahc-test-20):

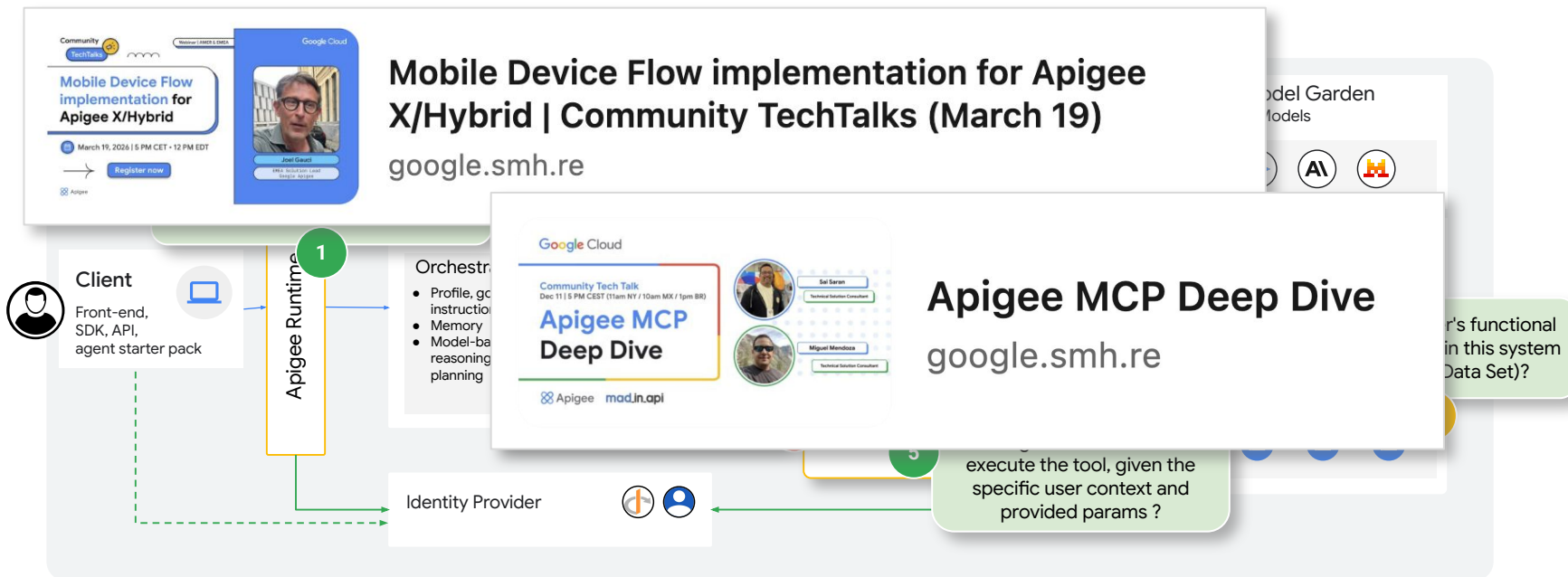
- Product details:**
 - Name: biscuit-coffee-admin
 - Display name: Biscuit Coffee Admin Product
 - Description: Provides access to the entire Biscuit Coffee API.
 - Space: N/A
 - Environments: default-prod
 - Access: internal
 - Request approval: Automatic
 - API quota: N/A
 - LLM token quota: N/A
 - Allowed OAuth scopes: N/A
- Operations:** Specify operations allowed on an API proxy, including resource paths, HTTP methods, and quotas.

Proxy	Path	Method(s)	Api quota	Custom attributes
Biscuit-Coffee-Shop	/	ALL		
- LLM Operations:** Specify operations allowed on an API proxy, including model, resource paths, and token quotas.

Proxy	Path	Model	Method(s)	Quota	Custom attributes
No rows to display					
- Payload Operations:** Specify payload operations to apply quota upon.

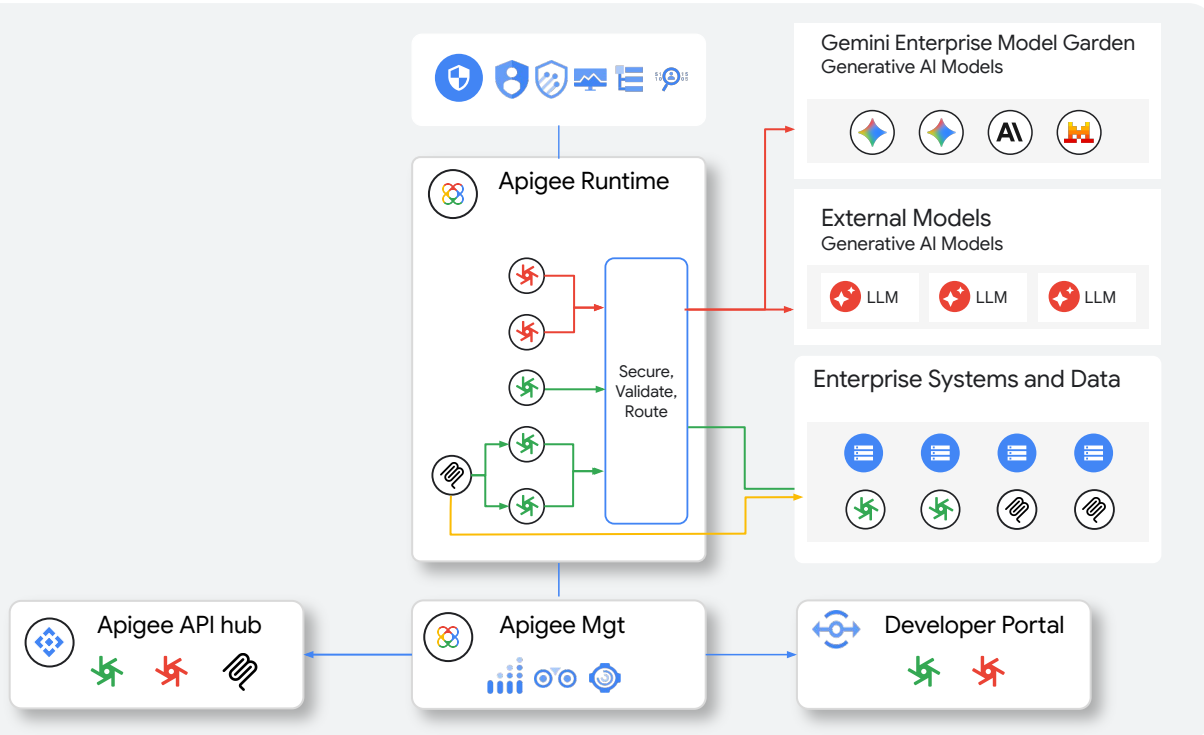
Proxy	Protocol	Details	Quota	Custom attributes
mcp-proxy-prod	MCP	Type: LIST		
mcp-proxy-prod	MCP	Type: CALL, Tool: getStoreLocation		
mcp-proxy-prod	MCP	Type: CALL, Tool: ...		

MCP Authentication / Authorization Use Case Samples

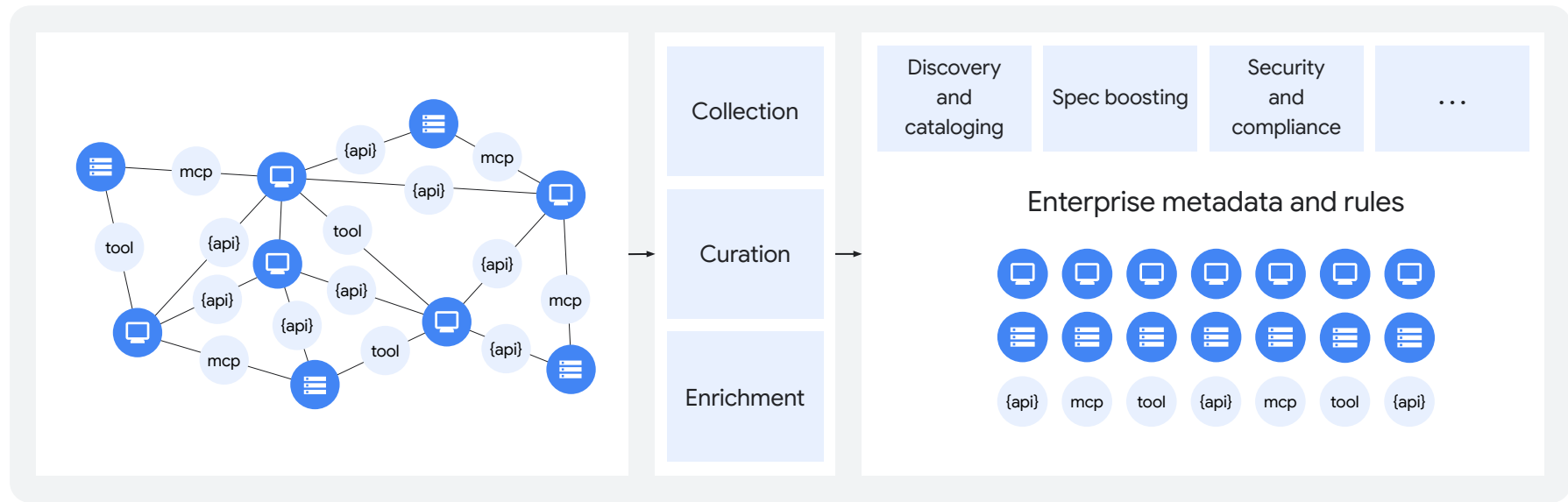


API hub: from APIs to Curated Enterprise Truth

API hub: APIs, **Curated Enterprise Truth**



API hub: Discovery and Organization of agentic tools





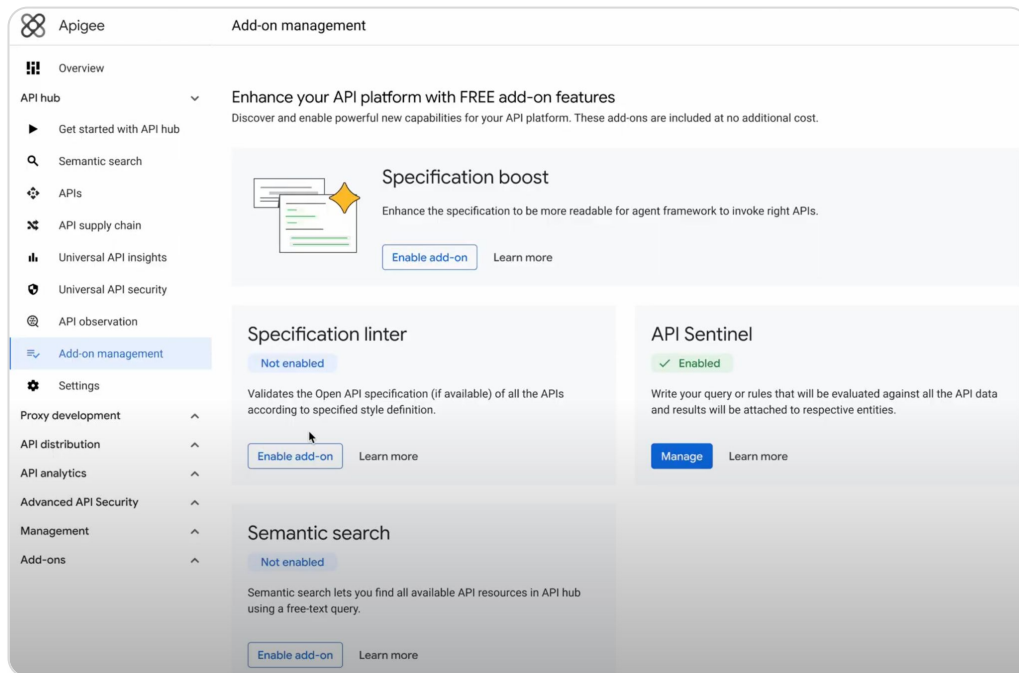
Apigee API hub: Centralized API Portfolio Governance

Apigee API hub provides centralized design-time and portfolio governance by acting as the single source of truth for all enterprise APIs (from Apigee, third-parties, and other gateways). This enables platform teams to gain visibility, enforce standards, and manage the full lifecycle of their API assets, accelerating reuse and consistency.

Key Governance Capabilities:

- **Specification Linting & Validation:**
Enforces design consistency, quality, and compliance *before* APIs are published or consumed, "shifting left" on governance.
- **Lifecycle Management:**
Provides a clear signal to consumers about an API's readiness and support status, preventing the use of unapproved or retired APIs.
- **Rich Metadata & Taxonomy:**
Allows teams to govern the portfolio by **owner**, **business-unit**, **data-sensitivity**, or any other enterprise taxonomy, making APIs filterable and policies auditable.
- **API Supply Chain & Dependency Mapping:**
Enables governance teams to understand the impact of changes, identify critical dependencies, and manage the health of the entire API ecosystem.

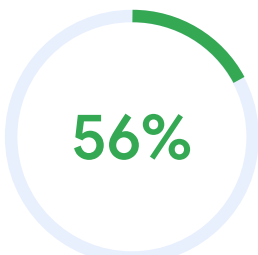
Advanced Governance powered by Google AI



- **Semantic Search**
Find the right API with the ease of asking a colleague
- **API Sentinel** (preview)
“Analyse any API that expects Government ID as input”
- **Specification boost** (preview)
(see next slide)

Optimizing APIs for agentic use

Developed by **Google DeepMind** to enrichment API specifications for agentic consumption



Increase in accuracy for E2E agent execution

When comparing an AI-booster spec to a human-edited spec

```

1 openapi: 3.0.0
2 info:
3   title: Simple API
4   description: Simple API to perform addition, a basic
5     arithmetic operation.
6   version: 1.0.0
7 paths:
8   /add:
9     summary: Adds two numbers
10    parameters:
11      - name: a
12        in: query
13        required: true
14        schema:
15          type: integer
16      - name: b
17        in: query
18        required: true
19        schema:
20          type: integer
21    responses:
22      "200":
23        description: Successful response
24        content:
25          application/json:
26            schema:
27              type: integer
28
29  /addition:
30    summary: Adds two numbers
31    description: Perform addition of two integer numbers,
32      a and b, and returns their sum.
33    operationId: addNumbers
34    tags:
35      - Arithmetic Operations
36    parameters:
37      - name: a
38        in: query
39        required: true
40        description: The first integer operand for addition.
41        schema:
42          type: integer
43          format: int32
44          description: An integer value (32-bit).
45          examples:
46            - 5
47      - name: b
48        in: query
49        required: true
50        description: The second integer operand for
51        addition.
52        schema:
53          type: integer
54          format: int32
55          description: An integer value (32-bit).
56          examples:
57            - 10
58    responses:
59      "200":
60        description: Successful response containing the sum
61        of the two numbers. The result is provided as an integer.
62        Note: Arithmetic overflow/underflow conditions (e.g., if the
63        sum exceeds the representable range of a 32-bit integer) are
64        not explicitly handled by this endpoint and may result in an
65        error or an undefined numerical result.
66        content:
  
```

Creating **Curated Enterprise Truth** for AI Agents

“Your AI is ~~only~~ as trustworthy as your tools”



discover,
understand,
use

Agents

Agents are built using only trusted tools to Enterprise Truth

 **Gemini Enterprise**



discover,
curate,
govern,
productize

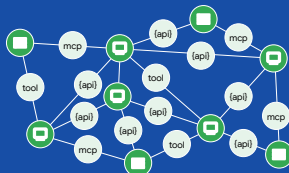
Curated Enterprise Truth

Information, data, APIs, and connectors to trusted sources, designed and productized for AI consumption



All enterprise resources

A mix of trusted and untrusted resources, not known to be ready for AI



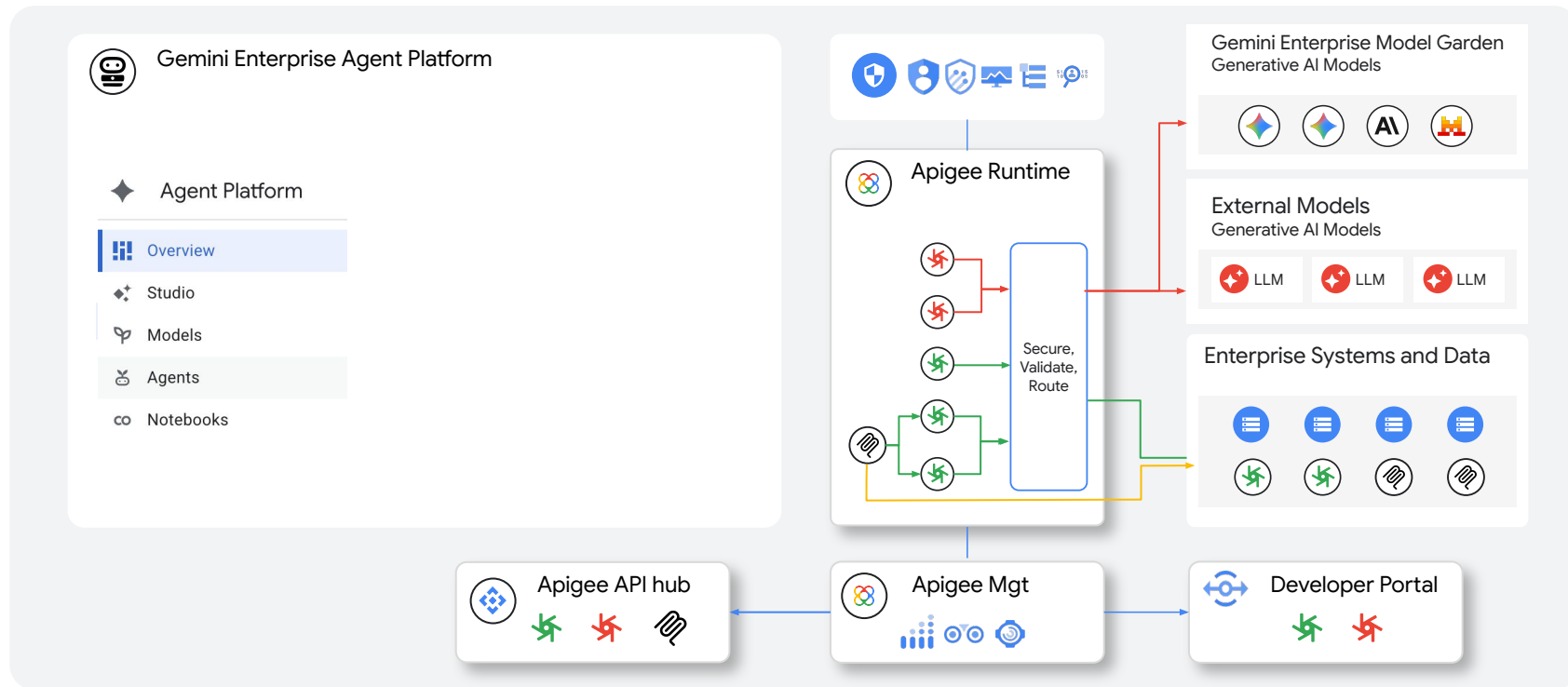
??


API Metadata

 Apigee X Organization	 Apigee Edge Organization
 Apigee hybrid Organization	 Apigee OPDK Organization
 3rd party API gateway	 specific API data source #1

Gemini Enterprise Agent Platform

Gemini Enterprise Agent Platform



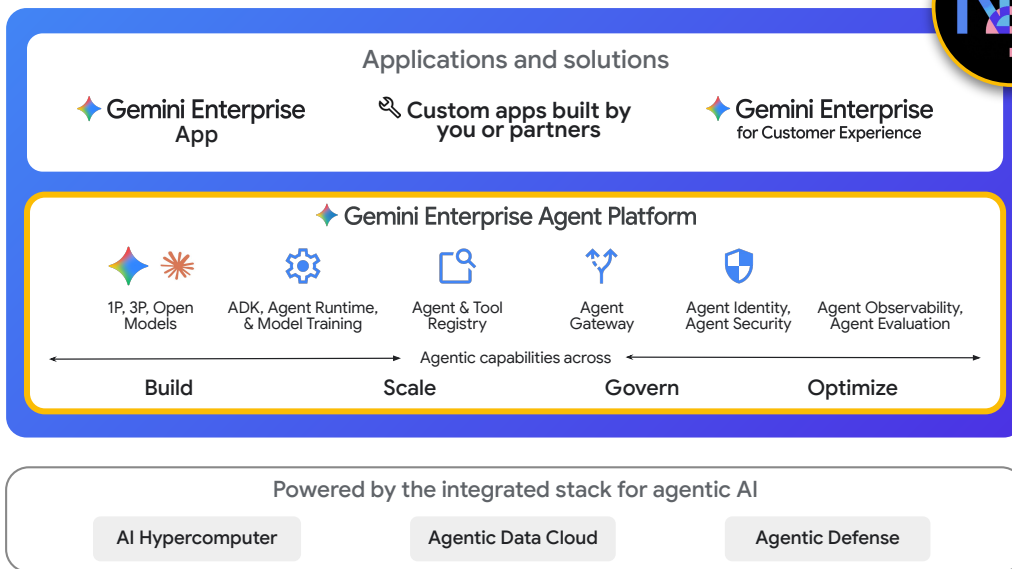
Gemini Enterprise Agent Platform: Build. Scale. Govern. Optimize.

Agent Platform

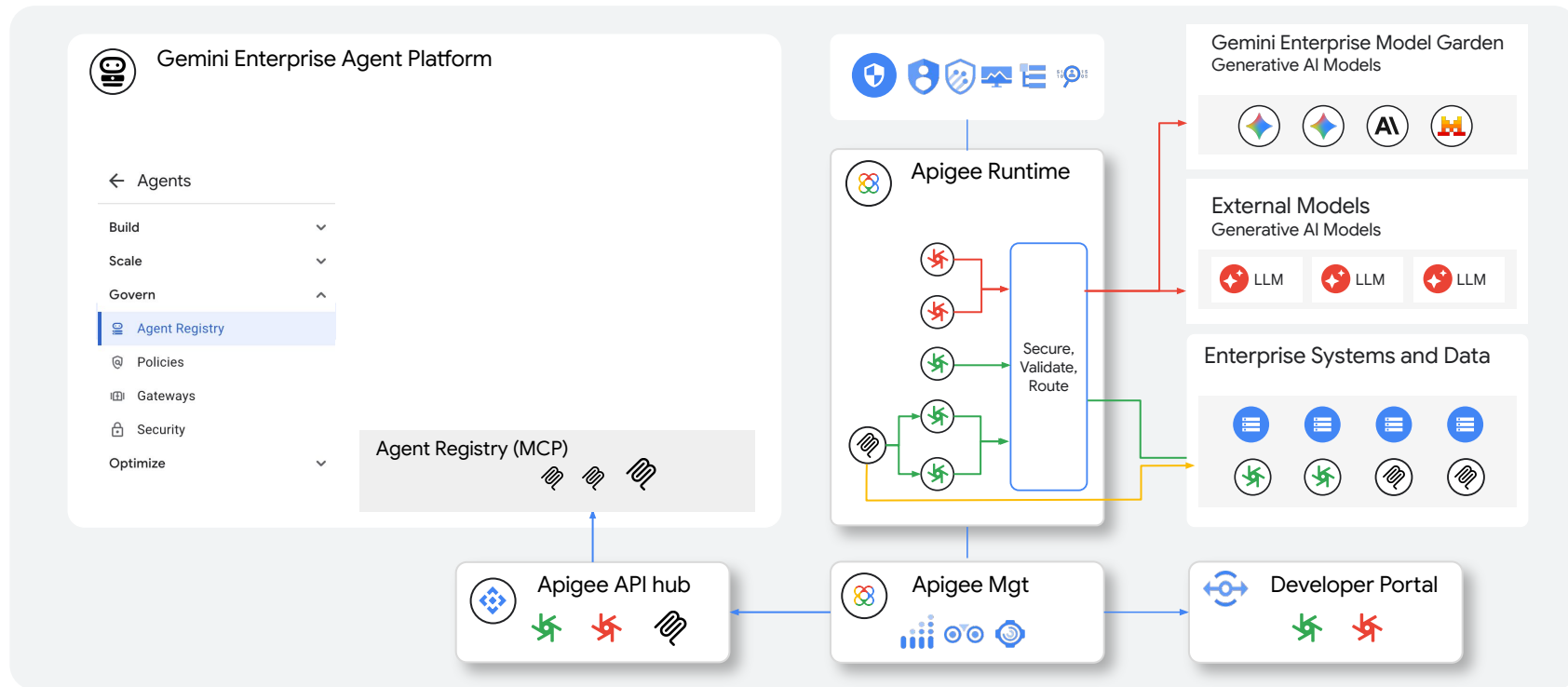
Gemini Enterprise Agent Platform is our new, comprehensive environment to **build, scale, govern, and optimize agents**.

It integrates the Model Garden, Model Builder, and Agent Builder capabilities of Vertex AI with new, enterprise-grade features for agent integration, DevOps, and security.

Gemini Enterprise



Gemini Enterprise Agent Platform & Tools Registry



Gemini Enterprise Agent Platform & Tools Registry

Google Cloud | bap-emea-apigee-5 | Search (/) for resources, docs, products, and more

Agent Platform / Agents / Registry / MCP Servers

← Agents | Registry | Add Agent | Add MCP Server | Add Endpoint

Build | Scale | Govern | Agent Registry | Policies | Gateways | Security | Optimize

Registry

@ Search for agents, MCP servers

Agents | MCP Servers | Endpoints

Location (All) | Discover Google Cloud MCP servers

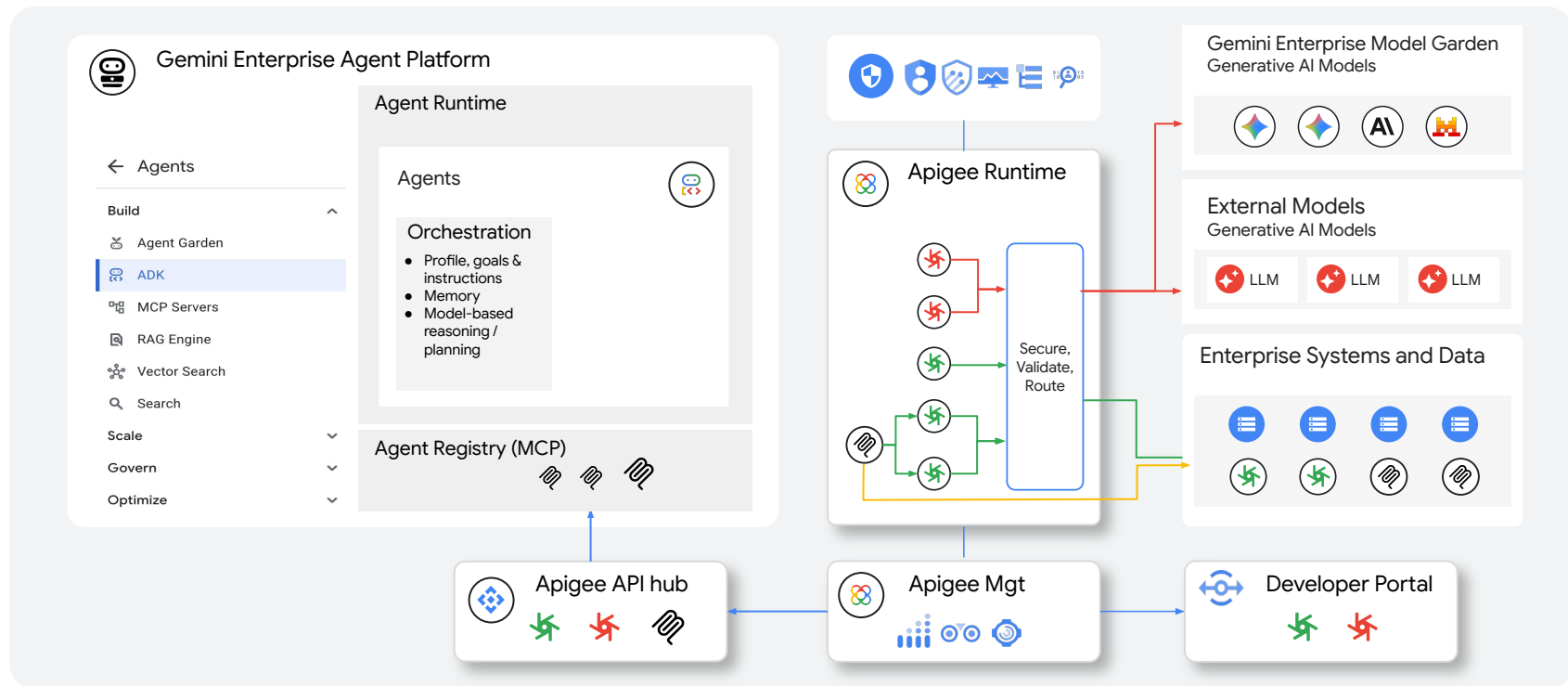
Filters | Hide system-created MCP servers

Name	MCP Server ID	Description	Runtime	Location ↑	Tools	Actions
cl-airport-mcp	...9cab9a64-0666-46db-b4a0-92873cb266be	Get Airports list and details	API Hub	europe-west1	2	⋮
cm-mcp-server	...1bca466a-f060-4754-8877-3571861c6725	-	API Hub	europe-west1	3	⋮
agentregistry.googleapis.com	...locations:global:agentregistry	MCP server which exposes Agent...	Google MCP	global	12	⋮
aiplatform.googleapis.com	...locations:global:aiplatform	Model Context Protocol (MCP) ser...	Google MCP	global	47	⋮
apihub.googleapis.com	...1020259423319:locations:global:apihub	-	Google MCP	global	16	⋮
apptopology.googleapis.com	...locations:global:apptopology	Service for generating and retriev...	Google MCP	global	7	⋮
bigquery.googleapis.com	...locations:global:bigquery	BigQuery MCP server provides tool...	Google MCP	global	6	⋮
bigquerydatatransfer.googleapis.com	...locations:global:bigquerydatatransfer	BigQuery DTS MCP server provide...	Google MCP	global	9	⋮
bigquerymigration.googleapis.com	...locations:global:bigquerymigration	BigQuery Migration MCP server pr...	Google MCP	global	5	⋮
ces.googleapis.com	...1020259423319:locations:global:ces	MCP server for Gemini Enterprise f...	Google MCP	global	60	⋮
cloud-sql	...locations:global:sqladmin	Cloud SQL Admin API for MCP	Google MCP	global	15	⋮
cloudresourcemanager.googleapis.com	...locations:global:cloudresourcemanager	MCP Config for Cloud Resource M...	Google MCP	global	1	⋮
cloudtrace.googleapis.com	...locations:global:cloudtrace	An MCP server that provides tools ...	Google MCP	global	2	⋮
compute.googleapis.com	...locations:global:compute	This is an MCP server which provi...	Google MCP	global	29	⋮
container.googleapis.com	...locations:global:container	This is an MCP server which provi...	Google MCP	global	8	⋮
dataplex.googleapis.com	...locations:global:dataplex	MCP server for interacting with Kn...	Google MCP	global	11	⋮
discoveryengine.googleapis.com	...locations:global:discoveryengine	This is an MCP server which provi...	Google MCP	global	2	⋮
firestore.googleapis.com	...locations:global:firestore	Firestore MCP Server provides tool...	Google MCP	global	15	⋮
geminicloudassist.googleapis.com	...locations:global:geminicloudassist	The Gemini Cloud Assist MCP Ser...	Google MCP	global	5	⋮
logging.googleapis.com	...locations:global:logging	MCP for Logging API	Google MCP	global	6	⋮
maptools.googleapis.com	...locations:global:maptools	This is an MCP server provided by ...	Google MCP	global	3	⋮

Show debug panel

Build and Deploy agents

Build and publish agents



Tools in ADK

A tool is a function that an agent can call to interact with the world.

Pre-built Google Tools

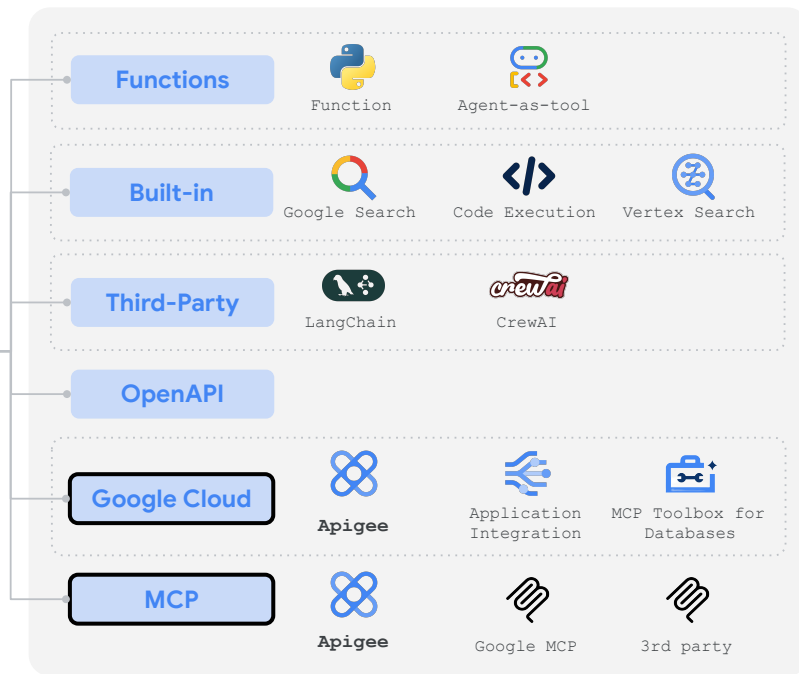
Ready-to-use. Eg. Google Search for web access and Vertex AI Search for querying your own private data (RAG).

Third-Party Tools

ADK integrates popular libraries like LangChain and CrewAI.

Custom Tools

Turn any Python function into a tool that your agent can use to perform specialized tasks, connect to proprietary APIs, or execute unique algorithms.



ADK: Seamless Apigee API hub (API) integration for Agents



```
from google.adk.tools.apihub_tool.apihub_toolset import APIHubToolset

# Initialize API hub instance
API_HUB_LOCATION=f"projects/{PROJECT_ID}/locations/{LOCATION}/apis"

# Define authentication
auth_scheme = your-[API Key,OAuth2,Service Account,OpenIDC]-config
Auth_credential = your-credentials

# Create API tool from API hub definition
apihub_toolset = APIHubToolset(
    name="your-tool-name",
    description="Tool description",
    apihub_resource_name=f"{API_HUB_LOCATION}/your-apidatahub-API-ID",
    auth_scheme=auth_scheme,
    auth_credential=auth_credential,
)
```

ADK: Seamless Tools Registry (MCP) integration for Agents



```
from google.adk.tools.api_registry import ApiRegistry

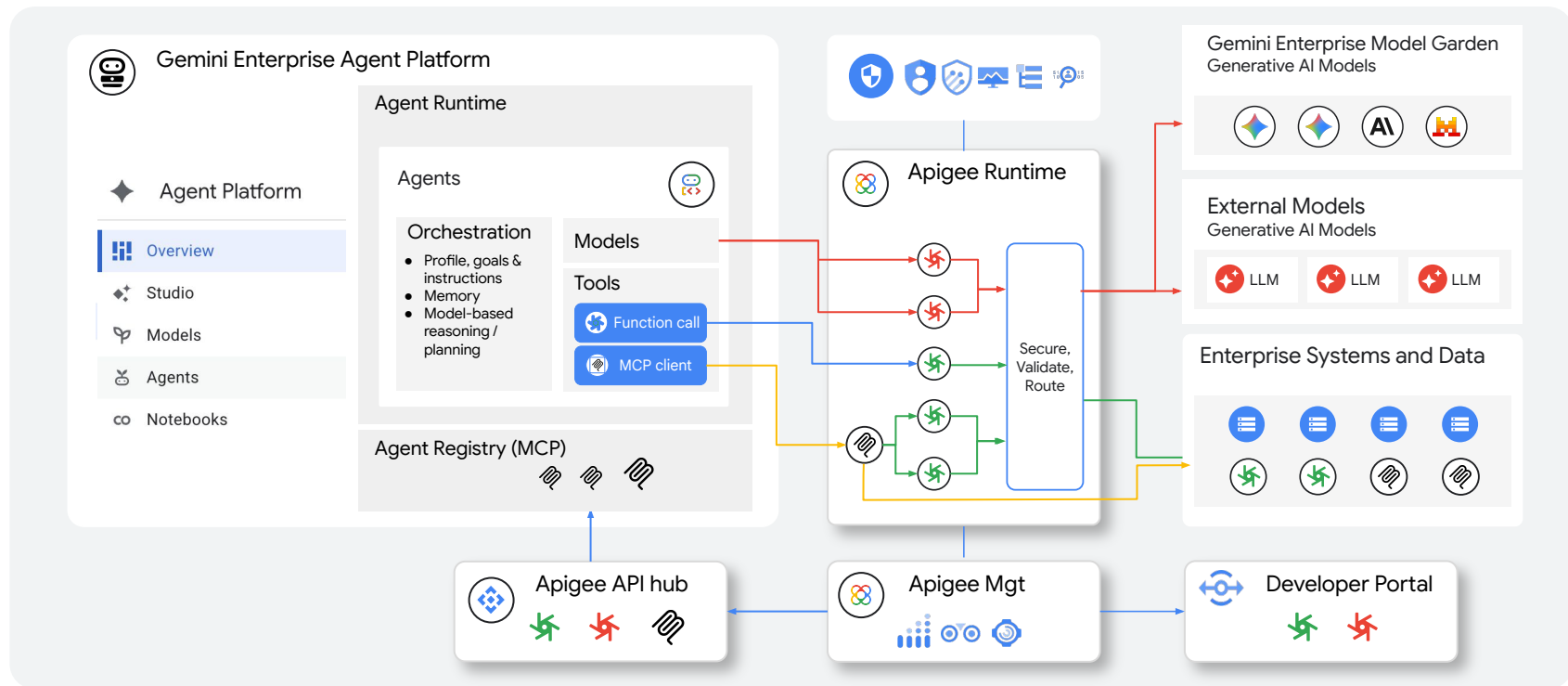
PROJECT_ID = {PROJECT_ID}
MCP_SERVER_NAME =
"projects/{PROJECT_ID}/locations/{LOCATION}/mcpServers/apihub-120e427d-ef81-4af0-b126-362
59d6dfdb8.e467f26c-efe0-4c5f-asf1-e209647ceda6.14abafef-2d81-43se-9846-a80623b4674e"

api_registry = ApiRegistry(PROJECT_ID)
registry_tools = api_registry.get_toolset(
    mcp_server_name=MCP_SERVER_NAME,
    tool_filter=["apihub-...abafef-2d81-43de-9846-a80623b4674e.getsolarestimation"]
)

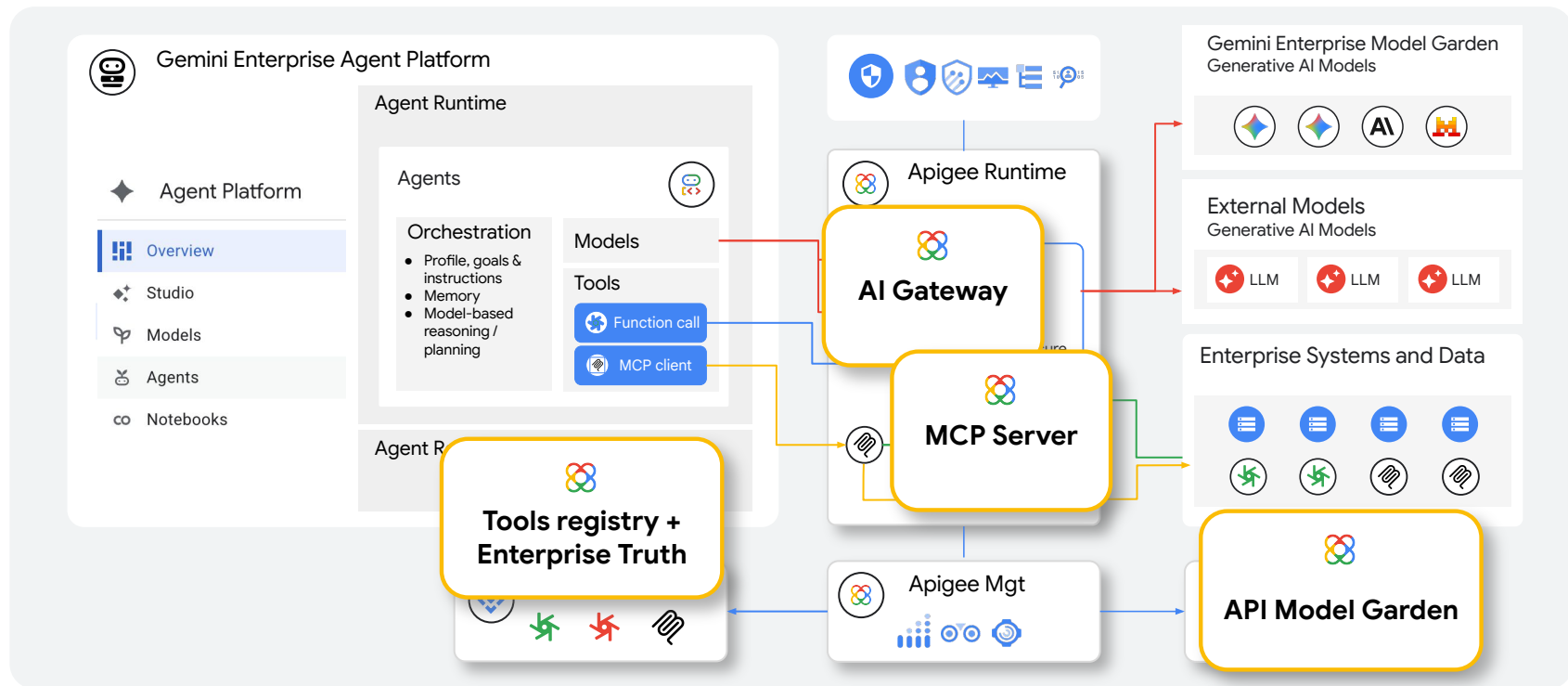
root_agent = LlmAgent(
    model=model,
    name="sample_agent",
    instruction="Use the tools you have access to help answer user questions",
    tools=[registry_tools],
)
```

Conclusion

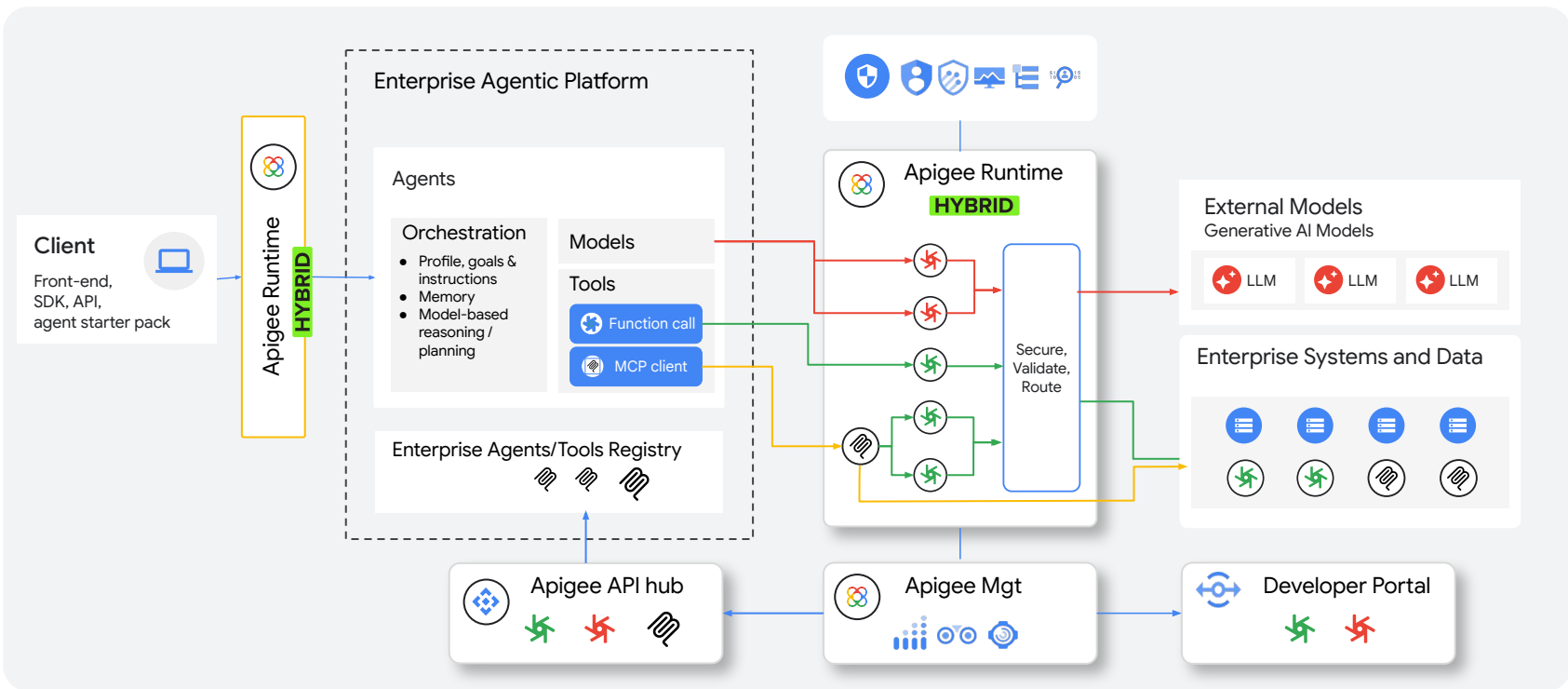
Build and publish agents with Agent Platform and Apigee



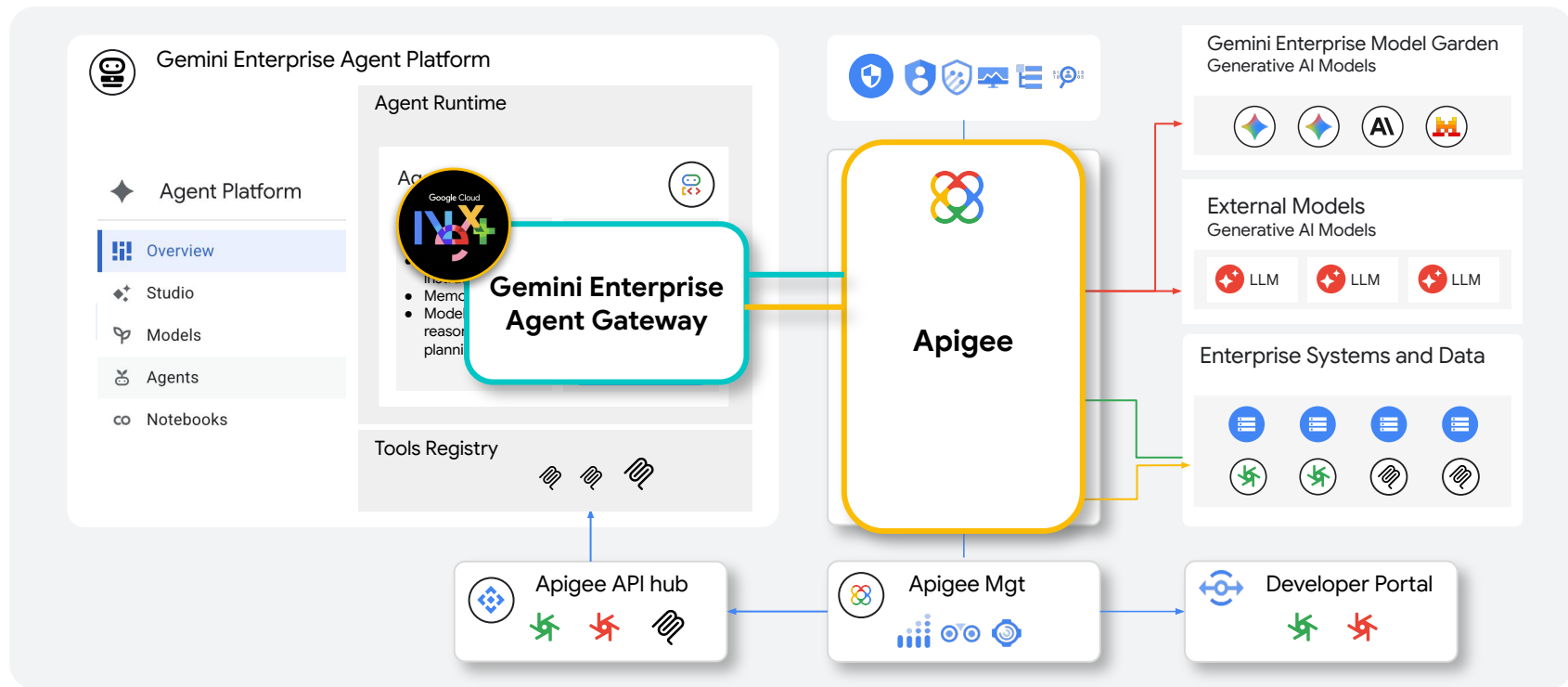
Build and publish agents with Agent Platform and Apigee



But also... Frontend-to-Agent Integration outside of Gemini Enterprise Agent Platform



Next? Agent governance and Agent Gateway with Apigee

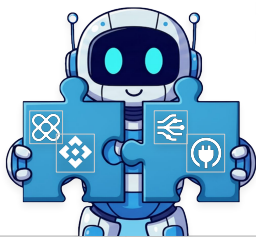
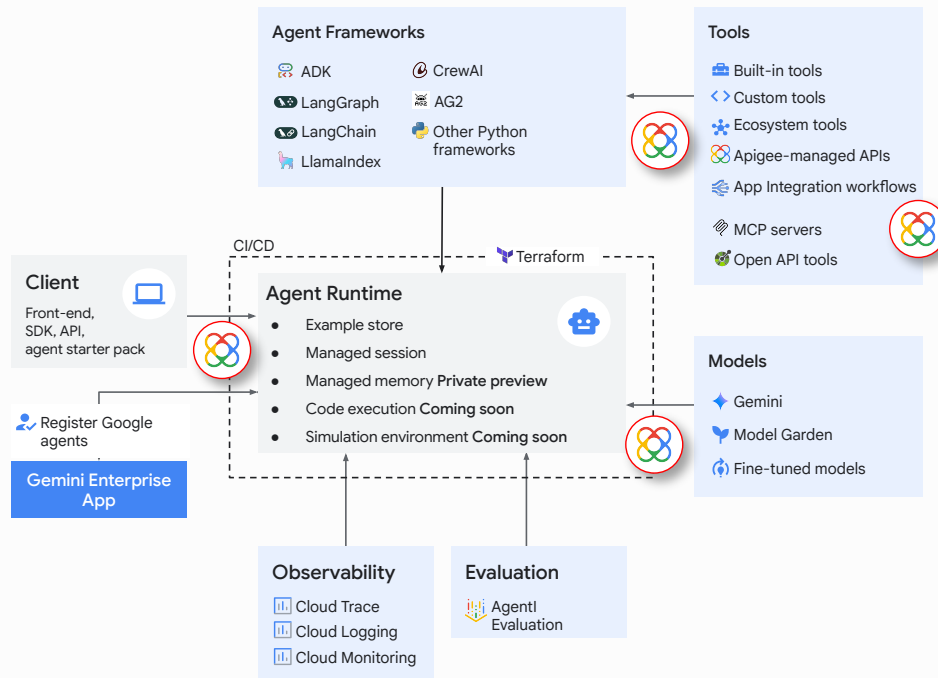


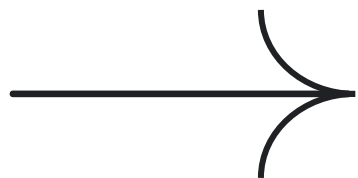
Key takeaway

Build, manage and govern agents with the most open platform

Apigee

- Security
- Traffic management
- Observability
- Productization & Monetization
- Registry & Governance
- AI Gateway
- Agent tools & Tools repository (MCP)
- ADK toolset
- ...





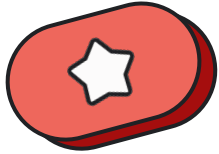
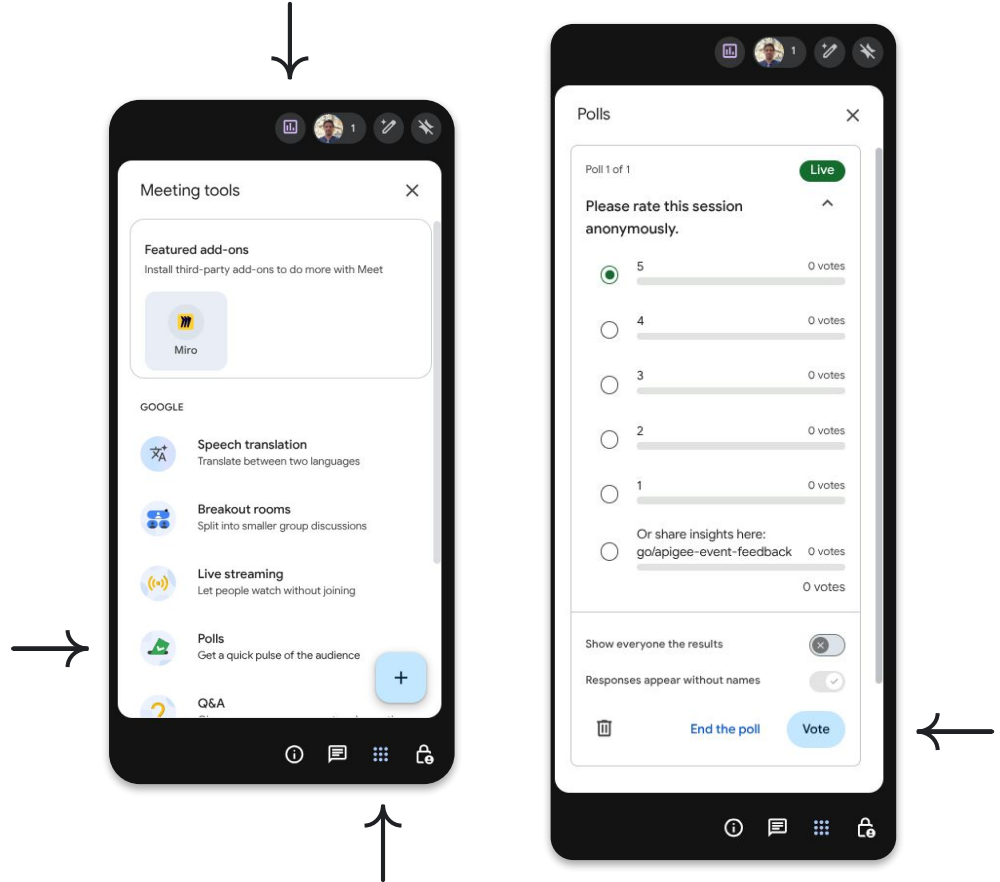
Q&A



Please share your feedback!

Help us make our sessions even better!

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



→ Catch up!



Catch up with Next 26'

-  **Build production-ready agents on Google Cloud:** A guide for architects and CTOs.
-  **Agent Security at Scale:** Protect against the OWASP Top 10 Application Risks.
-  **Unlocking Enterprise Actions:** Watch the highlights of bridging APIs to AI Agents.
-  **Build Connected AI:** Orchestrate tools and agents with registries and ADK.



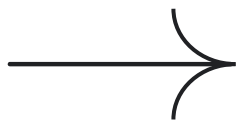
Upcoming Events

- May 28, with Nicola Cardace
Apigee Production go-live checklist
- June 4, with Joel Gauci
Extending Agent Gateway Capabilities with Apigee
- June 11, with Nigel Walters
Powering Gemini Enterprise with Apigee APIs



Community

TechTalks



Thank You