Shipping Autonomous Agents Safely with Open Standards, Observability, and Control.

Agent Governance & Security



Rao Surapaneni
VP, Gemini Enterprise & Agent Platform Governance
Cloud AI

Google Cloud

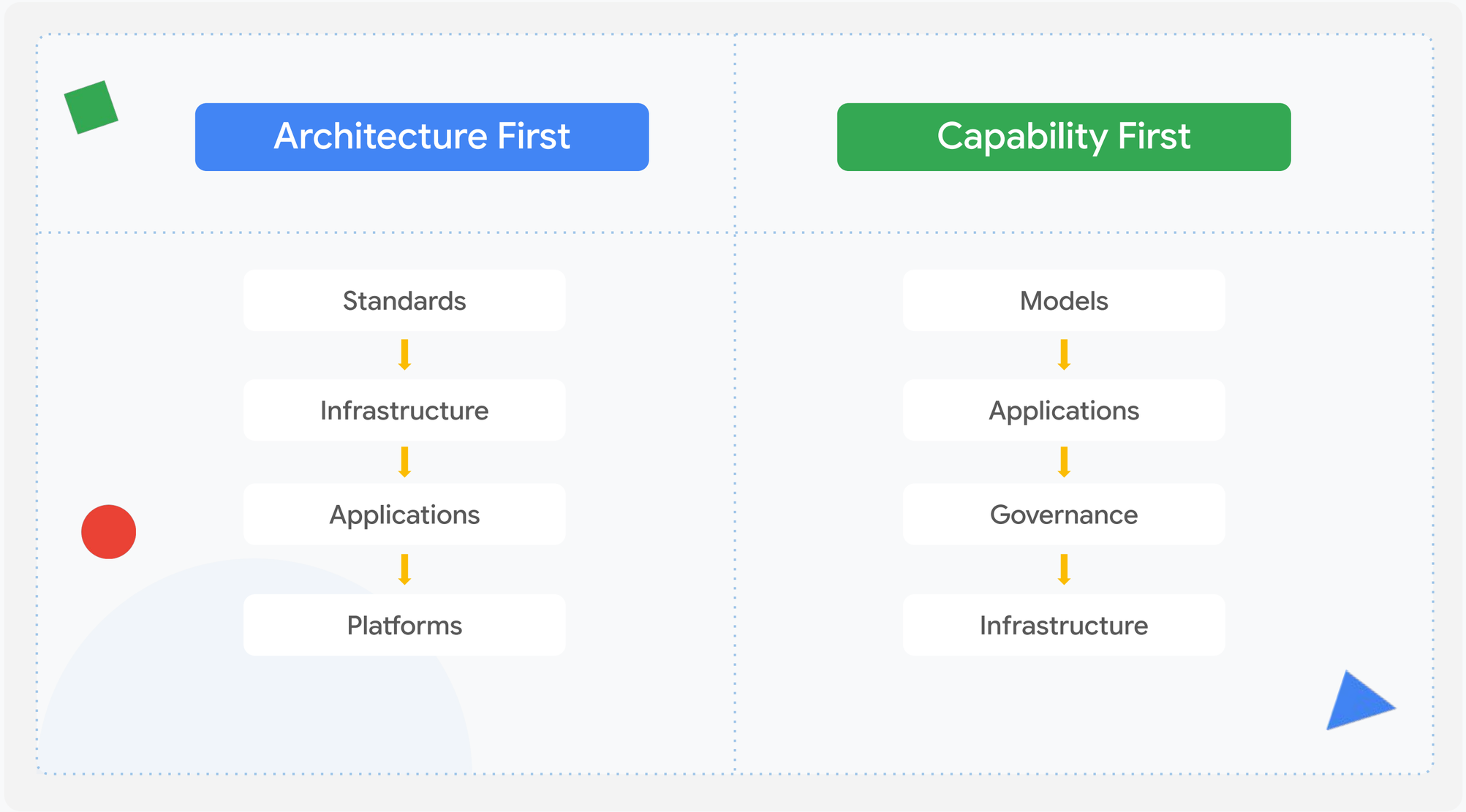
Evolution of Internet vs Internet of Agents

Architecture First



Capability First

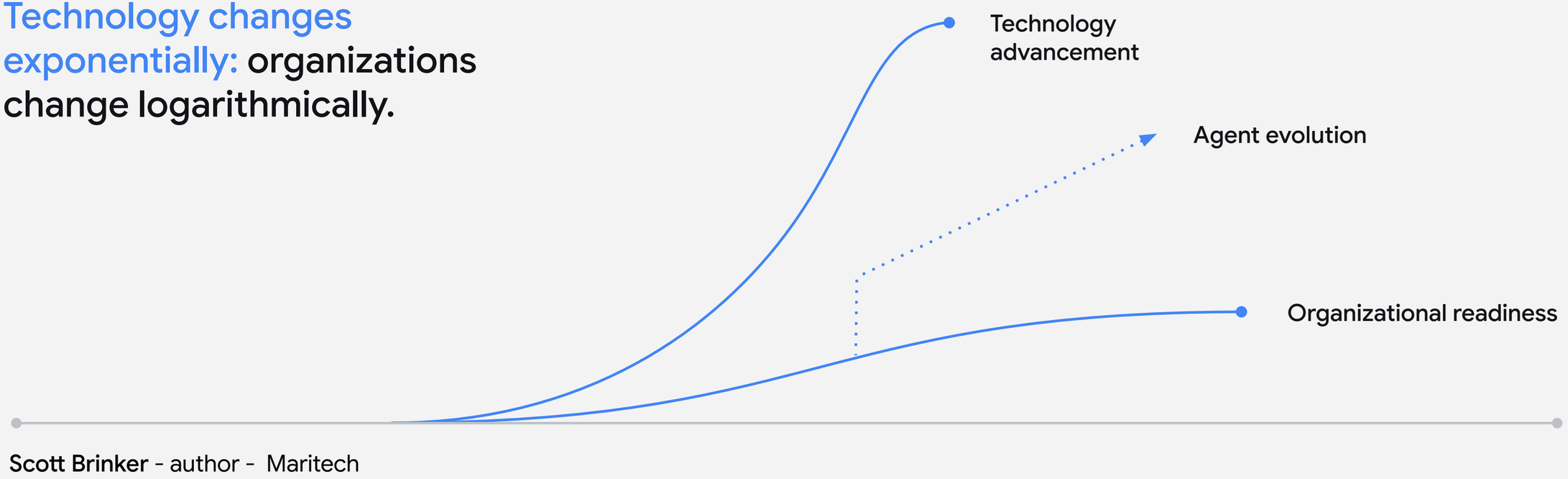



Architecture First
Capability First
Standards
Infrastructure
Applications
Platforms
Models
Applications
Governance
Infrastructure

Acceleration

Capability vs Capacity to safely harness and drive business value.
Our goal is to help you close the gap.

Technology changes exponentially: organizations change logarithmically.



Scott Brinker - author - Maritech

Capability acceleration results in

Faster sprawl

01

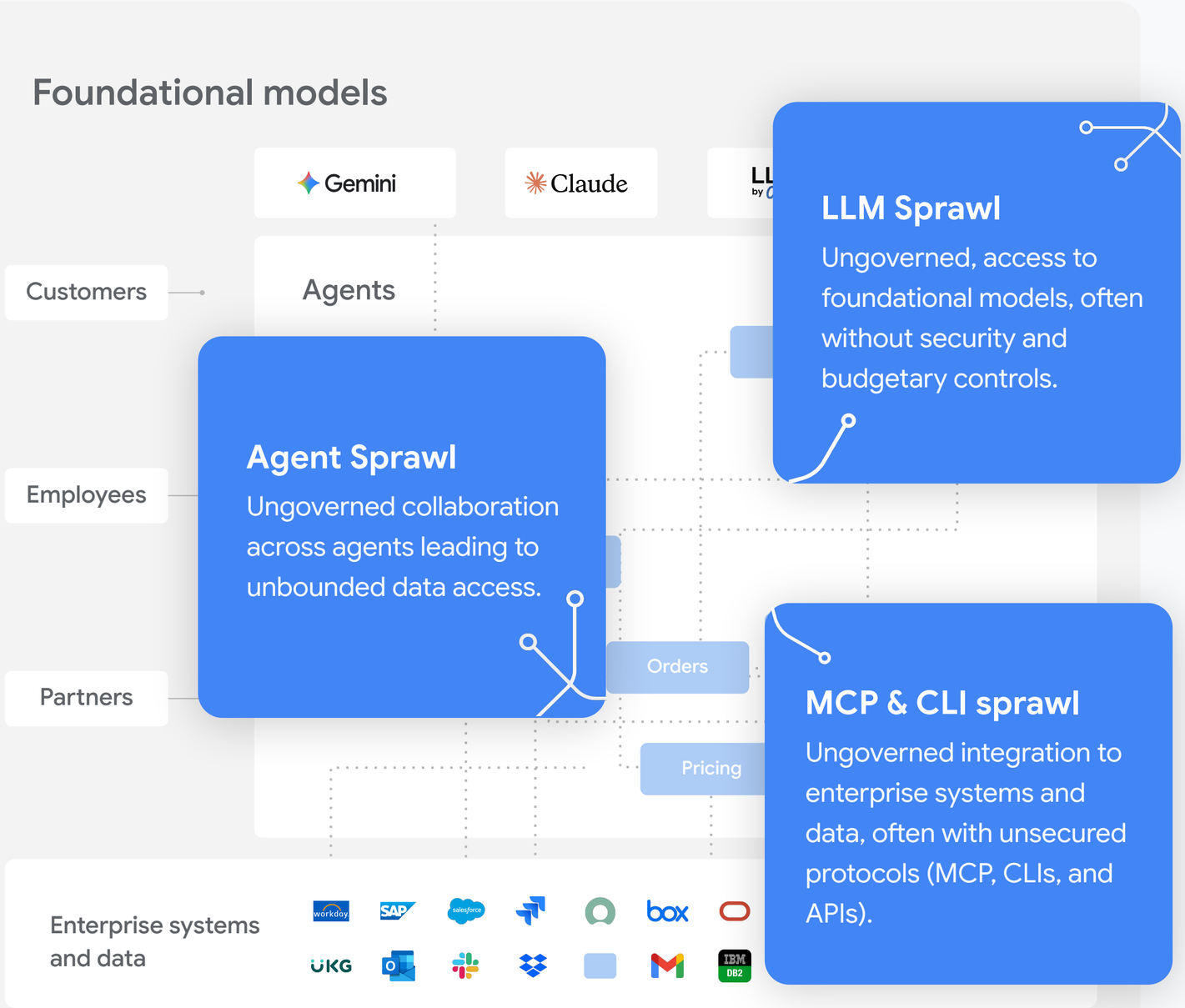
Fragmented landscape

02

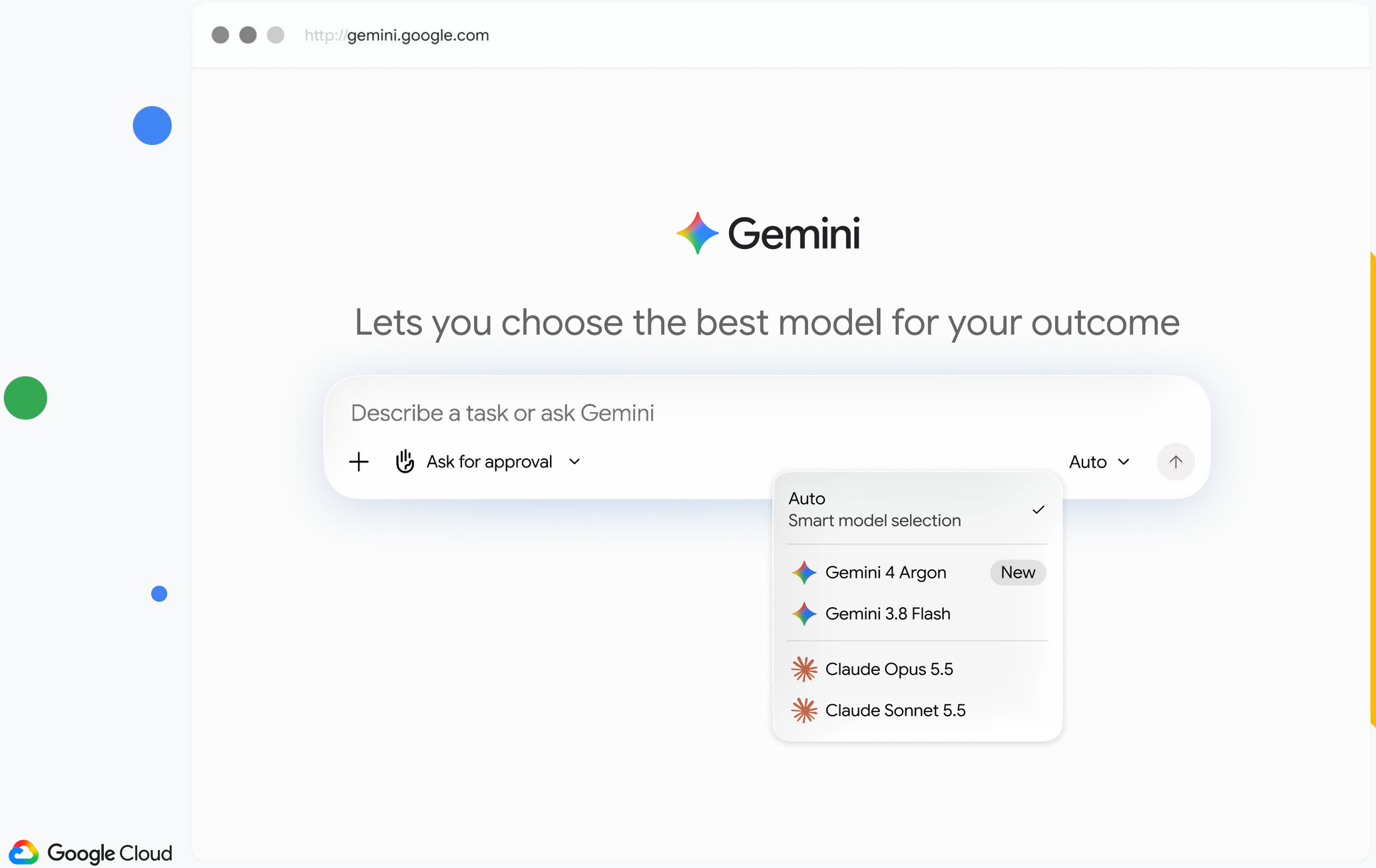
Expanding surface of unmanaged tools and runtimes

03

Difficult to manage without growing bespoke infrastructure



Google Cloud



Google Cloud

Gemini platform

Build

- Agent Development Kit
- 3P agent frameworks
- Managed Agents API
- Agent Studio

Gemini API and Model Garden

- Gemini models
- 3P and open models
- Model training
- Model inference

Tools, data, and other agents

- Plugins
- Grounding
- RAG and KGs
- Skills and MCP
- Search
- APIs and connectors
- A2A and A2UI
- AP2 and UCP
- Cloud Marketplace

Scale

- Agent Runtime
- Agent Sessions
- Agent Sandbox
- Agent Memory Bank

Govern

- Agent Gateway
- Agent Identity
- Agent Registry
- Agent Anomaly Detection
- Model Armor
- Agent Policy
- Agent Security
- Agent Compliance

Optimize

- Agent Evaluation
- Agent Simulation
- Agent Observability
- Agent Optimizer

Capability acceleration results in

Purpose-built infrastructure powering Gemini for business

Agent Compute Engine Announcement

Agent Compute Engine

Speed with Efficiency →

Instantly spin up, pause, and resume high-performance agent microVMs at Gemini scale

Hardware Protected Isolation →

Secure cloud hypervisor microVMs and Hardware-rooted trust with Titanium, Google's IPU.

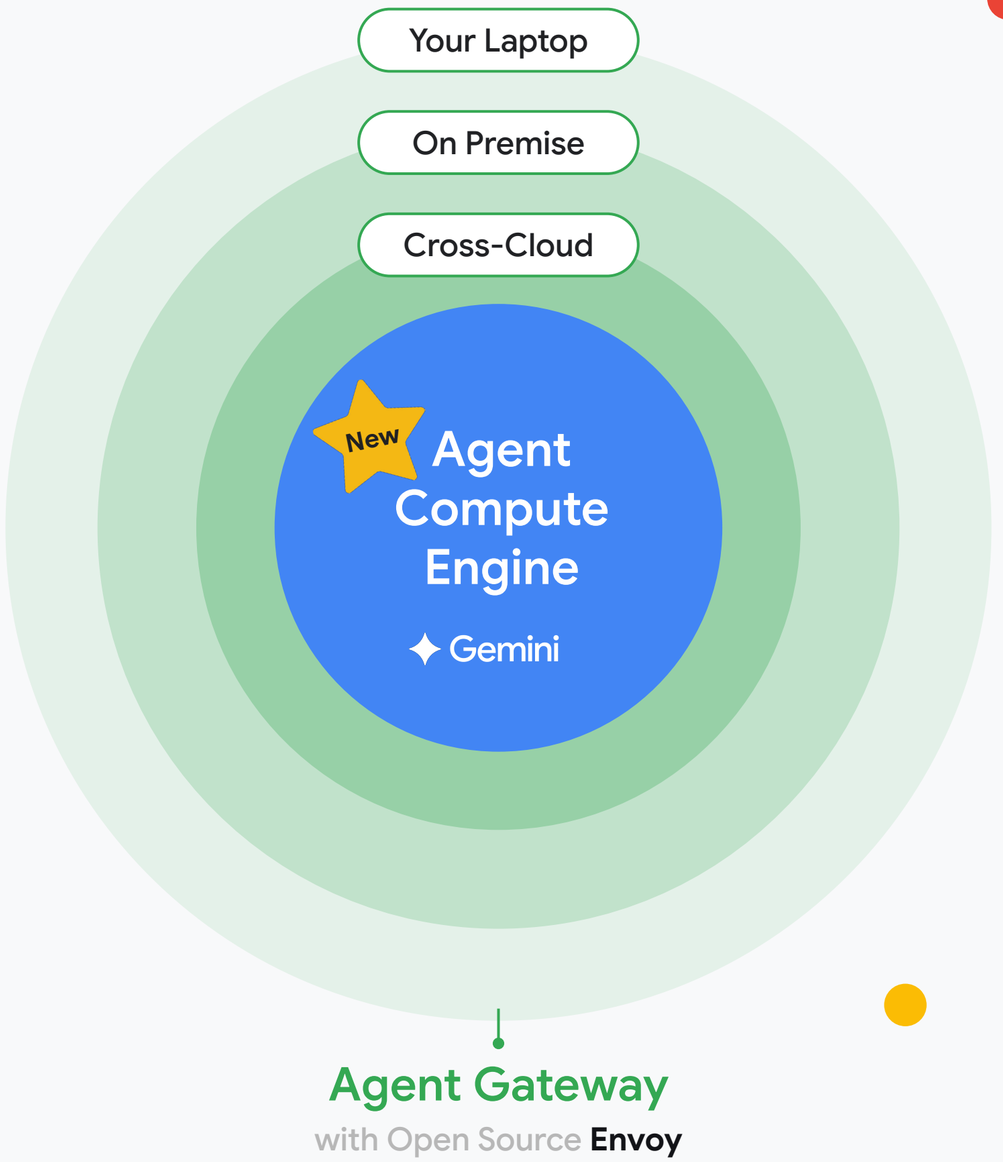
Agent Governance

Govern Anywhere →

Open with Envoy on any cloud, on-prem, or your laptop.

Control Every Token →

Every request goes to the right model. Every budget holds in real time.



Google Cloud

Nearly 90% of the Fortune 100 run on Gemini. Now, you can build AI agents on the exact same foundation.

Agent Governance for Enterprise Control Plane

Own Governance and Business IP

Identity

Per Agent, User → Agent, SPIFFEE / OIDC

Registry

Agent Cards, MCPs, Skills,Plugins

Policy

IAM/CEL, Semantic, HITL rules

Observability

OTEL GenAI Traces, Audit, Evals, Cost

Data Plane

API Gateway, Model Gateway, Agent Gateway (A2A & MCP aware) Default-deny egress, content scanning, DLP, rate/cost limits

Google Cloud

Enterprise Technology Leaders

Can you run a swap drill in under 2 days?

01

Swap a Model

Switch seamlessly across Frontier, Open Weights, and Proprietary models via standard Model APIs.

02

Swap a Harness

Move between ADK, 3P agent frameworks, and Vendor SaaS harnesses without rebuilding governance.

03

Swap an Agent

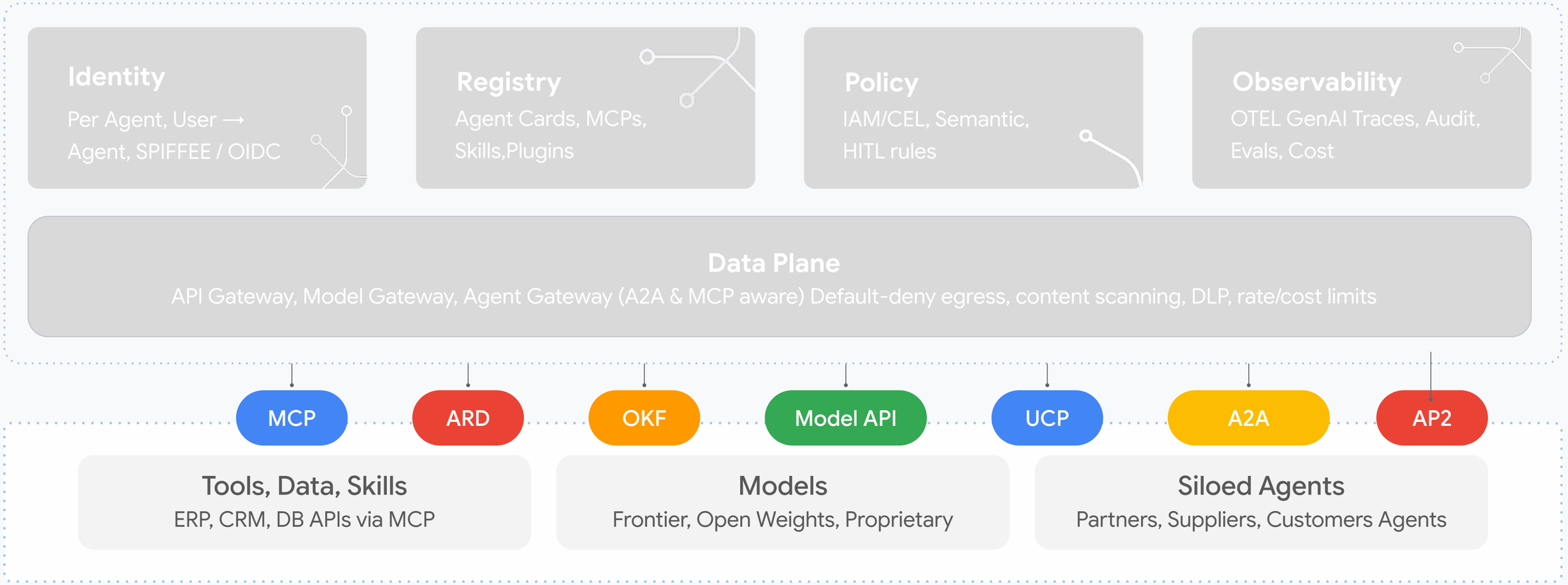
Replace or upgrade specialized internal and partner agents via A2A and Agent Registry.

Retain Memory, Conversation History, Config.

Enterprise identity, policy, observability, and business IP remain intact across every swap.

Google Cloud

Standard Interfaces to Intelligence & Data



Google Cloud

Best Practices

1. Demand standard interfaces in RFPs
2. Emit OTEL GenAI traces
3. Use Federated Standards based Identity
4. Store Agent definitions as code
5. Use Agent Gateway to enforce enterprise policies
6. Evals for Everything

Thank you.

Learn more

Gemini platform

Agent Compute Engine

Agent Development Kit (ADK)

Agent Engine & Runtime

Agent Gateway & Governance

Model Armor

Agent Evaluation & Observability

Google Cloud