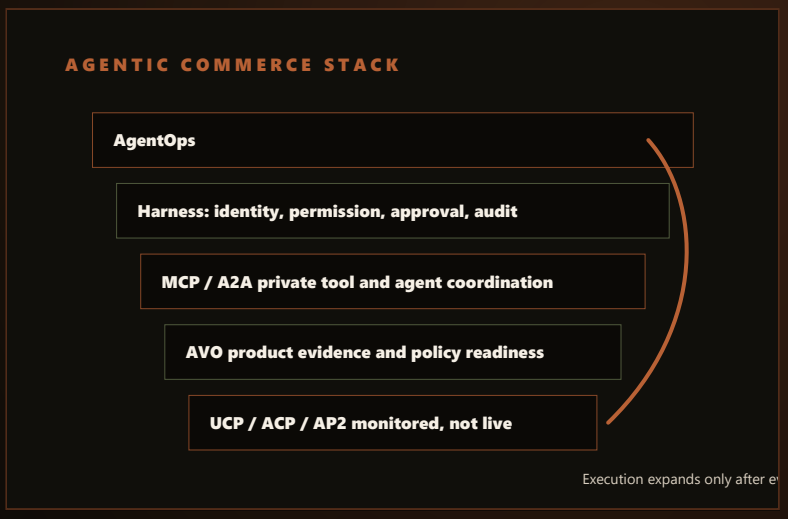
AGENTIC COMMERCE / RESEARCH BRIEF

Commerce Protocol Stack Overview

A SOTA briefing on the protocol layers shaping governed agentic commerce.



01	AVO first
02	MCP/A2A private
03	Payments deferred

AGENTIC COMMERCE STRATEGY

The build-now layer is product evidence, not checkout.

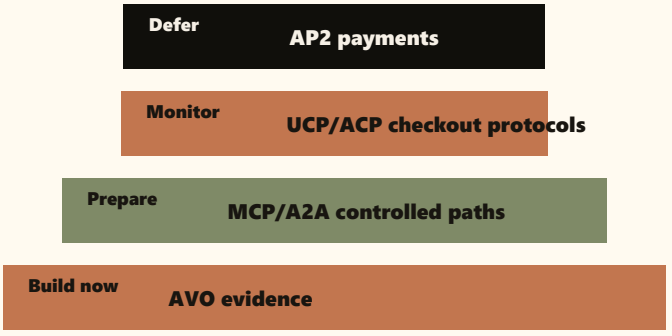
Agentic commerce is moving from chat interfaces toward protocol-mediated buying journeys. That creates an opportunity for HARNEXA, but the highest-risk layers - checkout, payment, refunds, and autonomous writes - must remain gated. HARNEXA should position the protocol stack as an operating architecture: AVO prepares product evidence, MCP/A2A connect tools and specialists, UCP/ACP/AP2 are monitored for commerce execution, and Harness/AgentOps keep control visible.

01
AVO is the entry wedge before public agentic checkout.

02
Public execution should stay disabled until demand, legal review, sandbox, and cost guardrails exist.

03
The buyer needs a roadmap that separates monitoring, readiness, and build-now surfaces.

Agentic commerce maturity stack



MCKINSEY TECHNOLOGY / QUANTUMBLACK / BUILDING THE FOUNDATIONS FOR AGENTIC AI AT SCALE

Agentic AI value depends on reliable data, stable interfaces, controlled execution, and visibility into behavior.

ACCENTURE / PULSE OF CHANGE 2026

AI investment remains a 2026 C-suite priority, with leaders increasingly looking for revenue growth rather than only cost reduction.

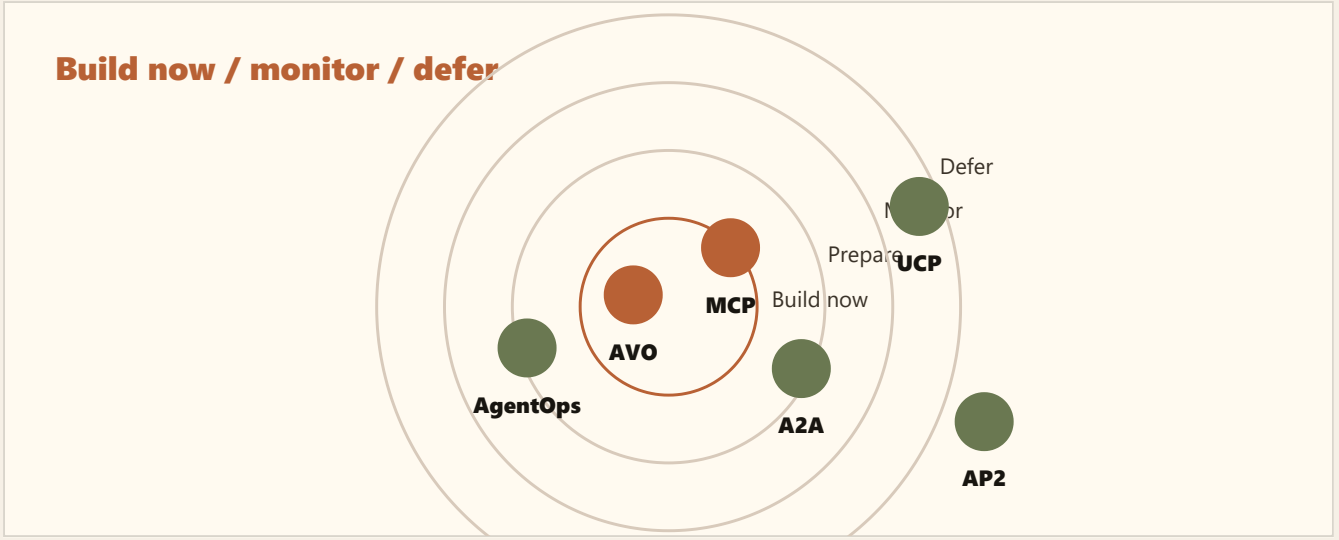
BOSTON CONSULTING GROUP / THE $200 BILLION AI OPPORTUNITY IN TECH SERVICES

Agentic AI is expected to expand technology-services demand as enterprises look for partners to design, deploy, and operate autonomous systems.

AGENTIC COMMERCE HORIZON STACK

Stack layers to separate.

Commerce protocol stack: product evidence and tool access sit below controlled execution and AgentOps review. Read the artifact as a market stack: AVO and controlled protocol readiness can move now; payment and autonomous execution wait for demand, review, and guardrails.



AVO
Make product, policy, availability, and proof data legible to answer engines and commerce agents.

MCP/A2A
Connect tools and specialist agents through narrow, permissioned, auditable interfaces.

UCP/ACP/AP2
Monitor emerging commerce and payment rails before enabling any autonomous checkout path.

AGENTOPS
Operate scorecards, audit review, cost bands, drift checks, and revocation drills.

ROADMAP DECISION

Decide what to build, monitor, prepare, and defer.

Use the session to turn agentic commerce hype into a staged roadmap with one buyer workflow, one evidence layer, and explicit no-build boundaries.

INSPECTION QUESTIONS

- Which layer is mature enough to build now, and which should remain monitored?
- Is product evidence structured enough for AI answer panels and guided selling?
- What legal, security, budget, and sandbox conditions would unlock payment work?
- How will HARNEXA prove protocol readiness without premature execution?

DO NOT SHIP UNTIL

- Do not build a broad protocol stack before a buyer workflow is validated.
- Do not let payment architecture precede legal and sandbox review.
- Do not use one protocol label to blur tool, commerce, and payment risk.

READINESS	Run PRISM and AVO checks before protocol or checkout implementation.	Readiness score, AVO gaps, product evidence map, and workflow owner.
PROTOTYPE	Build read/propose protocol paths only, with write and payment operations blocked.	Denied-action tests and audit trail.
DECISION	Activate execution work only after demand, legal review, ADR, sandbox, and cost controls.	Founder-approved implementation ADR and payment risk memo.

SOURCE LEDGER

Source ledger and commerce boundary

The brief combines external research signals with HARNEXA's implementation boundary: identity, permission, approval, audit, CLEAR evaluation, and no autonomous public execution.

MCKINSEY TECHNOLOGY / QUANTUMBLACK

Building the foundations for agentic AI at scale

McKinsey frames data quality, shared meaning, stable interfaces, observability, and controlled execution as scale requirements for agentic AI.

https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/building-the-foundations-for-agentic-ai-at-scale

ACCENTURE

Pulse of Change 2026

Accenture reports that 86% of C-suite leaders plan to increase AI investment in 2026 and 78% see AI as more beneficial to revenue growth than cost reduction.

https://www.accenture.com/us-en/insights/pulse-of-change

BOSTON CONSULTING GROUP

The $200 billion AI opportunity in tech services

BCG estimates agentic AI can unlock up to $200 billion in net new technology services demand over five years as buyers move from pilots to scale.

https://www.bcg.com/publications/2026/the-200-billion-dollar-ai-opportunity-in-tech-services

RESEARCH STANCE

External research is cited as market signal; HARNEXA interpretation is kept separate from source claims.

BUYER ARTIFACT

Every report includes a concrete visual artifact that can be inspected in a sales, risk, or architecture review.

OPERATING BOUNDARY

AVO first, governed tool access second, checkout deferred. The asset is for governed review, not autonomous production execution.

HARNEXA BOUNDARY

Technical governance aid only. Not legal advice or compliance certification. HARNEXA AI builds audit-ready foundations for qualified review. No PDF in this library claims EU AI Act certification, legal advice, payment readiness, or autonomous production execution.